X-Ways Software Technology AG

X-Ways Forensics/ WinHex

Integrierte Software für computerforensische Untersuchungen.

Werkzeug für Datenrettung und IT-Sicherheit.

Hexadezimal-Editor für Dateien, Datenträger und Arbeitsspeicher.

Benutzerhandbuch

Inhaltsverzeichnis

1 Einleitung

1.1 Über WinHex und X-Ways Forensics

X-Ways Software Technology AG
Carl-Diem-Str. 32
32257 Bünde
Deutschland

Web: https://www.x-ways.net/
Angebote und Online-Bestellungen unter:
https://www.x-ways.net/order-d.html
E-Mail-Adresse: mail@x-ways.com

Amtsgericht Bad Oeynhausen HRB 7475. Vorstand: Dipl.-Wirtsch.inf. Stefan Fleischmann. Aufsichtsratsvorsitzende: Dr. Marlies Horstmeyer.

WinHex wurde programmiert und weiterentwickelt seit 1995. Diese Anleitung entspricht dem Stand der Online-Hilfe von WinHex/X-Ways Forensics 21.1 und wurde zuletzt im April 2024 aktualisiert. Die Dokumentation wird in der Hauptsache auf Englisch gepflegt. Große Teile sind ins Deutsche übersetzt.

Die Software kann ausgeführt werden unter Windows 7, Windows 8/8.1/ Server 2012, Windows 10/Server 2016/Server 2019/Server 2022, Windows 11; 32-Bit und 64-Bit; Standard, PE und FE, mit variierendem Funktionsumfang. U. U. ist sie auch noch lauffähig unter Windows XP, Windows 2003 Server, Windows Vista/Server 2008, mit Einschränkungen. Ein Teil der Funktionaltitä ist auch bei Ausführung unter Linux+Wine verfügbar. Allerdings funktionieren einige Kopierschutzmethoden (darunter Dongles) unter Linux+Wine gar nicht.

Übersetzung der Benutzeroberfläche: Chinesisch: Sprite Guo. Japanisch: Takao Horiuchi und Ichiro Sugiyama (nicht allgemein verfügbar). Französisch: Jérôme Broutin und Henri Pouzoullic, aktualisiert von Bernard Leprêtre. Spanisch: José María Tagarro Martí. Italienisch: Andrea Ghirardini. Portugiesisch: Heyder Lino Ferreira. Polnisch: ProCertiv Sp. z o.o. (LLC).

Für besonders zahlreiche und maßgebliche Anregungen zur Entwicklung von X-Ways Forensics und X-Ways Investigator gebührt unser Dank dem Landeskriminalamt Rheinland-Pfalz.

Dank an Dr. A. Kuiper für seine Methode, Videos mit MPlayer zu verarbeiten.

Zu den professionellen registrierten Benutzern (Liste seit ca. 18 Jahren nicht mehr gepflegt) gehören Universitäts- und nationale Forschungseinrichtungen (z. B. das Institut für Informatik der Technischen Universität München, das Deutsche Zentrum für Luft- und Raumfahrt, die Technische Versuchs- und Forschungsanstalt der Technischen Universität Wien, das Institut für Astronomie der Universität Wien, das Oak Ridge National Laboratory in Tennessee, USA), Behörden wie die Bundesstelle für Flugunfalluntersuchung, das Landeskriminalamt Rheinland-Pfalz, das Landeskriminalamt Niedersachsen, das Zollkriminalamt Köln, die Kriminalpolizeiinspektion Schweinfurt, die Landespolizeidirektion Freiburg, die Kriminalpolizei Passau, diverse nationale Strafverfolgungsbehörden und militärische Einrichtungen insbes. in den USA und Deutschland, Ministerien wie das Australische Verteidigungs-

ministerium sowie Unternehmen aus den verschiedensten Branchen, z. B. Siemens AG, Siemens Business Services, Siemens VDO AG, Infineon Technologies Flash GmbH & Co. KG, Toshiba Europe, Hewlett Packard, Microsoft Corp., Ericsson, Commerzbank AG, National Semiconductor, Analytik Jena AG, Novell Inc., Ontrack Data International Inc., Deloitte, KPMG Forensic, Ernst & Young, Lockheed Martin, BAE Systems, TDK Corporation, Seoul Mobile Telecom und Visa International.

1.2 Rechtliches

Lizenzvereinbarung

Hinweise

Der MD5 Message-Digest wurde entwickelt von RSA Data Security Inc.

X-Ways Forensics enthält Software von Igor Pavlov, www.7-zip.com, und eine Implementierung von Adler32 von Arnaud Bouchez.

FuzZyDoc™ is a trademark of X-Ways Software Technology AG.

X-Ways Forensics verwendet ResIL, ein Fork von DevIL. ResIL wurde unter LGPL veröffentlicht (http://www.gnu.org/copyleft/lesser.html), Version 2.1. Der Quellcode kann heruntergeladen werden von http://sourceforge.net/projects/resil.

X-Ways Forensics enthält ein angepasstes Kompilat von libPFF. libPFF wurde unter LGPL

veröffentlicht (http://www.gnu.org/copyleft/lesser.html), Version 3.0. Der Original-Quellcode kann von http://libpff.sourceforge.net/ heruntergeladen werden.

X-Ways Forensics verwendet Dokan. Dokan wurde unter LGPL veröffentlicht (http://www.gnu.org/copyleft/lesser.html), Version 3.0. The Quellcode kann heruntergeladen werden von https://dokan-dev.github.io.

X-Ways Forensics uses WimLib. WimLib is governed by the LGPL (https://www.gnu.org/licenses/lgpl-3.0.html), version 3. The source code can be downloaded from https://wimlib.net.

X-Ways Forensics uses lzfse. Copyright (c) 2015-2016, Apple Inc. All rights reserved. The source code can be downloaded from https://github.com/lzfse/lzfse. Copyright (c) 2015-2016, Apple Inc. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of the copyright holder(s) nor the names of any contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

X-Ways Forensics uses Zstandard software (zstd). Copyright (c) Meta Platforms, Inc. and affiliates. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. * Neither the name Facebook, nor Meta, nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Die Unterstützung von Windows Event-Logs (.evtx) basiert auf Arbeit von Andreas Schuster.

MiniZ: The MIT License. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the

Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

TinyXML: Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-). 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)". THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Unicode: Copyright 2001-2004 Unicode, Inc. Disclaimer This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt. Limitations on Rights to Redistribute This Code Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

ZLib from http://zlib.net/: This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following

restrictions: 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required. 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software. 3. This notice may not be removed or altered from any source distribution.

FFmpeg from https://www.ffmpeg.org/: Governed by the LGPL (http://www.gnu.org/copyleft/lesser.html), version 3.0.

1.3 Lizenzierung

Sie dürfen WinHex bis zu 45 Tage lang kostenlos ausprobieren. Für den regulären Gebrauch und für den Gebrauch als Vollversion, benötigen Sie eine Lizenz. Sollen mehrere Benutzer die Software gleichzeitig betreiben wollen oder ein Benutzer die Software an mehreren Rechnern auf einmal, benötigen Sie entsprechend viele Lizenzen. Lizenzvereinbarung. Anders als mit der Evaluationsversion können Sie mit der Vollversion Dateien speichern, die größer als 200 KB sind, mit dem Disk-Editor Sektoren schreiben und virtuellen Arbeitsspeicher editieren. Der Lizenzierungsstatus wird beim Programmstart angezeigt sowie in der Info-Box (dem Fenster, das erscheint, wenn Sie die Versionsnummer in der oberen rechten Ecke anklicken).

- Private Lizenzen sind zu einem reduzierten Preis verfügbar für den nicht-kommerziellen Einsatz außerhalb von Unternehmen, Institutionen und öffentlicher Verwaltung.

- Professionelle Lizenzen erlauben die Benutzung der Software in *jeder* Umgebung (privat oder gewerblich, zu Hause, in Unternehmen, Organisationen und öffentlicher Verwaltung) und ermöglichen die Benutzung eigener Scripte.

- Specialist-Lizenzen erlauben zusätzlich das Aufrufen von Befehlen im Specialist-Menü, das Auslesen der Dateisysteme exFAT, Ext2, Ext3, Ext4, CDFS/ISO9660 und UDF, bieten Optionen zum optischen Hervorheben von freiem Speicher und Schlupfspeicher sowie Unterstützung für das Zusammensetzen von RAIDs, für dynamische Platten von Windows, Linux LVM2, einige weitere Spalten im Verzeichnis-Browser und das sektorweise Klonen/Sichern eines Datenträgers auch in umgekehrter Reihenfolge. Besonders für IT-Sicherheitsexperten von Nutzen.

- WinHex Lab Edition versteht zusätzlich die Dateisysteme HFS, HFS+/HFSJ/HFSX, ReiserFS, Reiser4, XFS, BtrFS (multiple disks via LVM2 or RAID setups are supported, but not BtrFS multi-device setups), UFS1, UFS2, APFS (unverschlüsselt), QNX, und sie erlaubt das Erzeugen von Datei-Containern und das Ausführen von normalen X-Tensions.

- Lizenzen für X-Ways Forensics („forensische Lizenzen“) ermöglichen zusätzlich die mächtige Verwaltung von Fällen, die automatische Erstellung von Berichten, den internen Viewer und die separate Viewer-Komponente, die Galerie-Ansicht, viele weitere Operationen beim Erweitern des Datei-Überblicks, viele weitere Spalten und Filter im Verzeichnis-Browser (und die Reihenfolge der Spalten kann geändert werden), Kommentare und Vermerke sowie Unterstützung für die Dateisystem ReiserFS, Reiser4, HFS, HFS+, UFS und XFS. Ferner

erlauben sie die Erstellung und Interpretation von Evidence-Files (.e01), die Erkundung von SquashFS-Dateisystemen (solchen, die auf GZIP/zlib, LZMA, LZO oder XZ basieren) **u. v. a. m.**! Besonders nützlich für Ermittler in der Computerforensik.

X-Ways Investigator ist eine vereinfachte Version von X-Ways Forensics. Sie hat nicht die gesamte Funktionalität von X-Ways Forensics, nicht mal die gesamte Funktionaltität von WinHex, und konzentriert sich auf eher nicht-technische Aspekte wie Begutachtung von Bildern, Dokumenten und E-Mails. Benutzer von X-Ways Forensics können die Benutzeroberfläche von X-Ways Forensics vorübergehend reduzieren zu der von X-Ways Investigator, um sich einen exakten Eindruck davon zu verschaffen, welche Menübefehle und Optionen verfügbar sind, und um zu entscheiden, ob X-Ways Investigator in ihrer Organisation dabei behilflich sein kann, die Auswertetätigkeit auf mehrere Benutzer aufzuteilen, von denen einige auf völlig andere Bereiche als Computerforensik spezialisiert sind. X-Ways Investigator ist nicht wirklich als eigenständig einsetzbares Produkt gedacht.

Die maximale Anzahl von gleichzeitigen Zeichensätze in der Textanzeige hängt auch vom Lizenztyp ab (s. Ansicht-Menü). Ein vollständigerer Vergleich der Lizenztypen findet sich online unter http://www.x-ways.net/winhex/comparison-d.html. Bestellungen können Sie unter http://www.x-ways.net/order-d.html aufgeben.

1.4 Weitere Unterschiede zw. WinHex & X-Ways Forensics

Die Benutzeroberfläche von WinHex (dessen ausführbare Datei winhex.exe heißt oder winhex64.exe) identifiziert sich immer als WinHex, die von X-Ways Forensics (xwforensics.exe oder xwforensics64.exe) als X-Ways Forensics. Die gemeinsame Programmhilfe und das gemeinsame Benutzerhandbuch verwenden allerdings zumeist statisch den Namen „WinHex“, manchmal „X-Ways Forensics“.

WinHex und X-Ways Forensics teilen sich eine gemeinsame Code-Basis. X-Ways Forensics bietet unzählige zusätzliche Features gegenüber WinHex mit einer Specialist-Lizenz, aber erlaubt kein Editieren von Datenträger-Sektoren oder interpretierten Images und enthält die von WinHex bekannten sicheren Datenlöschfunktionen nicht. In X-Ways Forensics werden Datenträger, interpretierte Image-Dateien, virtueller Arbeitsspeicher und physischer RAM-Speicher ausschließlich schreibgeschützt (im Nur-Lesen-Modus) geöffnet, um forensisch sicheres Arbeiten zu gewährleisten, bei dem keinerlei Veränderung von Beweisen geduldet wird. Dieser strenge Schreibschutz in X-Ways Forensics stellt sicher, dass die Original-Asservate nicht versehentlich verändert werden können, was vor Gericht von wesentlicher Bedeutung sein kann.

Nur wenn Sie nicht an strenge Regeln gebunden sind und/oder aggressiver vorgehen möchten/müssen (weil z. B. ein Bootsektor repariert werden soll oder als geheim eingestufte oder irrelevante Daten gelöscht werden müssen), können Sie als Benutzer von X-Ways Forensics WinHex statt X-Ways Forensics ausführen. Mit WinHex können Sie Datenträgersektoren editieren sowie ganze Datenträger, freien Speicher, Schlupfspeicher, ausgewählte Dateien und ausgewählte Datenträgerbereiche sicher überschreiben (wipen).

Benutzer von X-Ways Forensics können einfach die ausführbare Programmdatei xwforensics.exe

kopieren und die Kopie winhex.exe nennen (bzw. für die 64-Bit-Edition xwforensics64.exe kopieren und die Kopie winhex64.exe nennen), um WinHex zu bekommen. Das Setup-Programm erzeugt solche Kopien im Zielverzeichnis automatisch. Oder Sie können harte Verweise statt Kopien anlegen (höherer Coolness-Faktor). Wenn das Programm als *winhex*.exe ausgeführt wird, identifiziert es sich überall als WinHex (in der Benutzeroberfläche, im Fallbericht, im Fallprotokoll, in Beschreibungen von Datenträger-Sicherungen und in allen Bildschirmfotos) und verhält sich als WinHex. Diese Version ist vom Funktionsumfang her das non plus ultra. Sie vereinigt die volle Palette forensischer Features von X-Ways Forensics und die Sektoreditiermöglichkeiten und sicheren Datenlöschfunktionen von WinHex.

1.5 So legen Sie los mit X-Ways Forensics

Die neuesten Download-Instruktionen, sofern Ihre Update-Berechtigung noch gilt, erhalten Sie bei Abfrage Ihres Lizenzstatus' hier. Weitere Informationen über die Installation von WinHex und X-Ways Forensics erhalten Sie hier.

Extrahieren Sie die Dateien im Download von X-Ways Forensics in ein Verzeichnis Ihrer Wahl. Eine Installation mit dem Setup-Programm ist nicht erforderlich. Das Programm ist portabel und kann auch direkt von einem USB-Stick auf anderen Computern ausgeführt werden, z. B. einem Live-System, das Sie untersuchen möchten. Laden Sie auch die Viewer-Komponente herunter (die im Standard-Download nicht enthalten ist, weil sie nur sehr viel seltener aktualisiert wird). Verwenden Sie die 64-Bit-Edition der Viewer-Komponente für die 64-Bit-Version von X-Ways Forensics. Standardmäßig wird die Viewer-Komponente extrahiert im Unterverzeichnis \viewer (32 Bit) bzw. \x64\viewer (64 Bit) erwartet. Wir weisen darauf hin, dass die Viewer-Komponente anders als X-Ways Forensics Dateien in dem Profil des Benutzers erzeugt, der aktuell eingeloggt ist. Wenn Sie vermeiden möchten, dass Dateien in einem zu untersuchenden Live-System erzeugt werden, dann lassen Sie X-Ways Forensics die Viewer-Komponente nicht verwenden. Sie können auch MPlayer herunterladen, wenn Sie X-Ways Forensics Standbilder aus Videos produzieren lassen möchten, um diese in der Galerie anzuzeigen. Neuere Releases können immer in das existierende Verzeichnis eines älteren Releases extrahiert werden. Sie dürfen bestehende WinHex.cfg-Konfigurationsdateien von früheren Releases in neueren Releases weiterverwenden (aber niemals umgekehrt).

Um eine portable Installation von X-Ways Forensics oder X-Ways Investigator und sein Icon auf einer bestimmten Maschine mit .xfc-Falldateien zu verknüpfen, können Sie die Anwendung zumindest einmal explizit als Administrator ausführen und sie wieder beenden, während ein beliebiger der anpassbaren Standardpfade auf denselben Laufwerksbuchstaben verweist, auf dem Ihre Windows-Installation liegt, um der Anwendung einen Fingerzeig darauf zu geben, dass Sie der Besitzer des aktiven Windows-Systems sind und kein Problem damit haben, dass darauf schreiben zugegriffen wird. Das kann entweder der Pfad sein, in dem Sie die Anwendung ausführen, der Pfad, in dem Fälle erzeugt und erwartet werden, der Pfad, wo standardmäßig Datenträgersicherungen erstellt und erwartet werden, oder der Pfad für temporäre Dateien.

Zum Kennenlernen von X-Ways Forensics empfehlen wir Ihnen, folgendes auszuprobieren: Erst einmal legen Sie einen neuen Fall an (im Falldaten-Fenster). Dann fügen sie ihm ein Asservat hinzu (z. B. Ihr eigenes Laufwerk C:, Festplatte 0 oder bereits vorliegende Images von

Datenträgern). Per Rechtsklick im Verzeichnisbaum lassen sich Verzeichnisse mitsamt dem Inhalt aller Unterverzeichnisse rekursiv im Verzeichnis-Browser ausgeben. Klicken Sie also z. B. im Verzeichnisbaum mit der rechten Maustaste auf das Stammverzeichnis, sehen Sie alle Dateien des gesamten Dateisystems auf einmal. Gleichzeitig können Sie auch dynamische Filter einsetzen (Optionen | Verzeichnis-Browser), um sich etwa auf Dateien mit einem bestimmten Namen oder Typ, einer bestimmten Größe oder bestimmten Zeitstempeln zu konzentrieren.

Weitere entscheidende Funktionen in X-Ways Forensics finden Sie im Kontextmenü des Verzeichnis-Browsers (dort z. B. auch die Möglichkeit, Dateien herauszukopieren) sowie im Suchen-Menü (dort die Parallele Suche) und im Specialist-Menü (dort vor allem „Datei-Überblick erweitern“). Mit letzterer Funktion kann man Dateien einzeln oder massenweise gezielt weiterverarbeiten, z. B. Inhalte von Archiven oder E-Mails und Datei-Anhänge mit in den Datei-Überblick aufnehmen, Bilder auf Hautfarbenanteile untersuchen, Dokumente auf Verschlüsselung usw. usf.

Man kann X-Ways Forensics für tausend verschiedene Zwecke einsetzen. Daher sind unserer Meinung nach Schritt-für-Schritt-Anweisungen (erst hier klicken, dann dort, dann im Fenster darüber nachschauen) nicht der richtige Weg, um die Software zu erklären. Diese Programmhilfe/dieses Handbuch soll vielmehr die verfügbare Funktionalität akkurat beschreiben und Sie die verschiedenen Funktionen kreativ kombinieren lassen, um ein bestimmtes Ziel zu erreichen. Das Denken wird dem Benutzer dabei nicht abgenommen; er muss wissen, was er tut, und wie Resultate zu interpretieren sind.

Die 64-Bit-Edition ist besonders in Situationen empfehlenswert, in denen ein 32 Bit großer Adressraum unzureichend sein kann, wenn Sie Festplatten oder Images analysieren, die viele Millionen Dateien enthalten, oder wenn Sie mit vielen Millionen Suchtreffern hantieren, vorausgesetzt, dass Sie eine Menge physischen Arbeitsspeicher installiert haben. Bestimmte Operationen, die die Rechenleistung des Prozessors besonders beanspruchen (z. B. Hashen oder Verschlüsseln oder Entschlüsseln) können in der 64-Bit-Edition auch schneller sein.

2 Allgemeines

2.1 Werkzeug Hex-Editor

Ein Hexadezimal-Editor ist in der Lage, den Inhalt einer Datei jedes Typs vollständig anzuzeigen. Im Gegensatz zu einem Text-Editor kann er *alle* Bytes einer Datei darstellen, auch Steuerzeichen (für Zeilenumbruch, Tabulator usw.) und Programmcode, und zwar unter Angabe einer zweistelligen Zahl des Hexadezimalsystems (16er-System).

Ein Byte ist eine Kombination aus 8 Bits. Jedes Bit enthält entweder eine 0 oder eine 1, hat also einen von zwei möglichen Zuständen. Ein Byte kann daher einen von 2^8 (=256) verschiedenen Werten annehmen. Da 256 das Quadrat von 16 ist, kann jedes Byte durch eine zweistellige Zahl aus dem Hexadezimalsystem repräsentiert werden. Jede der beiden Stellen steht für eine Tetrade (auch: ein Nibble) eines Bytes, d. h. 4 Bits. Die möglichen Ziffern dabei sind 0-9 und A-F. Durch

Änderung dieser Ziffern kann man einem Byte einem neuen Wert zuweisen.

Genauso ist es möglich, die Zeichen zu editieren, die jedem Byte zugeordnet sind (Textmodus, s. a. „Zeichen eingeben“). Diese Zeichen können z. B. Buchstaben oder Satzzeichen sein. Beispiel: Ein Byte, das den dezimalen Wert 65 hat, wird vom Hex-Editor in der Hexadezimal-Schreibweise mit 41 angeben (**4**•16+**1**=65) und in der Zeichenschreibweise mit dem Buchstaben „A“. Die Zuordnung von Zeichen gibt der sog. Zeichensatz an.

Entscheidend beim Editieren einer Programmdatei (z. B. .exe-Datei) ist, dass nicht die Länge der Datei (die Anzahl der Bytes, die sie enthält) und die relativen Positionen von Programmcode und Daten verändert werden. Dies würde die Ausführbarkeit des Programmcodes beeinträchtigen. Es ist generell zu beachten, dass Änderungen an Dateiinhalten zu anormalen Verhaltensweise der zugehörigen Programme führen können. Für viele Zwecke genügt es, sich auf das Editieren des in einer Datei vorkommenden Textes beschränken. Es ist in jedem Fall ratsam, vor dem Bearbeiten eine Sicherung der Datei anzulegen.

Sie werden feststellen, dass WinHex vor der Benutzung aller entscheidenden Funktionen Sicherheitsabfragen durchführt, die Fehlbedienungen vorbeugen.

2.2 Byte-Reihenfolge

Mikroprozessoren unterscheiden sich darin, an welcher Position sie das niederwertigste Bytes innerhalb eines Datentyps, der mehrere Bytes enthält, ablegen. In Systemen mit Prozessoren von Intel®, MIPS®, National Semiconductor und VAX steht das niederwertigsten Byte an erster Stelle. Daten eines aus mehreren Bytes bestehender Datentyps (z. B. 32-Bit-Integertyp, Unicode-Zeichen) stehen im Speicher beginnend mit dem niederwertigsten („little end“) und endend mit dem höherwertigstem Bytes. Zum Beispiel wird die Hexadezimalzahl 12345678 als 78 56 34 12 gespeichert. Dies wird das *Little-Endian*-Format genannt.

Motorola- und Sparc-Prozessoren dagegen setzen voraus, dass das niederwertigste Byte an hinterster Stelle steht. Mehrfach-Byte-Daten werden beginnend mit dem höchstwertigen Byte („big end“) und endend mit dem niederstwertigem Byte gespeichert. Zum Beispiel wird die Hexadezimalzahl 12345678 als 12 34 56 78 gespeichert. Dies wird das *Big-Endian*-Format genannt.

2.3 Ganzzahlige numerische Datentypen

Format/Typ	Bereich	Beispiel
8 Bit, vorzeichenbehaftet	-128...127	FF = -1
8 Bit, vorzeichenlos	0...255	FF = 255
16 Bit, vorzeichenbehaftet	-32.768...32.767	00 80 = -32.768
16 Bit, vorzeichenlos	0...65.535	00 80 = 32.768
24 Bit, vorzeichenbehaftet	-8.388.608...8.388.607	00 00 80 = -8.388.608
16 Bit, vorzeichenlos	0...16.777.215	00 00 80 = 8.388.608
32 Bit, vorzeichenbehaftet	-2.147.483.648...2.147.483.647	00 00 00 80 = -2.147.483.648
32 Bit, vorzeichenlos	0...4.294.967.295	00 00 00 80 = 2.147.483.648
64 Bit, vorzeichenbehaftet	-2^{63} ($\approx -9 \cdot 10^{18}$)... $-2^{63}-1$ ($\approx 9 \cdot 10^{18}$)	00 00 00 00 00 00 00 80 = -2^{63}

Von ganzzahligen numerischen 16-Bit-Werten (Words) ist in Little-Endian-Systemen erst das niederwertige, dann das höherwertige Byte gespeichert. Bei 32-Bit-Werten (Größe: 4 Bytes) verhält es sich entsprechend mit den Words (den 2 Bytes großen Bestandteilen).

Wenn beispielsweise in einer Datei die Hex-Werte 10 27 stehen, so entspricht dies als numerischer 16-Bit-Wert der Hexadezimal-Zahl 2710 (was ins Dezimalsystem umgerechnet 10000 bedeutet). Ebenso erscheint die Hexadezimal-Zahl 123 als 23 01. Das Byte mit dem Wert 23 ist das niederwertige (es enthält die Einer- und die 16er-Stelle der Zahl) und kommt daher zuerst.

Eine weitere Besonderheit ist beim Interpretieren von Daten-Bytes als numerische Werte zu beachten: Zahlen, die größer als die Hälfte der Maximalzahl verschiedener Werte eines Zahlentyps sind (8 Bit: 2^8=256, 16 Bit: 2^{16}=65536), können als negative Zahlen übersetzt werden. Der Hex-Wert 8235 (der in einer Datei als 35 82 erscheint, s. o.), kann ins Dezimalsystem zu 33333 umgerechnet werden. Ein Programm, das den 16-Bit-Wert aber vorzeichenbehaftet liest, erhält die Zahl -32203. Diese zweite Möglichkeit ergibt sich, wenn von der Übersetzung als vorzeichenloser Wert die Maximalzahl verschiedener numerischer Werte des Zahlentyps subtrahiert wird (Beispiel: 33333-65536=-32203).

Die Darstellung in der Statusleiste, der Daten-Dolmetscher (der Daten in allen obigen Formaten auf einmal übersetzen kann) und die Funktion „Ganze Zahl suchen“ im Suchen-Menü berücksichtigen die genannten Besonderheiten automatisch.

Der Daten-Dolmetscher beherrscht alle o. g. Integer-Typen sowie zusätzlich vorzeichenlose 48-Bit-Integer.

2.4 Gleitkomma-Datentypen

Typ	Bereich	signifikante Stellen	Bytes
float (single)	$\pm 1{,}5^{-45}...3{,}4^{38}$	7-8	4
real	$\pm 2{,}9^{-39}...1{,}7^{38}$	11-12	6
double (double)	$\pm 5{,}0^{-324}...1{,}7^{308}$	15-16	8
long double (extended)	$\pm 3{,}4^{-4932}...1{,}1^{4932}$	19-20	10

Die Bezeichnungen stammen aus der Programmiersprache C, in Klammern ist die entsprechende Pascal-Bezeichnung angegeben. Der Typ real ist nur in Pascal vorhanden.

Die Gleitkommazahlen werden im Computer unter Zuhilfenahme von Zweierpotenzen abgebildet. Gespeichert werden die Mantisse m und der Exponent E aus der Darstellung $m \cdot 2^E$. Beide Werte enthalten ein Vorzeichen. Die Gleitkomma-Datentypen unterscheiden sich in ihrem Wertebereich (=der Anzahl der für den Exponenten reservierten Bits) und der Genauigkeit der Werte (=der Anzahl der für die Mantisse reservierten Bits).

Rechenoperationen mit Gleitkommazahlen werden in Intel-Architekturen vom mathematischen Koprozessor ausgeführt während der Hauptprozessor wartet. Der Intel 80x87 rechnet mit einer Genauigkeit von 80 Bit, RISC-Prozessoren häufig mit 64 Bit.

Hexadezimal-Werte in einem Editierfenster können vom Daten-Dolmetscher in alle vier Gleitkomma-Datentypen übersetzt werden.

2.5 Datumstypen

Die folgenden Datumsformate werden vom Daten-Dolmetscher unterstützt.

- **MS-DOS Datum & Zeit (4 Bytes)**

Das niederwertige Word bestimmt die Zeit, das höherwertige das Datum. Wird von zahlreichen DOS-Funktionen und von den FAT-Dateisystemen benutzt.

Bits	**Inhalt**
0-4	Sekunden geteilt durch 2
5-10	Minuten (0-59)
11-15	Stunde (0-23)
16-20	Tag (1-31)
21-24	Monat (1=Januar, 2=Februar usw.)
25-31	Jahre seit 1980

- **Win32 FILETIME (8 Bytes)**

Ein ganzzahliger 64-Bit-Wert, der die Anzahl der seit dem 1. Januar 1601 vergangenen 100-

Nanosekunden-Intervalle angibt. Wird in der Win32-API benutzt.

- **OLE 2.0 Datum & Uhrzeit (8 Bytes)**

Ein Gleitkommawert (Double), dessen ganzzahliger Bestandteil die Zahl der seit dem 30. Dezember 1899 vergangenen Tage angibt (Datum). Der Bruchanteil wird als die Uhrzeit interpretiert (z. B. 1/4 = 6:00 Uhr). Dies ist der OLE-2.0-Standarddatumstyp. Er wird bspw. auch von MS Excel verwendet. ICQ 7.0 verwendet OLE 2.0 Zeitstempel in Big Endian für Chat-Nachrichten.

- **ANSI SQL Datum & Uhrzeit (8 Bytes)**

Zwei aufeinanderfolgende ganzzahlige 32-Bit-Werte. Der erste gibt die Anzahl der seit dem 17. November 1858 vergangenen Tage an (Datum). Der zweite bestimmt die Anzahl der seit Mitternacht vergangenen 100-Mikrosekunden-Intervalle (Uhrzeit). Dieser Datumstyp ist ANSI-SQL-Standard und wird in Datenbanken verwendet (u. a. in InterBase 6.0).

- **UNIX, C, FORTRAN Datum & Uhrzeit (4 Bytes)**

Ein ganzzahliger 32-Bit-Wert, der die Anzahl der seit dem 1. Januar 1970 vergangenen Sekunden angibt. Dieser Datumstyp wird bzw. wurde in UNIX, in C und C++ („time_t“) sowie in FORTRAN-Programmen seit den 80er Jahren verwendet. Gelegentlich ist er auch definiert als die Anzahl der seit dem 1. Januar 1970 vergangenen *Minuten*. In den Optionen des Daten-Dolmetschers lässt sich die verwendete Zeiteinheit einstellen.

- **Mac HFS+ Datum & Uhrzeit (4 Bytes)**

Ein ganzzahliger 32-Bit-Wert, der die Anzahl der seit dem 1. Januar 1904 GMT vergangenen Sekunden angibt (HFS: Ortszeit). Das letzte repräsentierbare Datum ist der 6. Februar 2040 um 06:28:15 Uhr GMT. Die Datumswerte lassen Schaltsekunden außer Betracht. Sie enthalten jedoch Schalttage in jedem ganzzahlig durch 4 teilbaren Jahr.

- **APFS Datum & Uhrzeit (8 Bytes)**

- **Java Datum & Uhrzeit (8 Bytes)**

Ein ganzzahliger 64-Bit-Wert, der die Anzahl der seit dem 1. Januar 1970 vergangenen Millisekunden angibt. Wird, wie bei Java Standard, üblicherweise im Big-Endian-Format gespeichert, aber im Speicher von BlackBerry im Little-Endian-Format verwendet.

- **Mac Absolute Time, a.k.a. Mac epoch time (4 Bytes)**

Ein ganzzahliger 32-Bit-Wert, der die die Anzahl der seit dem 1. Januar 2001 vergangenen Sekunden angibt.

2.6 ANSI-/IBM-ASCII

ANSI-ASCII ist der der in WinHex verwendete Name einer Erweiterung des ASCII-Zeichensatzes, der in Nicht-Unicode-Windows-Anwendungen verwendet wird. Er wurde von Microsoft ANSI genannt nach dem American National Standards Institute, aber nicht tatsächlich von diesem Institut definiert. Es existieren diverse regionale Varianten, von denen eine in Windows aktiv ist, typischerweise Codepage 1252 in Ländern, in denen eine westeuropäische Sprache gesprochen wird. MS-DOS und Kommandozeilenfenster von Windows benutzen den IBM-ASCII-Zeichensatz (anderswo auch als OEM- oder DOS-Zeichensatz bezeichnet). All diese 8-Bit-Erweiterungen des 7-Bit-ASCII-Zeichensatzes unterscheiden sich in der Zuordnung von Zeichen, deren Wert 127 übersteigt. Wenn Sie beispielsweise einen Text mit dem Windows-Notizblock (notepad.exe) verfassen und in ANSI-Codierung abspeichern und ihn sich später mit dem type-Befehl in einem Kommandozeilenfenster ansehen, dann werden Umlaute und diverse Sonderzeichen nicht richtig dargestellt. Einige der regionalen ANSI-Codepages sind Doppelbyte-Codepages, d. h. sie verwenden sogar 2 Bytes für einige Zeichen statt nur 1 Byte pro Zeichen.

Wählen Sie daher im Ansicht-Menü „IBM-ASCII“ nur dann, wenn Sie mit WinHex eine Datei editieren, die zu einem DOS-Programm gehört. Sie sehen dann die in der Datei enthaltenen Texte wie sie auch in diesem Programm erscheinen. Die von ihnen eingegebenen Zeichen werden dann umgekehrt auch richtig in diesem DOS-Programm dargestellt. Wenn Sie hingegen eine typische Windows-Datei bearbeiten (Initialisierungsdateien von Windows-Programmen, Windows-Programmdateien usw.), sollten Sie die Option „ANSI-ASCII“ aktivieren.

Den in der Textspalte verwendeten Zeichensatz/die Codepage wählen Sie im Ansicht-Menü oder durch Klick oben auf die Textspalte, da, wo der Name der aktiven Codepage angezeigt wird. Mit der Funktion „Konvertieren“ im Bearbeiten-Menü können Textdateien von einem Zeichensatz in den anderen konvertiert werden.

Die ersten 32 ASCII-Zeichen sind weder Buchstaben oder Zahlen noch Satzzeichen. Es handelt sich um Steuerzeichen.

Hex	Steuerzeichen	Hex	Steuerzeichen
00	Null	10	Data Link Escape
01	Start of Header	11	Device Control 1
02	Start of Text	12	Device Control 2
03	End of Text	13	Device Control 3
04	End of Transmission	14	Device Control 4
05	Enquiry	15	Negative Acknowledge
06	Acknowledge	16	Synchronous Idle
07	Bell	17	End of Transmission Block
08	Backspace	18	Cancel
09	Horizontal Tab	19	End of Medium
0A	Line Feed	1A	Substitute
0B	Vertical Tab	1B	Escape
0C	Form Feed	1C	File Separator
0D	Carriage Return	1D	Group Separator

0E	Shift Out	1E	Record Separator
0F	Shift In	1F	Unit Separator

2.7 Prüfsummen, Hashes, Digests

Eine Prüfsumme ist eine Kennzahl zur möglichst eindeutigen Identifizierung von Daten. Zwei Datensätze mit der gleichen Prüfsumme sind mit hoher Wahrscheinlichkeit exakt (Byte für Byte) gleich. Es kann z. B. sinnvoll sein, die Prüfsumme von Daten *vor* und *nach* einer möglicherweisen fehlerbehafteten Übertragung zu berechnen. Ist sie in beiden Fällen gleich, dann sind die Daten mit hoher Wahrscheinlichkeit unverändert geblieben. Allerdings können Daten mit bösartiger Absicht so manipuliert werden, dass ihre Prüfsumme trotz Änderung gleich bleibt. Dadurch wird die Manipulation nicht bemerkt. Diese Möglichkeit schließen Digests aus.

Prüfsummen können in WinHex z. B. mit einem Befehl im Extras-Menü berechnet werden.

Die Standard-Prüfsumme wird berechnet als Summe, indem die Daten als Folge von Integer-Zahlen interpretiert werden, auf einem 8-Bit-, 16-Bit-, 32-Bit- oder 64-Bit-Akkumulator. Die exakte Operationsmodus hängt ab von einer Einstellung in Optionen | Sicherheit. Ein CRC (Cyclic Redundancy Code) wird mit einem komplizierteren, auf Polynomdivision beruhenden Algorithmus berechnet, der sicherer ist. Das drückt sich in einer niedrigeren Wahrscheinlichkeit dafür aus, für zwei verschiedene Dateien durch Zufall dieselbe Prüfsumme zu erhalten.

Beispiel: Wenn in einer Datei durch fehlerhafte Übertragung zwei Bytes verfälscht werden, sich die Abweichungen aber genau ausgleichen (z. B. erstes Byte +1, zweites Byte -1), dann bleibt die Standard-Prüfsumme im Gegensatz zum CRC unverändert.

Ein „Digest“ (engl.) ist ähnlich einer Prüfsumme eine Kennzahl zur eindeutigen Identifizierung von Daten. Digests sind aber mehr als Prüfsummen. Es handelt sich um „starke“ Einweg-Hashcodes, die Datenintegrität mit extrem hoher Sicherheit garantieren. Daten können in bösartiger Absicht so manipuliert werden, dass ihre Prüfsumme trotz Änderung gleich bleibt. Diese Möglichkeit schließen Digests aus. Es lassen sich mit vorstellbarem computerunterstütztem Rechenaufwand keine Daten finden, die denselben Digest besitzen wie vorgegebene andere Daten.

Natürlich können durch Verwendung von Digests auch zufällige, etwa durch fehlerhafte Übertragung entstandene Datenveränderungen festgestellt werden, aber dafür reichen Prüfsummen aus, die viel schneller berechnet werden können.

WinHex kann folgende Digests berechnen: MD4, MD5, SHA-1, SHA-256, RipeMD-128, RipeMD-160, Tiger128, Tiger160, Tiger192 sowie TTH (Tiger Tree Hash) und ed2k (nur mit Specialist- oder forensischer Lizenz).

2.8 Attribut-Legende

A: zu archivieren
R: schreibgeschützt
H: versteckt
S: System
X: nicht indexiert
P: Reparse-Punkt in NTFS
O: offline
T: temporär
I: hat Object-ID
C: komprimiert auf Dateisystemebene
c: komprimiert in Archiv
E: verschlüsselt auf Dateisystemebene
e: verschlüsselt in Archiv
e!: dateiformatspezifisch verschlüsselt/DRM
e?: hohe Entropie, evtl. vollverschlüsselt
(Res): Ressource in HFS+
($EFS): Verschlüsselungsmetadaten in NTFS
(INDX): Index-Attribut in NTFS (wenn kein Verzeichnis)
(ADS): alternativer Datenstrom in NTFS
(SC): in einer Schattenkopie gefunden
(SUID): Set User ID
(SGID): Set Group ID

File mode:
l=symbolic link
c=character device
b= block device
s=socket
p=pipe

Permissions:
owner read/write/execute
group read/write/execute
other read/write/execute

2.9 Technische Hinweise und Beschränkungen

- Technische Daten

Unterstützte Datenträgergröße:	mind. 131 TB
Unterstützte Volume-/Partitionsgröße:	131 TB-1 Byte
Unterstützte Dateigröße in Datei-Überblicken:	mind. 120 TB-1 Byte
Allg. max. Sektorzahl:	2^{40}-1

Allg. max. Clusterzahl:	2^{32}-1
Maximalzahl von Hash-Werten pro Hash-Datenbank:	2^{31}-1
Maximalzahl von Hash-Werten pro Hash-Datenbank:	2^{31}-1
Maximalzahl von Werten in der PhotoDNA- Datenbank in 64 Bit:	ca. 58,8 Mio.
Dateisystem-Unterstützung für Partitionen >2^{32} Sektoren:	NTFS, Ext*, XFS, Reiser*
Dateisystem-Unterstützung für Partitionen >2^{32} Cluster:	NTFS, Ext4, XFS
Zugreifbare physische Datenträger gemäß Nummerierung in Windows:	0-127
Maximalzahl gleichzeitig offener interpretierter Images partitionierter Datenträger	100
Maximalzahl gleichzeitig offener Partitionen und interpretierter Volume-Images	256
Unterstützte Anzahl von Objekten in einem Datei-Überblick in 64 Bit:	>536 Millionen
Maximalzahl von Suchbegriffen in einem Fall	8191
Maximalzahl von Suchtreffern pro Asservat:	211.969.638
Maximalzahl geöffneter Datenfenster:	1000
Max. Anzahl gleichzeitiger Programminstanzen:	99
Max. Anzahl umkehrbarer Tastatureingaben:	65535
Verschlüsselungstiefe:	128-256 Bit
Offset-Darstellung:	hexadezimal/dezimal

- Die Fortschrittsanzeige bei länger andauernden Operation zeigt in Prozent den Anteil des Vorgangs an, der bereits erledigt ist. Bei allen Suchen- und Ersetzen-Operationen zeigt sie jedoch die relative Position in der aktuellen Datei an. Dies entspricht dem bereits erledigten Anteil des Vorgangs, wenn in der gesamten Datei gesucht wird, also die Option „Nur im Block suchen“ nicht verwendet wird.

- Von Ihnen für Ver- und Entschlüsselung eingegebene Schlüssel werden nicht auf der Festplatte gespeichert. Sofern die entsprechende Sicherheitsoption gewählt ist, werden sie in verschlüsselter Form im Arbeitsspeicher gehalten, solange WinHex läuft.

- Such- und Ersetzen-Funktionen laufen generell schneller ab, wenn kein Jokerzeichen verwendet und (bei Text-Suche) nach Groß- und Kleinschreibung unterschieden wird. Außerdem gilt: Je länger die Such-Zeichenfolge, desto schneller die Such-Funktion.

- Beim Suchen mit aktivierter Option „Vorkommen zählen“ und beim Ersetzen ohne Bestätigung bieten sich für einen Suchalgorithmus zwei Alternativen für das Verhalten bei Fundstellen an, die in Sonderfällen zu unterschiedlichen Ergebnissen führen. Dies soll anhand eines Beispiels verdeutlicht werden:

  In der Zeichenfolge „ananas“ wird nach *ana* gesucht; das Vorkommnis beim ersten Zeichen wurde gefunden.
  1. Möglichkeit: Ab dem zweiten Zeichen wird wieder nach *ana* gesucht. Beim dritten Zeichen wird dann ein Vorkommnis registriert.
  2. Möglichkeit: Die drei mit der Suchzeichenfolge übereinstimmenden Zeichen werden übersprungen. *ana* wird erst wieder ab dem vierten Zeichen gesucht, in *nas* also nicht mehr gefunden.

  In WinHex wird der zweiten Alternative gefolgt, da sie für das Zählen von Vorkommen und das Ersetzen ohne Bestätigung meistens sinnvollere Ergebnisse liefert. (Wenn Sie normale

Suchvorgänge mit F3 fortsetzen oder Ersetzen *mit* Bestätigung wählen, wird nach der ersten Methode verfahren.)

Special Performance Enhancements

File header signature searches, block-wise hash matching, FILE record searches, searches for lost partitions, and physical simultaneous searches are sparse-aware operations when dealing with certain compressed and sparse .e01 evidence files. That means that areas that on the original hard disk were never written and thus still zeroed out or areas that had been wiped on the original hard disk or consciously omitted areas in cleansed images are skipped and almost require no time, because their data neither has to be read nor decompressed nor further processed (searched/hashed/matched against the block hash database).

Sparse-awareness is active for .e01 evidence files that were created by X-Ways Forensics and X-Ways Imager with a chunk size of 32 KB, 128 KB or 512 KB. Also possibly for images created by 3rd party software, depending on the settings and the internal layout. Operations are not sparse-aware on images of Windows dynamic disks, images of LVM2 disks, and on reconstructed RAIDs based on .e01 evidence files.

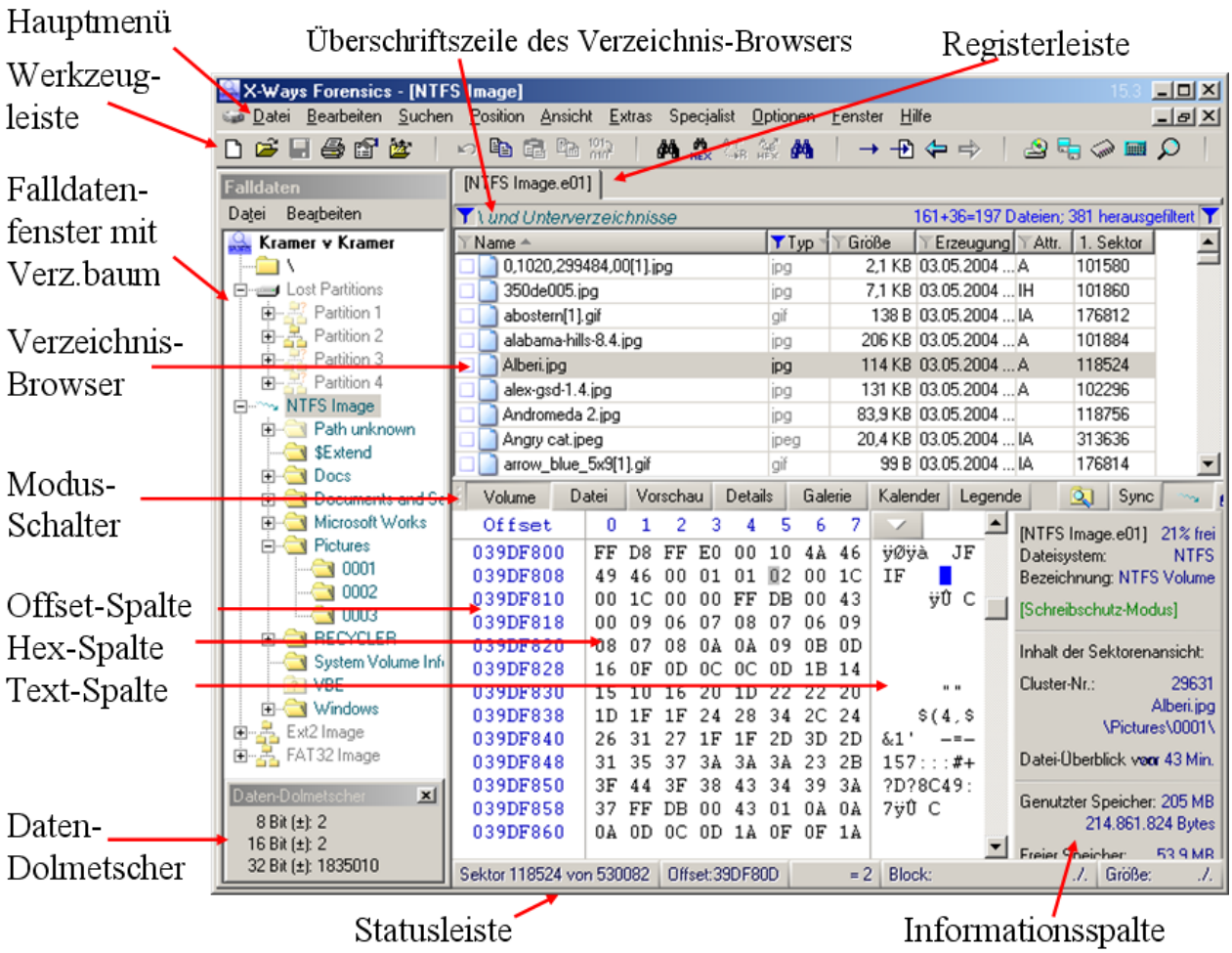
Logical searches and indexing in files stored in an NTFS file system are also sparse-aware at the .e01 evidence file level, and generally logical searches in virtual "Free space" files.

Logical searches and indexing in NTFS, Ext*, XFS and UFS file systems are sparse-aware at the file system level. That means no time is wasted on large sparse areas within sparse files. Those areas are ignored, regardless of whether the evidence object is an .e01 evidence file, raw image, RAID, or actual disk.

3 Benutzerschnittstelle

3.1 Overview

Wie die diversen Bestandteile der Benutzeroberfläche heißen, können Sie folgendem Bildschirmfoto entnehmen:



3.2 Start-Center

Das sog. Start-Center ist ein Dialogfenster, das optional beim Programmstart angezeigt wird und als vereinfachte Schalttafel für den Beginn Ihrer Arbeit mit WinHex gedacht ist. Es erlaubt Ihnen, sowohl Dateien, Datenträger, virtuellen Speicher und Ordner zu öffnen als auch bis zu 255 zuvor geöffnete Dokumente (16 in der Voreinstellung, Liste links). Dies können Dateien, Ordner, logische Laufwerke oder physische Datenträger sein. Wenn diese wieder geöffnet werden, stellt WinHex die letzte Cursor-Position, die Scroll-Position und den Block (falls definiert) wieder her, wenn die entsprechende Option nicht ausgeschaltet ist.

Vom Start-Center aus haben Sie auch Zugriff auf *Projekte* und *Fälle* (Liste rechts oben). Ein Projekt besteht aus einem oder mehreren zu editierenden Dokumenten (Dateien oder Datenträger). Es merkt sich die Cursor-Positionen, die Größe und Positionen der Fenster und einige Anzeige-Optionen. Indem Sie eine Fensteranordnung als Projekt speichern, können Sie Ihre Arbeit in mehreren Dokumenten genau dort fortsetzen, wo Sie sie verlassen haben, mit einem einzigen Klick. Dies ist besonders nützlich für wiederkehrende Aufgaben. Wenn Sie ein Projekt laden, werden erst alle zum gegenwärtigen Zeitpunkt geöffneten Fenster automatisch geschlossen.

Außerdem speichert WinHex automatisch die Fensteranordnung am Ende einer WinHex-Sitzung als Projekt und kann sie beim nächsten Mal wiederherstellen. Jedes Projekt wird in einer .prj-Datei gespeichert. Ein Projekt kann gelöscht bzw. umbenannt werden, indem Sie im Start-Center das Kontextmenü benutzen oder das Projekt markieren und die Entfernen- bzw. F2-Taste auf Ihrer Tastatur drücken.

Nicht zuletzt ist das Start-Center auch der Ort, an dem Sie *Scripte* verwalten können. Mit Hilfe des Kontextmenüs lassen sich Scripte auf die Syntax prüfen, bearbeiten, neu erstellen, umbenennen und löschen. Um ein Script auszuführen, klicken Sie es entweder doppelt an oder nur einfach und betätigen dann den OK-Schalter.

3.3 Verzeichnis-Browser

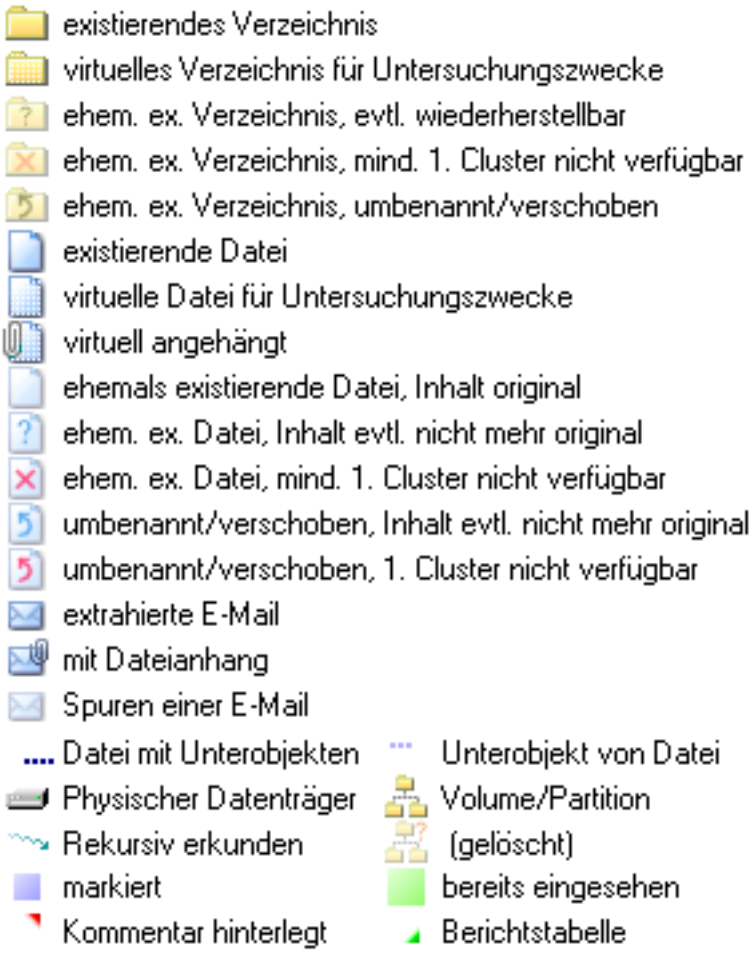
3.3.1 Allgemeines

Der wohl zentralste Bestandteil der Benutzeroberfläche von WinHex und X-Ways Forensics ist der sog. *Verzeichnis-Browser* an, der der Liste auf der rechten Seite im Windows Explorer ähnelt. Die Hauptaufgabe des Verzeichnis-Browsers ist die Anzeige von und Interaktion mit dem Datei-Überblick. Voller Funktionsumfang nur mit forensischer Lizenz. Der Verzeichnis-Browser listet standardmäßig zuerst Verzeichnisse gruppiert auf, dann Dateien. Komprimierte Dateien werden in blauer Schrift angezeigt, verschlüsselte in grüner Schrift. Klicken Sie Dateien oder Verzeichnisse im Verzeichnis-Browser mit der rechten Maustaste an, um ein Kontextmenü zu erhalten. Dieses enthält Befehle, um eine Datei oder ein Verzeichnis zu öffnen, ein Verzeichnis zu erkunden, den Anfang einer Datei oder eines Verzeichnisses auf dem Datenträger zu finden, den zugehörigen Verzeichniseintrag (FAT) bzw. Datei-Datensatz (NTFS) zu finden, die zugehörigen Cluster in einem separaten Fenster aufzulisten usw.

Beim Navigieren von einem Verzeichnis zum anderen, Erkunden von Dateien mit Unterobjekten (z. B. E-Mails, die Dateianhänge haben), Navigieren von einem Unterobjekt zu seinem übergeordneten Objekt, Aktivieren oder Deaktivieren von Filtern, Ausprobieren verschiedener Sortierkriterien usw., beachten Sie, dass Sie ganz leicht zu einer vorherigen Ansicht zurückkehren können, indem Sie den Zurück-Befehl im Navigationsmenü oder den Zurück-Schalter in der Symbolleiste nutzen.

Die **Icons** werden in der Legende direkt im Programm erklärt (nur mit forensischer Lizenz). Ehemals existierende Dateien und Verzeichnisse werden im Verzeichnis-Browser mit blasseren Icons dargestellt. Icons mit einem blauen Fragezeichen zeigen an, dass der Originalinhalt einer Datei oder eines Verzeichnisses noch immer verfügbar sein kann. Gelöschte Objekte, von denen bekannt ist, dass sie nicht mehr zugreifbar sein (weil entweder ihr erster Cluster in der Zwischenzeit anderweitig verwendet wurde, weil er unbekannt ist oder weil sie eine Größe von 0 Bytes haben), haben Icons mit einem roten Kreuz. Icons mit einem Pfeil auf FAT- (nur mit Specialist-Lizenz oder höher) und (nach Erweitern des Datei-Überblicks) NTFS-Partitionen zeigen umbenannte oder verschobene Dateien mit ihrem Originalnamen bzw. in ihrem früheren

Verzeichnis an. Auf Reiser4 sind dies verschobene Dateien mit ihrem jetzigen Namen im früheren Verzeichnis. Ein blauer Pfeil zeigen an, dass Inhalte für die Dateien verfügbar sind (wenn auch nicht die Originalinhalte von vor dem Umbenennen bzw. Verschieben). Ein roter Pfeil zeigt an, dass keine Inhalte verfügbar sind.



In der Überschriftszeile des Verzeichnis-Browsers sehen Sie links den gerade erkundeten Pfad (bei rekursiver Erkundung in kursiver Schrift und türkiser Farbe). Wenn Sie einen beliebigen Bestandteil des aktuellen Pfads anklicken, navigiert das direkt zu dem Verzeichnis (oder der Datei mit Unterobjekt), auf dessen Namen Sie geklickt haben. Rechts sehen Sie die Anzahl der aufgelisteten Dateien und Verzeichnisse, ggf. aufgeschlüsselt in existierende Objekte + ehemals existierende Objekte + virtuelle Objekte. Außerdem wird die Anzahl der aufgelisteten markierten Dateien angezeigt, sofern davon welche markiert sind. Die Zahl der aktiven Filter wird ebenfalls angezeigt, neben dem blauen Filtersymbol links. Spaltenbasierte und nicht-spaltenbasierte aktive Filter werden dabei separat gezählt. Diese Anzeige kann hilfreich sein, weil spaltenbasierte Filter zu Spalten aktiv sein könnten, die derzeit nicht im Verzeichnis-Browser sichtbar sind, und dass nicht-spaltenbasierte Filter aktiv sind ist ansonsten evtl. nur dann offensichtlich, wenn man im Dialogfenster mit den Verzeichnis-Browser-Optionen nachsieht.

Der Verzeichnis-Browser kann Dateien und Verzeichnisse aufsteigend oder absteigend **sortieren** und zeigt die zwei vorhergehenden Sortierkriterien mit einem helleren Pfeil weiterhin an. Wenn Sie z. B. zuerst die Dateinamensspalte anklicken und dann die Dateierweiterungsspalte, sind alle

Dateien mit der gleichen Erweiterung intern immer noch nach Namen sortiert. Um das sekundäre und tertiäre Sortierkriterium zu neutralisieren, halten Sie die Umschalt-Taste gedrückt, wenn Sie eine Spaltenüberschrift zum Festlegen des Hauptsortierkriteriums anklicken. Intern wählt dies die interne ID als sekundäres Kriterium aus. Dies stellt sicher, dass die Reihenfolge der Objekte mit identischen Daten für das Hauptsortierkriterium wohldefiniert ist und reproduzierbar, auch wenn zwischendurch nach anderen Kriterien sortiert wird. Egal wie Sie sortieren, die virtuellen Dateien auf Volume- und Disk-Ebene (die freien Speicher, Volume-Schlupf, unpartitionierte Bereiche usw. abdecken) werden immer ganz unten aufgelistet, weil man mit ihnen besser separat verfährt und nicht wie mit normalen Dateien.

The column that functions as the primary sort criterion is also the target of “jump as you type”. That is, you can type the first character or first few characters of the entry that you are looking for when the directory browser has the focus to automatically navigate and select the first or next matching item in the list, starting from the current position. For example, if the directory browser is sorted by the Type column, type “z” if you wish to find the first zip file in the list. If however there is another file listed with a type starting with “z”, one that precedes “zip” alphabetically, for example “zac”, then type the next character (before the feature times out and forgets the “z” that you have already entered), in this case “i”, until you find what you are looking for or nothing happens any more (if there is no matching item). Matching occurs in a cycle. That means even if the current position shows a zip file, you can type any preceding letter to jump to the first matching item from the top again, for example “d” for .docx. If you are looking for .docx files, but find a large group of .doc files, then you need to type all four characters of docx, because only the “x” distinguishes docx from doc.

3.3.2 Virtuelle Objekte

Wenn verwaiste Objekte gefunden werden, also z. B. gelöschte Dateien, deren ursprünglicher Pfad vom Programm nicht rekonstruiert werden kann, oder allgemein, wenn der ursprüngliche Pfad dem Programm nicht bekannt ist, werden die betroffenen Objekte in einem speziellen virtuellen Verzeichnis namens „Pfad unbekannt“ angezeigt.

Mit einer Specialist- oder forensischen Lizenz sehen Sie im Stammverzeichnis virtuelle Dateien, die es Ihnen erlauben, besondere Bereiche in Dateisystemen einzusehen. Diese werden immer am unteren Ende der Liste gruppiert angezeigt:

Dateisystembereiche: Reservierte Sektoren und/oder Cluster, die vom Dateisystem selbst für interne Zwecke in Beschlag genommen wurden.

Freier Speicher: Cluster, die vom Dateisystem nicht als „in Gebrauch“ markiert sind. Hängt von den Optionen des Datei-Überblicks ab.

Brachliegender Speicher: Bereiche in einem Volume, von denen WinHex nicht weiß, wofür sie verwendet werden, insbesondere Cluster, die vom Dateisystem als „in Gebrauch“ markiert sind, deren exakte Zuordnung von X-Ways Forensics aber nicht festgestellt werden konnte. Das kann der Fall sein, weil das Dateisystem diese Cluster aus den Augen verloren, also vergessen hat, dass sie in Wirklichkeit wiederverwendbar wären (bei FAT auch „verlorene Clusterketten“

genannt). Normalerweise gibt es keinen brachliegenden Speicher. Die Größe des brachliegenden Speichers und die Nummer des ersten brachliegenden Clusters werden erst berechnet, wenn erforderlich (z. B. wenn Sie die virtuelle Datei zum ersten Mal anklicken), weil das je nach Anzahl der Cluster insgesamt zeitaufwendig sein kann.

Dateisystemschlupf: Sektoren am Ende einer Partition, die nicht vom Dateisystem verwendet werden, weil sie keinen weiteren ganzen Cluster ergeben.

Indirekte Blöcke (Ext2, Ext3, UFS): Spezielle Blöcke (Cluster), die Blocknummern enthalten. Nicht Teil von „Dateisystembereiche".

Unbeachtete Attribut-Cluster (NTFS): Cluster, die nicht-residente Attribute enthalten, die von X-Ways Forensics nicht speziell verarbeitet wurden. Nicht Teil von „Dateisystembereiche".

.journal (ReiserFS): Blöcke, die den feststehenden Journalling-Bereich bilden. Auf Ext3 und HFS+ wird das Journal nicht als virtuelle Datei angesehen, weil es dort vom Dateisystem selbst in fest zugeordneten Datensätzen definiert wird.

3.3.3 Filter

Sie können Filter basierend auf Kriterien (Spalten) wie Dateiname, Beschreibung, Dateityp-Kategorie, Attribute oder Hash-Set einschalten. Immer wenn ein aktiver Filter tatsächlich Dateien oder Verzeichnisse herausfiltert, wird das mit einem blauen Filtersymbol in der Überschriftszeile des Verzeichnis-Browsers kenntlich gemacht, und Ihnen wird angezeigt, wie viele Objekte genau aus der Liste ausgelassen wurden. Sie haben auch die Möglichkeit, durch Klick auf die Icons für "Datei öffnen"/"Datei speichern" ganz rechts in der Überschriftszeile des Verzeichnis-Browsers, Filter- und Sortiereinstellungen in separaten Dateien abzulegen und jederzeit wieder hereinzuladen. Solche Dateien erhalten die Dateinamenserweiterung ".settings". Beachten Sie bitte, dass es nicht garantiert ist, dass Einstellungen anderer Versionen der Software geladen werden können.

Sie haben die Möglichkeit, mehrere .settings-Dateien auf einmal zu laden, die alle auf unterschiedliche Dateien abzielen, unter Einsatz verschiedener Filter (intern kombiniert mit UND oder ODER), und alle daraus resultierenden Dateien werden mit demselben Vermerk versehen. Das erlaubt komplexe verschachtelte Filterbedingungen, sowas wie Dateien vom Typ A, sofern Sie enthalten sind in Pfad X, plus Dateien vom Typ B, wenn sie nicht gelöscht wurden, sowie Dateien, deren Namen das Wort Y oder Z enthalten und die das System-Attribut gesetzt haben usw. usf. Ein Filter für den sich daraus ergebenden Vermerk wird automatisch aktiviert.

Immer wenn ein oder mehrere Filter aktiv sind, die auch tatsächlich Dateien im aktuellen Inhalt des Verzeichnis-Browsers herausfiltern, werden zwei blaue Filtersymbole in der Überschriftszeile des Verzeichnis-Browsers angezeigt. Diese machen deutlich, dass die aktuelle Ansicht wegen aktiver Filter unvollständig ist, und sie ermöglichen es Ihnen auch, alle Filter mit einem einzigen Mausklick zu deaktivieren, um sicherzustellen, dass Sie keine Datei übersehen, wenn Sie den Filter nicht mehr wollen. Sie können spaltenbasierte Filter mit einem einzigen Mausklick auf das Filtersymbol im Spaltenkopf aktivieren oder deaktivieren, wenn Sie

gleichzeitig die Umschalt-Taste gedrückt halten. Die Optionen des betreffenden Filters bleiben in diesem Fall unverändert.

The filters have been given some "intelligence" when navigating from a parent file to a child file or vice-versa, so that the filters "know" when it's a good time to be turned off.
For example:
- If you are using a filter to focus on all extracted e-mail messages recursively, and then you double-click an individual e-mail message to have a look at its attachments in the directory browser, the filter is automatically deactivated, so that you can actually see these attachments. A simple click on the Back button returns to the previous point of exploration and restores the previous filter settings and the last selection, so that you can easily continue reviewing the next e-mail message!
- If you are using a filter to focus on videos or documents, and then you double-click a video or a document to see the video stills exported for that video or the embedded pictures in that document, respectively, the filter is automatically deactivated, too.
- When you are viewing video stills only, in a gallery, and you use the Backspace key or "Find parent object" menu command to navigate to the video that this still belongs to (e.g. in order to play that video), then any active filters will be turned off so that the video can actually be listed. A simple click on the Back button returns to the previous overview of stills, enables the previous filters again, and restores the last selected item, so that you can easily continue with the next still!
- This works analogously when systematically looking at e-mail attachments, if occasionally for relevant attachments you would like to view the containing e-mail message (and e.g. print it or include it in a report) and then return to the list of attachments.

3.3.4 Spalten und Filter

Die meisten Filter und viele Spalten sind nur mit höheren Lizenztypen verfügbar, gekennzeichnet mit z. B. [FOR].

Name

Name der aufgelisteten Datei oder des aufgelisteten Verzeichnisses und (nur mit forensischer Lizenz, nur bei Verzeichnissen und Dateien mit Unterobjekten) in Klammern farblich abgesetzt optional die Gesamtzahl der jeweils hierarchisch untergeordneten Dateien im Dateiüberblick. Erlaubt das Filtern anhand einer oder mehrerer Dateinamensmasken, einer pro Zeile. Dieser Filter ist nützlich, wenn Sie eine Liste relevanter Dateinamen oder Stichwörter haben und schnell herausfinden möchten, ob Dateien mit solchen Namen vorhanden sind.

Der Filter kann auf zwei verschiedene Arten betrieben werden. Erstens können Sie Ausdrücke angeben, die jeweils mit dem ganzen Namen abgeglichen werden, wobei Sternchen als Jokerzeichen fungieren können, wie z. B. "*.jpg". Bis zu zwei Sternchen pro Maske sind erlaubt, wenn sie an ihrem Anfang und ihrem Ende vorkommen. Ausschließen können Sie Dateien mit einer Maske, die mit einem Doppelpunkt (:) beginnt. Beispiel: Alle Dateien mit Namen, die mit "A" anfangen und nicht das Wort "Garten" enthalten: "A*" in einer Zeile und ":*Garten*" in einer weiteren Zeile. Wenn mehrere positive Ausdrücke angegeben werden, werden sie logisch mit einem ODER verknüpft; negative Ausdrücke (:)

mit einem UND.

Wenn die Option "Teilwort-Suche in Dateinamen" aktiv ist, dann gelten die obigen Regeln nicht. Es wird dann stattdessen eine *Suche innerhalb* der Dateinamen nach den angegebenen Zeichen bzw. optional regulären Ausdrücken durchgeführt. Z. B. geben Sie einfach "Rechnung" ein, um Dateien zu finden, in deren Name das Wort auftritt, nicht "*Rechnung*". Eine Erklärung der Features von regulären Ausdrücken finden Sie unter Suchoptionen. Der Anker $ funktioniert hierbei nicht.

The amount of text that can be pasted into the Name filter has been extended to 2 million characters. That doesn't mean that X-Ways Forensics can efficiently use a filter with many tens of thousands of characters or more. When in doubt, use the "Match against full name" option, not the substring search, for better performance.

If an original name is found for a file in the Windows recycle bin or in an iPhone backup or certain other files during metadata extraction, that name is displayed in the Name column with the current unique name in square brackets. The current unique name is now also shown in square brackets in the case report. Both names are targeted by the Name filter.

Kleine Dreiecke in der unteren rechten Ecke einer Namenszelle erinnern Sie daran, dass es Vermerke für die betreffende Datei gibt. Unterschiedliche Farben unterscheiden zwischen automatisch erzeugten Vermerken und solchen, die vom Benutzer selbst zugewiesen wurden.

Der Kopf der Namensspalte erlaubt es, alle aufgelisteten Objekte mit einem einzigen Mausklick schnell zu markieren oder zu entmarkieren. Er dient auch als Hinweis darauf, ob sich unter ggf. sehr vielen aufgelisteten Objekte markierte oder nicht markierte Objekte befinden.

Existent — Zeigt an, ob eine Datei eine existierende Datei oder ein Unterobjekt einer existierenden Datei ist oder nicht (existierend gemäß dem Bezugssystem, z. B. Dateisystem), entweder mit einem Häkchen oder einem mathematischen Symbol oder in natürlicher Sprache, abhängig von den Notationsoptionen. Ein dritter Zustand ist "virtuell". Um basierend auf dem Existenzzustand zu filtern, verwenden Sie bitte den Beschreibungsfilter. Bitte beachten Sie, dass Sie auch nach dem Existenzzustand gruppieren können (s. Verzeichnis-Browser-Optionen) und nach dieser Spalte sortieren können.

Beschreibung — Textuelle Beschreibung des Objekts. Die Spalte informiert über ähnliche Eigenschaften wie das Icon in der Namensspalte, z. B. ob es sich um eine Datei oder ein Verzeichnis oder eine extrahierte E-Mail oder ein Video-Standbild handelt. Sie gibt den Existenz-/Löschzustand eines Objekts an und es sich um eine virtuelle Datei für Untersuchungszwecke handelt oder um eine aus Sektoren ausgegliederte Datei, handelt. Sie beschreibt auch den Zustand des Objekts im Datei-Überblick (z. B. markiert oder bereits eingesehen). Welche Texte in der Spalte angezeigt werden kann in den Notationsoptionen individuell eingestellt

werden (über die Allg. Optionen). Dass die Einstellungen der Beschreibungsspalte Teil der Notationsoptionen sind, hat den Vorteil, dass Sie zwei verschiedene Einstellungen haben können, eine allgemein für den Verzeichnis-Browser und eine andere speziell für den Befehl „Liste exportieren“. Das kann nützlich sein, weil es in einer exportierten Liste ja keine Icons gibt, anhand derer Sie die Art des Objekts und seinen Löschzustand erkennen könnten, anders als im Verzeichnis-Browser.

Diese Spalte erlaubt es auch, nach den abgedeckten Eigenschaften zu filtern oder danach zu sortieren, was den Beschreibungsfilter zu einem der wichtigsten Filter macht. U. a. können Sie Folgendes bei Bedarf herausfiltern:

- existierende Dateien (nützlich, wenn Sie sich lediglich für ehemals existierende Dateien interessieren [die sich in existierenden Verzeichnissen befinden können])
- ehemals existierende Dateien und Verzeichnisse.
- markierte Dateien und Verzeichnisse.
- halb markierte Dateien und Verzeichnisse (die mind. 1 markierte und mind. 1 nicht markierte Datei enthalten).
- *nicht* markierte Dateien und Verzeichnisse.
- Dateien, die als bereits eingesehen gekennzeichnet sind.
- Dateien, die nicht als bereits eingesehen gekennzeichnet sind.
- ausgeblendete Dateien und Verzeichnisse.
- *nicht* ausgeblendete Dateien und Verzeichnisse.

Der schnellste Weg, um zum Filterdialog zu gelangen, ist ein Rechtsklick auf die Überschriftszeile des Verzeichnis-Browsers. Dieser Weg steht Ihnen sogar dann offen, wenn die Beschreibungsspalte gar nicht sichtbar ist. (Evtl. benötigen Sie die Beschreibungsspalte im Verzeichnis-Browser gar nicht, wenn Ihnen das Icon zur Identifizierung der Art des Objekts genügt.) Das Trichtersymbol, das den Filter der Beschreibungsspalte repräsentiert, hat vier mögliche Farben: 1) Grau, wenn inaktiv, wie auch bei anderen Filtern üblich. 2) Grau mit einer ganz, ganz leichten Tendenz zu blau, fast nicht von grau unterscheidbar, wenn der Filter zwar theoretisch aktiv ist, aber nur ausgeblendete Dateien herausfiltern würde, wovon es aber im erkundeten Pfad nicht mal welche gibt. 3) Blaugrau, wenn nur ausgeblendete Dateien vom Filter ausgesondert werden und das auch tatsächlich passiert. 4) Normal blau, um Ihre Aufmerksamkeit darauf zu lenken, dass der Beschreibungsfilter aktiv ist und nicht nur ausgeblendete Dateien heraussiebt, sondern auf andere Eigenschaften achtet. Das zurückhaltende Farbschema wurde eingeführt, weil viele Benutzer es für den Normalzustand halten, wenn ausgeblendete Dateien tatsächlich herausgefiltert werden, weil sie sie genau zu dem Zweck ausblenden, um sie nicht mehr zu sehen. Dann ist die Erinnerung daran durch ein ins Auge springendes Blau unnötig ablenkend.

Der Filter für Video-Standbilder hat eine besondere Option, die es erlaubt, auch das zugehörige Video aufzulisten, und zwar jeweils direkt vor dessen Einzelbilder. Auf diese Weise ist es leicht zu sehen, welche Bilder aus welchem Video stammen, und Sie können direkt Kommentare zum Video eingeben oder

das Video mit einem Vermerk versehen, ohne hin- und her zu navigieren und ohne auf die weniger intuitive Bedienungsweise zurückgreifen zu müssen, Objekte mit Vermerken versehen, die Sie gar nicht sehen können (mit der Option „für übergeordnete Datei“). Die Kacheln, die die Videos repräsentieren, können zudem in der Galerie als visuelle Trennelemente dienen, wenn Sie „ersatzweise Miniaturansichten“ in den Galerie-Optionen ausschalten. Dann fällt es sehr leicht zu sehen, wo die Bilder des nächsten Videos anfangen.

Der Filter erlaubt es auch, sich allgemein auf gecarvte (aus Sektoren ausgegliederte) Dateien zu konzentrieren, oder speziell solche, die entweder an Sektorgrenzen gefunden wurden oder nicht, z. B. nach einer Datei-Header-Signatur-Suche auf Byte-Ebene, um Mülldateien zu entfernen, die unter nicht an Sektorgrenzen gecarvten Dateien häufiger anzutreffen sind. You can also focus on files from which text was extracted for logical searches (by OCR or decoding), with a certain minimum number of characters (like 5 or 10, 255 at most), for example to avoid pictures in which a few characters have been recognized merely erroneously, i.e. pictures that not actually do contain text.

Eine spezielle Einstellung für den Filter erlaubt es, sich auf solche Dateien zu konzentrieren, deren Erzeugungsdatum später ist als ihr Änderungsdatum, d. h. solche Dateien, die offenbar kopiert wurden und dadurch mit einem neuen Erzeugungsdatum versehen wurden. Über die Notationsoptionen können solche Dateien mit dem Wort "kopiert" gekennzeichnet werden. Das Vorhandensein dieses Wortes kann dann für die bedingte Zelleinfärbung herangezogen werden, so dass Sie schnell sehen, welche Dateien vermutlich Originaldateien auf dem betreffenden Datenträger sind und welche kopiert wurden. Das Wort "kopiert" ist allerdings sprachabhängig (evtl. wichtig zu bedenken, wenn Sie Ihre Einstellungen für die bedingte Zelleinfärbung mit Benutzern in anderen Ländern teilen).

Erw. — Dateinamenserweiterung/Dateiendung. Der Teil des Dateinamens, der dem letzten Punkt folgt, sofern vorhanden, es sei denn, der letzte Punkt ist das allererste Zeichen im Dateinamen (nicht unüblich in der Unix-/Linux-Welt).

Typ [INV, FOR] — Dateityp. Wenn die Header-Signatur einer Datei nicht gezielt überprüft wurde (s. Datei-Überblick erweitern), ist diese Spalte bloß eine Wiederholung der Dateiendung und wird grau angezeigt. Andernfalls, wenn die Prüfung der Dateisignatur die wahre Natur der Datei enthüllt hat, wird eine typische Endung dieses Dateiformats ausgegeben. Diese Endung wird in Schwarz angezeigt, wenn sie identisch ist mit der tatsächlichen Endung im Dateinamen, oder in Blau, wenn die tatsächliche Endung nicht mit dem Typ der Datei übereinstimmt. Ein komfortabler Filter kann für diese Spalte aktiviert werden. In dem Filterdialog können Sie individuelle Dateitypen oder ganze Kategorien wählen. Sie können die Auswahl laden und speichern. Es gibt Schalter, mit denen Sie alle Kategorien auf einmal ein- und aufklappen können. Das Aufklappen aller Kategorien kann nützlich sein, wenn Sie schnell einen bestimmten Dateityp auffinden möchten, indem Sie die ersten Buchstaben eintippen, während das Baumfenster den Eingabefokus hat.

Beachten Sie bitte, dass Überschneidungen zwischen Dateityp-Bezeichnungen offensichtlich werden können, wenn zum Filtern gewählte Dateitypen geladen werden, aus .settings-Dateien oder aus Fällen. Wenn Sie z. B. ursprünglich "mmf" = "MailMessage File" (Kategorie E-Mail) ausgewählt hatten, dann werden Sie feststellen, dass nach dem Laden auch "mmf" als "Yamaha SMAF" gewählt ist (Kategorie Sound/Music). Das ist normal und ändert nicht das Verhalten des Filters, der im Zweifelsfall sowieso zur Sicherheit gleich bezeichnete, andere Typen mit erfasst, damit nichts übersehen wird.

Typ-Status [INV, FOR]

Der **Status** der Dateityp-Spalte. Anfänglich „nicht geprüft". Nach der Dateisignatur-Überprüfung (im Rahmen einer Datei-Überblickserweiterung oder des Ladens einer Datei in die Vorschau oder Galerie) gilt: Wenn eine Datei sehr klein ist (weniger als 8 Bytes groß), ist der Status „unerheblich". Wenn weder die Dateiendung noch die Signatur in der Dateitypsignatur-Datenbank aufgeführt ist oder den internen Algorithmen bekannt ist, lautet der Status „nicht verzeichnet". Wenn die Signatur gemäß Datenbank oder gemäß einem internen Algorithmus zu der Endung passt, ist der Status „bestätigt". Wenn die Endung aus der Datenbank bekannt ist, aber keine Signaturdefinition und kein interner Algorithmus den Dateityp identifizieren kann, sehen Sie als Status „nicht bestätigt". Wenn die Signatur bekannt ist und es keine Dateinamenserweiterung gibt oder nur eine bedeutungslose wie .dat oder .tmp, oder wenn eine standardisiertere Typkennung gesetzt wird, ist der Status „neu erkannt". Wenn die Signatur in einer Datei von den Definitionen in der Datenbank erkannt wird oder ein interner Algorithmus den Dateityp erkennt, aber die Dateiendung zu einem *anderen* Dateityp gehört, die Datei also mutmaßlich eine irreführende Endung hat, ist der Status „anders erkannt". Filter verfügbar.

Zusätzlich kann diese Spalte einen Hinweis auf die Konsistenz des Formats von Dateien diverser unterstützter Typen geben, entweder in Form von "OK", "irregulär" oder "defekt", für gecarvte Dateien u. U. sofort, für andere u. U. nach der Typprüfung oder der Metadaten-Extraktion. "Irregulär" kann bedeuten unvollständig, inkonsistent, unerwartet, nicht einsehbar, ... alles, was irgendwie nicht normal ist. Z. B. im Fall von JPEG kann irregulär bedeuten, dass am Ende der Datei keine Footer-Signatur gefunden wurde.

Eine Erklärung des Dateityp-Rangs und des Konzepts von Dateityp-Gruppen findet sich in der Beschreibung der Datei File Type Categories.txt.

Typ-Beschreibung [INV, FOR]

Zeigt den Namen des zugehörigen Anwendungsprogramms an, wofür die Dateiendung eine Abkürzung ist o. ä., je nach Angabe in File Type Categories.txt. Wenn dieselbe Dateiendung mehrfach in der Definitionsdatei vorkommt, werden all ihre Bedeutungen aufgelistet. Z. B. kann .pm ein Perl-Modul sein, ein PageMaker-Dokument, eine Pegasus-Datei oder eine X11-Pixmap-Datei.

Typ-Kategorie [INV, FOR]

Dateityp-Kategorie, zu der der Dateityp gehört, gemäß Definition in „File Type Categories.txt" (s. u.). Filter verfügbar. Sie können mehrere Dateityp-Kategorien auf einmal zum Filtern auswählen, über ein Dialogfenster anstelle des schneller nutzbaren aufklappbaren Menüs. Sollte derselbe Dateityp bzw. dieselbe

	Dateiendung mehrfach definiert sein und zu unterschiedlichen Kategorien gehören, wird jeweils nur eine Kategorie angezeigt. Der Kategoriefilter funktioniert jedoch trotzdem. Der Kategoriefilter kann mit einem aufklappenden Menü aktiviert werden. In demselben Menü sehen Sie auch eine Statistik über die Anzahl der Dateien in jeder Kategorie, die gegenwärtig im Verzeichnis-Browser aufgelistet sind (bzw. bei ausgeschaltetem Kategoriefilter aufgelistet würden).
Asservat [INV, FOR]	Der Name des Asservats, dessen Teil die Datei oder das Verzeichnis ist. Nützlich in einem rekursiv erkundeten Asservatüberblick, wenn also der Verzeichnis-Browser alle Dateien aus allen Asservaten zeigt. Ein Sortieren nach dieser Spalte richtet sich nach der Asservatnummer, die in den Asservateigenschaften angezeigt wird. Diese richtet sich i. d. R. nach der Position des Asservats im Fallbaum.
Pfad	Pfad der Datei oder des Verzeichnisses. Fängt mit einem umgekehrten Schrägstrich an, relativ zum Stammverzeichnis des Dateisystems. Filter verfügbar. Die Filterausdrücke werden als Teilworte interpretiert, die auf einen beliebigen Teil des Pfades passen können. Jokerzeichen sind nicht erforderlich.
Vollpfad [SPE, LAB, FOR]	Der Vollpfad enthält den Namen der Datei bzw. des Verzeichnisses selbst. Nach dem Vollpfad zu sortieren, ergibt eine nützliche Reihenfolge, weil Unterobjekte dabei direkt ihren jeweiligen Eltern folgen. Das funktioniert auch dann, wenn einige Elterndateien/Verzeichnis/E-Mails exakt denselben Namen haben. Filter verfügbar.
Elter-Name, Unterobjekte [INV, FOR]	Beide Spalten sind mit Filtern ausgestattet. Der Filter für Unterobjekte erlaubt es Ihnen beispielsweise, schnell alle E-Mails zu finden, die einen Datei-Anhang mit einem bestimmten Namen haben. Auch beim Exportieren kann es schön sein, für eine E-Mail auch die Namen der Attachments mit auszugeben. Der Filter für den Elter-Namen ermöglicht es, schnell alle Attachments zu finden, die an E-Mails mit bestimmten Wörtern im Betreff angehängt waren. Beachten Sie, dass sich die Filter der Spalten Name, Elter-Name und Unterobjekte die gleichen Einstellungen teilen und sich gegenseitig ausschließen. D. h. sie können nicht gleichzeitig aktiv sein, sondern deaktivieren einander.
Größe	Logische Größe der Datei (d. h. Größe ohne Schlupf) bzw. physische Größe eines Verzeichnisses. Physische Dateigröße und (für Dateien in NTFS-Dateisystemen) initialisierte Größe können Sie im Datei-Modus in der Informationsspalte sehen. Wenn die rekursive Auswahlstatistik aktiv ist, wird mit einer forensischen Lizenz als Größe von Verzeichnissen die Gesamtgröße aller Dateien angezeigt, die direkt oder indirekt in dem jeweiligen Verzeichnis enthalten sind, andernfalls die Größe der Datenstrukturen des Verzeichnisses im Dateisystem. Filter verfügbar. Um Dateien mit unbekannter Größe aufzulisten, können Sie die Filterbedingung ≤ -1 einstellen. Die modulo-Option erlaubt es z. B., Dateien herauszufiltern, deren Größe kein Vielfaches der Sektorgröße ist, wenn Sie etwa auf der Suche sind nach Roh-Images oder Container-Dateien von TrueCrypt/VeraCrypt.
Erzeugung	Zeitpunkt (Datum und Uhrzeit), an dem die Datei oder das Verzeichnis in dem Dateisystem erzeugt wurde. Wird in den meisten Linux-Dateisystemen nicht gespeichert.
Änderung	Zeitpunkt (Datum und Uhrzeit), an dem die Datei oder das Verzeichnis zuletzt

geändert wurde. Auf FAT ist die Uhrzeit nur auf 2 Sekunden genau. Auf CDFS wird der einzige verfügbare Zeitstempel in dieser Spalte angezeigt, auch wenn er nicht notwendigerweise die letzte Änderung angibt. Filter verfügbar.

Zugriff — Zeitpunkt (Datum und Uhrzeit), an dem auf die Datei oder das Verzeichnis zuletzt lesen oder anderweitig zugegriffen wurde. In NTFS werden diese Zeitstempel in grau dargestellt, wenn sie identisch sind zum jeweiligen Erzeugungszeitstempel, weil dies auf den meisten Systemen wahrscheinlich bedeutet, dass diese Zeitstempel gar nicht gepflegt werden, aus Performanzgründen, und dass sie daher nicht sehr bedeutsam sind. Auf FAT wird nur das Datum gespeichert. Filter verfügbar.

Record-Änderung — Zeitpunkt (Datum und Uhrzeit), an dem der FILE-Record (NTFS) bzw. die Inode (Linux-Dateisystem) der Datei oder des Verzeichnisses zuletzt geändert wurde. Dies sind Dateisystem-Datenstrukturen, die Metadaten über Dateien enthalten. Filter verfügbar.

Löschung — Zeitpunkt (Datum und Uhrzeit), an dem die Datei oder das Verzeichnis in dem Dateisystem gelöscht wurden. Generell nur in Linux-Dateisystemen verfügbar, und u. U. bei NTFS (nach einer intensiven Datei-System-Datenstruktur-Suche und dem Einsehen der $UsnJrnl:$J-Datei in dem Dateisystem, falls es sie gibt). Nicht zu verwechseln mit dem sog. Löschdatum, das Ihnen u. U. lustigerweise andere forensische Tools in NTFS-Dateisystemen anzeigen, für Dateien, die im Dateisystem gar nicht gelöscht wurden. Filter verfügbar.

Erzeugung des Inhalts [INV, FOR] — Erzeugungszeitstempel, der aus intern in Dateien diverser Typen gespeicherten Metadaten extrahiert werden kann (Liste der Typen s. Dokumentation des zugehörigen Befehls im Kontextmenü), wie dort von dem Programm gespeichert, das die Datei erzeugt hat. Interne Zeitstempel sind üblicherweise weniger flüchtig als Zeitstempel im Dateisystem und z. T. schwieriger zu manipulieren. Sie können insbes. nützlich zur Erhärtung bestimmter Annahmen oder Schlussfolgerungen sein. If an official creation timestamp is found in the internal metadata, that timestamp will be presented in this column. If not, various other plausible timestamps may be used as a substitute, even a timestamp derived from the filename if necessary. That way around 60% of all JPEG files can be presented with a Content created value. Filter verfügbar.

Mehr über die diversen Zeitstempel-Spaten im nächsten Kapitel.

Attr. — DOS/Windows-Attribute auf den Dateisystemen FAT und NTFS. Unix/Linux-Permissions und Filemode auf den Unix-/Linux-/Mac-Dateisystemen. Verwendet einige proprietäre Symbole, die in der Legende erklärt werden (nur mit forensischer Lizenz).
„Partielle Initialisierung“ bedeutet, dass dem Dateisystem (NTFS oder exFAT) zufolge weniger Bytes als die logische Dateigröße angibt tatsächlich initialisiert/in die Datei geschrieben wurden, so dass die Daten am Ende der Datei undefiniert sind, ähnlich wie Dateischlupf nichts mit der Datei zu tun haben und schon vorher auf dem Datenträger an der betreffenden Stelle gespeichert waren. Sie können die initialisierte Größe im Dateimodus in der Informationsspalte sehen, und der nicht

initialisierte Bereich wird in einer anderen Farbe hervorgehoben.
Einige Attribute von Partitionen aus GUID-Partitionstabellen werden ebenfalls in der Attr.-Spalte angezeigt: system (=vom Betriebssystem benötigt), hidden (=nicht als Laufwerksbuchstabe geladen), read-only, shadow copy.
Beim Sortieren nach Attributen werden Dateien mit "interessanteren" Attributen zuerst aufgelistet, z. B. Attributen, die Verschlüsslung anzeigen. Dateien ohne gesetzte Attribute oder deren Attribute unbekannt sind, folgen als letztes.
Ein Filter ist verfügbar. For example, you can filter for any of the 9+3 bits of Unix-style file permissions specifically and combine them with OR, AND, or EQUAL. EQUAL requires a status of all 12 bits exactly as selected (whether set or not set). AND means you require ALL of the checked bits to be set, but don't care about the others. OR means you are satisfied already if ANY of the checked bits is set. SUID and SGID bits can be combined with a logical OR or AND. Please remember that if you are interested in directories with the sticky bit, you will need to include directories when exploring recursively and apply filters to directories, too (not the default setting). Please note that the logical operator for permissions should not be usually set to EQUAL because that will result in active filtering for permissions even if no permission bits are selected in the dialog box at all, unlike the OR or AND operators. EQUAL with no permission bits selected means to filter for files that have no permission bits set or files whose permissions are unknown..

Startsektor [nicht INV]

Die Nummer des Sektors, der den Anfang der Daten der Datei oder des Verzeichnisses enthält. Das Sortieren nach Startsektor sortiert nach physischer Anordnung auf dem Datenträger, und erlaubt es, physisch zusammenhängend gespeicherte Dateien nebeneinander zu sehen. This column is specially populated for files in Zip archives, with the sector that contains the local zip record of such a file. Clicking a file in a zip archive in Volume/Partition mode automatically jumps directly to its local zip record, which is followed by the (usually) compressed file data. This does not apply to files in nested zip archives. Es ist ein Filter verfügbar, der es erlaubt, Dateien zu identifizieren, deren Inhalte in bestimmten Sektorbereichen beginnen, z. B. weil diese definitiv von etwaigen bekannten defekten Sektoren betroffen sind oder jenseits des Endes von bekanntermaßen unvollständigen Images gespeichert sind. Bedenken Sie, dass Sie hier auf Wunsch physische (plattenbasierte) Sektornummern sehen können statt logische (partitionsbasierte) Sektornummern, s. Verzeichnis-Browser-Optionen. Mit der modulo-Option können Sie auf Dateien abzielen, die entweder an Clustergrenzen ausgerichtet sind oder nicht.

In the dialog window with the directory browser options this column can be turned into an "Offset" column, displaying decimal or hexadecimal start offsets of the data of files instead of start sector numbers. This is more precise information and available for most files. The title of the column will be changed accordingly in most places of the user interface. The offset can optionally be made a physical offset (from the point of view of the physical disk/image if shown in a partition) just like the sector number can be made a physical sector number. The filter of that column expects numbers of the same meaning as shown in the directory browser (i.e. either offsets or sectors, either logical or physical), and in the same

notation (decimal for sector numbers, decimal or hexadecimal for offsets). The directory browser context menu command "Find duplicates in list" can identify duplicates based on exact identical start offsets instead of just identical start sectors if the "First sector" column is populated with offsets.

Offset im Dateisystem [SPE, LAB, FOR]

Shows the offset of the defining data structure of a file or directory in the file system, i.e. the structure that is the basis for the inclusion of a file in the volume snapshot. That offset is where you can check details manually in case there are any doubts about where X-Ways Forensics got the file system level metadata from. This is also where you may apply a suitable template to get an alternative interpretation and where you can point disadvantaged users of other tools to as they may not be able to find such a crucial location otherwise or don't even get certain deleted files listed. Carved files and files that are embedded in other files for obvious reasons do not have such an offset in the file system (or in the case of carved files at least it is not known to X-Ways Forensics). The file system offset is also where you navigate to when you use the dedicated context menu command to locate a file's FILE record/inode/file entry/catalog key etc., as known from all versions. Clicking the FS offset cell of a file or directory automatically navigates to that offset instead of to the first data sector when in Disk/Partition/Volume mode.

Für ein Partition gibt der „Offset im Dateisystem“, sofern überhaupt verfügbar, den Offset an, an dem eine Partition definiert wurde, üblicherweise in einer Partitionstabelle.

ID

Zahlenschlüssel, der einer Datei oder einem Verzeichnis vom Dateisystem oder von WinHex zugeordnet wurde. Nicht notwendigerweise nur einmalig vergeben. Der Filter hilft dabei, weitere harte Verweise einer gegebenen Datei zu finden.

Int. ID

Der eindeutige interne Schlüssel einer Datei oder eines Verzeichnisses im Datei-Überblick. Objekte, die dem Datei-Überblick zuletzt hinzugefügt wurden, haben die höchsten Schlüsselwerte. Filter verfügbar. Nützlich z. B. und sehr einfach zu benutzen, wenn Sie sich auf die *x* zuletzt dem Datei-Überblick hinzugefügten Dateien konzentrieren möchten (nachdem Sie ihn erweitert haben) oder wenn Sie eine logische Suche bei interner ID *y* fortsetzen möchten (und Dateien herausfiltern, die evtl. schon zuvor durchsucht wurden).

For evidence objects that contain a huge number of files, the modulo option allows you to focus on a subset of files that is more or less representative of all files (though less random than files listed first when sorting by hash value). Applying the modulo operation to the internal ID will pick files from any directory, with any name, creation date etc. To see only 1,000 out of 100,000 files, i.e. every 100th file, use the operation "internal ID modulo 100 = 0". Also useful for testing purposes: If you wish to compare the performance of different hard disks, RAID systems, processors, configurations for volume snapshot refinements, you don't have to process all files in an evidence object. You can get quicker, yet likely representative results for example in 1/10 of the time if you only process every 10th file, pseudo-randomly selected by internal ID.

Even for normal work, examiners may not be required by their bosses/their prosecutor to conduct a 100% complete examination, for example if after review of a reasonably sized and representative subset you can extrapolate that about 10% of several 10,000 photos is illegal material.

Int. Elter [nicht INV]
Der eindeutige interne Schlüssel des Elternverzeichnisses (übergeordneten Verzeichnisses) einer Datei oder eines Verzeichnisses im Datei-Überblick. Das Wort Elter wird hier als Singular verwendet, wie in der Informatik und Biologie üblich. Nützlich z. B., wenn man Dateien und Verzeichnisse exportiert und es mehrere Verzeichnisse gleichen Namens im gleichen Pfad gibt (z. B. eins existierend, eins gelöscht), so dass man anhand der internen ID des Elters einer Datei ansehen kann, in welchem Verzeichnis sie liegt, auch wenn es sich allein aus dem Namen nicht eindeutig ergibt.

Eindeutige ID [INV, FOR]
An internal identifier of a file or directory that is unique within the entire case, not just within the volume snapshot of one evidence object, and unique for the whole life time of the case. The unique ID is easily readable. It contains a delimiter, separating evidence object ID and int. ID.

Eindeutige ID als GUID [INV, FOR]
Eindeutige ID formatiert als und ergänzt zu einer GUID.

Besitzer [FOR]
Die ID des Besitzers der Datei bzw. des Verzeichnisses, auf Dateisystemen, die diese Information aufzeichnen. Bei NTFS ist dies die SID, oder, wenn X-Ways Forensics diese mit Hilfe der bereits im aktuellen Fall gesichteten SAM-Registry-Dateien einem Benutzernamen zuordnen kann, der Benutzername. Filter verfügbar.

Gruppe [FOR]
Zeigt die ID der Gruppe an, die einer Datei in Linux-Dateisystemen zugeordnet ist.

Absender, Empfänger [INV, FOR]
Diese Spalten werden für von X-Ways Forensics aus E-Mail-Archiven extrahierte E-Mails und Datei-Anhänge gefüllt, sowie für ursprüngliche .eml-Dateien, wenn Metadaten aus ihnen extrahiert wurden. Sie bieten Filter an, in denen Sie einen beliebigen Teil einer E-Mail-Adresse oder eines Namens eingeben können, um nach bestimmten E-Mails zu suchen. Da der Filterausdruck als Teilwort interpretiert wird, sind Jokerzeichen nicht erforderlich. Sie können wählen, welche Empfängertypen Sie mit dem Filter adressieren möchten (To:, Cc: und/oder Bcc:). Sie können Empfänger der Typen To:, Cc: und Bcc: auch in separaten Spalten sehen, wenn Sie das bevorzugen. (nur forensische Lizenz)

Verweise [FOR]
Die Anzahl der sog. Hard Links der Datei oder des Verzeichnisses, d. h. wie oft sie bzw. es von einem Verzeichnis referenziert wird.

A hard link that just provides a short filename (SFN) to satisfy the legacy 8.3 requirements of old Microsoft DOS/Windows versions is not counted as a hard link. Instead, such files get their hard link count marked with a ° in the Links column of the directory browser. That way, the hard link count more accurately reflects the hard links actually present in the volume snapshot of X-Ways Forensics, and normal files always have a count of 1, whereas 2 or more means something more spe-

cial. If a hard link count of 1 is marked with an asterisk (*), that means that the file or directory is stored as hard-linked in the directory structure in HFS+ although it would not be necessary based on the hard link count. If the hard link count is grayed out, that designates files that will be optionally omitted during a logical search to avoid unnecessary duplicate search efforts and duplicate search hits.

Dateianzahl [INV, FOR] — Die Gesamtzahl der in einem Verzeichnis oder in einer Datei mit Unterobjekten im Datei-Überblick enthaltenen Dateien, rekursiv, d. h. auch weitere Unterverzeichnisse mit einschließend. Die Zahl kann je nach Einstellungen auch in der Namensspalte in Klammern gefunden werden. Wird nur mit forensischer Lizenz berechnet.

Trefferanz. [INV, FOR] — Die Anzahl der Suchtreffer, die in einer Datei gefunden wurden.

Begr.anzahl [INV, FOR] — Die Anzahl der Suchbegriffe (nicht Suchtreffer), die in einer Datei gefunden wurden. Diese Anzeige berücksichtigt alle Suchbegriffe, die jemals in parallelen Suchen in einem Fall gefunden wurden, nicht nur diejenigen, die ggf. in der Suchbegriffsliste ausgewählt sind, wenn Sie keine Suchtreffer gelöscht haben. Sie können nach dieser Spalte sortieren, um diejenigen Dateien ganz oben zu sehen, die am wahrscheinlichsten relevant sind (weil sie mehr von den Begriffen, nach denen Sie gesucht haben, enthalten). Diese Spalte wird nur für Asservate eines Falls gefüllt.

Suchbegriffe [INV, FOR] — Listet bis zu 25 der in der Datei gefundenen Suchbegriffe auf, die in der vorangehenden Spalte gezählt werden. Nützlich, um auch im normalen Verzeichnis-Browser schnell eine Vorstellung davon zu erhalten, was für Treffer es in einer Datei gab, ohne in die Suchtrefferliste wechseln zu müssen. (nur forensische Lizenz) Filter verfügbar, der nicht auf die 25 in der Spalte angezeigten Suchbegriffe beschränkt ist.

Seitenzahl [INV, FOR] — The page count is extracted from PDF and some Office file types as part of metadata extraction and shown in this column.

Pixel [INV, FOR] — Die groben Maße eines Bildes in KP (tausend Pixel) oder MP (Millionen Pixel, Megapixel), als Produkt aus Breite und Höhe, aus Effizienzgründen in sehr geringer Genauigkeit gespeichert. Die Abmessungen werden gleichzeitig mit der Hautfarbenerkennung berechnet, außerdem beim Betrachten der Bilder (Vollbildmodus, Vorschau oder Galerie). Nützlich, um z. B. unterscheiden zu können zwischen kleinen Bildchen aus dem Browser-Cache, die man sich beim Surfen im Internet einfängt, und hoch aufgelösten Digitalfotos, mit Hilfe des zugehörigen Filters. Der Filter erlaubt es, sich zu konzentrieren auf Bilder, die weniger oder gleich viele Pixel enthalten wie von Ihnen angegeben, oder mehr oder gleich viel, oder beides auf einmal. (Der Filter arbeitet aufgrund der geringen Genauigkeit der Speicherung nur annähernd exakt.) Sofern zumindest 1 Standbild aus einer Video-Datei exportiert wurde, sieht man die ungefähre Auflösung des Videos ebenfalls in dieser Spalte.

Analyse [INV, FOR] — Kombinierte Spalte, die von FuzZyDoc ermittelte Übereinstimmungen von Textdokumenten zeigt, sowie PhotoDNA-Zuordnungen von Bildern und den

berechneten Hautfarbenanteil von Bildern (oder die Tatsache, dass es sich um ein Schwarzweiß- oder Graustufenbild handelt oder um ein so kleines Bild, dass es keinen relevanten Inhalt haben kann). Verfügbar nach dem Erweitern des Datei-Überblicks, sofern die zugrundeliegende Technologie verfügbar ist. Sorting or filtering by this column is the most efficient way to discover traces of e.g. child pornography or search for scanned documents (gray scale or black & white pictures). Sorting by the Analysis column in descending order lists files with FuzZyDoc matches first (those files with the most confident matches for any hash set near the top, with lower percentages following), followed by PhotoDNA matches (showing the category names in an internal PhotoDNA hash database), followed by pictures with no PhotoDNA matches in descending order of their skin tone percentage. After that, irrelevant pictures are listed (picture with very small dimensions), and then files that are not pictures, and near the bottom black & white and gray scale pictures. Text color coding in that column makes it easier to distinguish between different kinds of categorizations. FuzZyDoc matches, PhotoDNA matches and color analysis results are mutually exclusive. That means that if a picture gets it colors analyzed and also a similarity with a PhotoDNA hash value is found, only the PhotoDNA category match is remembered in the Analysis column, not the skin tone percentage, because the PhotoDNA match is considered more helpful. A stylized P is displayed in the Analysis column for pictures for which at least one PhotoDNA hash value is stored in the volume snapshot. If that is the case, the hash value can be seen in Details mode.

Hash [SPE, LAB, FOR]

Bis zu zwei Hash-Werte können für eine Datei berechnet werden (z. B. MD5 und SHA-1) und werden dann in den beiden Hash-Spalten dargestellt. Filter verfügbar. Die Filter erlauben es, sich auf Dateien zu konzentrieren, für die kein Hash-Wert verfügbar ist, deren Hash-Werte mit einem bestimmten Hex-Wert beginnen (wenn Sie nur den Anfang eines Hash-Werts angeben) oder die einen bestimmten Hash-Wert haben (wenn Sie einen kompletten Hash-Wert angeben). Der Filter kann die Hash-Werte von Dateien mit bis zu 4 vom Benutzer in Hex-ASCII angegebenen Hash-Werten vergleichen. Das ist schneller als extra ein kleines Hash-Set in der Hash-Datenbank zu erzeugen, wenn Sie lediglich ein paar wenige Dateien finden möchten, z. B. Duplikate von Dateien mit einem bestimmten Hash-Wert, den Sie einfach aus der Hash-Spalte im Verzeichnis-Browser kopieren. Der einfachste Weg, diesen Filter so zum Auffinden von Duplikaten zu verwenden, der nicht einmal ein Kopieren und Einfügen von Hash-Werten erfordert, ist das Anklicken eines Hash-Werts einer gegebenen Datei mit der rechten Maustaste im Verzeichnis-Browser (sofern dieser dort in Hex-ASCII-Notation angezeigt wird, nicht in Base32) und dann den Befehl "Nach Duplikaten filtern" im Kontextmenü aufzurufen.

Die Hash-Spalte zeigt Pseudo-Hash-Werte in hellgrauer Farbe an, bis echte Hash-Werte berechnet werden [FOR]. Pseudo-Hash-Werte basieren nur auf den Metadaten einer Datei, nicht auf dem Datei-Inhalt. Sie sind daher auch für sehr große Dateien augenblicklich verfügbar. Sie erlauben es Ihnen, Dateien in zufälliger Reihenfolge aufzulisten, genauso als wenn Sie nach echten Hash-Werten sortieren, aber ohne, dass Sie erst Zeit investieren müssen, um echte Hash-Werte zu berechnen. Das ist nützlich z. B. für eine Vorab-Durchsicht (Triage),

wenn Sie nur wenig Zeit zur Verfügung haben und nur einen schnellen Blick auf zufällig ausgewählte Dateien in größeren Asservaten werfen möchten (z. B. Bilder in der Galerie), um sich eine Meinung darüber zu bilden, wie relevant das Asservat sein könnte.

Das Betrachten von Dateien in zufälliger Reihenfolge gibt Ihnen einen vollständigeren, repräsentativeren und akkurateren Eindruck davon, was in dem Asservat gespeichert, weil die ersten x% der aufgelisteten Dateien vielfältiger und repräsentativer für das gesamte Asservat sind, wenn sie in wirklich zufälliger Reihenfolge aufgelistet werden. Wenn Sie hingegen nach Name oder Pfad oder Größe oder Zeitstempeln o. ä. sortieren, sind viele der Dateien, die Sie sehen, wahrscheinlich in gewisser Weise ähnlich (von derselben Anwendung erzeugt oder vom Betriebssystem, vom selben Benutzer, für ähnliche Zwecke, erzeugt oder kopiert oder empfangen ungefähr zur selben Zeit, selber Dateityp, ...), so dass Sie mit etwas Pech nur irrelevante Dateien sehen, auch wenn es eine gleich große Gruppe von relevanten Dateien gibt. Bedenken Sie, wenn Sie im Verzeichnis-Browser gar nicht sortieren lassen, ist die Ansicht ebenfalls verzerrt, weil Sie die Dateien in der Reihenfolge sehen, wie sie vom Datei-Überblick referenziert werden, was ungefähr die Reihenfolge ist, in der die Dateien vom Dateisystem referenziert werden, also nicht zufällig.

Das Sortieren nach Hash-Werten kann mit einem beliebigen Filter kombiniert werden, z. B. um nur Bilder, die größer als 1 MB sind, in zufälliger Reihenfolge zu sehen, oder nur Dateien eines bestimmten Benutzers. Pseudo-Hashes sind nicht garantiert eindeutig. Es ist nicht mal sicher, dass sie gleich bleiben, wenn Sie ein Asservat schließen und wieder öffnen.

Welcher von potenziell zwei Hash-Werten pro Datei im Datei-Überblick in der Hash-Spalte angezeigt wird, kann in dem Dialogfenster mit den Verzeichnis-Browser-Optionen geändert werden. Entweder wird der erste Hash-Wert oder der zweite oder beide zu gleichen Zeit angezeigt (letzteres, wenn das Kontrollkästchen dafür halb angekreuzt ist). Der Hash-Spalten-Filter wird auf den Hash-Wert oder die Hash-Werte angewandt, die zu der Zeit angezeigt werden. Welche(r) Hash-Typ(en) in der Hash-Spalte angezeigt werden, kann man im Spaltenkopf sehen.

Hash-Set [INV, FOR]
: Die Namen der Hash-Sets in der internen Hash-Datenbank, in denen der Hash-Wert der Datei gefunden wurde. Bis zu 64 Treffer werden aufgeführt. Filter verfügbar. The Hash Set column shows known matches for both internal hash databases simultaneously. The filter can be used to filter for selected hash sets of one of the databases at a time. The database to choose hash sets from can be selected in the filter dialog.

Kategorisierung [INV, FOR]
: Kann manuell gesetzt werden über das Kontextmenü des Verzeichnis-Browsers, oder automatisch mit Hilfe von X-Tensions, Metadaten in Datei-Containern, durch Abgleich mit Hash-Datenbanken sowie auf anderen Wegen. Wenn Sie Hash-Datenbanken einsetzen, hängt die Kategorisierung von der Kategorie des Hash-Sets ab, in dem der Hash-Wert einer Datei gefunden wird. Anfangs werden

	alle Dateien als unbekannt behandelt. Wenn sie bekannt sind, sind sie entweder "irrelevant", "beachtenswert", oder "nicht kategorisiert". Filter verfügbar. Hinweis für Benutzer mit zwei Hash-Datenbanken: Die Kategorisierungsspalte zeigt nur eine Kategorie. Wenn Sie den Hash-Wert einer Datei in verschiedenen Datenbanken verschiedenen Kategorien zuweisen, werden Sie beim Abgleich gewarnt, und Sie erhalten eine exakte Information darüber, welcher Hash-Wert in welchen Hash-Sets in welchen Hash-Datenbanken den Konflikt ausgelöst hat. Die Kategorisierung als "beachtenswert" erhält im Zweifelsfall Vorrang.
Vermerke [INV, FOR]	Die Bezeichnungen der Vermerke, mit denen Dateien oder Verzeichnissen versehen wurden. Filter verfügbar. Wenn das Elter einer Datei vom Benutzer Vermerke bekommen hat, wird das in dieser Spalte für das Unterobjekt ebenfalls angezeigt, in hellgrau und mit einem Pfeil, es sei denn, das Unterobjekt selbst hat auch Vermerke. Dies erinnert den Benutzer, dass die Elterndatei bereits begutachtet und auf irgendeine Weise kategorisiert wurde, was es ihm u. U. erspart, nochmal dorthin zu navigieren.
Kommentare [INV, FOR]	Der Freitextkommentar, mit dem eine Datei oder ein Verzeichnis vom Benutzer versehen wurde. Filter verfügbar.
Metadaten [INV, FOR]	Interne Datei-Metadaten können aus Dateien diverser Typen beim Erweitern des Datei-Überblicks extrahiert und in dieser Spalte dargestellt werden. Es handelt sich um eine Untermenge der umfangreicheren Metadaten, die im Details-Modus präsentiert werden, und sie eignet sich vor allem zum Filtern, Exportieren und für die Ausgabe im Bericht. Sie kann editiert werden mit einem Befehl im Kontextmenü des Verzeichnis-Browsers. Bitte beachten Sie, dass das oft in der Metadaten-Spalte vorkommende Wort "Generator-Signature" intern nicht wörtlich gespeichert ist und daher nicht von einer logischen Suche oder dem Filter gefunden wird.
Generator-signatur [FOR]	Die aus der Metadatenspalte bereits bekannte Generator-Signatur, sofern vorhanden, wird hier zusätzlich in einer eigenen Spalte präsentiert, so dass Sie danach sortieren und ggf. logische Zusammenhänge zwischen Dateien erkennen können.
Gerätetyp [INV, FOR]	Diese Spalte zeigt für manche JPEG-, PDF-, Video- oder PNG-Dateien an, von was für einer Art von Gerät die Datei erzeugt wurde. Das kann z. B. ein Scanner sein oder einer der folgenden Gerätetypen: DSLR (single-lens reflex), mirrorless camera, digital back, video camera (camcorder), point and shoot (compact) camera, smartphone, smartphone front (secondary) camera, mobile phone, webcam/IPCam, action cam, monitor camera, or tablet. "Printer" für eine JPEG-Datei bedeutet, dass das Bild speziell für Druckzwecke erstellt wurde. "Screen" kann ein Bildschirmfoto sein, das von einem Bildschirm aufgenommen wurde, oder auch ein Wallpaper-Bild, das allein für die Anzeige auf einem Bildschirm gedacht ist. Der Gerätetyp wird aus der Generator-Signatur abgeleitet. Das Filtern nach dem Gerätetyp kann z. B. nützlich sein, wenn Sie sich speziell für eher private Fotos interessieren (mit der Frontkamera aufgenommene Selfies) oder für eher professionelle Fotos (die mit einer Spiegelreflexkamera oder einer digitalen Kamerarückwand aufgenommen wurden).
Strukturtyp	Diese Spalte kann bei der Metadaten-Extraktion befüllt werden. Filter verfügbar.

[INV, FOR]

Relevanz [INV, FOR]

Generische Relevanz einer Datei. Kann bei der Metadaten-Extraktion berechnet werden. Die generische Relevanz gibt eine Prognose des zu erwartenden Erkenntnisgewinns (knowledge gain), den man erzielen kann, wenn man die betreffende Datei untersuchen würde. Dazu ist es möglich in FTC.txt für jeden Dateityp eine Basis-Relevanz von 0 bis 5 zu definieren. Zusätzlich kann in den Optionen der Metadaten-Extraktion eine Gewichtung über die Dateigröße im Bereich 0 bis 100% vorgenommen werden. Die Option "Gewichtung der Aktualität" gewichtet zusätzlich noch die Aktualität der Datei. Dieser Wert ist jedoch mit 0% voreingestellt, da die Relevanz sonst nicht mehr global vergleichbar wäre. Für Dateitypen, für die eine Generatorsignatur berechnet werden kann, ermöglicht diese eine zusätzliche Berechnung der generischen Relevanz. Für Bilder gibt es zusätzliche Algorithmen, mit denen die generische Relevanz berechnet wird. Insbesondere für die Formate JPEG und PNG werden universelle Facetten, die grundsätzlich für alle Bilder verfügbar sind verwendet und es erfolgt einen Abgleich mit einer Datenbank, die Daten zu über 39.000 Geräten besitzt und mit der u.a. die Geräteklasse und der Bearbeitungszustand eines Bildes bestimmt werden können. Wenn Metadaten entfernt wurden, kann keine Bewertung über die Gerätedatenbank erfolgen. In diesem Fall werden die universellen Facetten für die Bewertung herangezogen. Zu den Facetten, die bislang verwendet werden, gehören:

1. der Dateiname (z.B. ob ein sog. "friendly name" verwendet wird oder eine bekannte Namenskonvention)
2. die Bittiefe in Bits per Pixel, die auch als tonale Auflösung (tonal resolution) oder als dynamic range bezeichnet wird
3. die Kompressionsqualität mit einem Wert zwischen 0 und 100, aus dem sich der Verarbeitungsgrad des Bildes einschätzen läßt. 0 bedeutet stark bearbeitet und 100 nahe am Originalzustand. Dazu wird eine emirische gewonnene Korellation zwischen Bildgröße in Pixel und der Bittiefe benutzt. Damit wird eine empirische Kompressionsqualität bestimmt, die das Optimierungspotential eines Bildes bestimmt. Bei einer Relevanz von 3.5 bei JPEG-Bildern ist ein Kompressionsoptimum erreicht. Für JPEG-Bilder, die nahe am originalen Bearbeitungszustand sind liegt die Relevanz dagegen bei 4.5.
4. die Bildgröße in Pixeln. Für diese Facette wird ein Propensity-Score Algorithmus verwendet, der für jedes Bild aus der Pixeldimension die Wahrscheinlichkeit mit der Metadaten zu erwarten sind bestimmt und damit eine Einschätzung des Bearbeitungszustandes berechnet, der für die Berechnung der Relevanz verwendet wird. Originale Bilder versprechen einen höheren Erkenntnisgewinn, ebenso singuläre Bilder, von denen es keine weiteren Kopien gibt.
5. die Generatorsignatur als ein herkunftsbasiertes Kriterium. Die Generatorsignatur ist eng verknüpft mit dem Bearbeitungszustand eines Bildes.
6. die Softwareklasse. Die höchste Bewertung hat der Wert "Firmware". Dieser wird als nahe am Originalzustand bewertet. Die schlechteste Bewertung hat der Wert "Unspecified". Hier wird davon ausgegangen, daß dieses Bild nicht als Dokument anzusehen
ist.

7. die Einhaltung der Normen für Formate insbesondere die Compliance mit den EXIF-Normen.
Die grundlegende Idee ist, wenn die Zeit für die Untersuchung begrenzt ist, man mit den Dateien mit der höchsten generischen Relevanz anfangen sollte, um die Chance zu maximieren, das, wonach man sucht, zu finden, sofern es existiert, und zwar möglichst rasch. Dazu können Sie nach der Relevanzspalte sortieren.

Metadata, Comments, and Event Description filters support the use of up to 4 expressions, which can be flexibly combined with AND and OR. The last combination always has priority. For example "A and B or C" is interpreted as "A and (B or C)". "A or B and C" is interpreted as "A or (B and C)". The expressions may start with a colon to indicate NOT at the expression level.

Zusätzliche Spalten für Suchtrefferlisten [INV, FOR]: Physischer/absoluter Offset, logischer/relativer Offset, Beschreibung der Art des Suchtreffers (Codepage/Unicode, ob in decodiertem Text, ob im Schlupf gefunden), Suchtreffer mit Kontextvorschau. Wenn der logische/relative Offset in grau angezeigt wird, dann ist es kein Offset in der betreffenden Datei, sondern in deren decodiertem Text.

Zusätzliche Spalten für Ereignislisten [INV, FOR]: Zeitstempel, Ereignistyp, Ereigniskategorie, Beschreibung.

Noch ein paar Tipps: Ein einziger Rechtsklick auf einen Spalten-Kopf im Verzeichnis-Browser schaltet einen Filter auf die schnellstmögliche Weise ein oder aus, ohne das Dialogfenster mit den Filtereinstellungen zu zeigen. Sie erhaltene eine textuelle Übersicht über alle gegenwärtig aktiven Filter mitsamt ihren Einstellungen (sofern über Dialogfenster definiert), indem Sie das blaue Trichtersymbol am linken oder rechten Ende der Überschriftszeile des Verzeichnis-Browsers mit der rechten Maustaste anklicken. You can sort by a column not only by clicking the header, but also through the dialog window that appears when pressing Ctrl+H. That window also allows you to activate and deactivate filters purely using the keyboard.

3.3.5 Mehr über Zeitstempel-Spalten

Die mit einer hochgestellten 2 bezeichneten Zeitstempelspalten enthalten alternative Zeitstempel [SPE, LAB, INV, FOR]. Im Fall von NTFS stammen diese Werte aus den 0x30-Attributen, und geben daher ggf. ehemalige Zeitstempel, die gültig waren, als eine Datei zuletzt umbenannt oder verschoben wurde, oder von vor einer etwaigen Rückdatierung. Rückdatierungen werden oft von Setup-Programmen und auch Windows selbst vorgenommen (der berüchtigte Erzeugungs-Zeitstempel-Tunnel-Effekt, s. http://support.microsoft.com/kb/172190), und natürlich von normalen Anwendungsprogrammen sowie von Benutzern zu diversen legitimen oder auch weniger hehren Zwecken. Beachten Sie, dass diese Spalten nur dann befüllt werden, wenn die zuvor gültigen Zeitstempel sich tatsächlich von ihren aktuellen Entsprechungen unterscheiden, und zusätzlich Änderung² und Record-Änderung² nur dann, wenn sie sich von Erzeugung² unterscheiden, damit der Bildschirm nicht unnötig mit redundanten Informationen überfrachtet wird. Das bedeutet, dass alle ²-Zeitstempel, die Sie sehen, tatsächlich zusätzliche Informationen enthalten und nicht einfach Duplikate sind.

Die Spalte Erzeugung² kommt auch für HFS+-Dateisysteme zum Einsatz, zur Anzeige der relativ neuen "Hinzugefügt"-Zeitstempel von Mac OS X Lion und neuer sowie iOS, sofern verfügbar und sofern sie sich tatsächlich von regulären Erzeugungsdatum unterscheiden. Diese Zeitstempel geben an, wann eine Datei zu dem bestimmten Verzeichnis, in dem sie enthalten sind, hinzugefügt wurden, auch wenn sie ursprünglich eher erzeugt wurden.

Für E-Mails gilt Folgendes: Die Zeitangabe in der "Date:"-Zeile im Header einer aus einem E-Mail-Archiv extrahierten E-Mail (wenn begleitet von einer Zeitzonenanzeige wie -0700 oder +0200) wird als Erzeugungsdatum und -zeit ausgegeben, sowohl für die Nachricht selbst als auch für etwaige Datei-Anhänge. Die Zeitangabe in der Zeile "Delivery-Date:" (oder falls nicht vorhanden in der ersten "Received:"-Zeile) wird als Datum und Uhrzeit der letzten Änderung angezeigt. E-Mail-Anhänge zeigen in den Spalten Erzeugung und Änderung einfach dieselben Zeitstempel wie die E-Mails, zu denen sie gehören, so dass Sie ihnen direkt ansehen, wann sie verschickt und zugestellt wurden, ohne zum Elternobjekt navigieren zu müssen. The record changed timestamp tells you when data in the data structure about the e-mail message in the OST file has changed, for example for a sent e-mail message when the user clicked the Send button or for a received e-mail message when it was delivered to the e-mail client or generally when a message was copied to another PST/OST archive.

Der kombinierte Filter für alle Zeitstempel-Spalten erlaubt das Filtern nach bestimmten Datumsbereichen (typische Anwendung) oder nach bloßen Uhrzeiten, an jedem beliebigen Datum. Wenn Sie z. B. interessiert sind an ungewöhnlicher Aktivität, die mitten in der Nacht auftrat, wenn der rechtmäßige Computerbenutzer nicht arbeitet, könnten Sie Zeiten wie 22:00:00 bis 05:59:59 filtern. Die Auswahl der richtigen Ortszeit für die Zeitstempel-Filter ist dabei offensichtlich von entscheidender Bedeutung.

Es gibt zwei verschiedene Arten von UND-Verknüpfungen für Zeitstempel-Filter. Eine strenge UND-Kombination (wenn voll gewählt) erfordert, dass alle gewählten Zeitstempel-Typen tatsächlich vorhanden/verfügbar sind und sie alle die Bedingungen erfüllen. Eine weiche UND-Kombination (halb gewählt) erfordert nur, dass die jeweils verfügbaren Zeitstempel die Filterbedingung erfüllen (und dass es wenigstens einen solchen Zeitstempel gibt). Hintergrund ist, dass nicht von allen Dateien alle Arten von Zeitstempeln bekannt sind.

Der Zeitstempel-Filter erlaubt es, sich auf NTFS-0x10-Zeitstempel zu konzentrieren, die eklatant rückdatiert aussehen im Vergleich zu ihren 0x30-Gegenstücken, und außerdem auf Erzeugungszeitstempel aus dem Dateisystem, die zeitlich vor der Erzeugung des Inhalts laut internen Datei-Metadaten liegen. Sie können einen Schwellwert in Millisekunden, Sekunden, Minuten, Stunden, Tagen, Wochen, Monaten oder Jahren angeben, der solche Zeitstempel-Diskrepanzen für Sie relevant macht, d. h. Sie können zur Bedingung machen, dass der Haupt-Erzeugungszeitstempel soviel älter ist als der entsprechende 0x30-Zeitstempel oder als der Zeitstempel der Erzeugung des Inhalts, wie Sie es einstellen. Wenn Sie einen UTC-basierenden Erzeugungszeitstempel aus dem Dateisystem vergleichen mit der Erzeugung des Inhalts laut internen Metadaten, die in einer unbekannten Ortszeit gespeichert ist (z. B. in PNG-Dateien), können Sie dabei berücksichtigen, wieviel Stunden Zeitdifferenz allein schon aufgrund dieses Basiseffekts zu erwarten sind. Um Sie zu unterstützen, werden UTC-basierende Erzeugungszeitstempel mit Ortszeiten vergleichbar gemacht, indem sie in die aktuelle Anzeige-Zeitzone umgerechnet werden. Bitte beachten Sie, dass Rückdatierungen meist automatisch erfolgen, aus diversen Gründen (z. B. beim Entpacken von Dateiarchiven zur Wiederherstellung

ursprünglicher Zeitstempel oder beim Installieren von Anwendungen durch Setup-Programme), und nicht notwendigerweise das Ergebnis eines Eingriffs durch einen Beschuldigten oder von Malware mit bösartigen Absichten sind. Wenn Sie an potentiellen manuellen Eingriffen interessiert sind, könnte es nützlich sein, zugleich einen Dateitypfilter einzusetzen, und genau die Dateitypen auf Rückdatierungen zu prüfen, bei denen es in Ihrem Fall wirklich einen Unterschied machen würde, z. B. Dokumente.

Alle 0x10-Zeitstempel von NTFS werden in ihren Zellen mit einem Rückdatierungssymbol (Icon) versehen, wenn sie älter sind als ihre entsprechenden 0x30-Gegenstücke (die Spalten mit der hochgestellten 2 im Kopf), und zwar soviel älter, dass der im Zeitstempel-Filterdialog eingestellte Schwellwert überschritten wird. Zellen mit Erzeugungszeitstempeln haben solch ein Symbol auch dann, wenn sie älter sind als der Zeitstempel der Erzeugung des Inhalts, wenn ein solcher in den internen Metadaten der Datei vorhanden war und extrahiert wurde. Die Differenz zwischen den beiden verglichenen Zeitstempeln wird rechts von dem Symbol angezeigt, gerundet auf Millisekunden, Sekunden, Minuten, Stunden, Tage, Wochen, Monat oder Jahre.

Bitte beachten Sie, dass Zeitstempel in FAT-Partitionen standardmäßig in Original-Ortszeit angezeigt und nicht umgerechnet werden, wenn Sie nicht in den Eigenschaften eines Asservats mit einem FAT-Dateisystem die vermutete Originalzeitzone auswählen, so dass die Zeitstempel für Anzeigezwecke in eine ggf. abweichende gewünschte Anzeigezeitzone konvertiert werden können. Für alle anderen Dateisysteme wird nach dem Zeitzonen-Konzept verfahren.

Zeitstempel im normalen Verzeichnis-Browser, die die Filterbedingung erfüllen, werden farblich hervorgehoben. In einer Ereignisliste werden Zeitstempel hervorgehoben, die mit dem Ereigniszeitstempel identisch sind.

Der unterstützte Bereich von Zeitstempeln ist 5. Mai 1829 bis 14. May 2514. Über- und Unterschreitungen werden in Form eines Vermerks „außerhalb der Grenzen“ angezeigt und können voneinander unterschieden und korrekt sortiert und gefiltert werden.

When sorting timestamps in one of the many timestamp columns, it may happen that UTC-based time stamps have to be compared to local timestamps with an undefined time zone reference or local timestamps with a user-defined time zone reference (user-defined meaning defined by the examiner), to see which one is earlier and which one is later. That happens for example for file system based timestamps in the case root window if one evidence object has an NTFS file system and the other a FAT file system. It also happens within the same evidence object for example when sorting internal creation timestamps retrieved from file contents, such as ordinary Exif timestamps in JPEG (which are local) and GPS timestamps in JPEG (which are stored in UTC). Sorting all such timestamps takes into account how these timestamps are displayed (in original local time or in a user-defined display time zone) such that the order is consistent with the displayed values, and not with how the timestamps are internally stored. That means for example that the local Exif timestamp 2017-01-01 14:01 LT is sorted after a UTC GPS timestamp 2017-01-01 14:00 +2, which is right if the undefined local time zone is equal to the display time zone, which in this example is UTC +2. That order of course can be wrong, as the unknown time zone of a local Content created timestamp could be somewhere to east of UTC +2. The order could also be wrong if the user-defined time zone reference of timestamps from a FAT file system is wrong.

3.3.6 FlexFilter

Zwei sogenannte FlexFilter sind in WinHex Lab Edition, X-Ways Investigator und X-Ways Forensics verfügbar, im Dialogfenster mit den Optionen des Verzeichnis-Browser. Sie können sich auf jede gewünschte Spalte im normalen Verzeichnis-Browser beziehen (d. h. nicht auf die besonderen Spalten von Suchtrefferlisten und Ereignislisten), mit einer beliebigen Anzahl von Teilwörtern, und sie können mit einem logischen ODER oder einem logischen UND miteinander verknüpft werden.

Z. B. sind diese Filter nützlich, wenn Sie sich auf Dateien konzentrieren möchten, die nicht innerhalb eines bestimmten zusammenhängenden Zeitraums erzeugt oder verändert wurden, sondern allgemein an bestimmten Wochentagen oder Wochenenden, d. h. in deren Zeitstempelspalten mit Notation im Langformat sich die Wörter "Samstag" oder "Sonntag" finden. Auch dann nützlich, wenn die jeweiligen spaltenspezifischen Filter Ihnen nicht so viele Möglichkeiten geben, wie Sie brauchen (z. B. für Autor, Absender und Empfänger können Sie derzeit nur einen Namen oder eine Adresse oder ein Teilwort angeben, und mit dem Beschreibungsfilter können Sie derzeit nicht auf jene zusätzlichen Hardlinks abzielen, die von bestimmten Operationen ausgenommen werden).

Die Farbe, die anzeigt, dass ein FlexFilter aktiv ist, ist violett statt blau, so dass er leichter von einem normalen spaltenbasierten Filter unterschieden werden kann. Beide FlexFilter haben eine NICHT-Option, und sie können sogar beide auf dieselbe Spalte abzielen, so dass Sie Ergebnisse erreichen können wie "zeige mir alle E-Mails mit dem Namen "Matthias" im Absenderfeld, in denen das Absenderfeld nicht den Domain-Namen "firma.de" enthält.

3.4 Modus-Schalter

Beim Untersuchen eines logischen Laufwerks, einer Partition oder einer Image-Datei mit einem Dateisystem, das von WinHex unterstützt wird, gibt es mehrere Schalter, die die Anzeige in der unteren Hälfte des Fensters (unter dem Verzeichnis-Browser) bestimmen. Erfordert eine forensische Lizenz.

Disk/Partition/Volume/Container

Ehem. „Sektoren“ genannt, zeigt diese Standard-Ansicht die binären Daten in allen Sektoren der vom aktiven Datenfenster repräsentierten Platte/Partition bzw. des Volumes/Container als Hexadezimal-Code, als Text oder als beides. Offsets und Sektornummern beziehen sich auf den Anfang der jeweiligen Platte/Partition bzw. des Volume/Containers.

Datei

Sieht dem Modus Disk/Partition/Volume/Container ähnlich, zeigt aber nur die Cluster an, die der Datei oder dem Verzeichnis zugeordnet sind, die bzw. das aktuell im Verzeichnis-Browser ausgewählt ist, in der Reihenfolge wie von der Datei verwendet, defragmentiert falls fragmentiert, dekomprimiert falls komprimiert, mit Offsets relativ zum Anfang der Datei. Wenn

Sie vom Datei-Modus in den Modus Partition/Volume wechseln, bringt Sie X-Ways Forensics automatisch an den Offset aus der Sicht der Partition/des Volumes, der dem Offset in der Datei entspricht, an dem der Cursor zuletzt positioniert war, auch wenn die Datei fragmentiert ist, wenn es einen entsprechenden Offset gibt (was nicht der Fall ist, wenn die Datei eine komprimierte oder virtuell angehängte Datei ist oder eine extrahierte E-Mail oder ein exportiertes Video-Einzelbild o. ä.).

Raw submode is available for NTFS-compressed and WofCompressed files in File mode to see the complete compressed data with slack. (The List Clusters command lists all clusters of such files including the slack as well. The slack area of the WofCompressed data is highlighted also in Partition/Volume mode.)

Vorschau

Prüft den Typ der aktuell im Verzeichnis-Browser ausgewählten Datei und zeigt die Datei mit Hilfe der separaten Viewer-Komponente an, es sei denn, die Viewer-Komponente ist nicht aktiv oder es handelt sich um ein Bild (unterstützte Typen s. Galerie) und die Viewer-Komponente soll nicht für Bilder verwendet werden. Selbst unvollständige Bilder (Datei z. B. wegen Fragmentierung nur partiell korrekt gerettet) können normalerweise teilweise angezeigt werden. Wenn die Viewer-Komponente nicht aktiv ist und es sich nicht um ein Bild in einem der unterstützten Formate handelt, wird ein rudimentäres ASCII-Text-Extrakt vom Anfang der Datei angezeigt.

Wenn Bilder im Vorschau-Modus von der internen Grafikanzeigebibliothek angezeigt werden, nicht von der separaten Viewer-Komponente, dann können sie 90°-Schritten gedreht werden, durch Klick mit der linken Maustaste nach links und mit der rechten Maustaste nach rechts. Fotos, die von Smartphones und Digitalkameras bestimmter großer Hersteller im Hochformat aufgenommen wurden, werden dennoch im Querformat gespeichert und müssen entweder nach links oder rechts gedreht werden, damit sie korrekt ausgerichtet sind. Der Vorschaumodus mit der internen Grafikanzeigebibliothek erledigt dies automatisch.

Ein Klick mit der mittleren Maustaste im Vorschaumodus auf ein von der internen Grafikbibliothek dargestelltes Bild spiegelt dieses Bild (d. h. vertauscht links und rechts) oder (wenn der Umschalttaste dabei gedrückt ist) kehrt das Bild um (d. h. vertausch oben und unten). Bitte beachten Sie, dass diese Operation zusätzlich zu einer etwaigen aktiven Drehung angewandt wird. Die aktuell aktive Drehung und die aktuell aktive Spiegelung werden in Form von einigen Symbolen in der oberen rechten Ecke angedeutet. Wenn keine Spiegelung angewandt wird, aber eine Drehung, zeigen die Buchstaben "UR" an, was in den Originalgrafikdaten die untere rechte Ecke war.

Sie haben die Möglichkeit, die Darstellung von Vorschau- und Details-Modus für dieselbe Dateien gleichzeitig zu sehen, indem Sie das "+" auf dem Details-Schalter anklicken während Sie sich im Vorschau-Modus befinden. Sie können danach den Details- oder Vorschau-Schalter erneut anklicken, um den betreffenden Modus wieder zum einzigen aktiven Modus zu machen.

Details

Enthält all die Informationen über eine einzige ausgewählte Datei aus allen Verzeichnis-Browser-

Spalten, inclusive denen, die gar nicht sichtbar sind. Sehr nützlich z. B., wenn der Pfad sehr lang ist und nicht in die Pfad-Spalte passt, u. U. sogar nicht einmal in Form der Tooltip-Anzeige in der Pfad-Spalte. Die ungefähre vorherige Rollposition im Details-Modus wird wiederhergestellt, wenn Sie im Verzeichnis-Browser eine andere Dateien auswählen oder wenn Sie das Datenfenster oder die gesamte Applikation schließen und erneut öffnen. Ein Klick auf das Diskettensymbol in der Statusleiste erlaubt es, den Inhalt des Details-Modus in eine HTML-Datei zu speichern.

Der Details-Modus zeigt außerdem die in einem NTFS-Dateisystem hinterlegten Zugriffsrechte an (gespeichert in Access Control Lists, ACLs). Jedes einzelne Recht hat typischerweise die Eigenschaft „Grant“ (=erlauben) oder „Deny“ (=verbieten). Zusätzlich hat es eine SID zugeordnet, für die dieses Recht gilt. Wann immer möglich, wird die SID in einen benutzerfreundlichen Namen übersetzt. Ein Recht gehört einer von vier Kategorien an: R = Read, Leseberechtigung; C = Change, Änderungsberechtigung; Full Access = Vollzugriff; Special Access = in diesem Fall werden die individuellen Rechte einzeln aufgeführt. Für jedes einzelne Zugriffsrecht sind zwei „Inheritance-Flags“ möglich: container inherit (CI), object inherit (OI) oder zwei „Propagation-Flags“: inherit only (IO), no-propagate inherit (NP)., Den Abschluss der Liste bildet gewöhnlich die Gruppenzugehörigkeit.

Der Details-Modus extrahiert auch die wesentlichen internen Metadaten aus OLE2-Compound-Dateien (z. B. MS-Office-Dokumenten vor Version 2007), MS Office 2007 XML, OpenOffice XML, StarOffice XML, HTML, MS Access, MDI, PDF, RTF, WRI, AOL PFC, ASF, WMV, WMA, MOV, AVI, WAV, MP4, 3GP, M4V, M4A, JPEG, BMP, EXE/DLL, JIDX (Java applet cache), THM, TIFF, GIF, PNG, GZ, ZIP, PF, IE Cookies, DMP Speicher-Dumps, hiberfil.sys, PNF, SHD & SPL Drucker-Spool, RecentFilecache.bcf, WIM Vista Image-Dateien, PhotoShop PSD, INDD (Adobe InDesign), DocumentSummary alternativen Datenströmen, tracking.log, .mdb MS Access database, manifest.mbdx/mbdb iPhone backup, IconCache.db u. v. a. m. Für MS-Office-Dokuments sehen Sie oft viele weitere Zeitstempel (z. B. wann zuletzt gedruckt), Thema, Autor, Organisation, Schlüsselwörter, Gesamtbearbeitungszeit u. v. a. m. Im Untermodus "IM", den Sie durch Klick auf den IM-Schalter aktivieren können, sehen Sie nur die internen Metadaten. Das macht es effizienter, viele Dateien auf ihre internen Metadaten hin zu prüfen, ohne mit der Maus nach unten rollen zu müssen. Insbes. ist dies nützlich für die Bildforensik, um Exif-Daten schnell zu begutachten. Auf den meisten Systemen kann man zwischen einem einspaltigen und einem zweispalten IM-Modus hin- und herschalten, wenn man die internen Metadaten von JPEG-Dateien abruft. Bei ausreichend hoher Bildschirmauflösung und Fensterbreite ist im zweispaltigen Modus kein vertikales Rollen erforderlich, d. h. man hat die gesamten internen Metadaten auf einen Blick vor sich, weil die Summary-Tabelle auf der rechten Seite zu sehen ist.

Für JPEG-Dateien gibt es ganz unten eine zusätzliche Tabelle. Diese Tabelle enthält die Generatorsignatur sowie wie die Verfassung („condition“) der Datei. Diese kann entweder „incomplete“ sein (wenn die Datei abgeschnitten wurde), „trailing data“ (wenn überschüssige Daten hinter dem Ende der JPEG-Daten zu finden sind) oder „rotated“. The condition "embedded" identifies pictures that were not generated as stand-alone files, but embedded in larger files, as thumbnails or reduced resolution alternates. That condition may also occur if JPEG metadata was retroactively removed with a tool. The condition "cropped" means that the dimensions of the picture in pixels are not known to be one of the standard dimensions of the generating device. That also means that the picture is not even considered to be potentially "relatively original", and

its relevance will be reduced compared to pictures that are considered "relatively original". The dimension will be displayed in blue in such a case.

The amount of slack (zero-value bytes) at the end of an EXIF segment is presented in Details mode if such slack is present. For example, iPhone 4 and iPhone 5 usually produce such an area of a variable length, but iPhone 7 does not. If the slack remains present after a rotation, that means the rotation was minimally invasive, without recompression (no loss of quality). If however a photo editing program rewrites the JPEG file, the slack will disappear.

The reported "size" of JPEG pictures has 1 or 2 values. Sizes that are not standard sizes with a common name (such as "XGA") are described as "thumbnail", "medium", "medium large", "large" or "big" based on the terminology established by Wordpress. If a generating device is identified, the field is named "sensor size" instead or - in the case of scanners - "paper size". Possible values for compression quality are very low, low, medium, and high. The compression quality is also quantified in a linear scale from 0 to 100. This number is not to be confused with the nominal/official JPEG quality, which does not take the actually achieved compression into account. The average number of bits per pixels in a JPEG picture is related to this and compared to the median value for that particular generator signature to put it into perspective.

The "processing state" depends on the detected generator, where each generator is now assigned to one of three generator classes D (device), E (editor), or C (content management system). JPEG files produced by generator class D are absolute originals. Their processing state is always "original". JPEG files produced by the generator class E are relative originals. Their processing state is always "Edited normally". Examples are photos published by news agencies like Reuters. The detected processing state of the third generator class (CMS like WordPress, Drupal, TYPO3, Joomla etc.) can assume different values. They are usually irregularly edited, i.e. their edited status is not officially indicated. The state can be deducted indirectly based on filename, generator signature, pixel dimension. The state "irregularly edited" can also result from picture manipulations. The state "EXIF stripped" refers to JPEG pictures, whose device origin was detected although no EXIF metadata is present. The device can potentially be detected based on generator signature, filename or a characteristic pixel dimension. The state "social media" is indicated separately because such pictures often have a higher intelligence value. Unlike news agency pictures they are rather semi-public in nature. The state "scaled" is new and refers to classical content management systems. It can be said with a high probability that such pictures have been released to the public. They were automatically and individually adapted to the respective output display in order to optimize the loading time of the web page. The state "minimized" is also new and indicates that the JPEG quality was reduced or that the file size was reduced by optimized recompression (jpeg-recompress, JPEGMini). The state "undefined" is a category for everything that remains. Such pictures are usually also the output of content management systems, those that do not identify themselves and whose format is not yet identified (which may change in future versions).

"EXIF compliance" is another aggregated single value, a score that allows to see whether a low quality photo editor was used to edit a photo. A good rating that JPEG pictures produced by Nikon or Canon cameras usually have is retained only by high quality photo editing programs. A bad rating for such pictures indicates editing by a low quality program. Irregularly coded fields in the EXIF data are marked with a star. Irregular might mean that a wrong data type was used or the permitted value range was violated or there are duplicate tags or a character string is not null-

terminated or contains slack. Some tags must not appear at the same time, some tags must be stored in a designated directory. Generally the EXIF presentation is not a simple unstructured output of all EXIF values, but it aims to provide background information and highlights certain parameters within their context to make examiners aware of irregularities. Already in their original files digital cameras produce characteric EXIF metadata errors. By editing a photo additional errors may be produced, or others may be fixed.

If the IFD GPS field in Exif metadata is available, but empty, or if it contains unvalid coordinates, this is an irregular situation, different from the IFD GPS not being present at all, and often means that the GPS data have been removed retroactively. It is reflected as "GPS format: NaN", where NaN means "not a number".

The DHT marker in JPEG files is evaluated. If the marker has the values as defined by the JPEG standard, it will be marked as "Standard", otherwise the number of table entries will be output. Practically all digital cameras use standard tables, but JPEGs encoded by social networks don't. They use optimized tables and achieve a file size reduction by around 5%.

Werte in den internen Metadaten von JPEG-Dateien, die keine Standardwerte/Voreinstellungen des jeweiligen Kamera-/Gerätemodells sind, sondern vom Benutzer vergeben oder von einem Bildbearbeitungsprogramm geändert wurden, oder einfach nicht für original/normal für das jeweilige Gerätemodell gehalten werden, werden in blauer Farbe hervorgehoben. If there is something unusual about the presence of GPS coordinates in JPEG files, those GPS coordinates are also highlighted in blue color. For example if the GPS coordinates are present and a GPS timestamp is absent, for a mobile device type that is known to always include both at the same time (sometimes depending on whether the front or back camera is used), or for a camera type that is known to not have GPS, it could mean that the coordinates have been retroactively embedded. GPS timestamps that are different from the time when the photo was taken are also highlighted in blue color. The GPS processing mode, if available, is listed in Details mode. This mode allows to estimate the reliability/precision of the coordinates. It is used by various manufacturers, and it can be one of the following values: unknown, GPS, Network, Hybrid, Fused, or CELLID. "Geolocation" shows the GPS coordinates in a notation as accepted by Google Maps, OpenStreetMap or Bing Maps. Three additional fields for Exif GPS data are output in Details mode where available: Altitude, Image direction, and GPS Error. Altitude might be helpful to judge the reliability of the geo coordinates. Image direction is a feature of high-end smartphones. For JPEG files created by many Samsung phones Details mode also shows firmware date and region, which can help to validate other metadata. The Summary part of the internal metadata of JPEG files has a field named "Light value". That value is derived from the well-known photography formula Ev=log2(N**2/t)+log2(100/ISO). The value range ends at around 16, which means full sunshine. This aggregated value can be interesting to some examiners because it allows to distinguish indoor and outdoor photos and because it allows to check whether the local time of a photo is plausible.

"Software class" aggregates various information and can be one of the following: Firmware, Adobe, PHP, Apple, Windows, Facebook/Instagram, Android, General, WordPress, Editor, Social Media, Google/Picasa, Scanner, WhatsApp, Video still, Website builder, Stock (for stock photos), Twitter, Amazon (for product photos from Amazon's shopping web site), Screenshot, Pinterest, Content, Camera, LinkedIn, Beautifier, Bing, MSN, Mastodon, and MS Office.

Ein weiterer Eintrag in der Summary-Tabelle ist der "Propensity score". Dieser kann Werte von 1 bis 99 annehmen. Die berechnete Relevanz basiert hauptsächlich auf diesem Wert. Der Wert gibt eine objektive statistische Wahrscheinlichkeit dafür an, dass ein Bild zusätzliche, entfernbare relevante Metadaten hat. Er könnte auch als Dokumentalität bezeichnet werden, also die Eigenschaft, als Dokument dienen zu können. Man kann diese zusätzliche Information auf ihre Konsistenz prüfen. Der "Propensity score" existiert generell für Rasterbilder (die in Pixeln abgemessen werden), insbes. auch für die Formate PNG und WEBP.

A processing state and other values (size, bits per pixel, filename analysis) are also output for PNG files. The same processing states as for JPEG are used, except "Irregularly edited" and "EXIF stripped" are not possible. The value "Original" is used only for screenshots, if they have passed a special test. A processing state is also presented for WEBP files, similar to PNG.

Diverse besondere Eigenschaften, die an Bilddateien festgestellt werden, werden im Details-Modus mit "Remark"-Nummern referenziert. Die Textdatei "Remarks.txt" im Installationsverzeichnis dokumentiert diese Nummern und bietet eine rudimentäre Erkärung.

Im Installationsverzeichnis finden Sie eine Datei namens „Phone Alias Table.txt“. Diese enthält Übersetzungen von internen Gerätebezeichnungen der Hersteller in menschenlesbare Marketingnamen, unter denen die Geräte tatsächlich bekannt sind. Insbes. Bezeichnungen von Samsung, Motorola, LG und Huawei muten eher kryptisch an und sind übersetzt besser verständlich. Diese Tabelle kann auch das Erscheinungsdatum und die Vertriebsregion einer Geräts enthalten. Ihr Format wird im Kopf der Datei erklärt, so dass Benutzer dabei helfen können, sie zu vervollständigen. Die Tabelle muss alphabetisch sortiert sein, weil das eine höhere Performanz erlaubt. Beachten Sie bitte, dass dies nur eine Hilfstabelle ist. Es bedarf entsprechender Einträge in „Generator Signatures.txt“ zur Erkennung und zur Kategorisierung in Geräteklassen.

The processing state "Original" of videos of the QuickTime format family is brought to your attention in Details mode, if applicable. However, this statement is not as strong as for JPEG pictures. The contents of such a video may have been changed in some irregular ways without a way of detecting it (e.g. exchange of individual frames). The statement refers to the format structure. Conventional editing tools practically always alter this structure, so "normal" editing will be detected.

Galerie

Prüft die Signatur aller Dateien im gegenwärtig sichtbaren Ausschnitt des Verzeichnis-Browsers, sofern das für diese Dateien im Datei-Überblick noch nicht erledigt wurde. Wenn eine Datei als Bild in einem unterstützten Format erkannt wird, wird eine Miniaturansicht angezeigt, sonst eine weiße Kachel mit dem Dateinamen, aber optional kann auch eine Miniaturansicht für solche Nicht-Bild-Dateien erzeugt werden (s. Optionen | Viewer-Programme). Indem Sie im Verzeichnis-Browser hoch- oder herunterrollen, bewegen Sie auch die Bilderliste im Galerie-Fenster. Sie können das Verzeichnis wechseln auch während die Miniaturansichten noch erzeugt werden. Durch Doppelklick auf eine Miniaturansicht erhalten Sie eine Ansicht des Bildes in voller Größe, wobei Sie mit den Tasten + und - hinein- und wieder herauszoomen können. Selbst unvollständige Bilder (Datei z. B. wegen Fragmentierung nur partiell korrekt gerettet) können normalerweise teilweise angezeigt werden. Die Galerie-Ansicht zeigt Dateien folgenden Typs an:

JPEG, PNG, GIF, TIFF, BMP, WEBP (nur das erste Bild, wenn animiert), HEIC, einige DICOM-Varianten, PSD, HDR, PSP, SGI, PCX, CUT, PNM/PBM/PGM/PPM, ICO. Die Galerie harmoniert nicht besonders gut mit Suchtrefferlisten.

Die Galerie kann jetzt in einem alternativen Modus operieren, der mit dem Schalter links vom Sync-Schalter aktiviert wird. In dem Modus stellt die Galerie nicht die aktuell im Verzeichnis-Browser aufgelisteten Dateien dar, sondern statt dessen die Unterobjekte eines einzigen gewählten Objekts, wenn es solche Unterobjekte gibt. Dies sind entweder nur direkte Unterobjekte oder (im ²-Modus) Unterobjekte rekursiv. Dies ist ein einzigartige Möglichkeit, um mit einem einzigen Mausklick einen schnellen Überblick über ganze Verzeichnisse oder Datei-Archive zu erhalten. Außerdem nützlich für Videos, von denen Sie zuvor Standbilder haben extrahieren lassen. Sie können jedes aufgelistete Unterobjekt mit der rechten Maustaste anklicken und diverse Operationen darauf anwenden. Die meisten aus dem Kontextmenü des Verzeichnis-Browsers bekannten Befehle sind verfügbar. Insbes. können Sie ein Unterobjekt auf diese Weise mit einem Vermerk versehen, ausblenden, markieren oder zu ihm im Verzeichnis-Browser navigieren, um die Metadaten in allen Spalten zu sehen (zurück zur vorherigen Ansicht geht es dann bekanntlich durch Klick auf den Zurück-Schalter). Die Unterobjekte werden in der Galerie in aufsteigender Reihenfolge ihrer internen ID aufgelistet. Die Auswahl der in Galerie spiegelt normalerweise exakt die Auswahl im Verzeichnis-Browser wieder. Bei der Darstellung der Unterobjekte einer gewählten Datei allerdings erlaubt die Galerie in sich selbst eine abweichende, separate Auswahl unter den Unterobjekten.

Wenn ein Einsehen-Fenster ein Bild darstellt (und wenn das Einsehen auf ein Bild zur gleichen Zeit beschränkt ist), wird dieses Einsehen-Fenster mit dem nächsten Bild aktualisiert, wenn Sie in der Galerie die Pfeiltasten benutzen. Insbesondere auf einem mehrere Monitore überspannenden Desktop nützlich, wenn das Einsehen-Fenster auf dem zweiten Monitor zentriert ist und die Galerie sich auf dem ersten Monitor befindet. Vermeidet, die Eingabe-Taste betätigen zu müssen, um das Bild einzusehen und dann eine weitere Taste, um das Einsehen-Fenster zu schließen und den Eingabefokus zurück auf die Galerie zu setzen.

Kalender

Gibt einen komfortablen visuellen Überblick über die Zeitstempel aller aufgelisteten Dateien und Verzeichnisse, aus allen 6 Zeitstempel-Spalten des Verzeichnis-Browsers, in Form eines Kalenders, bzw. bei Anzeige einer Ereignisliste einen ähnlichen Überblick über alle aufgelisteten Ereignis-Zeitstempel. Each day with at least one time stamp is marked in the calendar with a gray color. The more activity on a day, the darker the color. Weekends (Saturdays and Sundays) are specially marked with x. Hover the mouse over a day to find out how many timestamps exactly fall into that day. Left-click a day to select that day as the left boundary of the timestamp filter, or right-click it to define it as a right boundary. Middle-click a day to filter for timestamps on that particular day only. If the same file is listed more than once (which can happen in a search hit list if it contains more than 1 search hit), then its timestamps are also represented more than once in the calendar.

When not showing events, you can now decide which column's timestamp should be included in the calendar. Columns that are hidden (have a width of 0 pixels) are excluded, all other columns are included. The status bar reminds you which columns are included even if not currently visible because of horizontal scrolling.

Years in the calendar with no timestamps are grayed out. The number of a year is displayed in a darker shade of gray the more timestamps are listed for that. All shades of gray try to give the examiner a better and quicker impression of peaks or absence of activity.

Da die Anzahl der vom Kalender darstellbaren Jahre begrenzt ist, könnten kaputte Zeitstempel, die in der fernen Vergangenheit liegen, Sie der Möglichkeit berauben, die späteren Jahre, die Sie wirklich interessieren, zu sehen. wenn Sie keinen Filter setzen und Ereignisse mit Nonsense-Zeitstempeln nicht manuell löschen. Es lässt sich aber auch ein Mindestjahr einstellen, ab dem Zeitstempel vom Kalender dargestellt werden. Alle früheren Zeitstempel werden dann vom Kalender ignoriert, selbst wenn kein Filter aktiv ist. Standardmäßig ist das Mindestjahr das Jahr 2000. Um das zu ändern, klicken Sie die Jahreszahl des ersten angezeigten Jahres links im Kalendermodus an.

Beispiel: In welchem Zeitraum wurden die meisten JPEG-Dateien auf einer Partition verarbeitet? Klicken Sie mit der rechten Maustaste das Stammverzeichnis im Verzeichnisbaum (Falldatenfenster) an, um alle Dateien aus allen Unterverzeichnissen auf einmal (rekursiv) aufzulisten. Dann schränken Sie die Ansicht mit dem Dateityp-Filter auf JPEG-Dateien ein und schalten auf die Kalenderansicht um.

Roh

Im Vorschau-Modus sorgt der Roh-Modus bei Einsatz der Viewer-Komponente dafür, dass Nicht-Bild-Dateien als einfache Textdateien dargestellt werden. Dies kann nützlich sein z. B. bei HTML-Dateien, wenn Sie den HTML-Quellcode sehen möchten, oder bei .eml-Dateien, wenn Sie den vollständigen E-Mail-Header sehen möchten, oder generell wenn in einer Suchtrefferliste die Viewer-Komponente einen Suchtreffer nicht im Vorschau-Modus hervorheben kann (weil er etwas in den Metadaten oder im Steuercode enthalten ist, der im Roh-Modus sichtbar wäre, aber nicht im normalen Vorschau-Modus). Sie können den Roh-Modus dauerhaft einschalten, wenn Sie beim Aktivieren die Umschalt-Taste gedrückt halten.

File mode now offers a "raw" submode for NTFS-compressed files. In Raw mode you can actually see the compressed data as well as the sparse clusters, not the decompressed state of the file. This is useful for research or educational purposes and because theoretically small amounts of data could have been manually hidden in the not clearly defined, but implicitly existing slack area of each compression unit, which follows the compressed payload data.

VC

Der VC-Schalter ist sichtbar nur im Vorschau-Modus beim Einsehen von Bildern deren Typ von der internen Grafikanzeigebibliothek unterstützt wird. Standardmäßig wird diese internen Grafikanzeigebibliothek für die Vorschau und das Einsehen von Bildern verwendet. Wenn jedoch der VC-Schalter gedrückt ist, besorgt stattdessen die Viewer-Komponente die Darstellung (VC = viewer component), die auch für die Anzeige der Miniaturansichten in der Galerie verantwortlich ist.

Sync

Synchronisiert den Verzeichnis-Browser und den Verzeichnisbaum, so dass in einer rekursiven Ansicht das Auswählen einer Datei im Verzeichnis-Browser dazu führt, dass ihr Elternverzeichnis im Baum kenntlich gemacht wird. Der Sync-Modus bei nicht-rekursiver Erkundung hat eine ähnliche Wirkung wie die Option "Automatically expand to current folder" im Windows-Explorer. Das bedeutet, dass beim Navigieren von einem Verzeichnis zum anderen bei inaktivem Sync-Modus der Verzeichnisbaum links nicht mehr das aktuell erkundete Verzeichnis anzeigt und auch nicht bei Bedarf dessen Elternverzeichnis aufklappt. Ob der Sync-Modus aktiv ist oder nicht merkt sich das Programm getrennt für rekursive und nicht-rekursive Erkundung und für jedes Datenfenster einzeln.

Der Sync-Schalter im Asservatüberblicksfenster hat eine besondere Funktion. Das ist möglich, weil Verzeichnisnavigation in diesem Fenster ohnehin nicht möglich ist. Der Schalter steuert dann, ob das Wechseln von einem Datenfenster zum anderen, z. B. über die Registerleiste, das zugehörige Asservat bzw. dessen aktuell erkundetes Verzeichnis im Falldatenfenster hervorheben soll.

Erkundungsmodus

Schalter mit einem geschweiften türkisfarbenen Pfeil. Schaltet um zwischen normaler und rekursiver Erkundung. Beim rekursiven Erkunden sehen Sie nicht nur den Inhalt des aktuellen Verzeichnisses, sondern auch die Inhalte von all dessen Unterverzeichnisse, sowie deren Unterverzeichnissen usw. Um ein Verzeichnis rekursiv zu erkunden, können Sie es im Verzeichnisbaum auch rechts anklicken.

Unterstützung mehrerer Monitore

Es ist möglich die untere Hälfte des Datenfensters (mit dem Disk/Partitions/Volume-Modus, Datei-Modus, Vorschau, Galerie usw.) vom Datenfenster zu lösen, indem man die drei Punkte links von den Modus-Schaltern anklickt (2x). Dann kann diese Hälfte frei verschoben und in der Größe geändert werden. Bei Mehrmonitorsystemen ist es möglich, diesen Teil der Benutzeroberfläche auf einen anderen Bildschirm zu schieben und ihn dort sogar zu maximieren! Das Wiedereingliedern in das Hauptfenster geschieht durch erneutes Klicken auf die drei Punkte oder Klick auf den Minimieren-Schalter.

Beim ersten Klick auf die drei Punkte wird aus der unteren Hälfte des Datenfensters dessen rechte Hälfte. Das kann bei den heutzutage üblichen Breitbild-Monitoren von Nutzen sein, auf denen vertikaler Platz knapp ist, so dass Sie eine lange vertikale Liste von Dateien sichtbar haben können und gleichzeitig die volle Bildschirmhöhe auch für Vorschauen von seitenbasierten Dokumenten zur Verfügung haben, die zum Betrachten im Hochformat gedacht sind. Nützlich auch für die Galerie, und sehr effizient für Bilder im Hochformat, den Detailmodus sowie Hex-Editor-Anzeigen in den Modi Disk/Partition/Volume/Datei, die traditionellerweise in nur 16 Bytes pro Zeile unterteilt sind.

Ein Rechtsklick irgendwo außerhalb der Schalter in der Leiste mit den Modusschaltern zeigt oder versteckt nun die Trennlinie zwischen Verzeichnis-Browser und Schalterleiste. Wenn die Trennlinie sichtbar ist, kann sie mit dem Mauszeiger angesteuert und nach oben oder unten verschoben werden. Ungeachtet der Sichtbarkeit der Trennlinie kann man die Fensterunterteilung auch einfach nach einem Linksklick in der Leiste mit den Modusschaltern (außerhalb der

Schalter) bei gedrücktgehaltener Maustaste verschieben. Ohne die Trennlinie ist es etwas intuitiver, dass sich die rechte Hälfte der Leiste mit den Modusschaltern auf den Verzeichnis-Browser darüber bezieht und nur die linke Hälfte der Leiste auf die untere Hälfte des Datenfensters.

3.5 Statusleiste

Die Statusleiste zeigt beim Einsehen einer Datei folgende Informationen an:

1. Feld: aktuelle Seite und Anzahl der Seiten, auf denen die aktuelle Datei dargestellt wird
2. Feld: Cursorposition (Offset in der Datei)
3. Feld: ins Dezimalsystem übersetzte Hex-Werte an der Cursorposition
4. Feld: Blockanfang und -ende (falls festgelegt)
5. Feld: Größe des Blocks in Byte (dto.)

Durch einen Klick der linken Maustaste lässt sich...

- im 1. Feld eine andere Seite aufschlagen,
- im 2. Feld den Cursor zu einem bestimmten Offset bewegen,
- im 3. Feld das Format festlegen, in dem die Hex-Werte als Zahlen des Dezimalsystems interpretiert werden, und
- im 4. und 5. Feld den Block neu definieren.

Klicken Sie mit der rechten Maustaste, um in einem Feld der Statusleiste angezeigte Informationen in die Zwischenablage zu kopieren.

Durch einen Mausklick rechts im 2. Feld der Statusleiste können Sie von absoluter Offset-Darstellung (Standard) auf relative Datensatz-Offsets umschalten. Dies ist nützlich, wenn die von Ihnen im Hex-Editor untersuchten Daten aus gleich langen Datensätzen bestehen. Nachdem Sie deren Länge angegeben haben, wird Ihnen für die aktuelle Cursorposition anstelle des absoluten Offsets jeweils die Nummer des Datensatzes und der relative Offset darin angezeigt.

Ein Rechts-Klick auf das 3. Feld der Statusleiste erlaubt es außerdem, die vier Hex-Werte an der aktuellen Cursorposition in umgekehrter Reihenfolge in die Zwischenablage zu kopieren. Dies ist nützlich beim Verfolgen von Zeigern.

3.6 Daten-Dolmetscher

Der Daten-Dolmetscher ist ein kleines Fenster, das „Übersetzungsmöglichkeiten“ für die Daten an der aktuellen Cursorposition anbietet. Ob er angezeigt wird oder nicht, kann über das Anzeigen-Menü gesteuert werden, nicht über die Optionen des Daten-Dolmetschers. Manche Benutzer glauben, dass der Daten-Dolmetscher die Daten in einem ggf. definierten Block übersetzt. Das ist aber nicht der Fall. Was für ein Block definiert ist, ist völlig egal. Der Daten-Dolmetscher übersetzt immer die Daten von dem Byte an der aktuellen Cursorposition an. In den Optionen können Sie einstellen, welche Datentypen zu berücksichtigen sind. Zur Verfügung

stehen diverse ganzzahlige Datentypen (standardmäßig in dezimaler Schreibweise, optional hexadezimal oder oktal), die Bit-Darstellung eines Bytes, Worts oder Doppeltworts (Binär-Format), vier Gleitkomma-Datentypen, Assembler-Opcodes (Intel) und Datumstypen.

The Data Interpreter can interpret UNIX/C, Java/BlackBerry/Android and Mac Absolute timestamps stored as integer numbers in decimal ASCII text instead of in binary. You will find a context menu item for that as well as a checkbox in the options dialog. The Data Interpreter optionally translates timestamps of all formats except MS-DOS date & time to local time (the time zone defined in the General Options). You will find a context menu item for that as well as a checkbox in the option dialog.

Der Dolmetscher kann die meisten Datentypen auch rückwärts wieder in Hex-Werte übersetzen. Stellen Sie dazu sicher, dass Sie eine Datei im Editiermodus geöffnet haben, tragen Sie den gewünschten Wert ein und bestätigen Sie mit ENTER. Daraufhin schreibt der Daten-Dolmetscher die entsprechenden Hex-Werte an der aktuellen Position in das Editierfenster.

Mit einem Klick der rechten Maustaste können Sie ein Kontextmenü im Daten-Dolmetscher aufrufen und darin einstellen, ob die ganzzahligen und Gleitkomma-Datentypen im Little- oder Big-Endian-Format übersetzt werden sollen. Sie können auch zwischen dezimaler, oktaler und hexadezimaler Integer-Darstellung wählen. Dies und vieles mehr finden Sie auch im Dialogfenster mit den Daten-Dolmetscher-Optionen.

Die Zerlegung von GUIDs der Version 1 in Zeitstempel, Sequenznummer und MAC-Adresse im Daten-Dolmetscher und in Schablonen ist optional. In den Daten-Dolmetscher-Optionen können Sie die Zerlegung nun entweder wie bisher erzwingen (wenn ganz angekreuzt) oder sie verhindern (um immer die Standard-GUID-Notation in geschweiften Klammern zu sehen) oder die Zerlegung nur dann vornehmen zu lassen, wenn auch die Zeitstempel einigermaßen plausibel ist (wenn halb angekreuzt). Letzte Einstellung ist nützlich z. B. für Apple GPT-Werte, die vorgeben, GUIDs der Version 1 zu sein, aber tatsächlich verdrehten ASCII-Text statt gültige Zeitstempel enthalten.

Hinweise:

- Nicht alle Hex-Werte können in Gleitkomma-Zahlen übersetzt werden. Wenn eine Übersetzung nicht möglich ist, erscheint die Angabe NAN („**n**ot **a** **n**umber“) im Daten-Dolmetscher.
- Ebensowenig können alle Hex-Werte als Datumswerte jeden Typs übersetzt werden. Manche Datumstypen haben stark eingeschränkte gültige Wertebereiche.
- Redundanzen im Befehlssatz der Intel-Prozessoren schlagen sich in mehrfach vorkommenden Opcodes und mnemonischen Abkürzungen nieder. Floating-Point-Befehle werden im Daten-Dolmetscher nur als F*** angezeigt. Beschreibungen der den mnemonischen Abkürzungen entsprechenden Befehle können von Intel über das Internet bezogen werden. Das Dokument heißt „Intel Architecture Software Developer’s Manual Volume 2: Instruction Set Reference“ und liegt im PDF-Format vor.

3.7 Positions-Manager

In dem »Positions-Manager« genannten Fenster können unbegrenzt viele Datei- und Datenträger-Offsets mit Beschreibungen verwaltet werden. Diese werden Positionen genannt und dienen als Anmerkungen oder Lesezeichen. Er wird auch für Suchtreffer verwendet, wenn nicht mit einem Fall gearbeitet wird, ist aber *weitaus* weniger mächtig als eine Suchtrefferliste. Es ist leicht, zwischen mehreren Einträgen hin- und herzuspringen, indem Sie STRG+Links und STRG+Rechts drücken. Wenn Sie etwa in einer Datei eine markante Stelle ausfindig gemacht haben, auf die Sie evtl. später noch häufiger zurückkommen möchten, dann lohnt es sich, diese Stelle im Positions-Manager einzutragen. Sie können sie dann später schnell wiederfinden, ohne sie sich merken zu müssen. Klicken Sie auf „Neu“, geben Sie den Offset und anschließend eine Beschreibung (z. B. „Hier beginnt der Datenblock!“) ein. Beschreibungen dürfen bis zu 8192 Zeichen groß sein. Optional können alle Positionen, die im Positionsmanager verwaltet werden, im Datenfensterin einer von Ihnen festgelegten Farbe hervorgehoben werden und ihre Beschreibungen in gelben Tooltips dargestellt werden, wenn der Mauszeiger darüber bewegt wird. Sie können Positionen auch mit dem Kontextmenü des Datenfensters hinzufügen oder editieren, oder auch indem Sie im Datenfenster die mittlere Maustaste betätigen.

Klicken Sie die rechte Maustaste im Positions-Manager, um ein Kontextmenü zu erzeugen. Darin können Sie Positionen löschen, aus einer Datei laden oder in eine Datei speichern (letzteres auch als HTML). Wenn die Einträge des *allgemeinen* Positions-Managers geändert wurden, werden sie nach dem Beenden von WinHex grundsätzlich in der Datei *WinHex.pos* im WinHex-Verzeichnis gespeichert und für den nächsten Programmstart aufbewahrt. Nur Suchtreffer darin werden nicht permanent gespeichert, es sei denn, sie wurden per Kontextmenü bearbeitet.

There is the *general* Position Manager, which stores positions that are applied to *all* data windows, and there is the Position Manager for each evidence object in a case, which stores positions that were defined for that particular evidence object and that are applied only to that evidence object's data window. The former is invoked through the main menu (Navigation | Position Manager), the latter by clicking the right-most button in the middle of the screen when an evidence object is open, with crosshairs on it. That may explain it if you cannot find the positions that you have defined previously. Near the top of the data window it says *which* Position Manager you are currently looking at if the Position Manager is active.

Search hits in the general Position Manager are by default deleted as soon as the general Position Manager is closed, to avoid confusion as positions in the general Position Manager have no reference to a particular file or disk and are intentionally applied to whatever data source is active when invoked. If you wish to keep search hits, please change the corresponding option in the general Position Manager's context menu.

Das POS-Dateiformat ist unter http://www.x-ways.net/winhex/ vollständig dokumentiert.

3.8 Arbeitserleichterungen

- Menübefehle, die sich auf individuelle, *ausgewählte* Objekte im Verzeichnis-Browser oder einer Suchtrefferliste oder eine Lesezeichenliste beziehen, können in dem Kontextmenü gefunden werden, das erscheint, wenn man diese Objekte mit der rechten Maustaste anklickt. Sie finden solche Befehle nicht im Hauptmenü.
- Linke Maustaste..... Blockanfang festlegen (Doppelklick)
- Rechte Maustaste..... Blockende festlegen
- Rechte Maustaste..... Blockmarkierung aufheben (Doppelklick)
- UMSCH+Pfeiltasten ..... Block markieren
- ALT+1 ..... Blockanfang setzen
- ALT+2 ..... Blockende setzen
- Tabulatortaste ..... zwischen Text- und Hexmodus umschalten
- Einfg-Taste ..... zwischen Überschreib- und Einfüge-Modus umschalten
- ENTER ..... Start-Center aufrufen
- ESC ..... aktuellen Vorgang abbrechen, Blockauswahl aufheben, Dialogfenster oder Schablone verlassen
- PAUSE..... aktuellen Vorgang anhalten bzw. Fortsetzen
- STRG+S ..... speichert den aktuellen Fall, sofern nicht schreibgeschützt geöffnet
- F11 ..... „Offset aufsuchen“ wiederholen (mit STRG = von aktueller Position in umgekehrter Richtung)
- ALT++ ist eine Variante des Befehls „Offset aufsuchen“ speziell um eine bestimmte Zahl von Sektoren *abwärts* zu springen.
- ALT+- ist eine weitere Variante speziell um eine bestimmte Zahl von Sektoren *aufwärts* zu springen.
- UMSCH+F7..... Zeichensatz wechseln
- (UMSCH+)ALT+F11 ..... „Block verschieben“ wiederholen
- STRG+UMSCH+M..... Anmerkungen eines offenen Asservats aufrufen
- ALT+F2..... Auto-Hash (Prüfsumme oder Digest) neu berechnen
- STRG+F9 ..... Menü des Zugriffs-Schalters öffnen (bei Datenträgern)

- Pressing Ctrl+C in the directory browser now copies the textual data of the selected items into the clipboard, with the same notation as in the directory browser itself, otherwise similar to the Export List command.

- ALT+LINKS und ALT+RECHTS erlauben das Wechseln zwischen Datensätzen innerhalb einer Schablone (wie die Schalter „<“ und „>“). ALT+POS1 und ALT+ENDE wechseln zum ersten bzw. letzten Datensatz.

- ALT+G bewegt den Cursor im Editierfenster zur aktuellen Position in einer Schablone und schließt die Schablone.

- WinHex kann Dateien öffnen, die per Drag & Drop (mit der Maus) in das Programmfenster gezogen werden. Aber Windows verhindert Drag & Drop, wenn die Zielanwendung als Administrator ausgeführt wurde und die Quellanwendung nicht.

- Der Einsatz von Scripts kann Ihr Arbeiten mit WinHex effizienter machen.

- Als Befehlszeilenparameter wird auch der Name eines Scripts akzeptiert (s. dort).

- „Ungültige Eingabe”: Nach dem Schließen einer solchen Fehlermeldung zeigt das Blinken eines Steuerelements im darunterliegenden Dialogfenster an, welcher Wert ungültig ist und korrigiert werden muss.

- Die Offset-Schreibweise (dezimal oder hexadezimal) lässt sich durch einen Mausklick auf die Offsetdarstellung im Editorfenster umstellen. Die dezimale Schreibweise ist mit oder ohne führende Nullen verfügbar (Mausklick rechts).

- Klicken Sie probehalber auf die diversen Bereiche der Statusleiste (linke und rechte Maustaste).

Alle Editierfelder in der Benutzeroberfläche (bis auf solche für Passwörter und für die Breiten von Spalten im Verzeichnis-Browser) merken sich einen Verlauf mit bis zu 10 früheren Eingaben. Diese können eingesehen werden, indem Sie den winzigen Schalter anklicken, der in jedem Editierfeld mit gespeichertem Verlauf erscheint. Alternativ können Sie die F4-Taste drücken, genau wie in einer normalen herunterklappbaren Liste. Wenn Sie einen früheren Eintrag aus dem aufgeklappten Menü auswählen, wird er automatisch wieder in das Editierfeld eingetragen. Benutzern, die ihre Verläufe komplett löschen oder an andere Benutzer weitergeben möchten, sei gesagt dass die Verläufe in einer Datei namens History.dat gespeichert werden, wenn das Programm beendet wird. Diese Datei können Sie einfach kopieren oder löschen. Wenn Sie zwischen mehreren Sitzungen keine Verläufe speichern möchten, können Sie eine leere Datei namens History.dat selbst erzeugen und diese mit dem Schreibschutz-Attribut versehen. Das wird von X-Ways Forensics respektiert. Um eine bestimmten Eintrag für ein bestimmtes Editierfeld zu löschen, wählen Sie den Eintrag im aufgeklappten Menü bei gedrücktgehaltener Umschalt-Taste.

Since the days of Windows 95 (or perhaps even Windows 3.1?) users can press Ctrl+C to produce a plain-text representation of standard Windows message boxes in the clipboard. With message boxes in WinHex and X-Ways Forensics it works the same. Although this is an elementary feature in Windows for more than 20 years already and should be known to any experienced Windows user and although WinHex and X-Ways Forensics make users aware of that ("Did you know? ..."), the great majority of users for some reason still take graphical screenshots of message boxes and paste them into HTML e-mails, for example when they report error messages, although that is more work than simply pressing Ctrl+C and Ctrl+V and although it inflates the size of the e-mail unnecessarily, as a few ASCII characters need much less space them thousands of pixel values. That also means the screenshot will get lost if the e-mail is converted to plain text when being replied on, and of course the error message text will not be searchable in a graphical screenshot and cannot be conveniently selected and copied to the clipboard as text by the recipient, and the recipient cannot be sure of the exact Unicode value of certain characters for which multiple variants exist.

In WinHex and X-Ways Forensics it is even possible to copy a rudimentary ASCII representation of dialog boxes and almost all their control items (static text, push buttons, check boxes, radio buttons, list boxes, combo boxes, and tree view controls) including their states (unchecked, checked, half checked) by pressing Ctrl+C with an active dialog box on the screen (not if an edit box with a selection has the input focus). There is also a dedicated command in the window menu

of an dialog box. That menu is a.k.a. the system menu or control menu, and it pops up when right-clicking the title of a dialog box. This copy command is a very efficient way to show your settings in a certain dialog box to other users and let them copy strings for use in their own edit boxes, so that they don't have to type them, avoiding typos. The text representation is even more powerful than a screenshot because it shows the contents of edit boxes and list boxes completely, even if these controls have scrollbars and the contents exceed the physical boundaries of the controls on the screen. Unicode characters are supported. We suggest that users take screenshots of message boxes and dialog boxes only if absolutely necessary, for example if they wish to graphically highlight certain control items in a Photoshop or similar programs to get the message across.

Settings in practically all dialog boxes can also be conveniently saved to and loaded from files as needed, for example to share them with other users or for future use, via the system menu. This function can remember the selection states of the most important control types: check boxes, radio buttons, list boxes, combo boxes, and tree view controls. This works even if the controls are currently invisible. The settings are stored in files with the .dlg extension (for "dialog"), in the same directory as templates and scripts. The contents of edit boxes are also remembered. However, this function does not remember the contents/text labels of check boxes, list boxes, combo boxes, and tree view controls, e.g. which code page a check box represents in the Simultaneous Search dialog, which label names (Vermerkbezeichnungen) exist in the label filter list box, which external programs are listed in the Viewer Programs dialog window, which file types are listed in a tree view control etc. It also does not remember the order of controls or list items. It also does not remember settings in a dependent dialog window (which opens e.g. when clicking a "..." button). The functionality is not available for the Directory Browser Options dialog window. For the directory browser options please save and load .settings files by clicking the icons in the directory browser caption line. The functionality to store dialog window selections in files is very useful for example for the Export List command, where some users repeatedly need different settings for different purposes, and where the items in the list box are always the same (just the available columns), except after changing the language of the user interface.

3.9 Befehlszeilenparameter

1) Sie können die Namen von Dateien, die Sie automatisch bei Programmstart öffnen möchten, einfach in der Kommandozeile angeben, wenn nötig incl. Pfad. Physische Datenträger können auch geöffnet werden, z. B. geben Sie :0 an für Festplatte 0.

2) Die Befehlszeile kann auch zum Ausführen von Scripts zum Editieren von Dateien verwendet werden. Geben Sie dazu den Namen einer .whs-Script-Datei an. Solche Dateien werden nicht geöffnet, sondern ausgeführt.

3) Sie können eine X-Tension ausführen mit einem Befehl namens "XT". Diesen beiden Zeichen muss ein Doppelpunkt folgen und dann der Pfad und Dateiname der X-Tension.

4) Die Befehlszeile kann auch zum Öffnen von Fällen verwendet werden. Geben Sie dazu den Namen der .xfc-Falldatei als ersten Parameter an. Sie können einem solchen Fall sogleich Images

mit dem AddImage:-Befehl hinzufügen (s. u.). Wenn der Name oder Pfad einer .xfc-Datei als Parameter übergeben wird, wenn dies nicht der erste Parameter ist, und wenn zu dem Zeitpunkt, an dem der Parameter verarbeitet wird, bereits ein Fall offen ist, werden die Asservate des angegebenen Falls in den bereits geöffneten Fall importiert.

5) X-Ways Forensics (nicht X-Ways Investigator) unterstützt Kommandozeilen-Syntax, die es ermöglicht, a) Fälle zu erzeugen, c) Datenträger-Sicherungen, Datenträger, Verzeichnisse und Dateien hinzuzufügen, c) den Datei-Überblick aller hinzugefügten Asservate zu erweitern und d) Stichwort-Suchen laufen zu lassen. Beispiel:
xwforensics64.exe "NewCase:D:\Fall\Mein Fall" "AddImage:Z:\Images*.e01" "AddImage:Z:\Images\Mein Image.dd" RVS:~

Wenn für den Fall kein Pfad angegeben ist, wird dieser im Standard-Fälleverzeichnis angelegt. Die Anführungszeichen sind nur für Parameter mit Leerzeichen erforderlich. Wenn nach "NewCase" ein Semikolon statt ein Doppelpunkt folgt, erzeugt das einen neuen, eindeutigen Dateinamen, falls es bereits eine .xfc-Datei mit dem angegebenen Fallnamen gibt. Mit einem Doppelpunkt würde ein bestehender Fall ohne Rückfrage gelöscht und überschrieben. Der Befehl "NewCase" unterstützt relative Fallpfade und auch Verweise auf Umgebungsvariablen.

Zur Erweiterung des Datei-Überblicks aller Asservate im Fall (Befehl "RVS:~") oder nur neu hinzugefügter Asservate ("RVS:~+") wendet X-Ways Forensics dieselben Operationen an, wie sie laut der Datei WinHex.cfg zuletzt zuvor auf einen völlig unverarbeiteten Datei-Überblick angewandt wurden. Ein Bildschirmfoto des Dialogfensters mit den Erweiterungseinstellungen wird automatisch in das Fallprotokoll aufgenommen. Es ist entweder textueller oder grafischer Natur je nach Fallprotokolleinstellungen. Text in Meldungsfenstern, die normalerweise vom Benutzer weggeklickt werden müssen, werden während der Abarbeitung der Parameter AddImage und RVS ins Nachrichtenfenster umgeleitet. Dialogfenster hingegen, sollte es welche geben, werden nach wie vor angezeigt (Abhilfe s. u.).

Der Befehl "LST" kann eine Liste von Suchbegriffen laden. Wenn diesem Befehlscode ein Doppelpunkt folgt und dann der Name oder vollständige Pfad einer Textdatei mit 1 Suchbegriff pro Zeile und wenn dies einem RVS-Aufruf mit implizit angestoßener paralleler Suche vorangeht, dann werden die Suchbegriffe für diese Suche verwendet.

6) Der AddImage-Befehl unterstützt Sternchen. It also supports optional sub-parameters to force interpretation of an image as either a physical, partitioned medium (P) or volume (V) and to force interpretation with a certain sector size, where the sector size is optional, e.g.

AddImage:#P#Z:\Images*.dd
AddImage:#P,4096#Z:\Images*.dd

If you don’t specify these sub-parameters, a dialog window might pop up to ask the user for this input, but only in some very rare cases, only if not obvious to X-Ways Forensics from the data in the first few sectors what kind of image it is and if the image was not created by X-Ways Forensics or X-Ways Imager and if the image is not in .e01 evidence file format (e.g. raw image). Only if all three conditions are met at the same time plus you do not specify the sub-parameters, the dialog window will pop up.

7) Ein Kommandozeilen-Befehl namens "AddDir" ist verwendbar. Er wird von einem Doppelpunkt gefolgt, und dahinter geben Sie an, welches Verzeichnis Sie zum Fall hinzufügen möchten, z. B. AddDir:X:\. Wenn das Zeichen nach dem Doppelpunkt ein Sternchen ist, werden die Stammverzeichnisse aller verfügbaren Laufwerksbuchstaben zum Fall hinzugefügt: AddDir:*. Allerdings möchten Sie dabei Netzlaufwerke evtl. auslassen, da diese extrem groß und langsam zu erkunden sein können. Das Hinzufügen von Netzlaufwerken hängt von einer Option unter Optionen | Datei-Überblick ab. Wenn Sie X-Ways Forensics von einem Volume aus starten, das einen Laufwerksbuchstaben hat, wird dieser Laufwerksbuchstabe von dem Befehl übersprungen, in der Annahme, dass Sie gerade halbautomatisch ein Live-System triagieren oder logisch sichern und X-Ways Forensics dabei von Ihrem eigenen mitgebrachten externen Datenträgern gestartet haben. Der AddDir-Befehl erlaubt auch das Hinzufügen einzelner Dateien zum Fall.

8) Ein weiterer Kommandozeilen-Befehl namens "AddDrive" ist verfügbar. Auch an den Namen dieses Befehls schließt sich ein Doppelpunkt an, und dahinter geben Sie an, welcher Laufwerksbuchstabe zum Fall hinzugefügt werden soll, als Großbuchstabe. z. B.. AddDrive:C. Anders als ein Verzeichnis, das über das Betriebssystem erkundet wird, brauchen Laufwerksbuchstaben sektorweisen Zugriff (und daher Administrator-Rechte), und jegliches vorgefundenes Dateisystem wird von X-Ways Forensics selbst eingelesenm, sofern es unterstützt wird. Wenn das Zeichen nach dem Doppelpunkt ein Sternchen ist, werden alle verfügbaren Laufwerksbuchstaben im System dem Fall hinzugefügt: AddDrive:*. Auch hierbei sind Netzlaufwerke optional, und der Laufwerksbuchstabe mit X-Ways Forensics wird übersprungen. Wenn Sie AddDrive:* aufrufen, obwohl die Software ohne Administratorrechte ausgeführt wird, dann wird intern statt dessen automatisch AddDir:* ausgeführt. Wenn Netzlaufwerke bei Abarbeitung von AddDrive:* angetroffen werden, werden diese intern mit dem AddDir-Befehl hinzugefügt, da sie vom Betriebssystem ohne sektorweisen Zugriff erkundet werden müssen.

9) Wenn Sie für unterschiedliche Fälle unterschiedliche Einstellungen verwenden möchten, müssen Sie diese Einstellungen in verschiedenen WinHex.cfg-Dateien (in verschiedenen Verzeichnissen oder unter unterschiedlichen Namen) speichern und vor der Ausführung von X-Ways Forensics die gewünschte Datei einsetzen. Oder aber Sie verwenden den Parameter "Cfg:", der den Namen der Konfigurationsdatei angibt (ohne Pfad), aus der X-Ways Forensics bei Programmstart liest und in die es bei Programmende schreibt, Nützlich in Situationen, in denen eine andere Konfiguration als normalerweise zum Einsatz kommen soll (nicht die in der Datei WinHex.cfg). Insbes. wenn sie für eine automatisierte Ausführung andere Einstellungen brauchen, wahrscheinlich gezielt dafür voher definierte, mit bestimmten ausgewählten DÜE-Operationen, oder wenn Sie die Rückfrage, ob eine zweite Instanz gestartet werden soll,zwar normalerweise schätzen, aber nicht während einer automatisierten Ausführung, bietet sich dieser Parameter an. Ein solcher Parameter sieht beispielhaft so aus: "Cfg:Meine andere Einstellung.cfg". Die Anführungszeichen sind nur dann erforderlich, wenn der Dateiname Leerzeichen enthält. Die Maximallänge beträgt 31 Zeichen. Derzeit werden nun ANSI/ASCII-Zeichen unterstützt. Command line parameters are usually processed in the order in which you specify them except the Cfg: parameter is processed before all the others, so it does not matter where it goes. Beachten Sie bitte auch, dass bestimmte Einstellungen in anderen Dateien gespeichert werden, z. B. "X-Tensions.txt" und "Unwanted Metadata.txt".

10) You can load dialog window selections. This will usually override specific parts of the configuration that is initially read from a WinHex.cfg file, at the moment when the command line

parameter is processed (not when those parts of the configuration might affect what the application does). The command is "Dlg:", directly followed by the path of the .dlg file. Relative paths are supported, and you may use file masks to load multiple .dlg files in the same directory at the same time. After you save dialog window selections for future use with the command line please verify that they can be accepted by clicking OK after saving them. Only .dlg files created in v20.2 and later can be used.

11) A command line parameter named "Override" overrides message boxes and dialog boxes until the last command line parameter has been processed. The text of those boxes will be output to the Messages window (and thus indirectly also to msglog.txt, unless disabled), and either an automatic click on OK will be simulated (if the parameter is "Override:1") or a click on Cancel (in case of "Override:2"). If a message box has only one button, it does not matter which parameter value was specified. All of this helps to avoid interruptions and delays of automatic processing when the program is waiting for user input.

The default setting and recommended behavior (if no Override parameter is specified) is like "Override:0", where message boxes and dialog boxes are shown normally and potentially alert the user of critical error conditions and anomalies such as incomplete images, undetectable image format etc. The parameter takes effect immediately upon start-up, before regular processing of other parameters begins, even if the Override parameter is specified last in the command line.

The Override parameter also outputs the entire command line to the Messages window (even with the value "0"), and this happens at a time that depends on the position of the parameter within the command line. This allows users who study the log later to know what the simulated response to the suppressed message boxes and dialog boxes was.

12) Es ist auch möglich, einen physischen Datenträger (z. B. eine lokal angeschlossene Festplatte oder eine über F-Response geöffnete Festplatte oder Hauptspeicher-Datenquelle eines Rechners im Netz) automatisch über die Befehlszeile zu sichern, in X-Ways Imager und X-Ways Forensics. Der erste Parameter muss mit einem Doppelpunkt starten und dann die Nummer des Geräts in Windows angeben (z. B. ":1" für Festplatte Nr. 1, d. h. die 2. Festplatte). Das bewirkt, dass die Festplatte sofort nach Programmstart automatisch geöffnet wird. Der zweite Parameter sollte mit einem senkrechten Strich beginnen, gefolgt entweder von "e01" oder "raw", was das gewünschte Image-Dateiformat angibt, gefolgt von einem weiteren senkrechten Strich und Name und Pfad des Images, und dann optional Beschreibung und Name des Bearbeiters (z. B. also "|e01|G:\Ausgabedateiname.e01|Meine Beschreibung|Mein Name"). Es ist auch möglich, zwei Kopien des Images gleichzeitig erzeugen zu lassen, nämlich durch Einsatz eines Schrägstrichs: "|e01|G:\Kopie 1.e01/H:\Kopie 2.e01|Meine Beschreibung".

13) Als letzten Parameter können Sie "auto" angeben, wenn sich X-Ways Forensics nach Abschluss aller Arbeiten selbständig beenden soll.

3.10 Benutzerdefinierte Tastenkürzel

Im Dialogfenster mit den allgemeinen Optionen gibt es einen Schalter, den Sie anklicken können, um bis zu 20 Tastenkürzel für Befehle u. a. im Kontextmenü des Verzeichnis-Browsers selbst zu

definieren. Dies ist derzeit nur in X-Ways Forensics möglich. Die Tastenkürzel sollen Ihre Produktivität bei immer wiederkehrenden Standardaktivitäten erhöhen. Nur Tastenkombinationen mit den Tasten Strg, Strg+Alt, Alt Gr, Umschalt und Leertaste sind hierbei möglich. Bitte beachten Sie: Wenn Sie die Leertaste für irgendeine Tastenkombination als Basis festgelegt haben, kann sie nicht mehr zum Markieren oder Entmarkieren von Objekten im Verzeichnis-Browser verwendet werden. Die jeweils zweite Taste kann relativ frei gewählt werden, indem Sie sie einfach drücken, während das ausgegraute Editierfeld den Eingabefokus hat. Falls für die Taste Ihrer Wahl keine menschenlesbare Beschreibung angezeigt wird und Sie später vergessen, welche Taste Sie sich ausgesucht hatten, können Sie den hexadezimalen Tastaturcode für die Taste immer noch hier nachschlagen: https://msdn.microsoft.com/en-us/library/windows/desktop/dd375731(v=vs.85).aspx

Die folgenden rd. 80 Codes für **Befehle im Kontextmenü** des Verzeichnis-Browsers kommen theoretisch in Frage (nicht alle wurden getestet) und können als Zahl eingegeben werden:

9800: Mit externem Viewer-Programm Nr. 1 einsehen
9801: Mit externem Viewer-Programm Nr. 2 einsehen
9802: Mit externem Viewer-Programm Nr. 3 einsehen
...
9831: Mit externem Viewer-Programm Nr. 32 einsehen

9919: Dateityp definieren
9920: Zugehörige Datei aufsuchen
9921: Datei-Überblick für ausgewählte Dateien erweitern
9927: X-Tension auf ausgewählte Dateien anwenden
9928: Externe Datei anhängen
9931: Metadaten editieren
9932: Datei von ihrem Elternverzeichnis aus erkundet sehen
9933: Datei vom Stammverzeichnis aus erkundet sehen
9934: Elternobjekt aufsuchen
9935: Logische Suche in ausgewählten Dateien
9937: Externes Verzeichnis anhängen
9938: Sicher löschen
9939: Suchtrefferliste in Richtung eines bestimmten Verzeichnisses verlassen
9940: Doppelte Treffer in der Liste löschen
9941: Ausgeblendete Objekte auswählen
9942: Kommentar bearbeiten
9944: Einblenden
9945: Markierte Objekte auswählen
9946: Alle außer markierte Objekte ausblenden
9947: Markierte Objekte ausblenden
9948: Zum Container bzw. zur Minimalsicherung hinzufügen
9949: Suchtreffer vergrößern
9950: Suchtreffer verwandeln in aus Sektoren ausgegliederte Datei
9951: Ausgliederte und virtuelle Dateien vergrößern
9952: Suchtreffer einem anderen Suchbegriff zuordnen
9953: Fortlaufende Video-Einzelbildern extrahieren
9954: Suchtreffer in Bericht aufnehmen

9955: Als Laufwerksbuchstabe einbinden (ergibt nur einen Sinn, wenn genau ein Verzeichnis ausgewählt ist)
9956: Mit bevorzugtem Video-Abspielprogramm ansehen
9957: Mit bevorzugtem HTML-Einsehprogramm einsehen
9958: Mit bevorzugtem Texteditor einsehen
9959: Mit dem in Windows verknüpften Programm öffnen
9960: Eingesehene Objekte auswählen
9961: Mit einem noch zu bestimmenden externen Programm einsehen
9962: Anhand von Hash-Werten erkannte Duplikate entfernen
9963: Objekt anhand von interner ID aufsuchen
9964: Nach Relevanz sortieren
9965: Drucken
9966: Listeneintrag anhand von Positionsnummer aufsuchen
9967: Nicht sortieren
9968: Alles auswählen
9969: Nach dem Hash-Wert der ausgewählten Datei filtern (um Duplikate zu finden)
9971: Erkunden
9972: Suchtreffer als wichtig kennzeichnen
9973: Öffnen
9974: Zur definierenden Datenstruktur navigieren
9975: Liste exportieren
9976: Cluster auflisten
9977: Wiederherstellen/Kopieren
9978: Erkunden/Einsehen
9979: Auswahl umkehren
9980: In Hash-Datenbank aufnehmen

Es fallen Ihnen vielleicht einige verdächtige Lücken unter den fortlaufenden Nummern auf. Die fehlenden Nummern sind entweder undefiniert, der Aufruf des Befehls ist nicht empfehlenswert, oder die Nummern sind einfach nicht sinnvoll für benutzerdefinierte Tastenkürzel. Als Beispiel für letzteres mag der Befehl mit dem Code 9929 dienen. Dieser löscht einfach ausgewählte Suchtreffer oder Ereignisse, was natürlich bereits viel naheliegender durch Drücken der Entf-Taste erreicht werden kann. Diese Information soll ein ggf. bestehendes Bedürfnis auf Benutzerseite reduzieren, wahllos irgendwelche hier nicht genannten Nummern einfach blind auszuprobieren. Sollte dabei aber jemand auf die sagenumwobene Funktion „Alle Beweise finden“ stoßen, möge er oder sie sich aber bitte melden.

Bitte beachten Sie noch, dass Sie auch ohne das Festlegen solcher Tastenkombinationen das Kontextmenü des Verzeichnis-Browsers rein mit der Tastatur erreichen können, indem Sie die Kontextmenü-Taste drücken. (Kann normalerweise zwischen der rechten Windows-Taste und der rechten Strg-Taste gefunden werden.) Und einige Menübefehle haben bereits von Haus aus eine zugehörige Tastenkombination. Z. B. ist das Drücken der Eingabetaste gleichbedeutend mit einem Doppelklick (entweder Einsehen oder Erkunden je nach Ihren Einstellungen). Die Multipliziertaste auf dem Ziffernblock der Tastatur löst den Erkunden-Befehl aus. Entf bedeutet Ausblenden. Strg+Entf setzt Dateien auf den Zustand „noch von den Operationen der Datei-Überblicks-Erweiterung zu verarbeiten“ zurück und macht einige Erweiterungsoperationen rückgängig. Strg+Umsch+Entf entfernt Hash-Set-Treffer, Hash-Kategorie und PhotoDNA-Kategorisierung. Strg+Feststelltaste+Entf entfernt die Kennzeichnung als „Datei-Inhalt

unbekannt“ einer Datei. (Das ist nützlich z. B. wenn wegen vorübergehender E/A-Probleme X-Ways Forensics einige Dateien so gekennzeichnet hat, obwohl die Dateien sonst einwandfrei gelesen werden können.) Strg+C kopiert die im Verzeichnis-Browser zu sehenden Angaben zu ausgewählten Objekten in die Zwischenablage unter Verwendung bestimmter Einstellungen des Dialogfensters zu „Liste exportieren“.

Hauptmenü

Benutzerdefinierte Tastenkürzel sollten außerdem in der Lage sein, praktisch alle Befehle des Hauptmenüs aufzurufen, und auch dann, wenn andere Teile der Benutzeroberfläche als der Verzeichnis-Browser den Eingabefokus haben. Wenn sich der Code eines Menübefehls in einer künftigen Version ändern sollte, stellt X-Ways Forensics sicher, dass Tastenkürzeldefinitionen, die diesen Code verwenden automatisch inaktiv werden, damit nicht versehentlich ggf. eine andere Funktion ausgelöst wird. Um die Befehlscodes des Hauptmenüs herauszufinden (oder anders ausgedrückt die IDs der Menüeinträge), können Sie die ausführbare Datei des Programms in einem sog. Ressourcen-Editor öffnen und die Menüressource in der von Ihnen verwendeten Sprache ansehen. Ein besonders empfehlenswertes leichtgewichtiges Tool für diesen Zweck ist "Pelles C for Windows", das gleichzeitig auch ein ordentlicher C-Compiler und eine komplette Entwicklungsumgebung ist, die sich zum Erstellen von X-Tensions eignet. Benutzerdefinierte Tastenkürzel für Befehle im Hauptmenü sollten weniger wichtig sein als solche für das Kontextmenü des Verzeichnis-Browsers, weil im Hauptmenü bereits sehr viele Tastenkürzel voreingestellt sind. Selbst wenn nicht für den von Ihnen favorisierten Befehl, können Sie ihn immer noch erreichen, ohne die Hände von der Tastatur zu nehmen, beginnend mit der Alt-Taste. Als Ideen für mögliche sinnvolle Anwendungen sei gesagt, dass Sie zwischen rekursiver und nichtrekursiver Erkundung mit dem Befehlscode 122 hin- und herwechseln können, und der Befehlscode zum Erzeugen eines neuen Datei-Überblicks ist 109.

Befehlscodes für **Filter**
(Die Reihenfolge ist historisch bedingt, so wurden die Filter nach und nach eingeführt.)

9700: Name
9701: Typ
9702: Typstatus
9703: Kategorie
9704: Größe
9705: Pfad
9706: Absender
9707: Empfänger
9708: Zeitstempel
9709: Attr
9710: Hash 1
9711: Hash-Set
9712: Hash-Kategorie
9713: Vermerke
9714: Kommentare
9715: Metadaten
9716: Analyse
9717: Pixel

9718: Int. ID
9719: Eindeutige ID
9720: Suchbegriffe
9721: Besitzer
9722: Elternname
9723: Unterobjekte
9724: ID
9725: Autor
9726: Suchtreffer-Beschreibung
9727: Ereignis-Zeitstempel
9728: Ereignistyp
9729: Ereignis-Beschreibung
9730: Suchtreffer
9731: Startsektor
9732: Beschreibung
9733: Hash 2
9734: Vollpfad
9735: Flex-Filter 1
9736: Flex-Filter 2

Befehlscodes für **Modus-Schalter** und verwandte Schalter

122: Rekursive Erkunden
138: Aufklappmenü des Zugriffsschalters
172: Verzeichnis-Browser sichtbar machen bzw. verstecken
186: Positionsmanager sichtbar machen bzw. verstecken
223: Suchtrefferliste sichtbar machen bzw. verstecken
224: Ereignisliste sichtbar machen bzw. verstecken
225: Modus Disk/Partition/Volume/Container
226: Datei-Modus
227: Vorschau-Modus
228: Details-Modus
229: Galerie-Modus
230: Kalender-Modus
231: Legende
232: Sync-Modus
249: Roh-Vorschau-Modus
250: Viewer X-Tension Vorschau-Modus

4 Menü-Referenz

Vorbemerkung: Befehle im Hauptmenü (Datei, Bearbeiten, Suchen, ...) beziehen sich immer auf das gesamte aktive Datenfenster (das z. B. eine geöffnete Datei oder einen geöffneten Datenträger repräsentiert), oder auf noch vom Benutzer anzugebende Dateien oder Datenträger. Sie beziehen sich *niemals* auf im Verzeichnis-Browser ausgewählte Dateien. Dafür gibt es das

4.1 Kontextmenü des Verzeichnis-Browsers

Das Kontextmenü des Verzeichnis-Browsers erlaubt es dem Benutzer, direkt mit den aktuell ausgewählten Dateien bzw. Verzeichnissen im Verzeichnis-Browser zu interagieren (wohlgemerkt nicht mit den mit einem blauen Quadrat *markierten*). Es gibt eine Reihe von Befehlen, die in Abhängigkeit von den aktuell ausgewählten Objekten verfügbar sind. Ein Doppelklick auf Dateien oder Verzeichnisse löst je nach Kontext entweder „Einsehen“, „Erkunden“ oder den Aufruf des verknüpften externen Programms aus.

Einsehen

Hiermit können Windows Registry-Dateien und diverse Bilddateiformate mit dem internen Viewer eingesehen werden. Falls die separate Viewer-Komponente von X-Ways Forensics aktiv ist, werden alle anderen Dateien an diese Komponente übergeben. Falls nicht, wird stattdessen das erste installierte externe Programm aufgerufen. NTFS-Systemdateien immer in Form von Datenfenstern geöffnet.

Beim Einsehen einer Datei in einem separaten Fenster können Sie (Strg+) Bild abwärts/aufwärts drücken, um das Fenster zu schließen und die nächste Datei im Verzeichnis-Browser in einem neuen Fenster einzusehen. Wenn ein Einsehen-Fenster ein Bild darstellt und das Einsehen auf 1 Bild zur gleichen Zeit beschränkt ist, wird das Fenster beim Drücken der Pfeiltasten in der Galerie aktualisiert. Das ist besonders bei Verwendung eines übergreifenden Desktops nützlich, wenn das Einsehen-Fenster auf dem zweiten Bildschirm zentriert ist und die Galerie auf dem ersten Bildschirm angezeigt wird. Vermeidet, dass man die Eingabe-Taste drücken muss, um ein Bild einzusehen, und eine weitere Taste, um das Einsehen-Fenster wieder zu schließen, um den Eingabefokus zurück zur Galerie zu transferieren.

Beim Einsehen von Bildern mit der internen Grafikanzeigebibliothek haben Sie die Wahl, die Einseh-Fenster entweder auf dem Bildschirm zu zentrieren oder die Bildschirmkoordinaten der linken oberen Ecke oder der Fenstermitte nach dem Positionieren irgendwo auf dem Bildschirm zu speichern und für weitere Fenster wiederzuverwenden. Dazu öffnen Sie das Systemmenü des Fensters (das ist bekanntlich das Menü, das erscheint, wenn Sie die linke obere Ecke des Fensters anklicken). Sie können sich auch entscheiden, ob solche Einseh-Fenster immer im Vordergrund angezeigt werden sollen oder nicht, also sogar im Vordergrund der Fenster anderer Windows-Programme. Und nicht zuletzt können Sie auch optional die ungefähre Fenstergröße zum Einsehen weiterer Bilder einfrieren. Letzteres ist besonders nützlich in Verbindung mit der Möglichkeit, die Koordinaten der oberen linken Fensterecke einzufrieren, nur genau ein Einseh-Fenster auf einmal zu öffnen und Einseh-Fenster mit einem einzigen Mausklick auf eine Datei zu aktualisieren, so dass Sie an einer beliebigen Stelle auf Ihrem Bildschirm praktisch eine feste Vorschau von Bildern haben, während die untere Hälfte des Datenfensters einen anderen Modus als Vorschau zeigen kann, z. B. den Details-Modus.

Erkunden

Nur verfügbar für Verzeichnisse und Archive (ZIP, RAR, TAR, ...): Mit diesem Kommando navigiert man in diese mit dem Verzeichnis-Browser hinein. Ein Doppelklick auf ein Archiv oder Verzeichnis hat dieselbe Wirkung. Ein Kommando, das gleichzeitig alle Inhalte eines Verzeichnisses und aller seiner Unterverzeichnisse auflistet, finden Sie stattdessen im Kontextmenü des Verzeichnisbaums (im Falldatenfenster, "Rekursiv erkunden").

Viewer-Programme

Gezielt die selektierten Dateien an eines der externen Programme schicken, die aktuell konfiguriert sind, oder an das Programm, das in der aktuellen Windows-Installation mit dem Dateityp verknüpft ist. Diese Verknüpfung wird ausgewertet auf der Basis der Datei-Erweiterung, wie dies in Windows üblich ist.
Es besteht die Möglichkeit, Dateien in einem externen Programm zu öffnen, das Sie ad hoc bestimmen. Das Programm, das Sie auswählen, wird als ein Standard-Viewer-Programm gespeichert, wenn noch nicht alle Plätze für externe Programme belegt sind, und dann auch für das nächste Mal, wenn Sie denselben Menübefehl aufrufen, automatisch vorgeschlagen.

Öffnen

Öffnet die aktuelle Datei bzw. bei Verzeichnissen die Datenstrukturen des Verzeichnisses in einem eigenen Datenfenster. Im Gegensatz zu Datei | Öffnen, wo Dateien wie in anderen Applikationen mit Hilfe des Betriebssystems geöffnet werden können, ist dies eine forensische einwandfreie Operation, da sie keinerlei Zeitstempel o. ä. im Dateisystem beeinflusst, weil das Betriebssystem übergangen wird und die Logik zum Lesen des Dateiinhalts aus den richtigen Datenträgersektoren in WinHex selbst für diverse Dateisystem implementiert ist. Allerdings können an Dateien, die auf diese Weise geöffnet wurden, keine Änderungen vorgenommen werden. Im Fall eines Verzeichnisses werden die Datenstrukturen des Verzeichnisses geöffnet.

Drucken

Wenn die separate Viewer-Komponente aktiv ist, können Sie Dateien (oder gar Verzeichnisse) zum Drucken auswählen. Dabei ist es möglich, mehrere ausgewählte Dokumente ohne Unterbrechung zu drucken und ohne Klicks nach jedem Dokument, optional zusammen mit Unterobjekten (z. B. E-Mail-Anhänge zusammen mit der zugehörigen E-Mail). Das optionale Deckblatt enthält Datum und Uhrzeit, an denen der Druckauftrag gestartet wurde, und ausgewählte Metainformationen wie Dateiname, Pfad, Asservatname, Dateigröße, Beschreibung, Zeitstempel, Kommentare usw. Ganz unten auf das Deckblatt kann eine Vorschau der Datei gedruckt werden. Deren Format hängt von den Einstellungen der Viewer-Komponente im Vorschau-Modus ab, z. B. "Best Fit" oder "Actual Pixels" oder "Fit to Window Width" usw. Es handelt sich um ein dreistufiges Kontrollkästchen. Wenn nur halb gewählt, wird die Vorschau in deutlich helleren Farben gedruckt, um Tinte/Toner zu sparen oder um die Lesbarkeit zu erhöhen, falls Sie sehr viele Metadaten-Felder ausgeben lassen und diese bis über die Vorschau ragen. Das Deckblatt wird von X-Ways Forensics selbst gedruckt, die folgenden Seiten mit dem eigentlichen Dokument von der Viewer-Komponente. Sie können nur das Deckblatt drucken oder nur die Datei oder beides. Die Kopfzeile des Deckblatts, die den Benutzer nennt und Name und Version des zum Drucken verwendeten Programms, ist optional. Nützlich, wenn Sie den Ausdruck dem Beschuldigten oder einem Zeugen zeigen möchten und diese Personen den Benutzernamen des Ermittlers nicht wissen sollen.

Eine weitere Möglichkeit ist, X-Ways Forensics den Dateinamen und Pfad oben auf die erste Seite drucken zu lassen. Diese Option ist nicht denselben Pfadlängenbeschränkungen unterworfen wie der optional von der Viewer-Komponente gedruckte Header ("Print header", Job Name = %p). Um zu vermeiden, dass der Pfad auf der ersten Seite zweimal gedruckt wird, lassen Sie ihn entweder von X-Ways Forensics oder von der Viewer-Komponente drucken, nicht von beiden.

Wiederherstellen/Kopieren: s. separates Thema

Liste exportieren

Erfordert eine Specialist-Lizenz. Gibt Daten über die ausgewählten Objekte im Verzeichnis-Browser in eine tabulatorseparierte Textdatei oder in eine HTML-Datei aus. Diese kann in jedem Web-Browser betrachtet oder auch z. B. in MS Excel und MS Word einfach importiert und weiter bearbeitet werden kann. Eine dritte Möglichkeit (außer für Suchbegriffslisten) ist eine XML-Datei. Die Daten können im gewählten Format alternativ auch einfach in die Zwischenablage kopiert werden, z. B. um sie direkt in einen extern bearbeiteten Bericht einzufügen. Die zu exportierenden Spalten sind frei wählbar. Sogar die Suchtrefferspalte kann exportiert werden, mitsamt dem textuellen Kontext, in dem jeder Suchtreffer steht, wobei der Suchbegriff selbst visuell durch eine gelbe Hintergrundfarbe hervorgehoben werden kann (nicht empfohlen für die Weiterverarbeitung in MS Excel). Sie können das Resultat in mehrere Dateien aufteilen lassen, um zum Beispiel zu verhindern, dass der HTML-Code so umfangreich wird, dass ein Internet-Browser ihn nicht mehr effizient laden kann und Speicherprobleme bekommt.

Es gibt eine Option, die Dateien aus dem Datenträger bzw. Image gleichzeitig herauszukopieren und von der HTML-Tabelle aus zu verlinken. Die Links sind in der Namensspalte zu finden. Das exakte Verhalten dieser Option wird von zwei Optionen des Fallberichts beeinflusst: "Dateien benennen nach" und "Datei-Anhänge in .eml-Elterndatei einbetten". Diese Option stellt eine interessante Layout-Alternative zur regulären Ausgabe von Berichtstabellen dar und kann auch als Alternative zum Befehl "Wiederherstellen/Kopieren" angesehen werden.

In der Namensspalte können Sie Originalnamen ausgeben lassen oder - sofern verfügbar - alternative Namen (wenn das Kontrollkästchen dazu ganz gewählt ist) oder beides (wenn sich das Kontrollkästchen in seinem mittleren Zustand befindet). Beim Exportieren einer Liste von Dateien und Verzeichnissen mitsamt Unterobjekten und Sortierung nach Vollpfad, so dass Unterobjekte direkt ihren jeweils übergeordneten Objekten folgen, im Format TSV oder HTML, ist eine Option namens „Einrückung“ verfügbar, die die Namen von Unterobjekten hierarchisch genau einrückt, so dass es einfach ist zu sehen, welche Objekte Unterobjekte von welchen übergeordneten Objekten sind, selbst wenn Sie nicht auf die u. U. sehr lange Vollpfadspalte schielen oder diese erst gar nicht mit als Spalte ausgeben. Die Einrückung kann stark oder weniger stark ausfallen (ganz oder nur halb gewählt).

Der Befehl merkt sich Notationseinstellungen separat von denen in den allgemeinen Optionen. Das ist nützlich, weil das Datenbank- oder Tabellenkalkulationsprogramm, in dem Sie die Daten ggf. importieren möchten, die Formatierung, die Sie gern im Verzeichnis-Browser sehen, evtl. nicht mag (z. B. Bruchteile von Sekunden in Zeitstempeln, Zeitzonenumrechnung, Wochentage im Datum, Trennzeichen zwischen Datum, und Uhrzeit, Zifferngruppierung usw. usf.). Während

das Dialogfenster des Befehls "Liste exportieren" auf dem Bildschirm zu sehen ist, stützt basiert die Anzeige des Verzeichnis-Browsers vorübergehend auf den Notationseinstellungen fürs "Liste exportieren", als eine Art Vorschau.

Kopieren: Extrahierter Text

Erlaubt das Kopieren des Textes, der durch Decodierung oder OCR-Texterkennung gewonnen wurde, von ausgewählten Dateien an andere Orte. Der Anwendungsbereich kann beschränkt werden auf Dateien, die tatsächlich unbedingt OCR benötigen (also vor allem Bilder und bestimmte PDF-Dateien), falls Sie nur an solchen Dateien interessiert sind. Der extrahierte Text kann intern im Datei-Überblick gespeichert werden für zukünftige logische Suchen oder zum Indexieren und für die Kontextvorschau von Suchtreffern. Er kann in die Kommentarfelder der Dateien übernommen werden, was sich besonders für geringe Mengen an Text eignet, wie etwa per Texterkennung in Bildern (nicht Scans) zu erwarten, z. B. um diese Texte in den Fallbericht oder in exportierte Listen aufzunehmen, optional mit einem erklärenden Präfix wie [OCR] oder [Extrahierter Text]. Der extrahierte Text kann auch in Form von Unterobjekten als Textdateien ausgegeben werden. Oder er kann in einer einzigen Textdatei auf Ihrem eigenen Datenträger gesammelt werden, oder gesammelt in die Zwischenablage kopiert werden. Es ist jede denkbare Kombination der o. g. Kopierziele möglich.

Fortlaufende Einzelbilder extrahieren

Extracts all frames specifically from a defined section of a selected video. Useful if a certain part of a video is of high interest and you need to carefully check visual details in certain frames or include them in the report. You can specify how many consecutive frames to extract and starting from which second. The number of frames that you need to cover a certain period of time can be deducted from the frame rate as shown in the Metadata cell (fps = frames per second). Please note that the start second may be interpreted very roughly only, depending on the frequency of keyframes (a.k.a. I-frames in MPEG) in the video. MPlayer can seek into a video file only based on keyframes. If for example a certain video file contains keyframes only every 4 seconds for example, then the start second of the extraction may be off by up to 4 seconds. Keep this in mind when you enter the number of frames that you need or the start second. That is, to be on the safe side, extract more frames than you may actually need and perhaps from an earlier start second.

The frames are saved as JPEG files in a directory of your choice on your own drive, where you can review them outside of X-Ways Forensics. If you like, you can of course attach the most relevant frames to the original video file in the volume snapshot as child objects. The frames are not stored within the volume snapshot by default so that the size of the volume snapshot does not unreasonably inflate with potentially mostly irrelevant and redundant pictures. If the output directory already contains extracted frames, files with identical relative frame numbers will be overwritten. Relative frame numbers always start with 00000001 for each extraction and increment with each frame. You may adjust the JPEG compression if necessary for stronger compression or better quality. (Of course you usually cannot expect a very good quality because videos are typically highly compressed already.)

Vermerke: s. separates Kapitel

Kommentar bearbeiten

Erfordert eine forensische Lizenz. Verwenden Sie diesen Befehl, um ein Objekt im Verzeichnis-Browser mit einem Kommentar zu versehen oder einen existierenden Kommentar zu bearbeiten oder zu entfernen. Nachdem Sie Kommentare vergeben haben, können Sie den Filter bequem so setzen, dass nur solche Dateien angezeigt werden, die mit einem bestimmten oder überhaupt mit einem Kommentar versehen wurden.

Metadaten bearbeiten

Erfordert eine forensische Lizenz. Erlaubt das Editieren des Metadatenfelds einer Datei, sobald Metadaten extrahiert wurden. Nützlich wenn Sie ausgewählte, aber nicht alle extrahierten Metadaten in einen Bericht ausgeben möchten.

Datei-Überblick erweitern und **Parallele Suche** in Objekten, die im Verzeichnis-Browser *ausgewählt* sind

Markieren/Markierung aufheben

Erfordert eine forensische Lizenz. Visuelle Markierung können per Kontextmenü gesetzt und wieder aufgehoben werden. Das Erweitern des Datei-Überblicks kann auf markierte Dateien beschränkt werden.

Ausblenden/Einblenden

Sie können im Verzeichnis-Browser ausgewählte Objekte (auch durch Drücken der Entf-Taste) oder alle im Datei-Überblick als markiert oder nicht markiert geführten Objekte ausblenden, so dass sie, wenn Ausgeblendetes tatsächlich herausgefiltert wird, im Verzeichnis-Browser nicht mehr aufgelistet werden und ausgeschlossen sind von der Galerie-Ansicht und von allen Befehlen im Kontextmenü des Verzeichnis-Browsers. Wenn Sie nur den Inhalt bestimmter Verzeichnisse auswerten möchten oder dürfen, können Sie anfangs alle Dateien in allen anderen Verzeichnissen ausblenden, um das sicherzustellen. Das Erweitern des Datei-Überblicks kann auf nicht ausgeblendete Dateien beschränkt werden. Tatsächlich nicht mehr aufgelistet werden ausgeblendete Objekte nur, wenn der entsprechende Filter in den Verzeichnis-Browser-Option eingeschaltet ist. Wenn Sie doch noch aufgelistet werden, dann in grauer Farbe, und die Ausblendung kann dann gezielt mit dem Kontextmenü des Verzeichnis-Browsers oder durch Drücken von Umsch+Entf wieder aufgehoben werden.

Duplikate in Liste finden: s. Duplikaterkennung

Nach Duplikaten filtern

Ability to filter for duplicates of a single selected file that are also currently listed in the directory browser, only if a hash value is available for the selected file and the other files. Actually filters for that hash value at that time, and thus does not depend on previous mass identification of duplicate files using the above-mentioned command “Duplikate in Liste finden”. In X-Ways Investigator the actual hash values are not displayed and cannot be computed, but they are imported from evidence file containers that come with hash values for files and can be used to

identify duplicate files.

Nach Ähnlichem filtern

Nutzt den Strukturtyp-Filter, um Dateien desselben Typs zu finden, die wahrscheinlich ungefähr zur gleichen Zeit von derselben Applikation oder vom selben Gerät mit denselben Einstellungen oder für denselben Zweck o. ä. erzeugt wurden. Diese Funktionalität wird verfügbar, wenn die Strukturtyp-Spalte befüllt wurde, für unterstützte Dateitypen.

In Suchtrefferlisten können Sie

1. *ausgewählte* Suchtreffer permanent löschen,
2. *doppelte* Suchtreffer permanent löschen. Suchtreffer werden als identisch/doppelt eingestuft, wenn sie entweder den gleichen physischen Offset haben oder, falls kein physischer Offset angegeben ist, wenn ihr logischer Offset und die zugehörige interne Datei-ID gleich sind. Im Zweifelsfall behält X-Ways Forensics den längeren Suchtreffer (weil "Meierhoff" z. B. wertvoller ist als "Meier") and bevorzugt Suchtreffer in existierenden Dateien.
3. Vergrößern: Erlaubt das Ändern der Größe und der Position der ausgewählten Suchtreffer. Wenn Sie z. B. nach einer Signatur suchen, die Datensätze in einer Datenbank identifiziert, und Sie erhalten viele Treffer mit dieser Signatur, aber Sie interessieren sich eigentlich für die Daten, die hinter der Signatur folgen und möchten diese exportieren, dann können Sie nun Offsets und Länge all dieser Suchtreffer nun auf einen Schlag geeignet anpassen. Nützlich auch beim Exportieren von Suchtreffern; dabei kann dann auf Wunsch der Suchtreffer selbst größer exportiert und der Kontext drumherum ggf. entfallen. Die Wirkung wird sofort sichtbar in der Kontextvorschau der Suchtrefferliste (aber nicht unbedingt sofort in der Hervorhebung in der unteren Hälfte des Datenfensters).
4. Mit einem weiteren Befehl können Sie Suchtreffer in ausgegliederte Dateien konvertieren. Das ist nützlich, wenn Sie die Suchtreffer als Dateien in einem Bericht ausgeben möchten, mit einem Vermerk oder Kommentar versehen oder ausdrucken möchten, Wiederherstellen/Kopieren darauf anwenden möchten o. ä. Beachten Sie, dass Suchtreffer, die sowohl einen physischen als auch einen logischen Offset haben, auf Sektor-Ebene ausgegliedert und im virtuellen Verzeichnis für gecarvete Dateien ausgegeben werden. Suchtreffer, die nur einen logischen Offset haben, werden innerhalb der Datei, in der sie gefunden wurden, ausgegliedert, und erscheinen als Unterobjekt. Suchtreffer im decodierten Text einer Datei sowie Suchtreffer in Verzeichnis-Browser-Spalten können nicht auf diese Weise in Dateien umgewandelt werden, sondern werden von dieser Funktion ignoriert.
5. Anderem Suchbegriff zuweisen: Sie haben nun die Möglichkeit, Suchtreffer zu kategorisieren, indem Sie sie separaten Suchbegriffen zuordnen. Wenn Sie z. B. mehrere relevante Treffer für den Suchbegriff "Rechnung" erhalten und einige Treffer in anderer Weise relevant sind als andere, können Sie diese anderen Suchbegriffen zuordnen wie "Rechnung ABC GmbH" oder "Rechnung XYZ AG" usw. Die so neu erzeugten Suchbegriffe erscheinen in der Suchtrefferliste, auch wenn nie wörtlich nach ihnen selbst gesucht wurde, und haben eher die Funktion von Kategorien.

Navigation

Befehle in diesem Untermenü erlauben u. a. das Sortieren von Dateien nach ihrer vermuteten generischen Relevanz (s. Metadaten-Extraktion) oder das Vermeiden von Wartezeit, wenn eine bestimmte Sortierung gar nicht benötigt wird.

Die Gruppe der Befehle im Navigationsmenü ermöglicht auch Interaktionen mit den aktuell ausgewählten Dateien auf einer eher technischen Ebene. Es ermöglicht, direkt die Datenstruktur im Dateisystem aufzusuchen, an der die betreffende Datei definiert ist (z. B. FILE-Record in NTFS, Inode in Ext2/Ext3/Ext4, Verzeichnis-Eintrag in FAT).

Im Navigationsmenü kann man sich außerdem eine Liste aller Cluster anzeigen lassen, die der gewählten Datei bzw. dem gewählten Verzeichnis zugeordnet sind. Diese Cluster-Liste kann per Kontextmenübefehl in eine Textdatei exportiert werden. Die Liste kann optional stark gekürzt und ihre Erstellung stark beschleunigt werden, indem die Cluster mitten in einem Fragment ausgelassen und durch Zeilen mit drei Punkten repräsentiert werden. Diese Option können Sie ebenfalls im Kontextmenü des Cluster-Listen-Fensters finden. Sie wirkt sich erst auf das nächste erzeugte Fenster aus. Die Kompaktfassung ist nützlich, wenn Sie sich lediglich dafür interessieren, von wo bis wo sich jede zusammenhängende Reihe von Clustern (=jedes Fragment der Datei) erstreckt.

Übergeordnetes Objekt aufsuchen: Navigiert zum Elternobjekt des gewählten Objekts und wählt es aus, genau wie das Drücken der Rücktaste. Dabei kann das Unterobjekt ein gewöhnliche Datei in einem Verzeichnis sein, oder eine E-Mail in einem E-Mail-Archiv oder ein Dateianhang zu einer E-Mail oder ein Bild in einem Dokument oder eine Datei in einem komprimierten Archiv usw.

Zugehöriges Objekt aufsuchen: Dieser Befehl erlaubt das bequeme Auffinden des sog. zugehörigen Objekts, wenn so etwas für die ausgewählte Datei bzw. das ausgewählte Verzeichnis existiert. Alternativ können Sie auch die Tasten Umschalt+Rücksetz betätigen.

Gewähltes Objekt in dessen Verzeichnis: Zeigt Ihnen die ausgewählte Dateien oder das ausgewählte Verzeichnis in der Umgebung ihrer/seiner Geschwister. Das kann hilfreich sein, um schnell zu überprüfen, ob es noch weitere relevante Dateien im selben Verzeichnis gibt oder um die Funktion einer Datei besser zu verstehen, wenn Sie sie in ihrem Umfeld/Kontext sehen.
Gewähltes Objekt aus Sicht des Stammverzeichnisses: Zeigt Ihnen die ausgewählte Datei inmitten aller Dateien des betreffenden Volumes, rekursiv vom Stammverzeichnis des Dateisystems aus erkundet. Sinnvoll z. B., um herauszufinden, ob es Dateien mit demselben Namen, derselben ID (könnten Vorgängerversionen aus einer Volume-Shadow-Copy sein), demselben Besitzer oder Absender oder mit ähnlichen Zeitstempeln o. ä. im selben Dateisystem gibt (dazu einfach entsprechend sortieren).
Beide Befehle können auch vom Asservat-Überblick-Fenster und von Suchtrefferlisten aus aufgerufen werden (so dass der frühere Befehl "Zu dieser Datei im Verzeichnis-Browser" überflüssig wird). Beachten Sie, Sie können durch einen Klick auf den Zurück-Schalter in der Symbolleiste bequem zur vorherigen Sicht zurückkehren!

"Pfad aufsuchen" navigiert zu einer Datei oder einem Verzeichnis mit dem von Ihnen angegebenen Pfad. "Int. ID aufsuchen" lokalisiert das Objekt mit der angegebenen internen ID, egal ob Datei oder Verzeichnis. Wenn ein Filter das Auflisten dieses Objekts verhindert, wird der Filter automatisch deaktiviert. "Eintrag Nr. aufsuchen" springt zu dem Objekt mit der angegebenen Position in der aktuellen Liste. Die Positionen eines jeden Objekts sehen Sie, wenn Sie mit Mauszeiger über dem Icon einer Datei oder eines Verzeichnisses verharren.

Kategorisierung

Dateien im Datei-Überblick werden standardmäßig als unbekannt angesehen. Dieser Zustand kann sich ändern zu irrelevant, beachtenswert oder nicht kategorisiert durch einen Abgleich mit einer Hash-Datenbank, durch Einsatz einer X-Tension, durch Übernahme von Daten aus Datei-Containern, durch Verwendung dieses Untermenüs und auf anderen Wegen. Der Status ist in der Spalte "Kategorisierung" sichtbar.

Datei-Überblick erweitern, Parallele Suche, X-Tensions ausführen

Diese Befehle sind vom Hauptmenü bekannt. Vom Verzeichnis-Browser-Kontextmenü aus können Sie auf ausgewählte Dateien angewandt werden.

In Hash-Datenbank aufnehmen

Erzeugt ein Hash-Set der aktuell ausgewählten Dateien und Verzeichnisse und ihrer Unterverzeichnisse direkt in der internen Hash-Datenbank, entweder in Form von normalen Datei-Hash-Werten oder in Form von Block-Hash-Werten oder PhotoDNA-Werten. Für normale Hash-Werte gibt es eine Option to create multiple hash sets in a single step, where the hash values of the selected files are put into hash sets that are named after each file's report labels (Vermerke). This is useful if you categorize notable files in one case using labels (e.g. based on different types of CP), and wish to quickly identify the same files again in other cases later, and automatically see the category that you had originally assigned, as the hash set name.

The checkbox for that is labelled "Name after labels, if any". If a selected file does not have any labels, its hash value will be assigned to the hash set named as you specify, just like if you do not check that checkbox.

This command can also be used to create a separate file with PhotoDNA hash values of the selected files or to just update file descriptions of files in the PhotoDNA hash database with the comments stored in the volume snapshot.

Externe(s) Datei/Verz. anhängen

Erfordert eine forensische Lizenz. Ermöglicht es, eine oder mehrere externe Dateien oder ein Verzeichnis mitsamt Unterverzeichnissen in den Datei-Überblick einzubinden und von X-Ways Forensics wie normale Dateien im Datei-Überblick weiter verarbeiten zu lassen. Nützlich, wenn Originaldateien z. B. übersetzt, konvertiert oder entschlüsselt werden müssen und das Ergebnis wieder in den ursprünglichen Datei-Überblick aufgenommen werden soll, im Originalpfad, zur weiteren Untersuchung, zur Aufnahme in den Bericht, zum Filtern, für Suchläufe usw. Sobald sie eingebunden sind, werden solche Dateien vollständig von X-Ways Forensics verwaltet, und ihr Inhalt wird dazu ins interne Asservat-Unterverzeichnis des Falls kopiert, so dass die Quelldateien entfernt werden können.

You will be asked to classify the files that you are attaching as what they actually are, e.g. video stills produced outside of X-Ways Forensics, e-mails extracted from e-mail archives outside of X-Ways Forensics, OLE2 objects, attachments of various kinds (in particular of PDF documents), etc. etc. If properly classified as video stills, the attached pictures will be used as

previews for the respective parent video file for example. The classification can be seen in the Description column.

Beim Anhängen einer einzigen Datei und gedrückt Halten der Umschalt-Taste schlägt X-Ways Forensics einen neuen Dateinamen vor, der auf dem Namen der ausgewählten Datei basiert, und die Datei wird im selben Verzeichnis eingefügt. Andernfalls werden die externen Namen der Dateien übernommen, und die Dateien werden Unterobjekte des gewählten Objekts. Späteres Umbenennen der virtuellen Dateien im Datei-Überblick ist immer noch möglich.

Wenn Sie ein externes Verzeichnis anhängen, werden Sie gefragt, ob das Verzeichnis selbst auch angehängt werden soll oder nur sein Inhalt. Normalerweise erzeugt X-Ways Forensics virtuelle Dateien in Unterverzeichnissen in neuen virtuellen Verzeichnissen im Datei-Überblick. Es gibt aber auch die Möglichkeit, die Dateien in existierenden Verzeichnissen im Datei-Überblick gleichen Namens unterzubringen, an derselben Stelle im Verzeichnisbaum. Nützlich, wenn Sie eine ganze Verzeichnisstruktur aus einem Image herauskopieren, um Dateien außerhalb von X-Ways Forensics zu konvertieren, zu entschlüsseln, zu übersetzen usw., wenn Sie das Ergebnis anschließen in den Datei-Überblick zurück übernehmen und die bearbeiteten Dateien neben ihren jeweiligen Original-Gegenstücken sehen möchten, in den entsprechenden Unterverzeichnissen. Dies kann z. B. hilfreich sein, wenn Sie PDF-Dokumente, die X-Ways Forensics Ihnen als nicht durchsuchbar meldet, mit Adobe Acrobat einer Texterkennung (OCR) unterwerfen möchten.

X-Ways Forensics can optionally adopt the timestamps of attached files in the volume snapshot (creation, modification and/or access). You can make use of this if you are sure that the timestamps are original and not the result of any of your own file copy/decoding/decryption activity etc.

Umbenennen

Erlaubt es, virtuelle Verzeichnisse und virtuell angehängte Dateien im Datei-Überblick umzubenennen, oder sogar normale Dateien, wenn die Umschalt-Taste gedrückt ist. Auch wenn letzteres im Zusammenhang mit Asservaten nicht unbedingt forensisch einwandfrei ist, kann es doch in speziellen Situationen hilfreich sein, z. B. wenn ein Dateiname oder Verzeichnisname zu lang ist, um die Datei aus einem Image herauszukopieren o. ä. Der Originalname wird weiterhin als alternativer Dateiname angezeigt. Beachten Sie, dass dieser Befehl eine Datei nicht im Dateisystem umbenennt (auf dem Datenträger und im Image wird nichts verändert!), sondern nur im Datei-Überblick, also in der internen Datenbank in X-Ways Forensics *über* das Dateisystem. Sie haben auch die Möglichkeit, direkt den alternativen Namen zu setzen, indem Sie beim Umbenennen die Umschalt-Taste gedrückt halten (in dem Moment, in dem Sie den OK-Schalter drücken).

Typ angeben

Ability to specify the type of selected files yourself. Useful if you wish to identify types or subtypes in an individual way unknown to X-Ways Forensics, for example to be able to filter by these types later. For instance, how about categorizing TIFF pictures that are digitally stored faxes as type "fax"? Remember you can define your own file types in File Type Categories.txt.

Vergrößern

Files found through a file header signature search and files that were carved within other files can be manually redefined by the user. You can reposition such files with a relative offset change (+/-), and/or to resize them, with either an absolute new size or with a positive or negative relative size adjustment (click the arrow button to toggle). You can resize multiple files at the same time with the same settings.

Sicheres Löschen

Die Daten von Dateien und Verzeichnisse, die im Verzeichnis-Browser ausgewählt sind, können in WinHex (nicht X-Ways Forensics) sicher getilgt werden. Die Daten im logischen Teil einer Datei (d. h. nicht die Daten im Dateischlupf) und die Daten in Clustern eines Verzeichnisses (die etwa in NTFS INDX-Puffer enthalten und in FAT Verzeichniseinträge) werden gelöscht/überschrieben mit einem vom Benutzer gewählten Hex-Wert-Muster. Der Existenzstatus einer Datei im Dateisystem ändert sich dadurch nicht, d. h. die Datei wird nicht als gelöscht markiert, die Cluster werden nicht freigegeben usw.. Keine Dateisystem-Metadaten werden aktualisiert, weil keine Datei-Schreibbefehle auf Betriebssystemebene dabei zum Einsatz kommen. Keine Dateisystem-Datenstrukturen ändern sich, keine Dateinamen werden gelöscht, nur Inhalte von Dateien werden überschrieben. Die einzige Ausnahme gibt es für NTFS: FILE-Records der ausgewählten Dateien in der MFT können optional zusätzlich gelöscht werden. Dateien, die in Archiven komprimiert sind, und generell Dateien innerhalb von anderen Dateien (z. B. E-Mails und Datei-Anhänge in E-Mail-Archiven) können nicht gelöscht werden. Ehemals existierende Dateien, deren Cluster bekanntermaßen für andere Dateien wiederverwendet wurden, werden nicht gelöscht. Beachten Sie, dass durch das Überschreiben von gelöschten Dateien u. U. Daten in Clustern gelöscht werden, die bereits zu anderen Dateien gehören. Daher wählen Sie besser nur existierende Dateien aus, wenn Sie das vermeiden möchten (konsistente Dateisysteme vorausgesetzt). Beachten Sie auch, dass Sie beim Löschen von aus Sektoren per Signatursuche ausgegliederte Dateien u. U. zu viel oder nicht genug Daten überschreiben, je nach erkannter/geschätzter Dateigröße und anhängig davon, ob die Dateien ursprünglich fragmentiert waren oder nicht. Und beachten Sie bitte, dass das sichere Löschen eines Verzeichnisses, d. h. Überschreiben der Daten in den Clustern, die dem Verzeichnis zugeordnet sind, zum Verwaisen von existiernden Dateien in dem Verzeichnis führt. Eine typischere Vorgehensweise mit dieser Funktion wäre das bloße sichere Löschen der Inhalte von Dateien, nicht das sichere Löschen der Daten eines Verzeichnisses, wenn mit dem Dateisystem noch weiter gearbeitet werden soll.

Nützlich z. B., wenn Sie Kopien von Images an Ermittler oder andere mit dem Fall befasste Personen weitergeben, die die Inhalte bestimmter Dateien nicht sehen dürfen. Auch nützlich, wenn Sie Datenträger, auf denen Kipo gefunden wurde, an den Besitzer zurückgeben müssen, nachdem die betreffenden Dateien gelöscht wurden. Außerdem nützlich, wenn Sie Images für Schulungszwecke präparieren, die Sie veröffentlichen möchten und in denen Sie urheberrechtlich geschützte Dateien (z. B. Betriebssystem-Dateien oder Anwendungsprogramme) nachträglich überschreiben wollen..

Sowohl erfolgreich gelöschte Dateien als auch Dateien, die nicht erfolgreich gelöscht wurden, werden beim Arbeiten mit einem Fall (nur mit forensischer Lizenz) mit geeigneten Vermerken ausgestattet, nach denen Sie filtern können, um das Ergebnis zu überprüfen.

Treffer als wichtig kennzeichnen

Kennzeichnet in einer Suchtrefferliste ausgewählte Treffer mit einer gelben Flagge und fügt sie der Liste wichtiger Treffer hinzu. Sie können auch die Leertaste drücken, um einen Suchtreffer als wichtig zu kennzeichnen oder diese Kennzeichnung wieder aufzuheben. Wenn Sie bei Aufruf des Menübefehls die Umschalttaste gedrückt halten, wird die Kennzeichnung bei allen ausgewählten Suchtreffern wieder entfernt.

Im Bericht ausgeben

Markiert in einer Suchtrefferliste ausgewählte Treffer mit einem grünen Gitter, so dass sie in den Fallbericht mit aufgenommen werden können.

Hexadezimal

In einer Suchtrefferliste haben Sie die Möglichkeit, Suchtreffer mitsamt ihrem Kontext in hexadezimaler Schreibweise anzuzeigen. Das kann speziell für technische Suchen nützlich sein, also nicht Stichwortsuchen in einer natürlichen Sprache, sondern Suchen nach Header-Signaturen, Trennzeichen, binären Markern usw. Diese Option wirkt sich auch auf die Ausgabe von Suchtreffern mit dem Befehl "Liste exportieren" aus.

4.2 Kontextmenü des Falldatenfensters

Einige der Befehle:

Teilbaum exportieren: Dieser Kontextmenübefehl im Falldatenfenster erlaubt es, eine pseudographische Darstellung des gewählten Teilbaums als Unicode-Textdatei auszugeben, die am besten mit einer Schriftart mit fixer Zeichenbreite einzusehen ist. Der exportierte Baum repräsentiert Unterverzeichnisse in ihrem aktuellen Zustand (aus- oder eingeklappt). Der Menübefehl ist für Asservate verfügbar und auch für Verzeichnisse, sofern Sie die Strg-Taste beim Anklicken eines Verzeichnisses im Fallbaum mit der rechten Maustaste gedrückt halten. Denken Sie daran, wenn Sie einen Teilbaum komplett rekursiv ausklappen möchten, können Sie dazu die Wurzel dieses Teilbaums anklicken und die Multiplikationstaste auf dem Nummernblock der Tastatur drücken.

Externe Dateien anhängen: This command allows to attach external files as child objects to their original counterparts (after decrypting, translation, convertion, OCRing, ...) in multiple evidence objects at the same time automatically if they are named after the unique ID of the original files. (The filename extension is ignored.) You can name the files after the unique ID when you copy them off the image with the Recover/Copy command, and you do not need to preserve the path, as the unique ID already fully identifies the file. Useful if you wish to apply external tools to the copied files which have problems with overlong paths, if you wish to bring back the result into the volume snapshot.

When attaching external files (e.g. after decrypting, converting, translating, ...), you are given four options:
1) the attached file can become a child object of the original file

or
2) the attached file can become a sibling of the original file (shown next to it, in the same directory)
or
3) the attached file can replace the original file (original file no longer present)
or
4) the attached file can replace the original file, and the original file can become a child object of the new file if still needed.
You can select the attachment method separately for ordinary files and e-mail attachments. The three latter methods are particularly useful for e-mail attachments because only direct child objects of .eml files are embeddedd in the parent .eml file when recovering/copying those .eml files. So if you would like to have the decrypted/converted/translated version of an attachment embedded in the .eml file, that version should not become grandchild object. If you want original and new version both to be embedded, make them siblings. If you do not need the original version embedded, replace it completely or preserve it only as a child object of the new version (i.e. grandchild of the .eml file).

The attached files adopt the classification of the original files, e.g. as extracted e-mail messages or OLE2 objects. If the original files have no special classification, the attached files will be simply marked as attached files.

Datei-Export zur Analyse: Dieser Menübefehl im Falldatenfenster kann auf den gesamten Fall und von dort aus auf ausgewählte Asservate oder auf das aktive Asservat angewandt werden. Er bedient die Schnittstelle zur externen Analyse von Dateien durch automatisierte Tools.

Es gibt auch für Verzeichnisse ein Kontextmenü. Dieses erscheint beim Rechtsklick in Abhängigkeit von den Einstellungen in den Allg. Optionen und vom gedrückt Halten der Umschalttaste. Andernfalls führt ein Rechtsklick auf ein Verzeichnis zu dessen rekursiver Erkundung.

4.3 Kontextmenü des Datenfensters

Wenn Sie in der Hex-Editor-Anzeige (bestehend aus Offset-Spalte, Hex-Spalte, Text-Spalte) einer Datei oder eines Datenträgers rechtsklicken, erhalten Sie ein Kontextmenü, mit dem Sie die Grenzen des Blocks definieren (Anfang und Ende) sowie einige weitere Befehle ausführen können, die sich auf den Block beziehen:

Hinzufügen zu Eigene Suchtreffer: Nur mit forensischer Lizenz. Möglichkeit zum manuellen Definieren von Suchtreffern. Immer dann, wenn Sie auf relevanten Text stoßen, sei es irgendwo mitten im freien Speicher im Modus Disk/Partition/Volume oder innerhalb einer bestimmten Datei im Modus Datei, können sie ihn als Block auswählen und dann per Rechtsklick als sogenannten "eigenen Suchtreffer" den "herkömmlichen" (d. h. vom Programm selbst gefundenen) Suchtreffern hinzufügen. Sie können eigene Suchtreffer zu beliebig benannten Suchbegriffen (Kategorien) zuweisen. Wenn z. B. das, was Sie gefunden haben, mit dem Beschuldigten A zu tun, können Sie einen Suchbegriff wählen, der nach A benannt ist. Wenn auch mit Beschuldigten B zusammenhängend, dann auch erneut zu einem weiteren Suchbegriff

(was dann später UND-Kombinationen erlaubt). Sie können eigene Suchtreffer auch "echten" Suchbegriffen zuweisen, die Sie bei einer automatischen Suche verwendet haben.
Eigene Suchtreffer können bequem in Suchtrefferlisten aufgelistet und von dort auch schön exportiert werden, genau wie herkömmliche (automatisch erzeugte) Suchtreffer. Zur besseren Kenntlichmachung und Unterscheidung von herkömmlichen Suchtreffern werden eigene Suchtreffer in der Beschreibungsspalte für Suchtreffer mit einem Stern (*) versehen. Sie können die richtige Codepage für eigene Suchtreffer selbst angeben, wenn Sie sie definieren, was notwendig sein kann, damit der Text auch in der Suchtrefferliste korrekt angezeigt wird. Eigene Suchtreffer werden mit Verweis auf ein Objekt im Datei-Überblick gespeichert, wenn Sie sie im Modus Datei definieren. Eigene Suchtreffer sind vorwärtskompatibel, d. h. ältere Versionen (v16.2 und neuer) können solche in v16.6 erzeugten Suchtreffer auch sehen.

Block als virtuelle Daten hinzufügen: Nur mit forensischer Lizenz. Siehe Bearbeiten-Menü.

Position hinzufügen: Erlaubt es Ihnen, sich an eine bestimmte Position, wie vom aktuell definierten Block angegeben, zu erinnern, entweder mit Hilfe des Allgemeinen Positions-Managers oder mit dem Positions-Manager des Asservats (wenn Sie mit einem Fall arbeiten und einen Block rechts anklicken, der in einem Asservat definiert ist; nur mit forensischer Lizenz). Erleichtert das Wiederauffinden derselben Position zu einem späteren Zeitpunkt, und kann dafür verwendet werden, die Struktur von Dateien oder Datensätzen eines bestimmten Formats, das Sie analysieren, schön farblich hervorzuheben und mit Hilfe von Tooltips zu erklären.

Wenn Suchtreffer im Dateimodus farblich hervorgehoben werden (s. Allgemeine Optionen), können Sie sie auch über das Kontextmenü löschen.

Sie können von hier aus auch das vollständige Bearbeiten-Menü erreichen.

4.4 Datei-Menü

Neu: Hier können Sie eine neue Datei anlegen. Es ist die gewünschte Größe der Datei in Bytes anzugeben (>0). Die neue Datei wird prinzipiell im Standard-Editiermodus geöffnet. Neu erzeugte Dateien können von WinHex optional bevorzugt im Speicher gehalten werden statt in einer temporären Datei auf einem Datenträger, aus Gründen der Performanz oder wegen nicht ausreichend zur Verfügung stehender Speicherkontingente oder aus Sicherheitsgründen. Wenn das Kontrollkästchen dafür ganz gewählt ist, signalisiert das, dass der Benutzer auf der Datenhaltung im Speicher besteht und dass die Funktion fehlschlagen soll, wenn nicht genügend Arbeitsspeicher verfügbar ist (oder kein ausreichend großer zusammenhängender Adressbereich im Fall der 32-Bit-Version). Dieselbe Einstellung wirkt sich auch aus auf das Einfügen von Daten aus der Zwischenablage in eine neue Datei über Bearbeiten | Zwischenablage | In neue Datei einfügen. Für eine neu angelegte im Speicher gehaltene Datei zeigt die Informationsspalte die Pufferadresse im logischen Speicheradressraum des Prozesses statt eines Pfades an. Bitte beachten Sie: Die Daten, mit denen Sie auf diese Weise hantieren, könnten immer noch von Windows auf einen Datenträger geschrieben werden, z. B. als Teil von pagefile.sys. Wenn es Ihr Ziel ist, Datenträger-Schreibvorgänge und die Verwendung von temporären Dateien zu vermeiden, möchten Sie vermutlich außerdem Datei-Sicherungen für die Rückgängig-Funktion abschalten unter Optionen | Rückgängig.

In X-Ways Forensics können Sie optional auch ein Platzhalter-Segment für .e01-Images erzeugen.

Öffnen: In einem Dateiauswahlfenster wählen Sie eine oder mehrere Dateien aus, die Sie mit dem Hex-Editor einsehen oder bearbeiten möchten. Sofern Sie nicht im Optionen-Menü programmweit den Direkt-Editier-Modus eingestellt haben, können Sie einen der drei Editier-Modi zum Öffnen der Datei(en) wählen.

Also allows to open physical disks, partitions and volumes as a file, by clicking a button labeled "Device..." in the file selection dialog. You can enter a device path such as
\\.\PhysicalDrive1 (for hard disk 1)
\\?\Volume{12345678-9abc-11a1-abcd-0123456789ab} (for a volume with that GUID)
\\.\C: (for a volume mounted as drive letter C:)
This functionality allows to open volumes that are not mounted as drive letters. To get an overview of volumes known to Windows, type "mountvol" in a command prompt window. You can also try to open exotic devices supported by Windows such as tapes and changers (not tested). Also this is how you can open alternate data streams whose path and name you know, which cannot be opened through the ordinary File | Open dialog, without opening the volume on which they reside.

Opening a hard disk as a file can be useful for example if you wish to clone that disk and if source and destination disk have different sector sizes (whether it makes sense in the first place to clone a hard disk despite the sector mismatch depends on the data). When treated as a file, there is no defined sector size and hence no possibility for a sector size mismatch. Device files can also be interpreted as disks like images can.

Speichern: Hier speichern Sie ein zuvor geöffnete Datei mit allen von Ihnen vorgenommenen Änderungen, nachdem Sie eine Sicherheitsabfrage mit „Ja“ beantwortet haben. Im In-Place-Editiermodus ist das Aufrufen dieses Befehls nicht notwendig. Beim Benutzen des Disk-Editors heißt dieser Befehl „Auf Disk schreiben“.

Speichern unter: Speichert eine Datei unter einem neuen Namen oder in einem anderen Ordner. Existiert bereits eine Datei mit diesem Namen, so werden Sie gefragt, ob die vorhandene Datei überschrieben werden soll.

Datenträger-Sicherung/Sicherung anlegen: s. u. „Sicherungen“

Minimalsicherung erstellen/überprüfen: s. u. „Minimalsicherungen“

Sicherung wiederherstellen: Wählen Sie eine Image-Datei aus, deren Inhalt (Datenträger-sektoren) Sie zurückspielen möchten auf den ursprünglichen oder einen anderen Datenträger, oder wählen Sie eine WinHex-Sicherungsdatei (.whx-Datei) aus, deren Inhalt (eine Datei oder Datenträger-Sektoren) Sie wiederherstellen möchten. Im Fall eines Images wird das Image als Quelle im Dialog "Datenträger klonen" voreingestellt (mit Specialist-Lizenz oder höher im interpretierten Zustand). Ohne Specialist-Lizenz oder höher können segmentierte WinHex-Sicherungsdateien wiederhergestellt werden, aber keine segmentierte Roh-Images.

Sicherungs-Manager: s. dort

Ausführen: Führt die aktuell dargestellte Datei mit allen evtl. vorgenommenen Änderungen aus. Es muss sich entweder um eine unter DOS oder Windows ausführbare EXE- oder COM-Datei handeln oder der Dateityp muss unter Windows mit einer Anwendung verknüpft worden sein. Dann wird dieses Programm gestartet und die aktuelle Datei geladen. Sie können mit dieser Funktion z. B. überprüfen, ob die vorgenommenen Änderungen in einer Programmdatei ihre Ausführbarkeit beeinträchtigt haben.

Drucken: Mit dieser Funktion können Sie einen Ausschnitt aus einer Editierfenster drucken. Geben Sie den Druckbereich in Form von Offsets an. Sie haben die Möglichkeit, einen Drucker auszuwählen und ihn einzurichten.
Bestimmen Sie den Zeichensatz für den Druck, ändern Sie ggf. die vorgeschlagene Schriftgröße und tragen Sie auf Wunsch einen Kommentar, der am Ende des Ausdruckes erscheinen soll, in das dafür vorgesehene Feld ein. Die empfohlene Schriftgröße berechnet sich als Druckauflösung (z. B. 720 dpi) geteilt durch 6 (z. B. 120).
Wenn Ihnen das Drucken mit WinHex nicht flexibel genug ist, können Sie auch einen Block definieren, ihn mit „Bearbeiten->Kopieren->Editoranzeige“ als Hex-Editor-formatierten Text in die Zwischenablage kopieren und in einem Textverarbeitungsprogramm weiterverwenden. Dort eignet sich dann besonders die Schriftart „Courier New“, Größe 10, zum Ausdruck auf DIN A4.

Eigenschaften: Hier können die Größe, Datum und Uhrzeit der Erzeugung, der letzten Änderung und des letzten Zugriffs sowie Attribute einer Datei oder eines Verzeichnisses in Ihrem eigenen Windows-System eingesehen und auch geändert werden. Änderbare Attribute sind A (zu archivierend), S (System), H (versteckt), R (schreibgeschützt), X (nicht zu indexieren), T (temporär) und ~ (sparse). Nach Eingabe neuer Werte in einem der drei Bereiche betätigen Sie den Eingabe-Schalter, damit die Änderungen in Kraft treten. Durch Klick auf den Schalter mit dem drei Punkten wählen Sie eine Datei aus, oder Sie geben Pfad und Name direkt in das Editierfeld daneben ein und drücken dann die Eingabe-Taste. Letzteres funktioniert auch, wenn Sie die Eigenschaften von Verzeichnissen abfragen oder ändern möchten.
Bitte beachten Sie, dass das Setzen oder Entfernen des Sparse-Attributs nicht notwendigerweise den Allokationszustand von bereits zugewiesenen Clustern ändert. Es hat jedoch definitiv einen Effekt, wenn Sie die betreffende Datei vergrößern durch Setzen einer größeren Dateigröße im selben Dialogfenster.

Verzeichnis öffnen: Öffnet ein Fenster das ein Verzeichnis Ihres eigenen Computers repräsentiert und Sie all dessen Dateien und Unterverzeichnisse sehen lässt.

Dateien öffnen: Wählen Sie einen Ordner aus, dessen Dateien Sie öffnen möchten. Wahlweise werden auch die Dateien in untergeordneten Ordnern berücksichtigt. Sie können Dateifilter verwenden (z. B.„w*.exe;x*.dll“) und einen Editiermodus auswählen, wenn Sie in WinHex nicht schon im Optionen-Menü den Nur-Lesen-Modus oder In-Place-Modus eingestellt haben. Optional werden nur solche Dateien geöffnet, die einen bestimmten Text oder bestimmte Hex-Werte enthalten. In diesem Fall stehen Ihnen noch weitere Suchoptionen zur Verfügung.

Geänderte speichern: All die von WinHex geöffneten Dateien, an denen Änderungen

vorgenommen wurden, werden mit ihrem aktuellen Inhalt gespeichert. Es erfolgen keine weitere Sicherheitsabfragen. Daher ist diese Funktion „mit Vorsicht zu genießen“.

Alle speichern: Sämtliche von WinHex nicht im Nur-Lesen-Modus geöffneten Dateien werden mit ihrem aktuellen Inhalt gespeichert. Es erfolgen keine weitere Sicherheitsabfragen.

Beenden: Hier können Sie WinHex schließen. Sie erhalten noch einmal die Möglichkeit, Änderungen an Dateien und Datenträgern zu speichern.

4.5 Bearbeiten-Menü

Rückgängig: Erlaubt Ihnen, Tastatureingaben und die Anwendung sonstiger Funktionen ungeschehen zu machen. Dazu müssen die entsprechenden Optionen aktiviert sein.

Ausschneiden: Bewirkt, dass der aktuelle Block aus der Datei entfernt und in die Zwischenablage kopiert wird. Der dahinter liegende Teil der Datei wird entsprechend vorgezogen.

Block/Alles/Sektor kopieren

- **normal:** Kopiert den markierten Block bzw. den gesamten Dateiinhalt bzw. den aktuellen Sektor in die Zwischenablage, so dass er später wieder eingefügt werden kann.
- **als Unicode/ANSI**: Specifically copies text from the text column as UTF-16 Unicode even when the text column is not displayed in Unicode, or specifically as ANSI-encoded text even when the text column is not displayed as ANSI ASCII.
- **in neue Datei:** Kopiert die Daten direkt in eine neue Datei (nicht über den Umweg Zwischenablage). Mit dieser Funktion kann man z. B. beliebige Daten von einem Datenträger schnell in Dateien umwandeln.
- **Hex-Werte:** Kopiert die Daten im Hexadezimal-Format in die Zwischenablage.
- **Editoranzeige:** Kopiert die Daten als Text so formatiert in die Zwischenablage, wie sie auch im Hex-Editor erscheinen, d. h. mit eine Offset-, einer Hex- und einer ASCII-Text-Spalte.
- **GREP-Hex:** Kopiert die Daten als Hex-Werte in GREP-Syntax.
- **C/Pascal-Quellcode:** Kopiert die Daten im C/Pascal-Quelltext-Format in die Zwischenablage.

Zwischenspeicher einfügen: Fügt den Inhalt der Zwischenablage, sofern er in einem kompatiblen Format vorliegt, an der aktuellen Cursorposition ein. Der Teil der Datei, der dahinter liegt, wird hinter die Einfügung versetzt.

Zwischenspeicher schreiben: Überträgt den Inhalt der Zwischenablage an die aktuelle Cursorposition und *überschreibt* dabei die Bytes der Datei, die dahinter folgen. Falls dabei das Dateiende erreicht wird, wird die Datei so weit wie erforderlich verlängert, damit die Daten Platz finden.

Zwischenspeicher in neue Datei schreiben: Legt eine neue Datei mit dem aktuellen Inhalt der Zwischenablage an.

Zwischenspeicher freigeben: Löscht den Inhalt der Zwischenablage gibt den von ihm genutzten

Teil des Arbeitsspeichers wieder frei.

Entfernen: Löscht den aktuellen Block aus der Datei. Der hintere Teil der Datei wird dann entsprechend vorgezogen. Der gelöschte Block wird *nicht* in die Zwischenablage kopiert. Wenn in allen geöffneten Dateien der Block gleich definiert ist (also an den gleichen Offsets beginnt und endet), können Sie diese Funktion wahlweise auch auf alle geöffneten Dateien anwenden.

Nullbytes einfügen: Lässt Sie eine bestimmte Anzahl von Bytes mit dem Wert Null an der aktuellen Cursor-Position einfügen.

Block als virtuelle Datei einfügen: (nur mit forensischer Lizenz) Wenn Sie manuell einen Block im Modus Volume/Partition/Disk/Datei definiert haben, können Sie ihn mit diesem Befehl dem Datei-Überblick als „herausgemeißelte“ (gecarvete) Datei im extra dafür vorgesehenen virtuellen Verzeichnis hinzufügen bzw. im Fall des Datei-Modus als Unterobjekt der Originaldatei. Nützlich, wenn Sie Daten in bestimmten Bereichen (wie im freien Speicher gefundenem HTML-Code oder E-Mails) als Datei behandeln möchten, um sie einsehen, gezielt durchsuchen oder kommentieren zu können oder um sie einem Bericht hinzuzufügen. Wenn Sie manuell eine Datei innerhalb einer anderen Datei im Modus Datei "herausmeißeln" (carven), wird die resultierende Datei in der Attr.-Spalte als Ausschnitt gekennzeichnet und kann entsprechend gefiltert werden. Bereits zuvor herausgemeißelte Bereiche in einer Datei werden im Modus Datei farblich hervorgehoben. Das ist nützlich, um den Benutzer daran zu erinnern, ob und wo er schon zuvor Ausschnitte aus einer Datei erstellt (z. B. innerhalb der großen virtuellen Datei "Freier Speicher) wenn er beim Durchsehen von Suchtreffern diese Datei erneut begutachtet.

Block festlegen: In einem Dialogfenster kann man die Offsets einstellen, die den Beginn und das Ende des aktuellen Blocks markieren, oder man gibt Beginn und gewünschte Größe an. Diese Funktion ist auch über die Statusleiste zugänglich. Sie lässt sich wahlweise auch auf alle geöffneten Dateien anwenden.

Alles auswählen: Legt den Dateianfang als Blockanfang und das Dateiende als Blockende fest.

Sektoren überlagern: s. dort

Konvertieren: s. dort

Daten modifizieren: s. dort

Block/Datei/Sektoren füllen: s. unten (Löschen und Initialisieren)

4.6 Suchen-Menü

Parallele Suche: s. o.

Indexierung, Suche im Index: s. o.

Index optimieren: s. o.

Wortliste exportieren: Verfügbar, sobald ein Index erstellt wurde. Erlaubt es, eine Liste aller Wörter im Index in eine Textdatei zu speichern. In dieser Liste sind alle Wörter enthalten, die in den indexierten Dateien vorkommen, und jedes Wort nur genau einmal. Nützlich für individuelle Wörterbuch-Angriffe auf Passwörter.

Text suchen: Diese Funktion sucht Vorkommen einer in ASCII max. 100stelligen Zeichenfolge in der aktuellen Datei (s. a. Suchoptionen). Unterstützt nur solche Unicode-Zeichen, die im Intervall 0x00...0xFF liegen. Eine mächtigere Variante stellt die „Parallele Suche" dar.

Hex-Werte suchen: Sucht Vorkommen einer Kombination von max. 100 jeweils zweistelligen Hex-Werten (s. a. Suchoptionen).

Text ersetzen: Diese Funktion ersetzt Vorkommen einer Zeichenfolge in der Datei durch eine andere (s. a. Ersetzen-Optionen). Unterstützt nur solche Unicode-Zeichen, die im Intervall 0x00...0xFF liegen.

Hex-Werte ersetzen: Funktioniert genau wie der Befehl „Text ersetzen", wird aber auf eine Folge von Hex-Werten angewandt (s. a. Ersetzen-Optionen).

Kombinierte Suche: Mit dieser besonderen Funktion können Sie eine komplexe Suche durchführen: In der aktuell angezeigten und einer auf einem Datenträger bestehenden Datei wird ein gemeinsamer Offset gesucht, an dem die beiden Dateien bestimmte Daten enthalten. Wählen Sie zunächst den Hex-Wert, der in aktuellen Datei an der gesuchten Position stehen soll. Geben Sie dann den Namen der zweiten Datei und den in ihr zu suchenden Hex-Wert an. WinHex sucht nun eine Stelle, an der in jeder Datei der jeweilige Hex-Wert steht.

Ganze Zahl suchen: Geben Sie eine natürliche Zahl (in den Grenzen eines vorzeichenbehafteter 64-Bit-Integer-Wertes) an. Die Funktion sucht dann diejenigen Bytes in der Datei, die als diese Zahl interpretiert werden könnten. Ist sie fündig geworden, gibt sie den Fundort und die entsprechenden Hex-Werte an und nennt das Format, in dem die Hexadezimal-Werte der eingegebenen Zahl entsprechen (s. a. Suchoptionen).

Gleitkommazahl suchen: Geben Sie eine Dezimalzahl (z. B. $12{,}34 = 0{,}1234 \times 10^2 = 0{,}1234e2$) und den Fließkomma-Datentyp an. Die Funktion sucht dann diejenigen Bytes in der Datei, die als diese Zahl interpretiert werden könnten. Ist sie fündig geworden, gibt sie den Fundort und die entsprechenden Hex-Werte an.

Textpassagen suchen: Sucht in der Datei einen Bereich mit aufeinanderfolgenden Buchstaben (a-z, A-Z; wenn Programm auf Deutsch gestartet auch äöüß in der Lateinisch-1-Codepage), Ziffern (0-9) und/oder Satz- und Leerzeichen. Diese Funktion erfüllt zum Beispiel dann ihren Zweck, wenn Sie in einer Programmdatei den sporadisch zwischen den Steuerzeichen vorkommenden Text finden möchten.
Regeln Sie, wie „sensibel" WinHex nach Vorkommen von Text sucht, indem Sie angeben, wie lang der Text sein muss, damit er als solcher erkannt wird.
Viele Dateitypen neueren Datums, darunter 32-Bit-Programmdateien, reservieren zwei Bytes für ein Zeichen statt eins (16-Bit-Unicode-Zeichensatz). Die Option „Unicode-Zeichen tolerieren"

bedeutet, dass auch alphanumerische ASCII-Zeichen, zwischen denen jeweils ein Byte mit dem Wert Null steht, als Text erkannt werden.

Globale Suche fortsetzen: Setzt einen bereits begonnenen globalen, d.h einen mit Option „In allen geöffneten Dateien suchen“ durchgeführten Suchvorgang, nach Anzeigen einer Fundstelle in der *nächsten* Datei fort. Soll zunächst in derselben Datei noch weiter gesucht werden, muss die Funktion „Suche fortsetzen“ benutzt werden.

Suche fortsetzen: Führt einen bereits begonnenen Suchvorgang, auch nach Vorkommen von Text, aber keinen Ersetzen-Vorgang, von der aktuellen Cursor-Position an fort.

4.7 Navigationsmenü

Offset aufsuchen: Setzt den Cursor auf einen von Ihnen gewünschten Offset, d. h. eine Position in der Datei. Gewöhnlich wird diese relativ zum Anfang der Datei (Offset 0) angegeben. Sie können den Cursor aber auch relativ von der aktuellen Position vorwärts und rückwärts und vom Dateiende aus rückwärts bewegen. Die Maßeinheit ist entweder ein Byte, ein Word (2 Bytes), ein DoubleWord (4 Bytes), ein Datensatz (wenn im Ansicht-Menü aktiv) oder ein Sektor. Verwenden Sie F11, um die gewählte Positionsveränderung zu wiederholen.

Seite/Sektor aufsuchen: Schlägt die von Ihnen angegebene Seite auf bzw. springt im Fall eines Datenträgers zum gewählten Sektor/Cluster. Beachten Sie, dass der Datenbereich auf FAT-Laufwerken mit der Cluster-Nr. 2 beginnt. The Go To Sector dialog, when applied to a physical disk, optionally allows to jump to the designated sector within the respective partition window, so that you can immediately see the allocation status of the corresponding cluster. Only for ordinary partitions, not Windows dynamic volumes or LVM2 volumes.

FAT-Eintrag/FILE-Record aufsuchen: Erlaubt es, bequem zu einem bestimmten Eintrag in der Dateizuordnungstabelle auf einem FAT-Laufwerk bzw, zu einem bestimmten FILE-Record in der Master File Table auf einem NTFS-Laufwerk zu springen.

Block verschieben: Verschiebt die aktuelle Block-*Markierung* (nicht die *Daten* im Block) nach vorne oder hinten. Geben Sie dazu die gewünschte Distanz in Byte an. Verwenden Sie ALT+F11, um die gewählte Blockverschiebung zu wiederholen, und UMSCH+ALT+F11, um in die jeweils umgekehrte Richtung zu verschieben. Diese Funktion kann z. B. beim Editieren einer Datei von Nutzen sein, die aus mehreren gleichartigen Datenfeldern (Records) derselben Länge besteht.

WinHex und X-Ways Forensics fertigen Aufzeichnung über die Offset-Sprünge, die Sie in einer Datei oder einem Datenträger durchführen, an und erlauben Ihnen, später innerhalb der Kette **vor** und **zurück** zu springen. Nur mit forensischer Lizenz: Mit Vor und Zurück können Sie auch bequem zurückkehren zu bestimmten Einstellungen des Verzeichnis-Browsers. Dies berücksichtigt erkundeten Pfad, rekursiv oder nicht rekursiv, Sortierkriterien, An-/Auszustand aller Filter, Einstellungen einiger Filter, einige Verzeichnis-Browser-Optionen. Die Befehle Vor und Zurück erlauben auch das erneute Aktivieren eines zuvor aktiven Datenfensterns, wenn Sie zwischen Fenstern hin- und herwechseln.

Dateianfang: Zeigt die erste Seite der Datei an und setzt den Cursor auf den Anfang der Datei (Offset 0).

Dateiende: Zeigt die letzte Seite der Datei an und setzt den Cursor auf das Ende der Datei (letztes Byte, Offset=Dateigröße-1).

Blockanfang: Setzt den Cursor auf den aktuellen Blockanfang.

Blockende: Setzt den Cursor auf das aktuelle Blockende.

Position markieren: Markiert die aktuelle Position optisch.

Markierung löschen: Löscht eine zuvor gesetzte Markierung vom Bildschirm.

Markierung aufsuchen: Setzt den Cursor auf die zuvor markierte Position.

Positions-Manager: s. „Positions-Manager“

4.8 Ansicht-Menü

Nur Text-Anzeige: Blendet die Hexadezimal-Spalte aus und verwendet die gesamte Breite des Editorfensters für die Text-Anzeige.

Nur Hex-Anzeige: Blendet die Text-Spalte aus und verwendet die gesamte Breite des Editorfensters für die Hexadezimal-Anzeige.

Zeichensatz: Wählen Sie einen Zeichensatz oder eine Codepage für die Text-Anzeige aus. Sie können auch durch Drücken von UMSCH+F7 zwischen verschiedenen Zeichensätzen/Codepages zyklisch wechseln. Die Voreinstellung ist ANSI-ASCII. Das ist die effizienteste und unkomplizierteste Anzeigemethode; sie ruft nur die einfachsten Windows-API-Funktionen auf und scheint Zeichen immer gemäß Codepage 1252 zu interpretieren, auch wenn die regionalen Einstellungen in Windows anders sind, sofern im Schriftart-Auswahldialog (über Allgemeine Optionen erreichbar) als Script "Western" ausgewählt ist.

To better utilize widescreen monitors and to assist examiners in particular in Asia, who may encounter text encoded in many different character sets and code pages in the same case, it is possible to see multiple text interpretations of binary data in the hex editor's text diplay at the same time depending on the license type. This is also useful to walk through the raw data of Outlook PST files that use cipher coding, to be able to read encoded ANSI text, encoded Unicode text, and totally unencoded text at the same time.

Personal license for WinHex: no more than 1 character set at a time
Professional license for WinHex: up to 2 character sets at a time
Specialist license for WinHex, X-Ways Investigator: up to 3 character sets at a time
WinHex Lab Edition: up to 4 character sets at a time
X-Ways Forensics: up to 5 character sets at a time

Es gibt die Möglichkeit zur Interpretation von Daten als nicht ausgerichteter Text in UTF-16 LE und UTF-16 BE in dem Modi Disk/Partition/Volume und Datei. Nicht ausgerichtet bedeutet, dass die Bytes für ein Zeichen an einem ungeraden Offset beginnen. Das macht einen Unterschied gegenüber ASCII bei allen Sprachen außer westeuropäischen Sprachen und macht einen auf diese Weise gespeicehrten Text erst tatsächlich lesbar.

Please note that any text *input* from the keyboard (when not in read-only mode) is interpreted as being based on the ANSI code page that is active in Windows, except if the primary text column is set to the IBM/OEM/DOS code page 850 (Latin I), in which case input is based on that code page.

Datensatz-Darstellung: Beim Editieren aufeinanderfolgender Datensätze, die alle die gleiche Länge aufweisen (z. B. Tabelleneinträge einer Datenbank), können Sie WinHex zur besseren visuellen Unterscheidung jeden zweiten Datensatz mit einer gesonderten Hintergrundfarbe anzeigen lassen. Die Farbe kann im Dialog „Allgemeine Optionen“ bestimmt werden. Außerdem bietet WinHex die Anzeige der aktuellen Datensatz-Nummer und des Offsets innerhalb dieses Datensatzes (also des *relativen* Offsets) in der Statusleiste an. Das alles basiert auf der Datensatzgröße und dem Offset des ersten Datensatzes, wie Sie es im Dialogfenster „Datensatz-Darstellung“ angeben.
Wenn Sie eines der beiden Datensatz-Features einschalten, erlaubt es der Befehl „Offset aufsuchen“ auch, die aktuelle Cursorposition um ein Vielfaches der aktuellen Datensatzgröße zu verschieben. Wenn relative Datensatz-Offsets aktiv sind, bewegen die Bild-auf-/ab-Tasten den Cursor in Einheiten der Datensatzgröße, außerwenn wenn Sie die Strg-Taste gedrückt halten.

Anzeigen: Das **Falldaten**-Fenster ist Teil der forensischen Benutzeroberfläche von WinHex/X-Ways Forensics und für die Bearbeitung von Fällen erforderlich (das heißt auch, dass das Ausblenden des Fensters einen etwaigen geöffneten Fall schließt). Der **Verzeichnis-Browser** ist für logische Laufwerke/Partitionen verfügbar, die mit dem Disk-Editor geöffnet wurden. Der **Daten-Dolmetscher** ist ein kleines Fenster, das „Übersetzungsmöglichkeiten“ für die Daten an der aktuellen Cursorposition anzeigt. Die **Symbolleiste** wird ebenfalls optional angezeigt. Das gleiche gilt für die **Registerleiste**, die es erlaubt, alle Editierfenster mit einem einfachen Mausklick anzuwählen. Die **Informationsspalte**, die Details über das editierte Objekt (Datei, Datenträger, RAM) aufführt, wird auch optional angezeigt.

Schablonen-Manager

Tabellen: Diese Funktion stellt Ihnen Übersichtstabellen zur Verfügung, in denen Sie zu Hexadezimal-Werten von 0 bis FF die Entsprechungen in Dezimalschreibweise, im IBM-ASCII-, ANSI-ASCII- und EBCDIC-Format ablesen können.

Zeilen & Spalten

Rollen synchronisieren: Synchronisiert bis zu vier Fenster auf identische absolute Offsets. Halten Sie die Umschalt-Taste beim Aufrufen dieser Funktion gedrückt, um die Fenster dazu nebeneinander statt übereinander anzuordnen.

Synchronisieren und vergleichen: Synchronisiert bis zu vier Fenster und zeigt unterschiedliche Bytewerte gesondert an. Wenn nicht mehr als zwei Fenster beteiligt sind, hält WinHex beim Rollen immer den anfänglichen Abstand zwischen Offsets der ersten angezeigten Bytes in den beiden Editierfenstern aufrecht. Nicht auf absolute Offsets zu synchronisieren ist nützlich z. B. beim Vergleich zweier Kopien der Dateizuordnungstabelle, die ja an unterschiedlichen Offsets liegen. Sie können zum nächsten bzw. vorherigen verschiedenen Byte springen, indem Sie die zusätzlich in einem der beteiligten Editierfenster bereitgestellten Schalter anklicken.

Anzeige aktualisieren: Erneuert die Anzeige im aktiven Editierfenster. Falls die aktuelle Datei von einem externen Programm geändert wurde, bietet WinHex an, etwaige in WinHex vorgenommenen Änderungen aufzugeben und die Datei nochmal neu zu laden.
Befüllt auch den Verzeichnis-Browser neu, wenn der Verzeichnis-Browser gerade den Eingabefokus hat. Nützlich z. B., wenn ein Filter für markierte Dateien aktiv ist und Sie die Markierung von einigen der aufgelisteten Dateien aufheben, wenn Sie die Liste im Verzeichnis-Browser dann aktualisieren möchten und die nicht mehr markierten Dateien verschwinden sollen.

4.9 Extras-Menü

Disk öffnen: s. „Disk-Editor“

Datenträger klonen: s. u.

Rekursives Erkunden: Wechselt für das aktuell im Verzeichnis-Browser dargestellte Verzeichnis in eine rekursive Ansicht oder zurück in eine normale Ansicht. In einer rekursiven Ansicht werden nicht nur die Dateien angezeigt, die sich direkt in diesem Verzeichnis befinden, sondern auch alle Dateien in alle Unterverzeichnissen und deren Unterverzeichnissen usw. Das erlaubt es z. B., ausgewählte Dateien aus unterschiedlichen Pfaden in einem einzigen Schritt wiederherzustellen/zu kopieren.

Dateien retten nach Typ: s. u.

Datei-Überblick neu einlesen: Verfügbar für Partitionen mit einem der unterstützen Dateisysteme. WinHex durchläuft alle Dateisystem-Datenstrukturen und Clusterketten und kann dadurch den Verzeichnis-Browser befüllen und für jeden Sektor/Cluster angeben, was in ihm gespeichert ist bzw. ob er unbelegt ist. Durch Dateioperationen auf dem betreffenden Laufwerk veralten diese Informationen allerdings, und ein erneutes Aufrufen dieser Funktion bietet sich an. Vgl. Sicherheitsoptionen.

Freien Speicher initialisieren: Vertrauliche Informationen könnten durch normale Lösch- und Kopiervorgänge in momentan unbenutzten Bereichen des Datenträgers liegen. Mit dieser Funktion kann der unbenutzte Speicher eines Datenträgers aus Sicherheitsgründen initialisiert (überschrieben) werden. Dies verhindert die Wiederherstellung von Daten aus diesem Bereich des Datenträgers. Verfügbar für Partitionen, die als Laufwerksbuchstabe geöffnet wurden. *Nur in WinHex verfügbar, nicht in X-Ways Forensics.*

Schlupfspeicher initialisieren: Überschreibt Schlupfspeicher (englisch „slack space“, die

unbenutzten Bytes im jeweils letzten Cluster einer Clusterkette, hinter dem tatsächlichen Ende der Datei) mit Nullbytes. Dies kann in Verbindung mit „Freien Speicher initialisieren“ benutzt werden, um vertrauliche Daten auf einem Laufwerk sicher zu löschen oder um den Platzbedarf eines komprimierten Datenträger-Backups zu minimieren (z. B. einer WinHex-Sicherung). Beenden Sie vor Verwendung dieser Funktion alle laufenden oder residenten Programme, die auf den Datenträger schreiben könnten. *Nur in WinHex verfügbar, nicht in X-Ways Forensics.*

MFT-Records initialisieren: Auf NTFS-Volumes kann WinHex alle gegenwärtig unbenutzten FILE-Records der $MFT (Master File Table) sicher löschen. Diese können Metadaten (z. B. Namen) und sogar Inhalte von ehemals existierenden Dateien enthalten.. *Nur in WinHex verfügbar, nicht in X-Ways Forensics.*

Verzeichniseinträge initialisieren: Auf FAT-Volumes kann WinHex alle gegenwärtig ungenutzten Verzeichniseinträge sicher löschen, um Spuren ehemals existierender Dateien sowie Informationen über frühere Namen oder Orte existierender Dateien aus dem Dateisystem zu entfernen. Besonders nützlich in Verbindung mit der Funktion zum Initialisieren des freien Speichers. *Nur in WinHex verfügbar, nicht in X-Ways Forensics.*

Verlorene Partitionen suchen: Ehemals existierende Festplatten-Partitionen, die nicht automatisch gefunden wurden, als die physische Platte (oder eine Image-Datei einer physischen Platte) geöffnet wurde, und die nicht im Zugriffsschalter-Menü aufgelistet werden, können mit diesem Befehl gefunden und entsprechend identifiziert werden. Er sucht nach der 0x55-0xAA-Signatur von Master Boot Records, Partitionssektoren und FAT-/NTFS-Bootsektoren sowie nach Ext2/Ext3/Ext4-Superblöcken, optional nur ab dem ersten Sektor, der der letzten (gemäß ihrer physischen Abfolge) Partition folgt, die bereits bekannt ist, und listet die neu gefundenen Partitionen im Verzeichnis-Browser auf. Funktioniert nur bei Sektorgröße 512 Bytes.

Als Partitionsanfang interpretieren: Wenn Sie den Anfangssektor einer (z. B. gelöschten) Partition auf einer physischen Festplatte finden, können Sie die Partition mit diesem Menübefehl einfach per Zugriffsschaltermenü zugreifbar machen. Wenn kein bekanntes Dateisystem beginnend am aktuell angezeigten Sektor erkannt wird, werden Sie gefragt, wie viele Sektoren in der neu zu definierenden Partition enthalten sein sollen.

Plattenparameter eingeben: Benutzen Sie diese Funktion für einen physischen Datenträger, um erkannte Gesamtzahl von Sektoren oder optional (kann freigelassen werden) die Zahl der Zylinder, Köpfe und Sektoren pro Spur anzupassen (Zylinder, Köpfe und Sektoren pro Spur sind heutzutage praktisch allesamt bedeutungslos). Dies kann nützlich sein, um auf etwaige Überhangsektoren am Ende des Datenträgers zugreifen zu können (falls die Zahl der zugreifbaren Sektoren nicht automatisch richtig erkannt wurde) oder um das CHS-Koordinatensystem nach Ihren Wünschen zu ändern. Alternativ gibt es die Möglichkeit, die erkannte Sektorgröße von physischen Festplatten oder Images zu ändern. Wenn Sie die Sektorgröße ändern, wird die Gesamtzahl der Sektoren entsprechend angepasst. Wenn Sie z. B. die Sektorgröße von 512 Bytes auf 4 KB ändern (d. h. mit 8 multiplizieren), dann wird die Sektoranzahl automatisch durch 8 dividiert, um die insgesamt erkannte Plattenkapazität beizubehalten (in der Annahme, dass diese korrekt war).

RAM öffnen: s. „RAM-Editor“

Prozesse sichern: Erlaubt die Sicherung aller Daten im Speicher der laufenden Prozesse eines lebenden Systems in zusammenhängender, richtiger Reihenfolge der Speicherseiten. Die Erzeugungszeitstempel der jeweiligen Prozesse werden als Erzeugungszeitstempel der jeweiligen Speicher-Dumps sichtbar. Speicherseiten, deren Inhalt als ausführbarer Programm-Code gekennzeichnet sind (PAGE_EXECUTE*) sind optional und reduzieren, falls ausgelassen, die Gesamtdatenmenge, sofern Sie lediglich interessiert sind, Suchbegriffe oder Dateisignaturen suchen zu lassen, und nicht Malware-Untersuchung. Signatursuchen in den Speicher-Dumps (die als Dateien vom Typ "mem" gezeigt werden) können über die Suche nach eingebetteten Daten, einer der Funktionen von Datei-Überblick erweitern, veranlasst werden. Das Ausgabeverzeichnis von "Prozesse sichern" ist standardmäßig entweder ein Unterverzeichnis des aktuellen Falles oder, falls kein Fall aktiv ist, ein Unterverzeichnis des Verzeichnisses für Datenträgersicherungen. Es kann automatisch im Windows File Explorer geöffnet, wenn die Ausgabe fertig ist, und/oder dem aktuellen Fall als Verzeichnis hinzugefügt werden. Der Speicher-Dump von "Prozesse sichern" kann auch auf Ihrem eigenen System nützlich sein, wenn eine Anwendung, in der Sie Text eingegeben haben (z. B. ein E-Mail-Programm) plötzlich einfriert und Sie Ihren Text noch aus dem Prozess-Speicher retten möchten.

Dieser Befehl kann auch eine tabulatorgetrennte Liste aller Hauptfenster mit deren jeweiligen Titeln und zugehörigen Prozessen ausgeben plus (kommagetrennt), die Titel ihrer Unterfenster. Bildschirmfotos von einigen der Hauptfenster werden automatisch erzeugt und ausgegeben. Wenn diese Funktion ohne Administrator-Rechte ausgeführt wird, werden nur die Prozesse des aktuellen Benutzers berücksichtigt, sonst alle Prozesse. Ein Filter ist für die Prozess-Sicherung verfügbar. Sie können ihn genauso verwenden, wie andere Dateimasken-Filter in X-Ways Forensics. Die Eingabe "explorer.exe" würde beispielsweise nur den Speicherinhalt und die Fenster des Windows Explorer Prozesses ausgeben. ":C*" gibt alle Prozesse mit Ausnahme derer aus, deren Namen mit dem Buchstaben "C" beginnt, d. h. beispielsweise nicht "Chrome.exe". Die Dateimaske ist nicht abhängig von Groß- und Kleinschreibung. Mehrere Dateimasken können mit Strichpunkt getrennt hintereinander gehängt werden. (Allerdings ist die Gesamtlänge beschränkt.)

Einsehen: Verfügbar nur mit einer forensischen Lizenz. Ruft den internen Viewer auf.

Externe Programme: Ruft eins der im Optionen-Menü eingestellten externen Programme auf (wie etwa Quick View Plus) und öffnet darin die aktuelle Datei.

X-Ways Trace aufrufen: Nur verfügbar, wenn X-Ways Trace installiert ist. Diese Software kann die History/Cache-Dateien diverser Internet-Browser entschlüsseln.

Rechner: Startet den Windows-Rechner für sonstige Berechnungen (wissenschaftliche Ansicht empfohlen). Dazu muss sich die Datei „calc.exe“ im Windows-Ordner befinden.

Umrechnung: Diese Funktion können Sie benutzen, um Zahlen des Hexadezimal-Systems ins Dezimal-System oder umgekehrt zu übersetzen. Nach der Eingabe der Zahl betätigen Sie die ENTER-Taste. Bitte beachten Sie die Hinweise zum Thema „Numerische Datentypen“.

Tabellen: Diese Funktion stellt Ihnen Übersichtstabellen zur Verfügung, in denen Sie zu

Hexadezimal-Werten von 0 bis FF die Entsprechungen in Dezimalschreibweise, im IBM-ASCII-, ANSI-ASCII- und EBCDIC-Format ablesen können.

Vergleichen: Wählen Sie zwei Datenfenster (Dateien oder Datenträger) aus, die Sie Byte für Byte vergleichen möchten. Legen Sie fest, ob nach Unterschieden oder nach Übereinstimmungen gesucht werden soll. Sie geben außerdem an, wie viele Bytes verglichen werden sollen. Nach Erreichen einer gewissen Anzahl von Unterschieden/Übereinstimmungen kann der Vergleich abgebrochen werden. Der Bericht in Form einer Textdatei kann sonst ungewollt riesengroß werden. Der Vergleich beginnt an den jeweils angegebenen Offsets. Diese Offsets dürfen unterschiedlich sein, so dass z. B. das Byte an Offset 0 in Datei A mit dem Byte an Offset 32 in Datei B vergleichen wird, und das Byte an Offset 1 mit dem an Offset 33 usw. Wenn Sie Editierfenster für den Vergleich auswählen, wird die aktuelle Cursorposition automatisch hinter "Ab Offset" eingetragen.

In X-Ways Forensics there is also an option to output identified different or identical data areas as search hits (1 entry per matching area) instead of a text file (1 line per matching byte), for convenient review and navigation right within the program in the search hit list, similar to block hash matches. This option is only available if at least the 2nd data source is an evidence object. The result can be seen in the search hit list of that evidence object. Useful for example for users who wish to compare cloned disks with minor changes, if they have different hashes or one of them has been used a little more, to actually locate the differences and better understand what has caused them. Useful also to compare component disks of a hardware RAID level 0 system or a mirrored volumes, to check whether they are really absolutely identical, and if not to easily find the areas that differ, see how large they are, what kind of data these areas contain, and assess whether the second copy requires full treatment itself including carving, keyword searches etc.

Es gibt noch eine weitere Vergleichsfunktion in WinHex: Sie können auch Editierfenster miteinander vergleichen und das Rollen in den Fenstern synchronisieren (s. Ansicht-Menü).

Block/Datei analysieren: Die Daten im aktuellen Block bzw. in der gesamten Datei werden statistisch ausgewertet und das Ergebnis in einem Fenster graphisch veranschaulicht. WinHex ermittelt dazu die Häufigkeiten des Vorkommens aller 256 möglichen Bytewerte und bildet sie proportional in vertikalen Linien entsprechender Länge ab. Dabei wird die Höhe des Fensters optimal genutzt, d. h. die längste Linie (die den häufigsten Bytewert repräsentiert) reicht von unten bis zur Titelleiste des Fensters. Unter der Titelleiste können Sie abhängig von der Mauscursor-Position den relativen Anteil und die absolute Anzahl eines jeden Bytewerts ablesen.
Diese Funktion kann z. B. dazu eingesetzt werden, um Datenmaterial unbekannter Art (z. B. von ScanDisk wiederhergestellte verloren Cluster) zu analysieren. Audio-Daten, komprimierte Daten, ausführbarer Code u. a. lassen sich an charakteristische Grafiken erkennen.
Im Kontextmenü des Fensters lässt sich einstellen, ob Bytes mit dem Wert Null unberücksichtigt bleiben sollen. Dies kann in vielen Fällen die Aussagekraft der Grafik stark erhöhen. Vom Kontextmenü aus können Sie das Analysefenster auch drucken und die Analyse in eine Textdatei exportieren.
Wenn Sie kleinere Datenmengen analysieren lassen (weniger als 50.000 Bytes), wird die mit Zlib für diese Daten erzielbare Kompressionsrate in der Titelzeile des Analysefensters angezeigt. Diese Rate lässt ebenfalls Rückschlüssel über die Natur der Daten zu.

Hash berechnen: Berechnet für die aktuelle Datei, den aktuellen Datenträger bzw. den

gegenwärtig definierten Block eine der folgenden Prüfsummen/Digests: 8-Bit-, 16-Bit-, 32-Bit-, 64-Bit-Prüfsumme, CRC16, CRC32, MD5, SHA-1, SHA-256 oder PSCHF.

4.10 Datei-Tools

Verketten: Diese Funktion lässt Sie eine beliebige Anzahl bestehender Dateien auswählen, die aneinandergehängt eine Zieldatei bilden.

Zerlegen: Wählen Sie eine bestehende Datei, aus der Sie mehrere neue Dateien bilden möchten. Geben Sie für jede Zieldatei den Dateinamen an und den Offset der Quelldatei, an dem die Trennung vorgenommen werden soll. Die Quelldatei bleibt durch diese Funktion unberührt.

Verschmelzen: Geben Sie die Namen zweier Quelldateien und einer Zieldatei an. Die Bytes bzw. Words der Quelldateien werden abwechselnd in die Zieldatei geschrieben (wobei das erste Byte aus der zuerst ausgewählten Quelldatei stammt). Auf diese Weise lassen sich die in getrennten Dateien enthaltenen Odd- und Even-Bytes bzw. -Words zu einer Datei zusammenfügen (z. B. in der EPROM-Programmierung).

Aufspalten: Geben Sie die Namen einer Quelldatei und zweier Zieldateien an. Die Bytes bzw. Words der Quelldatei werden abwechselnd in die Zieldateien geschrieben (wobei das erste Byte/Word in die zuerst ausgewählte Zieldatei gelangt). Auf diese Weise lassen sich Odd- und Even-Bytes bzw. -Words in zwei separate Dateien überführen (z. B. in der EPROM-Programmierung).

Verhardlinken: Coole Funktion zum Erzeugen von harten Verweisen auf Dateien in NTFS-Dateisystemen. Nützlich z. B., wenn Sie spielerisch mit harten Verweisen während unserer Dateisystem-Schulung experimentieren oder wenn Sie dasselbe Image ein zweites Mal zum selben Fall hinzufügen möchten, was nur unter einen anderen Namen möglich ist, oder wenn Sie einen harten Verweise auf xwforensics.exe unter den Namen WinHex.exe erzeugen möchten, damit X-Ways Forensics als WinHex ausgeführt wird. Erst wählen Sie die existierende Datei aus, dann Pfad und Name des zusätzlichen harten Verweises.

Sparse kopieren: Kann eine ausgewählte Datei kopieren und dabei die spärlich mit Daten besetzte Natur einer NTFS-Sparse-Datei in der Zieldatei beibehalten. Das heißt z. B., wenn Sie eine 1 TB große Minimal-Datenträger-Sicherung, von der nur 100 MB an Daten alloziert sind, kopieren, ist dieser Vorgang praktisch sofort abgeschlossen, weil nur 100 MB von 1 TB Daten kopiert zu werden brauchen. Konventionelle Kopierfunktionen behalten die Sparse-Eigenschaft einer Datei nicht bei, sondern kopieren die Datenmenge, wie sie von der nominellen Größe er Datei angegeben wird, auch wenn intern die meisten Daten nicht alloziert sind und nur virtuell als binäre Nullen gelesen werden.

Verzeichnis replizieren: Copies a directory with all its files and subdirectories, recursively, and recreates individually NTFS-compressed source files as NTFS-compressed in the respective output folder if supported by the destination file system and any layer in between. The command does not retroactively compress such files after their creation, but writes them immediately as compressed, which is more efficient. However, it still has to copy/send the decompressed amount

of data of the source file. Supports overlong paths. Select the source directory first, then specify/create the destination directory. This function is useful for example if you wish to copy or move a case directory, which contains a few NTFS-compressed files that would be inefficient to store as uncompressed. Note that alternatively you can open a case and use the Save As command in the Case Data window for the same effect.

Vollzugriff erhalten: Übernimmt die Kontrolle über alle Dateien in einem von Ihnen angegebenen Verzeichnis (im aktuell verwendeten Windows-System, rekursiv). Gewährt allen Benutzern volle Zugriffsrechte, und benötigt Administrator-Privilegien.

Sicheres Löschen: Löscht eine oder mehrere Dateien auf magnetischen Datenträgern definitiv, so dass ihr Inhalt mit Datenrettungsprogrammen nicht rekonstruiert werden kann. Jede gewählte Datei wird in ihrer aktuellen Größe gemäß den Einstellungen überschrieben, auf die Länge Null gekürzt und dann im Dateisystem gelöscht. Zusätzlich wird ihr Name im Dateisystem unkenntlich gemacht. „Sicheres Löschen“ eignet sich daher für Dateien mit vertraulichen Informationen, die vernichtet werden sollen. *Nur in WinHex verfügbar, nicht in X-Ways Forensics.*

Rekursives Löschen: Dieser Befehl kann verwendet werden, um ein Verzeichnis mit all seinen Unterverzeichnissen rekursiv zu löschen, wenn diese mit dem Windows Explorer oder anderen Windows-Tools und Befehlen nicht gelöscht werden können, wegen unzulässiger Zeichen in Verzeichnis- oder Dateinamen oder wegen fehlender Rechte (wenn z. B. "Trusted Installer" der Besitzer ist), wenn Sie sich diese Rechte aber nehmen können (wenn Sie WinHex als Administrator ausführen; Sie werden evtl. gefragt, ob Sie vor dem Löschversuch Kraft Ihrer Administatorrechte Besitz von der ausgewählten Verzeichnisstruktur ergreifen möchten). Beachten Sie, dass Sie diesen Befehl nicht auf ein problematisches Verzeichnis direkt anwenden können, sondern nur auf dessen Elternverzeichnis.

4.11 Specialist-Menü

Nur verfügbar mit Specialist- oder forensischer Lizenz.

Datei-Überblick erweitern: siehe separates Kapitel

Technischer Detailbericht: Zeigt Informationen über den aktiven Datenträger bzw. die aktive Datei an und lässt Sie diese kopieren, z. B. in einen Bericht den Sie anfertigen. Besonders ausführlich bei physischen Festplatten, zu denen Details über jede Partition und allen keiner Partition zugeordneten Speicherlücken aufgeführt werden. Unter Windows XP berichtet WinHex auch den Passwortschutz-Status von ATA-Festplatten.
Nur mit forensischer Lizenz: X-Ways Forensics versucht, versteckte sog. Host Protected Areas (HPAs, auch bekannt als ATA-geschützte Bereiche) sowie Device Configuration Overlays (DCO-Bereiche) auf [S]ATA-Festplatten erkennen. Ein Meldungsfenster mit einer Warnung wird angezeigt, falls eine künstlich herabgesetzte Festplattengröße festgestellt wird. Sofern erfolgreich ermittelt, wird die tatsächliche Gesamtzahl der Sektoren laut ATA im Detailbericht mit aufgelistet. Auch einige wichtige SMART-Status-Informationen werden angezeigt für über [S]ATA angeschlossene Festplatten, die SMART unterstützen. Useful to check for one's own

hard disk as well as that of suspects. For example, you can learn how often and how long the hard disk was used and whether it has had any bad sectors (in the sense that unreliable sectors were replaced internally with spare sectors). If a hard disk is returned to a suspect and he or she consequently complains about bad sectors and accuses you of having damaged the disk, a details report created when the hard disk was initially captured can now show whether it was already in a bad shape at that time. Also, seeing that spare sectors are in use means knowing that there is additional data to gain from the hard disk (with the appropriate technical means).

The following metadata about BitLocker and BitLocker To Go volumes is output: Volume creation timestamp, textual volume description, encryption method, protection type, and volume master key last modification timestamps. BitLocker-related timestamps are also output to the event ist.

The Technical Details Report also checks for certain read inconsistencies that can occur with flash media (for example USB stick of certain brands/models, but not others) in data areas that have never been written/used, where the data is undefined. The data that is read in such areas, for example when imaging the media, may depend on the amount of data that is read at a time with a single internal read command. The result is mentioned in the report. If inconsistencies are detected ("Inconsistent read results!" in the report), you will see a message box, which offers to read sectors in smaller chunks from that device as long as it is open, which likely yields the expected zero value bytes instead of some random looking non-zero pattern data when reading such areas. Use of this option does not give you data that is somehow more accurate or original (undefined is undefined and does not mean zeroed out) or contains more or less evidence, it can just have a big impact on compression ratio achieved and reproducibility of hash values with other tools, which may use different chunk sizes for reading and thus produce different data and hash values. Note that it is possible that read inconsistencies occur that are not detected by X-Ways Forensics, because a complete check would be very slow. Again, these inconsistencies are not fatal and not the fault of the software, and they can be explained. Note that the Technical Details Report is routinely created already when you start disk imaging with the File | Create Disk Image command, so you do not need to invoke the report yourself prior to imaging.

Es gibt die Möglichkeit, die Zeichen in der Seriennummer von Festplatten im Zweifelsfall zusätzlich paarweise vertauscht anzeigen zu lassen. Das ist nützlich für Benutzer bestimmter Hardware-Schreib-Blocker, die die Seriennummer u. U. verdreht weitergeben.

Image als Datenträger interpretieren: s. separates Kapitel

Als Laufwerk einbinden: s. separates Kapitel

Betriebssystemweiter Schreibschutz: Hier können Sie lokal angeschlossene physische Datenträger (auch Wechseldatenträger, aber keine optischen) innerhalb von Windows mit einem Schreibschutz versehen. Das betrifft auch all Partition/Volumes, die auf diesen Datenträgern liegen. Der Effekt gilt im gesamten Betriebssystem, in allen Anwendungen, auch auf Sektorebene in WinHex selbst, egal welcher Editiermodus aktiv ist. Dies kann nützlich sein, um Originaldatenträger zu schützen, die es zu sichern oder zu untersuchen gilt (allerdings erst nachdem Windows sie bemerkt und auf sie zugegriffen hat), und auch Ihre eigenen Datenträgern, die zu untersuchende Images enthalten. Dies kann ein Schutz sein vor versehentlicher Änderung, Löschung oder Datenbeschädigung (z. B. sich neu einschleichende Dateisystemfehler). Die

Wirkung bleibt so lange bestehen, bis Sie den Schreibschutz wieder entfernen oder Ihren Computer neu starten. Um Windows davon abzuhalten, neu angeschlossene physische Datenträger "anzufassen", bevor Sie sie mit einem Schreibschutz versehen können (d. h. um sie anfangs im Windows-Modus "offline" zu betreiben), müssten Sie das automatische Mounten in Windows ausschalten (und überprüfen, dass das auch wirklich funktioniert). Wenn Sie den Schreibschutz für einen Offline-Datenträger einschalten, wird gleichzeitig der Offline-Status auf Online geändert. Vorsicht, versuchen Sie nicht, die Datenträger in den Schreibschutzmodus zu versetzen, die Ihr Windows-System zum Funktionieren braucht!

Dieser Befehl erlaubt es auch, gezielt nur bestimmte Partitionen/Volumes in den schreibgeschützten Zustand zu versetzen, wenn sie auf GPT-partitionierten Datenträgern gespeichert und mit einem Laufwerksbuchstaben verknüpft sind, also nicht notwendigerweise den gesamten physischen Datenträger. Bitte beachten Sie noch, dass der Schreibschutz eines Volumes nicht selektiv aufgehoben werden kann, wenn der zugrundeliegende physische Datenträger schreibgeschützt ist. Wenn der Versuch, einen Schreibschutz auf einer einzelnen Partition auf einem MBR-partitionierten Datenträger zu etablieren, fehlschlägt, wird Ihnen angeboten, diesen alle Partitionen dieses Datenträgers anzuwenden.

RAID-System zusammensetzen: s. separates Kapitel

Freien Speicher extrahieren: Durchläuft das gegenwärtig geöffnete logische Laufwerk und sammelt alle unbenutzten Cluster in einer von Ihnen anzugebenen Zieldatei. Nützlich um Datenfragmente von vormals existierenden Dateien, die nicht sicher gelöscht wurden, zu untersuchen. Nimmt keine Änderungen am untersuchten Laufwerk vor. Die Zieldatei muss auf einem anderen Laufwerk abgelegt werden.

Schlupfspeicher extrahieren: Sammelt Schlupfspeicher (englisch „slack space“, die unbenutzten Bytes im jeweils letzten Cluster einer Clusterkette, hinter dem tatsächlichen Ende der Datei) in einer Zieldatei. Jedem Vorkommen von Schlupfspeicher werden Zeilenumbrüche vorangestellt und die Nummer des Clusters, in dem er gefunden wurde, als ASCII-Text. Ansonsten ähnlich wie „Freien Speicher extrahieren“. WinHex kann Schlupfspeicher von Dateien, die auf Dateisystemebene komprimiert oder verschlüsselt sind, nicht erfassen.

Partitionslücken extrahieren: Erfasst die Speicherbereiche einer physischen Festplatte, die zu keiner Partition gehören, in einer Zieldatei, zur schnellen Untersuchung, um herauszufinden, ob dort etwas versteckt ist oder übrig geblieben von früheren Partitionierungen.

Text extrahieren: Erkennt Text anhand der von Ihnen anzugebenden Parameter, erfasst alle Vorkommnisse in einer Datei, auf einem Datenträger oder innerhalb eines Speicherbereichs und schreibt diese in eine Datei. Diese Art von Filter ist nützlich, um auszuwertende Datenmengen beträchtlich zu verringern, wenn z. B. bei einer forensischen Computeranalyse Hinweise in Form von Text (wie E-Mails, Dokumente) gesucht werden. Die Zieldatei kann leicht in benutzerdefinierte Größen zerlegt werden. Diese Funktion kann auch auf Dateien mit gesammelten Schlupf- oder freiem Speicher angewandt werden, oder auf beschädigte Dateien in einem proprietären Format, die nicht mehr von der zugehörigen Applikation, wie MS Word, geöffnet werden können, um zumindest unformatierten Text zu retten.

Datei-Container: s. o.

Externe Virenprüfung: (nur mit forensischer Lizenz) Schickt alle Dateien oder alle markierten Dateien im Datei-Überblick eines Asservats, optional nur solche unterhalb einer bestimmte Größe, an einen externen Viren-Scanner. Dateien, die vom Viren-Scanner im Ausgabeverzeichnis gesperrt, gelöscht oder umbenannt werden, werden mit dem Vermerk „Virenverdacht“ versehen. Es liegt in der Verantwortung des Benutzers sicherzustellen, dass ein Viren-Scanner aktiv ist, dass er das Verzeichnis für temporäre Dateien beobachtet und dass er infizierte Dateien tatsächlich sperrt, löscht oder umbenennt. Nachdem X-Ways Forensics überprüft hat, ob die Datei extern gesperrt, gelöscht oder umbenannt wurde, löscht es sie, wenn sie noch existiert.

Bates-Nummerierung: Versieht alle Dateien innerhalb eines bestimmten Ordners und seiner Unterordner für die forensische Verwendung mit einer Bates-Nummerierung. Fügt ein bis zu 13 Zeichen langes konstantes Präfix und eine eindeutige laufende Nummer zwischen Dateinamen und Dateinamenserweiterung ein, ähnlich wie Anwälte Papierdokumente für spätere Bezugnahme kennzeichnen.

Sicherer Dateiexport: Auch „trusted download“ genannt (vertrauenswürdiges Überspielen von Daten). Löst ein potenzielles Sicherheitsproblem. Wenn als vertraulich oder geheim eingestuftes Material von einem klassifizierten auf einen nicht-klassifizierten Datenträger übertragen wird, muss sichergestellt sein, dass keine überschüssigen Informationen in einem Cluster- oder Sektorüberhang ungewollt mit der eigentlichen Datei mit kopiert werden, da dieser sog. Schlupfspeicher (s. o.) noch vertrauliches oder geheimes Material von einem früheren Zeitpunkt enthalten kann, an dem er noch einer anderen Datei zugeordnet war. Dieser Befehl kopiert die ausgewählte(n) Datei(en) nur in ihrer aktuellen tatsächlichen Größe, und kein weiteres Byte mehr. Er kopiert nicht ganze Sektoren oder Cluster, wie es konventionelle Kopierbefehle tun. Es können mehrere Dateien eines Ordners auf einmal kopiert werden.

4.12 Optionen-Menü

Allgemeine Optionen: s. o.

Viewer-Programme: s. u.

Sicherheitsoptionen: s. u.

Rückgängig-Optionen: s. u.

Daten-Dolmetscher-Optionen: s. Daten-Dolmetscher

Editier-Modus: Erlaubt es, den Editier-Modus programmweit zu bestimmen. (Das Kontextmenü der Informationsspalte erlaubt es, den Editier-Modus gezielt nur für das aktive Editierfenster zu ändern.)

4.13 Fenster-Menü

Fenster-Manager: Listet alle Datenfenster auf und gibt Ihnen die Möglichkeit, schell zwischen einzelnen Fenstern zu wechseln. Sie können im Fenster-Manager auch einzelne Datenfenster schließen und etwaige Änderungen speichern.

Anordnung als Projekt speichern: Schreibt die gegenwärtige Fensterkonstellation (geöffneter Fall, geöffnete Datenfenster, Lage der Datenfenster auf dem Bildschirm, Position des Cursors in jedem Datenfenster, ausgewählter Block, ...) in eine Projektdatei. Vom Start-Center aus können Sie das Projekt dann zu einem späteren Zeitpunkt wieder laden und die Editierpositionen in allen Dokumenten wiederherstellen lassen, um Ihre Arbeit dort fortsetzen zu können, wie Sie sie verlassen haben, oder um die Arbeit im Fall einer wiederkehrenden Aufgabe bequem aufnehmen zu können.

Alle schließen: Schließt alle offenen Datenfenster und damit alle momentan dargestellten Dateien, Datenträger usw. Wenn Sie Daten editiert (geändert) haben, werden Sie für jedes einzelne Datenfenster, das nicht gespeicherte Änderungen enthält, gefragt, ob Sie die Änderungen speichern oder verwerfen möchten.

Ohne Abfragen schließen: Funktioniert wie »Alle schließen«, aber ohne Ihnen die Möglichkeit zu geben, etwaige Änderungen an den Daten in den Datenfenstern zu speichern, ohne Sie einzeln für jedes solche Datenfenster zu fragen. Da dies ein ziemlich gefährlicher Befehl ist, weil Sie große Mengen an Arbeit verlieren könnten, wenn Sie Daten in vielen Datenfenstern editiert hatten, wird es eine Warnung ausgegeben und Sie können die Ausführung des Befehls abbrechen. Es ist klar, dass eine Bestätigung erforderlich ist, bevor der Befehl ausgeführt wird, weil die Bezeichnung des Menübefehls mit drei Punkten abschließt (so ist die Konvention).

Übereinander/Horizontal/Vertikal: Ordnet die Datenfenster wie beschrieben an.

Minimieren: Verkleinert alle Datenfenster.

Symbole anordnen: Richtet verkleinert dargestellte Datenfenster ordentlich am unteren Rand des Hauptfensters aus.

4.14 Hilfe-Menü

Inhalt: Ruft die Inhaltsübersicht der Programmhilfe auf.

Setup: Lässt Sie die Sprache der Benutzeroberfläche umschalten. Wenn Sie Deutsch wählen, erhalten Sie die Gelegenheit, (fast) alle ß durch ss ersetzen zu lassen. Diese Einstellung ist für Benutzer in der Schweiz und in Liechtenstein gedacht.

Initialisieren: Mit dieser Funktion können Sie die Voreinstellungen sämtlicher Optionen wiederherstellen. Alternativ dazu können Sie die Datei »winhex.cfg« löschen, bevor Sie das Programm starten.

Deinstallieren: Mit dieser Funktion können Sie das laufende Programm von Ihrem System entfernen, selbst wenn Sie nicht das Setup-Programm zur Installation verwendet haben.

UI Text Adjustments: You can rename many directory browser columns to your liking, for example in order to keep continuity in the user interface between earlier and future versions, or for compatibility in data transfers (e.g. Export List command), or because a certain column title has not been translated to your preferred Latin-based user interface language and you would like to see your own translation of the English title, or because you prefer to see "Attributes" instead of the abbreviation "Attr.", etc. In the dialog window with the directory browser options you can simply right-click a column title for that, and will then be given the opportunity to replace the title with your own wording.

Many more text fragments (strings) in the user interface are customizable, through this menu command in the Help menu. You would need to identify the exact standard text fragment to replace and provide your own version of it. If the text that you are looking for is not found and you don't know exactly how it is stored internally, you can search for it in the file "language.dat". Your customizations are stored in the file "UI Text Adjustments.txt" and can be shared with other users. The file can presumably be used in future versions as well, as long as the original text fragments remain the same. It simply consists of one adjustment per line, with the original text first and the replacement second, delimited by a tab character (meaning those few original texts that already contain a tab character cannot be adjusted). You may also edit that file manually. Please note that the translations of non-Latin languages are available as simple text files and can thus be changed in those files much more directly.

Online: Lädt in Ihrem Web-Browser, sofern Sie eine Internet-Verbindung haben, Webseiten wie die Homepage von X-Ways, das Support-Forum, die Seite zum Abonnieren des Newsletters in Ihrem Browser oder die Seite, auf der Sie Ihren Lizenzstatus, aktuelle Download-Links sowieso Upgrade-Angebote abfragen können. Es gibt eine außerdem Option zum **gelegentlichen Prüfen auf Updates** bei Programmstart (**online**), und Sie können auch jederzeit wenn Sie möchten auf Updates prüfen lassen. Dabei wird u. U. die Verfügbarkeit einer neueren Version oder eines neuen Service-Releases der aktuell verwendeten Version (keine Vorab-Versionen) angezeigt, und Sie erhalten die Möglichkeit zum sofortigen Herunterladen. Es werden keinerlei Daten von innerhalb des Programms an das Internet übertragen, z. B. Auch keine System-Information, Benutzer-Informationen oder Dongle-ID, weder direkt noch verschlüsselt oder anonymisiert, nicht mal die aktuell verwendete Versionsnummer, sondern gar nichts. Diese Option ist standardmäßig aktiv nur dann, wenn das Programm davon ausgehen kann, dass es auf dem eigenen System des Benutzers ausgeführt wird (wenn von Laufwerk C: aus gestartet oder wenn es mit dem Setup-Programm installiert wurde). Die Prüfung findet nicht schon beim ersten Programmstart statt, so dass Sie auf jeden Fall die Gelegenheit haben, diese Option auszuschalten, bevor etwas passiert. Angesichts der Tatsache, dass die meisten Systeme, auf denen X-Ways Investigator und X-Ways Forensics verwendet werden, keine Internet-Verbindung haben, hat diese Option nur eine begrenzte Wirkung.

Klick auf die Versionsnummer ganz rechts in der Menüleiste: Zeigt Information über die Software an, insbes. die Programmversion, Freischaltzustand, wieviel freier Speicher dem Programm zur Verfügung steht auf dem Laufwerk für temporäre Dateien und Image-Dateien, ob

das Programm explizit mit Administratorrechten ausgeführt wurde, ob das MS Visual C++ 2013 Redistributable Package (für die neueste Version der Viewer-Komponente und Dokan) installiert ist und ob zumindest das MS Visual C++ 2005 Package installiert ist (für v8.5.2 der Viewer-Komponente sowie noch ältere Versionen). Some of this information can be important when running X-Ways Forensics on a live system, i.e. a system that is not your own and that you wish to examine.

4.15 Windows-Kontextmenü

Das Kontextmenü sehen Sie, wenn Sie im Windows-Explorer oder auf dem Desktop ein Objekt mit der rechten Maustaste anklicken. WinHex erscheint im Kontextmenü nur, wenn die entsprechenden Optionen eingeschaltet sind.

Editieren mit WinHex: Öffnet die gewählte Datei in WinHex.

Ordner in WinHex öffnen: Lässt Sie alle Dateien des gewählten Ordners in WinHex öffnen (wie „Ordner öffnen“ im Datei-Menü).

Datenträger editieren: Öffnet den gewählten Datenträger im Disk-Editor von WinHex. Wenn Sie die SHIFT-Taste gedrückt halten, wird statt des logischen Laufwerks der zugehörige physische Datenträger geöffnet.

WinHex stellt in der Statusleiste und im Positions-Manager eigene Kontextmenüs zur Verfügung.

5 Forensische Features

5.1 Image als Datenträger interpretieren

Dieser Befehl im Specialist-Menü behandelt eine geöffnete und aktive Image-Datei entweder als logisches Volume (möglicherweise mit einem unterstützten Dateisystem) oder als physischer (möglicherweise partitionierter) Datenträger. Das ist nützlich, wenn Sie den Inhalt eines Disk-Image untersuchen möchten, einzelne Dateien aus dem Dateisystem extrahieren möchten usw., ohne auf Unterstützung durch das Betriebssystem angewiesen zu sein. Beim Interpretieren als physischen Datenträger kann WinHex die im Image enthaltenen Partitionen öffnen wie von einer »echten« physischen Festplatte. Dieselbe Funktionalität wird intern auch dann eingesetzt, wenn Sie in X-Ways Forensics Images einem Fall hinzufügen und bei jedem späteren erneuten Öffnen, und außerdem dann, wenn Sie den Befehl Datei | Öffnen aufrufen und dem Programm bei der Gelegenheit schon mitteilen, dass die zu öffnende Datei ein Image ist.

Es ist auch möglich, dateiübergreifende Roh-Images zu interpretieren, also Image-Dateien, die aus einzelnen Segmenten beliebiger Größe bestehen (sog. "spanned image files"). Damit WinHex

ein dateiübergreifendes Image erkennt, gibt es ein paar Benennungsregeln, die unterstützt werden
1) Das erste Segment darf eine beliebige nicht-numerische Dateinamenserweiterung haben (z. B. .dd oder .img). Dann muss das zweite Segment .002 heißen, das dritte Segment .003 usw.
2) Das erste Segment darf eine der folgenden numerischen Dateinamenserweiterungen haben: .001, .0001, .00001, .000, .0000 oder .00000. Die folgenden Segmente müssen die Zählweise dann fortlaufend fortführen mit der exakt selben Anzahl von Ziffern, also entweder drei, vier oder fünf.
3) abc.bin, abc_1.bin, abc_2.bin, ...
Für 1) und 2) müssen alle Segmente denselben Basisnamen haben (den Teil vor der Erweiterung). Der Befehl Datenträger-Sicherung erzeugt kompatibel benannte Disk-Image-Segmente. Das Segmentieren ist nützlich, da die maximal unterstützte Dateigröße in FAT32-Dateisystemen oder auf Datenträgern wie DVD stark beschränkt ist. Es kann auch der Risikoreduktion dienen (je kleiner die Segmente, desto weniger katastrophal ist der Datenverlust, wenn aufgrund eines Dateisystemfehlers eine Datei verlorengeht) und könnte einen Geschwindigkeitsvorteil mit sich bringen (wenn das Betriebssystem oft benötigte Daten effektiver puffern kann, wenn diese in kleineren Segmenten enthalten sind).

In seltenen Fällen ist WinHex u. U. nicht in der Lage, die Natur eines Images, also ob es ein Image eines physischen, partitionierten Datenträgers oder eines Volumes ist, zu erkennen, und interpretiert die Daten im Image daraufhin falsch. Um Abhilfe zu schaffen, können Sie die Umschalt-Taste beim Aufruf dieses Befehls gedrückt halten, damit WinHex nicht selbst entscheidet, sondern Sie fragt. Sie haben dann außerdem die Gelegenheit, die korrekte Sektorgröße anzugeben und im Fall eines Roh-Images einen zusätzlichen Speicherort, an dem weitere Image-Datei-Segmente zu finden sind (falls Sie diese aus Speicherplatzmangel auf zwei Laufwerke aufteilen mussten). Sollte es Probleme bei der Erkennung des Dateisystems in einem Volume geben, können Sie die Umschalt-Taste beim Öffnen dieses Volumes gedrückt halten, um WinHex das von Ihnen darin vermutete Dateisystem mitzuteilen.

ISO-CD-Images (Mode 1 und Mode 2 Form 1) mit 2.352 Bytes pro Sektor werden auch unterstützt, sofern sie nicht segmentiert sind, sowie (mit einer forensischen Lizenz) auch Hauptspeicher-Dumps. Auch VMware Virtual Machine Disk Images (VMDK) und Images von Virtual PC (VHD, VHDX) sowie Virtual Box Disk Images (VDI) des Standard-Untertyps "sparse" und der Untertypen "fixed size" und "diff" (Snapshots) können interpretiert werden. Snapshot-Images können nur dann interpretiert werden, wenn das Eltern-Image, auf das sie sich beziehen, verfügbar ist und zuvor geöffnet und interpretiert wird. VMDK-Images mit ESXi Host-Sparse-Extents (auch “Copy-on-Write Disks” oder COWD genannt), wie von ESXi-Servern z. B. für Snapshots von virtuellen Maschinen verwendet, werden nicht unterstützt. Nur allozierte Bereiche in Images von virtuellen Maschinen sind editierbar. X-Ways Forensics und X-Ways Investigator können auch .e01-Evidence-Files interpretieren, die mit dem Befehl Datenträger-Sicherung erstellt werden können, außerdem unverschlüsselte Ex01-Evidence-Files.

Es ist außerdem möglich, Images diverser Typen (Roh-Images und die meisten VHD/VHDX/VMDK/VDI sowie Backup-Bundles von Apple Time Machine in Form der Datei „com.apple.TimeMachine.MachineID.plist“) und Natur (Disk oder Volume) sogar dann zu interpretieren, wenn sie innerhalb von anderen Images gespeichert sind (forensischen Datenträger-Sicherungen von Ihnen selbst), ohne sie erst aus dem äußeren Image herauszukopieren, sofern sie nicht aus mehreren Segmenten bestehen. Das kann eine Menge Zeit ersparen, insbes. dann, wenn Sie nach dem Interpretieren des enthaltenen Images schnell sehen,

dass es nicht wirklich relevant ist, und natürlich auch Speicherplatz. Klicken Sie das Image dazu im Verzeichnis-Browser mit der rechten Maustaste an und öffnen Sie es mit dem Öffnen-Befehl in einem separaten Datenfenster. Danach interpretieren Sie das Image mit dem Befehl im Hauptmenü als Datenträger. Und danach, wenn der Datei-Überblick erstellt wurde und Sie das Image für relevant halten, fügen Sie es dem aktiven Fall wie gewöhnlich über den Befehl "Zum aktiven Fall hinzufügen" im Kontextmenü der Registerkarte des Datenfensters hinzu oder mit dem Hinzufügen-Befehl im Datei-Menü des Falldatenfensters. Image files within TAR archive should also work, which is handy for VMDK virtual machine disks within OVA files (open virtualization archives in TAR format).

Lose $MFT-Dateien können direkt und bequem interpretiert werden, als wären sie Images von NTFS-Partitionen, um zumindest eine vollständige Auflistung aller Dateien und Verzeichnisse zu erhalten, mitsamt Pfad, Zeitstempeln und Attributen. Es ist dann möglich, residente Dateien zu öffnen (solche Dateien, die klein genug sind, um in einen FILE-Record zu passen), aber natürlich keine sonstigen Dateien. Nützlich in besonderen Situationen, wenn Sie lediglich die $MFT vorliegen/gesichert haben, nicht das gesamte Dateisystem.

5.2 Fallbearbeitung

Die integrierte Umgebung für Computerforensik in WinHex kann nur mit einer forensischen Lizenz benutzt werden. Sie bietet eine komplette Fall-Verwaltung an, automatische Protokoll- und Berichterstellung und verschiedene zusätzliche Features wie Galerie-Ansicht, Dateisignatur-Prüfung, Erkennung von geschützten Festplattenbereichen und Erkennung von Hautfarben in Bildern.

Wenn Sie WinHex zum ersten Mal starten, werden Sie gefragt, ob Sie die Software mit der forensischen Benutzeroberfläche starten möchten. Das heißt, das Falldaten-Fenster wird angezeigt, WinHex im Schreibschutz-Modus ausgeführt und Sie werden gefragt, ob die Ordner für temporäre Dateien und Falldaten korrekt eingestellt sind, um zu verhindern, dass WinHex Dateien auf das falsche Laufwerk schreibt.

Um an einem Fall zu arbeiten, stellen Sie sicher, dass das Falldaten-Fenster (links im Hauptfenster) sichtbar ist. Wenn es das nicht ist, schalten Sie Ansicht | Anzeigen | Falldaten ein.

Vom Datei-Menü aus können Sie einen neuen Fall erstellen (neu beginnen), einen existierenden Fall öffnen, den aktiven Fall schließen, den aktiven Fall speichern, eine Sicherung der Falldatei und des Fallverzeichnisses in Form eines ZIP-Archivs erstellen (nur für Dateien bis 4 GB möglich), und einen automatischen Bericht zum aktiven Fall erzeugen. Als Asservate können Sie Datenträger hinzufügen oder Images (Dateien, die wie Datenträger interpretiert werden, s. Specialist-Menü) sowie Hauptspeicher-Abbilder und Verzeichnisse auf Ihrem eigenen Computer. Das Hinzufügen eines Verzeichnisses anstelle einer ganzen Partition oder einer ganzen Festplatte kann nützlich sein, wenn das relevante Verzeichnis oder die relevante Datei auf einem Laufwerk mit vielen irrelevanten Dateien liegt, wenn Sie lediglich einige wenige dieser Dateien einsehen, hashen durchsuchen, auf Metadata prüfen oder in einem Datei-Container aufnehmen möchten.

Ein Fall wird in einer .xfc-Datei gespeichert (xfc steht für X-Ways Forensics Case) und in einem

Unterordner desselben Namens, nur ohne die .xfc-Erweiterung. Dieser Unterordner und dessen Unterordner werden automatisch beim Anlegen des Falls erzeugt. Den Basisordner für Ihre Fälle können Sie unter Allgemeine Optionen auswählen. Es ist nicht erforderlich, einen Fall explizit zu speichern, es sei denn, Sie möchten sicher sein, dass er zu einem bestimmten Zeitpunkt gesichert ist. Ein Fall wird spätestens dann automatisch gespeichert, wenn er geschlossen wird oder Sie das Programm verlassen. Die einzige Ausnahme ist die Verwendung des Befehls "Fall schließen (nicht speichern)". For example if you have accidentally lost your carefully set tag marks (by untagging all, with a misdirected click in the column header) or if you accidentally lost labels (by pressing Ctrl+0 for all selected files), it is important to invoke that special menu command as soon as possible, before the auto-save interval elapses next time, to avoid that the volume snapshot(s) will be saved. Afterwards you can open the case again, and find everything as it was last time when the case was saved, which means that on average you will only lose half the amount of work that you get done within the auto-save interval, not everything.

Im Fenster „Eigenschaften“ eines Falls können Sie einen Fall nach Ihren Konventionen benennen oder ihm eine Nummer zuweisen. Datum und Zeit der Anlage des Falls werden aufgenommen und angezeigt. Der interne Fall-Dateiname ist ebenfalls zu sehen. Sie können eine Beschreibung des Falls (beliebiger Länge) angeben sowie den Namen des Bearbeiters, dessen Organisation und Anschrift usw. Sie können von hier aus auch die automatische Mitprotokollierung für den Fall aus- oder einschalten. Optional werden immer die Unterverzeichnisse der jeweiligen Asservate im Fallordner als Standard-Ausgabeordner beim Wiederherstellen/Herauskopieren von Dateien aus Dateisystemen vorgeschlagen. Diese Eigenheit können Sie ausschalten, wenn Sie z. B. Dateien von verschiedenen Asservaten in einen einzigen Ausgabeordner kopieren möchten.

Sie können bis zu zwei Codepages, die sich für die Bearbeitung des Falls eigenen (also typisch sind für die Region, in der die zu untersuchenden Originaldatenträger verwendet wurden). Diese Codepages werden beim Benennen von .eml-Dateien basierend auf der Betreffzeile benutzt (.eml-Dateien, die aus E-Mail-Archiven extrahiert wurden). Wenn beide Codepages identisch sind, hat das keine negativen Auswirkungen. Wenn sie identisch mit der derzeit in Windows aktiven Codepage sind, haben sie überhaupt keine Auswirkungen. Diese Codepages werden auch benutzt, um Dateinamen in Zip-Archiven nach Unicode zu konvertieren. The first code page can be defined as an expected code page in Outlook PST files. Für Ext*-Dateisysteme können Sie bei der Interpretation von Datei- und Verzeichnisnamen bei Bedarf auf eine bestimmte alternative Codepage (also nicht UTF-8) zurückzugreifen oder deren Verwendung sogar zu erzwingen. Dazu versetzen Sie das Kontrollkästchen neben der zweiten fallspezifischen Codepage in den halb oder ganz gewählten Zustand. Diese Codepage wird verwendet für Namen, die nicht wie in Linux üblich in UTF-8 codiert sind, in bestimmten Altsystemen oder in speziellen Umgebungen, in denen eine andere Codepage eingestellt wurde.

Zwei Arten von proaktiven Filtern, basierend auf Namen und Zeitstempeln, können in den Eigenschaften eines Falls aktiviert werden. Proaktive Filter ermöglichen es, einen anfänglich erzeugten Datei-Überblick einzuschränken. Dateien, die die Filterbedingung(en) nicht passieren, werden in keinen Datei-Überblick aufgenommen, der erzeugt wird, während solche Filter aktiv sind. Verzeichnisse sind von der Einschränkung nicht betroffen und werden normal aufgenommen. Die Filter wirken sich nur auf Partitionen/Volumes und Datei-Archive aus, die Asservate sind, und alle Dateien, die direkt in ihnen gefunden werden durch Verfolgen der Datenstrukturen des jeweiligen Dateisystems bzw. Archivs. Sie beschränken nicht das Hinzufügen von Dateien, die auf irgendeine andere Art und Weise gefunden werden, z. B. über

eine Datei-Header-Signatur-Suche oder durch Prüfen von Dateien, die bereits im Datei-Überblick enthalten sind, auf eingebettete Daten o. ä. Proaktive Filter sind besondere Filter, weil sie verhindern können, dass Dateien überhaupt in einen Datei-Überblick gelangen können: Dateien, die Sie nicht benötigen oder nicht dort haben möchten oder die Sie gar nicht zu Gesicht bekommen sollten. Entweder weil Ihre Aufgabe oder Ihr Augenmerk beschränkt ist auf bestimmte Dateien, deren Namen oder Zeitstempelbereiche im voraus bekannt sind oder weil das Asservat (Sicherung oder Datei-Archiv) so groß ist, dass Sie allein durch das Vermeiden von Hunderten von Millionen Dateien massiv Zeit und Hauptspeicher einsparen oder das Volume überhaupt erst für X-Ways Forensics verdaulich machen (d. h. die Größe eines Datei-Überblicks innerhalb der unterstützten Grenzen halten können). Die Erzeugung des Datei-Überblicks selbst kann auf diese Art merklich beschleunigt werden, wenn das Asservat eine Sicherung ist, und all die nachfolgenden Schritte (Navigieren, Auflisten, Sortieren, Filtern, Erweiterung des Datei-Überblicks) sind weniger rechenintensiv, wenn sie bereits im Vorhinein die Aufnahme einer so großen Zahl ungewollter Dateien verhindern konnten. Die Anzahl der proaktiv ausgelassenen Dateien wird während der Erzeugung des Datei-Überblicks im Fortschrittsanzeigefenster dargestellt. Nach Abschluss der Erzeugung des Datei-Überblicks ist die Gesamtzahl solcher Dateien im Status des Datei-Überblicks ersichtlich, im Dialogfenster für die Erweiterung des Datei-Überblicks. Eine Warnung, dass ein proaktiver Filter greift, wird pro Sitzung einmal im Nachrichtenfenster ausgegeben, wenn ein Datei-Überblick erzeugt wird.

Es gibt die Option, den Hash einer Datenträgersicherung sofort automatisch nach dem Hinzufügen zum Fall zu überprüfen, sofern ein solcher Hash-Wert vorhanden ist, oder (wenn das Kontrollkästchen ganz angekreuzt ist) einen solchen Hash-Wert bei der Gelegenheit von Grund auf neu zu berechnen, wenn kein Wert vorgefunden wird. Neu erzeugte Fälle erben diese Einstellung vom letzten geöffneten Fall, dessen Eigenschaften Sie mit OK bestätigen. Das bedeutet auch, dass Sie Images per Befehlszeile überprüfen lassen können, mit dem AddImage-Befehl. Das Ergebnis wird ausgegeben 1) im Nachrichtenfenster, 2) in der Datei msglog.txt, wenn gewünscht, und 3) in den Eigenschaften des Asservats, d. h. der Repräsentation des Images im Fall.

Falldateien können mit einem Passwort geschützt werden. Dies ist keine Verschlüsselung, sondern nur eine Art Sperre. Falldateien, die mit X-Ways *Investigator* gesperrt wurden, können notfalls mit dem Super-User-Passwort geöffnet werden, wenn ein solches zum Zeitpunkt des Speicherns bereits in der verwendeten Installation hinterlegt war (undokumentiert, Details auf Anfrage).

When creating a new case, you have the option to make X-Ways Forensics recognize evidence objects that are physical media (not images) by their own intrinsic properties, not by the Windows disk number. Using this option will prevent earlier versions of X-Ways Forensics from opening the case. The advantage is that you may add multiple hard disks or external USB disks or sticks to the case that are attached to the computer at different times and get the same disk number assigned by Windows. Another advantage is that if the number of the same disk as assigned by Windows changes, X-Ways Forensics will still recognize the disk. Useful especially for triage, when not working with images. Please note that X-Ways Forensics may be unable to recognize external media already known to the case if next time they are attached through a different hardware write blocker. In that situation you can still use the "Replace with new disk" command in the evidence object context menu to point X-Ways Forensics to the correct disk. Note that component disks of an internally reconstructed RAID (read disks, not images) are still

remembered by the Windows disk number when re-opening a RAID that you have added to a case.

When clicking the “Passwords...” button, the case's password lists for encrypted general purpose file archives will open in your preferred text editor for editing.

Wenn Sie den mit „SIDs...“ bezeichneten Schalter anklicken, sehen Sie eine Sammlung aller Kombinationen von SIDs und Benutzernamen, die bei der Bearbeitung des Falls angetroffen wurden (gesammelt aus SAM-Registry-Hives in allen Windows-Installationen in Images und auf Datenträgern, die jemals dem Fall hinzugefügt wurden). Sie werden von X-Ways Forensics verwendet, um SIDs in Benutzernamen aufzulösen, wenn mit diesem Fall gearbeitet wird.

Das mächtigste Konzept in X-Ways Forensics, welches die systematische und vollständige Auswertung von Dateien auf Computer-Datenträgern erlaubt, ist der sogenannte *erweiterte Datei-Überblick*. Es ist möglich, solche erweiterten Datei-Überblicke für alle Asservate in einem Fall in einem Schritt zu erstellen und alle Asservate mit Datei-Überblicken logisch auf einmal mit Hilfe des global Fallwurzelfensterns zu durchsuchen. Beachten Sie, dass es möglich ist, eine flache Ansicht aller existierender und gelöschter Verzeichnisse aus allen Unterverzeichnissen auf einer Partition oder einer Image-Datei einer Partition zu erhalten, indem man das Stammverzeichnis rekursiv erkundet. Zum rekursiven Erkunden eines Verzeichnisses (d. h. Auflisten seines Inhalts incl. des Inhalts all seiner Unterverzeichnisse und deren Unterverzeichnisse) klicken Sie es im Verzeichnisbaum mit der *rechten* Maustaste an. Um ein Verzeichnis zu markieren, klicken Sie im Verzeichnisbaum mit der mittleren Maustaste an.

Backups

Der Befehl "Sichern/Wiederherstellen" im Kontextmenü des Falldatenfensters erlaubt es, bequem ein Backup des Datei-Überblicks des gewählten Asservats anzufertigen. Backups können mittels desselben Befehls später jederzeit wiederhergestellt oder auch gelöscht werden (klicken Sie einen Eintrag in der Liste der Backups rechts an, um den Lösch-Befehl zu erhalten). Ein solches Backup ist wie ein Snapshot eines Datei-Überblicks. Nützlich, wenn Sie der Meinung sind, dass Sie später zu einer bestimmten Verarbeitungsstufe zurückkehren (d. h. alle folgenden Änderungen des Datei-Überblicks rückgängig machen) möchten, beispielsweise weil Sie aufwendig Tausende Dateien markiert haben, die Sie nicht verlieren wollen, bevor Sie mit experimentellen Einstellungen eine Datei-Signatur-Suche laufen lassen, die ggf. viele Schrott-Dateien erzeugt; bevor Sie externe Dateien mit Optionen, die Sie noch nie ausprobiert haben, anhängen lassen; bevor Sie eine X-Tension laufen lassen, die aus einer fremden Quelle stammt; bevor Sie ausgeblendete Dateien völlig aus dem Datei-Überblick entfernen lassen. Vermerke, Ereignisse und Suchtreffer sind im Backup ebenfalls enthalten. Suchtreffer können aus dem Backup nur wiederhergestellt werden, wenn sich die Suchbegriffsliste des Falles in der Zwischenzeit nicht geändert hat. Indexe sind im Backup nicht enthalten, können aber natürlich manuell gesichert werden.

Derselbe Befehl, angewandt auf den gesamten Fall (klicken Sie zu diesem Zweck den fett dargestellten Fallnamen rechts an), erlaubt die Erzeugung eines Backups für den gesamten Fall, einschließlich aller Datei-Überblicke aller Asservate, aller Vermerke, Ereignisse, Suchbegriffe, Suchtreffer, Indexe, Image-Datei-Pfade, usw. usf. Solche Backups können über dasselbe Dialogfenster wiederhergestellt werden. Solche Backups können auch mit dem "Fall öffnen"-

Befehl direkt geöffnet werden, falls notwendig, da es sich um vollständige Kopien des Falles handelt. (Die Backup-.xfc-Dateien werden aber mit dem Attribut "versteckt" versehen, da sie eigentlich nur innerhalb von X-Ways Forensics direkt verwendet werden sollen.)

Um einen Fall oder ein Backup eines Falls komplett manuell zu *löschen*, müssen Sie die .xfc-Datei und sein zugehörigen Verzeichnis selben Namens mit all seinen Unterordnern löschen.

5.3 Mehrbenutzerfähigkeit für größere Verfahren

X-Ways Forensics und X-Ways Investigator unterstützen eine *arbeitsteilige Auswertung* durch mehrere Benutzer (Ermittler) im selben Fall, wobei die Software diese Benutzer anhand ihrer Benutzerkonten in Windows unterscheidet und ihre Ergebnisse getrennt verwaltet. Die Benutzer können dieselben Asservate desselben Falls gleichzeitig öffnen. MMaximal werden 255 Benutzer pro Fall unterstützt. Benutzer werden intern anhand Ihrer Windows-Benutzerkonten erkannt.

Mehrere Benutzer können dieselben Asservate im selben Fall gleichzeitig zur Untersuchung öffnen. Mit demselben Fall ist dieselbe Falldatei gemeint, keine Kopie, gespeichert in einem gemeinsam genutzten Verzeichnis im Netzwerk oder auf einem Terminal-Server. X-Ways Forensics ist dafür verantwortlich, Vermerke, Kommentare und das Hinzufügen von Dateien zum Datei-Überblick zu synchronisieren und Benutzer auf Zugriffskonflikte hinzuweisen, bevor diese eintreten, oder sie in den meisten Situationen ganz zu vermeiden.

Alle relevanten Optionen zu diesem Thema lassen sich erreichen durch einen Klick auf den Schalter namens „Mehrbenutzer-Optionen“ im Eigenschaftsfenster des Falls. Insbesondere können Sie beim Erzeugen eines Falls (dann und nur dann) X-Ways Forensics dazu veranlassen, *nicht* zwischen verschiedenen Benutzern zu unterscheiden. Das kann nützlich sein, wenn Sie wissen, dass *nur* Sie den Fall bearbeiten werden und Sie ihn auf verschiedenen Computern bearbeiten werden, auf denen Sie lokale Windows-Benutzerkonten mit unterschiedlichen SIDs unterhalten, so dass Sie immer als derselbe Benutzer behandelt werden. Auch nützlich, wenn mehrere Ermittler denselben Fall zu unterschiedlichen Zeiten bearbeiten sollen und dabei all ihre Ergebnisse direkt miteinander teilen möchten.

Eine weitere Option koordiniert bestimmte Zugriffe auf Datei-Überblicke (Hinzufügen von Dateien sowie Editieren von Kommentaren und Metadaten) *sorgfältiger*. Kann die Verwendung des Programms beschleunigen, wenn ausgeschaltet. Das Ausschalten dieser Synchronisation ist empfehlenswert nur für Fälle, die definitiv nur von 1 Benutzer zur gleichen Zeit bearbeitet werden.

Vermerke und Kommentare verschiedener Ermittler können optional optisch unterschieden werden, by showing the creating examiner's initials (default), or alternatively other abbreviations of their names or (if no abbreviation is specified) their complete usernames. Examiners can choose whether or not they get to see labels of other users or only their own (or, if half checked, only their own labels plus those of unknown users). The same file can get a particular label only by 1 examiner. X-Ways Forensics imports and shows newly created labels of simultaneous other users in shared analysis mode when re-opening an evidence object or when case auto-save interval elapses or when manually invoking the Save Case command. The option to show initials for la-

bels is represented as a 3-state checkbox. If half-checked, it has an effect on the directory browser only, not for the Export List or Recover/Copy command for example and not in the case report.

X-Ways Forensics remembers the "tagged", "already viewed" and "excluded" status of files separately for each examiner. You can choose to adopt the "already viewed" status of files in volume snapshots from all other examiners when opening evidence objects. That is useful if the goal is to avoid duplicate work, if you do not wish to review files that were reviewed by any of your colleagues already. Please note that individual file statuses ("tagged", "already viewed" and "excluded") as well as search hits of other users are lost if one examiners *removes* items from the volume snapshot.

Search hits and search terms are stored on a per-user basis as well. The first examiner opening an older case with v17.5 or later will absorb the search hits and search terms that were stored in the case by v17.4 or earlier. The "Multi-user support options" dialog window contains a button that allows you to import the search hits and search terms of another user. An option is available to limit the import of another user's search hits to search hits that are marked as notable or to that user's manually defined search hits (so-called user search hits). Another option allows to *take away* the search hits from the other user when importing them. Useful if the other user is going to resume his work later and will want to import *your* search hits back when he or she is taking over again, to avoid duplications of search hits, because your search hits include his or her hits already after you have imported them.

Um *alle* Ergebnisse eines Kollegen/einer Kollegin zu sehen (Vermerke, Suchtreffer, markierungen, Eingesehen-Status von Dateien, Ausgeblendet-Status von Dateien), können Sie den Fall im Schreibschutzmodus als diese(r) Kollege/in öffnen. Dazu versehen Sie das Kontrollkästchen "Optionen..." beim Öffnen eines Falls mit einem Häkchen. Sie können Kolleg(inn)en darin hindern, einen Fall schreibgeschützt als Sie selbst zu öffnen, wenn Sie möchten.

Das Kontrollkästchen "Optionen..." erlaubt es, einen Fall in einem der folgenden drei Modi zu öffnen:

1) den gesamten Fall als schreibgeschützt (Falldatei und Datei-Überblicke),
2) arbeitsteilige Auswertung (mit der Möglichkeit, Vermerke zu erstellen, Kommentare, Suchtreffer, virtuelle Dateien und Markierungen, sowie sich bereits eingesehene Dateien merken zu lassen und Dateien auszublenden)
3) normal, unbeschränkt

Falls derselbe Benutzer denselben Fall (dieselbe Kopie) in mehr als 1 Instanz des Programms gleichzeitig öffnen möchte, hat er zwei Möglichkeiten dafür. Entweder
1) wird der gesamte Fall incl. Asservate in der zweiten Instanz als schreibgeschützt geöffnet *oder*
2) der Benutzer öffnen den Fall als ein separater, fiktiver Benutzer (als sein "Alter Ego") mit separatem Dateistatus, separaten Suchtreffern, Vermerken usw. (die gemeinsame Benutzung des Falls und der Asservate wird von X-Ways Forensics genauso koordiniert, als ob das Alter Ego ein echter anderer Ermittlerkollege wäre, obwohl der Benutzername in Windows derselbe ist).

The aforementioned "Options..." checkbox allows you at any time to open the case as your alter ego, not only when opening the same case in a second instance of the program. It also allows you to open a case in shared analysis mode if it is not open anywhere else at the moment.

Multiple users running searches, creating Vermerke, entering or editing comments, editing extracted metadata, tagging files, excluding files, marking files as already viewed is all supported for the same evidence object at the same time. *Removing* items from a volume snapshot while the evidence object is open somewhere else, however, is forbidden and will be refused by the program. The goal of the multi-user coordination in v17.5 and later is to support concurrent *analysis*/*review* work by multiple examiners. *Removing* files from a volume snapshot is not considered ordinary review/analysis work. Volume snapshot refinements should be done systematically *in advance*.

The initials of the examiner who has attached files to the volume snapshot or manually carved files in v17.5 and later can be seen in square brackets next to the filename, so that it is easy to tell who has introduced such files to the case.

Technical changes to the way how multiple simultaneously users are coordinated are reserved. To be on the safe side, please make sure that simultaneous users are running the same version of the software.

Last not least v17.5 allows you to review the processing history of a case in its properties. This reveals which versions were used on it (recorded only by v17.3 SR-10 and later, v17.4 SR-4 and later and v17.5 and later) and by which users (recorded only by v17.5 and later).

You may turn *off* "Coordinate processing by simultaneous users more carefully" for some performance benefits if there is only user of a case at a time.

There is an option to always suggest shared analysis mode when opening a case. That mode can be useful even for the first of many simultaneous users that open the same case because only in that mode newly created Vermerke are shared out to other simultaneous users at regularly intervals (depending on the case auto-save option).

Weitere Möglichkeiten zur verteilten Auswertung

Option 1: Mehrere Anwender von X-Ways Forensics können gleichzeitig in ihrer jeweils eigenen Kopie desselben Falls arbeiten (immer sowohl die .xfc-Datei kopieren als auch das zugehörige Unterverzeichnis) und ihre Ergebnisse untereinander austauschen oder alle Ergebnisse in der Hauptkopie des Falls zusammenfassen, indem sie Vermerke (d. h. ihre Kategorisierung aller relevanten Dateien und E-Mails) exportieren und importieren.

Option 2: Potentiell relevante Dateien werden aus den Originalasservaten in mehrere Datei-Container kopiert. Diese Container werden dann von verschiedenen Ermittlern gleichzeitig in neu erstellten Fällen (in X-Ways Forensics oder X-Ways Investigator) ausgewertet. Auch sie können ihre Vermerke exportieren, woraufhin sie wieder im Originalfall importierbar sind.

Beide Befehle, der Export und der Import von Vermerken, können im Kontextmenü des Fallbaums gefunden werden. Das Exportieren wird auf der Fall- und Asservatebene unterstützt, das Importieren auf der Fallebene. Bitte beachten Sie, dass Sie Vermerke nicht mehr in den Originalfall importieren können, wenn Sie in der Zwischenzeit einen neuen Datei-Überblick erstellt haben oder Objekte aus dem Datei-Überblick entfernt haben, denn dann ist nicht mehr

garantiert, dass die internen IDs der Dateien gleich bleiben und eine sichere Zuordnung möglich ist. Das Importieren funktioniert nur, wenn man in dasselbe Asservat importiert, aus dem auch exportiert wurde. Gemeint ist Asservat in einem Fall in X-Ways Forensics/Investigator oder in einer Kopie desselben Falls. Dass es ggf. dasselbe Image in einem anderen Fall ist, hilft nicht und kann X-Ways Forensics/Investigator nicht wissen. Auch wenn es derselbe Fall ist, gibt es ein Problem, wenn man das Image aus dem Fall zwischendurch entfernt und dann später wieder hinzugefügt hat. Dann ist es für X-Ways Forensics wie ein neues Asservat. Man kann jedoch auch von einem Container in einem neuen Fall aus exportieren (z. B. beim Anwender von X-Ways Investigator) und wieder in das ursprüngliche Asservat im Originalfall, aus dem die Dateien im Container ursprünglich stammen, importieren (z. B. beim Anwender von X-Ways Forensics), weil im Container Informationen zur Identifizierung des ursprünglichen Asservats enthalten sind.

Verteilte Erweiterung von Datei-Überblicken

X-Ways Forensics erlaubt es, die Datei-Überblicke *verschiedener* Asservate desselben Falls unter Einsatz mehrerer Rechner im selben Netz gleichzeitig zu erweitern, um durch Parallelisierung Zeit zu sparen.

Jeder Benutzer/Computer öffnet dieselbe .xfc-Falldatei (dieselbe Kopie auf demselben Computer). Alle teilnehmenden Benutzer/Computer oder alle bis auf einen (die Hauptinstanz) müssen den Fall als teilweise schreibgeschützt öffnen, d. h. nur verteilte Auswertearbeit und Datei-Überblicks-Erweiterungen erlaubend. Das können Sie erreichen, indem Sie in dem Dialogfenster zum Öffnen des Falls „Optionen...“ ankreuzen, oder Sie werden ohnehin automatisch danach gefragt, wenn Sie den Fall öffnen, wenn dieser bereits in einer anderen Sitzung als nicht schreibgeschützt geöffnet ist (d. h. in der Hauptinstanz). Andere Instanzen sehen die Ergebnisse der Erweiterung spätestens, wenn diese abgeschlossen ist und das Asservat erneut geöffnet wird. Der Fall braucht dazu nicht erneut geöffnet zu werden.

Es besteht die Möglichkeit, einzelne Asservate (nicht nur den ganzen Fall) gezielt so zu öffnen, dass der Datei-Überblick als schreibgeschützt behandelt wird, über einen gesonderten Befehl im Kontextmenü des Asservats im Falldatenfenster. Bitte beachten Sie, dass dies überhaupt nichts damit zu tun hat, wie das Asservat selbst (der Datenträger oder das Image) gehandhabt wird. X-Ways Forensics ändert niemals die Daten in Sektoren von Datenträgern oder interpretierten Images, wenn diese als Asservat geöffnet werden. Nur der Datei-Überblick, d. h. die Datenbank mit Informationen über alle gefundenen Dateien und Verzeichnisse, ist entweder schreibgeschützt oder, und das ist der Normallfall, änderbar.

5.4 Asservate/Beweisobjekte

Sie können jeden an den Computer angeschlossenen Datenträger (wie Festplatte, SSD, Speicherkarte, USB-Stick, CD-ROM, DVD, ...), eine Image-Datei, ein Verzeichnis, ein Dateiarchiv oder eine normale einzelne Datei dem aktuellen Fall hinzufügen. Dadurch wird das Objekt permanent mit dem Fall verbunden (es sei denn, Sie entfernen es später wieder aus dem Fall), in der baumartigen Fallstruktur angezeigt und fortan als Asservat oder Beweisobjekt bezeichnet. Im Fallordner wird für jedes Asservat ein Unterordner angelegt, wo Dateien, die Sie

aus dem Asservat herauskopieren, standardmäßig abgelegt werden, so dass immer offenkundig ist, von welchem Asservat genau (und aus welchem Fall) wiederhergestellte Dateien stammen.

Im Fenster der Asservat-Eigenschaften können Sie eine Bezeichnung oder eine Nummer für das Asservat nach Ihren Namenskonventionen eingeben. Sie können die Reihenfolge von Asservaten im Fallbaum ändern mit Hilfe der kleinen Pfeilschalter oben links, außer für »abhängige« Asservate (Partitions, die zu einem physischen Datenträger gehören). Datum und Zeit des Zuordnens des Asservats zum aktuellen Fall werden aufgenommen und angezeigt. Die programminterne Bezeichnung eines Asservats wird ebenso angezeigt wie seine Originalgröße in Bytes. Sie können Kommentare beliebiger Länge, die sich auf das Asservat beziehen, eingeben. Eine technische Beschreibung wird von X-Ways Forensics automatisch hinzugefügt (wie aus dem Technischen Detailbericht im Specialist-Menü bekannt, jedoch zusätzlich einige grundlegende Information über Windows-Installationen, sofern in einer Partition gefunden). Sie können einen oder zwei Hash-Werte (Prüfsumme oder Digest) des Asservats berechnen und später überprüfen lassen, so dass Sie sicherstellen können, dass die Datenauthentizität in der Zwischenzeit nicht beeinträchtigt wurde. MD5-Hashes in Evidence Files werden automatisch beim Hinzufügen zum Fall importiert. The button with the folder and magnifying glass allows to quickly open the default output directory for the evidence object. Hold the Ctrl key while clicking to navigate to the internally used directory instead, where the volume snapshot is stored.

Um Images oder Datenträger einem Fall hinzuzufügen, verwenden Sie die »Hinzufügen«-Befehle im Datei-Menü des Falldaten-Fensters. Im Fall von Images gibt es die Möglichkeit, direkt nach dem Hinzufügen einer oder mehrerer Images den Datei-Überblick der neuen Asservate zu erweitern. Dateiübergreifend gespeicherte (segmentierte) Zip- und 7z-Archives im Stil von 7-Zip und WinZip werden auch unterstützt. Stellen Sie bitte lediglich sicher, dass Sie immer das *erste* Segment dem Fall hinzufügen. Bei Erzeugung mit 7-Zip heißt dieses .001 und bei Erzeugung mit WinZip .z01. Bei passwortgeschützten (verschlüsselten) Zip-, 7z- und Rar-Archiven werden Sie nach dem Passwort gefragt. Das Passwort kann im Fall gespeichert werden, so dass Sie es beim nächsten Öffnen eines solchen Asservats nicht erneut einzugeben brauchen.Sie können nicht mit einem Fall verknüpfte Images und Datenträger auch mit dem »Hinzufügen«-Befehl im Kontextmenü der Registerkarte des Datenfensters in den Fall aufnehmen. Wenn die Images eines Falls im Fallverzeichnis gespeichert sind (nicht zu verwechseln mit dem Fälleverzeichnis), werden sie immer automatisch wiedergefunden, auch wenn sich der Pfad des Falls ändert. Ein individueller fallspezifischer Standardpfad für Sicherungen kann in den Eigenschaften des Falls aktiviert und festgelegt werden. Dieser hat dann Priorität vor dem generischen Standardpfad für Sicherungen. Der fallspezifische Pfad darf ein relativer Pfad sein, wobei . sich auf das Fallverzeichnis bezieht und .. auf dessen übergeordnete Verzeichnis. Bitte beachten Sie, dass es aus Performanzerwägungen empfehlenswert sein kann, Falldaten und Sicherungen auf zwei separaten physischen Datenträgern abzulegen.

Der Befehl „Durch neues Image ersetzen“ im Kontextmenü eines Asservats erlaubt es Ihnen, einen Originaldatenträger, der einem Fall als Asservat zugeordnet wurde, durch ein Image dieses Datenträgers zu ersetzen (was nützlich ist, wenn Sie ihn erst kurz in Augenschein nehmen möchten, bevor sie ihn sichern), ohne den Datei-Überblick zu verlieren, Suchtreffer, Kommentare usw. Kann auch verwendet werden, um X-Ways Forensics einfach den neuen Pfad eines Images mitzuteilen, falls dieses verschoben wurde oder sich der Laufwerksbuchstabe geändert hat, oder wenn sich der Dateiname des Images geändert hat oder dessen Typ (z. B. Roh-Image konvertiert in ein komprimiertes und verschlüsseltes .e01 Evidence-File). Falls es sich um

ein physisches, partitioniertes Asservat handelt, sollte dieser Befehl auf das Elternobjekt angewandt werden, nicht auf die Kindobjekte (Partitionen). Die Änderung wird dann automatisch auch auf die Kindobjekte durchgereicht. Wenn das neu angegebene Image ein Image eines anderen Datenträgers ist oder ein anderer Datei-Container oder derselbe Datei-Container in einem anderen Zustand (der weiter gefüllt wurde), so dass der Datei-Überblick gar nicht übereinstimmen kann, dann erhalten Sie wahrscheinlich eine Fehlermeldung, weil die Größe des neu angegebenen Images sich vom bisherigen Image unterscheidet. Immer wieder versuchen Benutzer von X-Ways Forensics, mit diesem Befehl ein Asservat in einem Fall durch ein *anderes* Asservat zu ersetzen, obwohl dies überhaupt keinen Sinn ergibt, weil dann alle technischen Beschreibungen, der Datei-Überblick, Suchtreffer, Kommentare, Vermerke nicht mehr passen. Diese Benutzer beschweren sich dann auch oft noch darüber, dass eine Fehlermeldung kommt, weil X-Ways Forensics i. d. R. anhand der Größe merkt, dass das neue Image ein völlig anderes Image ist. Wenn aber ein Asservat A im Fall nicht mehr gebraucht wird und ein neues Asservat B dem Fall hingefügt werden soll, dann kann man einfach A entfernen und B neu hinzufügen. Eine andere Möglichkeit gibt es nicht und ist weder sinnvoll noch erforderlich.

Es ist möglich, ein Asservat auch dann zu öffnen, wenn der zugehörige Datenträger/das Image gerade nicht verfügbar ist, über einen speziellen Befehl im Kontextmenü des Asservats, um zumindest den Datei-Überblick einsehen zu können. Das bedeutet, Sie können alle Datei-Metadaten sehen, die im Datei-Überblick gespeichert sind (Dateiname, Pfad, Dateigröße, Zeitstempel, Attribute usw.), können die meisten Filter verwenden usw., aber können keine Daten in Sektoren sehen und keine Dateien öffnen/einsehen.

Im Asservat-Überblick können Asservate mit einer gelben Flagge als wichtig markiert werden, über das Verzeichnis-Browser-Kontextmenü oder einfach durch Drücken der Leertaste. Die gelbe Flagge ist dann im Falldatenfenster zu sehen und immer, wenn Sie Asservate auswählen, z. B. für die rekursive Erkundung vom Asservat-Überblick aus oder beim Erzeugen eines Berichts.

In den Eigenschaften von Asservaten mit einem FAT-Dateisystem können Sie optional definieren, welche Zeitzone den in Ortszeit gespeicherten Zeitstempel in dem Dateisystem zugrundeliegen, wenn Sie davon eine konkrete Vorstellung haben. Die Zeitzone hängt ab von den Einstellungen in dem Computer oder Gerät, der/das in das Dateisystem geschrieben hat. (Bedenken Sie, dass solche Einstellungen sich im Laufe der Zeit ändern können und eine einzige Zeitzone u. U. nicht ausreicht, um alle Zeitstempel korrekt darzustellen.) Wenn Sie den Zeitzonenbezug definieren, werden Zeitstempel aus der Dateisystemebene gemäß der gewählten Anzeigezeitzone dargestellt und nicht mehr basierend auf ihrer ursprünglichen Zeitzone. Sie werden intern von Ortzeit nach UTC umgerechnet (gemäß dem von Ihnen angegebenen Zeitzonenbezug) und dann von UTC in die Anzeigezeitzone. Dies geschieht in dem Augenblick, in dem die Zeitstempel angezeigt werden. Die Wirkung ist nicht dauerhaft; die Einstellungen zum Zeitzonenbezug können jederzeit wieder geändert werden. Die Definition eines Zeitzonenbezugs geht verloren, wenn ein Fall in Versionen vor v19.3 geöffnet werden.

Beim Kopieren von Dateien aus FAT-Dateisystemen in einen Datei-Container werden die direkt aus dem Dateisystem stammenden Zeitstempel gekennzeichnet als auf einer unbekannten lokalen Zeitzone basierend, so dass sie nicht umgerechnet werden in eine bestimmte Anzeigezeitzone, wenn den Container jemand in der Zukunft begutachtet. Wenn Sie hingegen sicher sind, welches die ursprüngliche Zeitzone war und dies als Zeitzonenbezug im Quellasservat definieren, werden die Zeitstempel darauf basierend für die Ablage im Container nach UTC umgerechnet und dort

permanent als UTC-Zeitstempel gekennzeichnet. In diesem Zustand werden die Zeitstempel später je nach gewählter Anzeigezeitzone bei der Darstellung auf dem Bildschirm umgerechnet, auch wenn Sie später Ihrer Meinung revidieren sollten und im Quellasservat den Zeitzonenbezug wieder ändern. Der Datei-Container ist in sich abgeschlossen und hat keine aktive Verbindung zu den Quellasservat, sobald die Dateien kopiert wurden.

Ein Befehl im Kontextmenü des Falls erlaubt das Importieren von Asservaten aus einem anderen Fall in den aktuell geladenen Fall, z. B. wenn Sie verschiedene Fälle (an denen vielleicht unterschiedliche Benutzer gleichzeitig gearbeitet haben, um die Arbeit aufzuteilen) zu einem einzigen Fall zusammenfassen möchten. Standardmäßig werden alle Asservate eines Falls importiert. Wenn Sie die Umschalttaste zu Beginn des Importvorgangs gedrückthalten, werden nur als wichtig gekennzeichnete Asservate importiert, d. h. solche, die im Quellfall mit einer gelben Glühlampe markiert sind. Dieser Befehl importiert (kopiert) auch den Datei-Überblick des Asservats, mit seinen Vermerken, Kommentaren, Lesezeichen, Suchtreffern, Indexen, Ereignissen, RAID-Zusammensetzungsparametern, Zeitzonenauswahl u. v. a. m., aber keine Sicherungen von Datei-Überblicken und keine im anderen Fall eingetragene Benutzer (sofern die Unterscheidung von Benutzern überhaupt aktiv ist), und die etwaige Unterscheidung von Vermerken und Suchtreffern verschiedener Benutzer geht verloren. Dem aktuellen Benutzer, der den Import vornimmt, werden die Ergebnisse zugeschlagen. Vermerkbezeichnungen im gewählten importierten Fall, die es auch Zielfall gibt, werden mit letzteren verschmolzen. Der Zeitstempel des Hinzufügens zum Fall in den Asservateigenschaften wird in den Zielfall übernommen. Die eindeutigen IDs von Dateien werden in dem neuen Fall anders sein. Allerdings können Vermerke für das Asservat zwischen Quell- und Zielfall ausgetauscht (exportiert und importiert) werden, weil die Datei-Überblicks-ID und die internen IDs beibehalten werden. Der Befehl zum Importieren eines Asservats kann auch eingesetzt werden, um einfach ein Asservat des aktuellen Falls zu duplizieren. Wählen Sie dazu einfach die .xfc-Datei des aktuell geladenen Falls aus, um das für die als wichtig gekennzeichneten Asservate zu erledigen. Dies kann nützlich sein, um zwei unterschiedlich erweiterte Datei-Überblicke gleichzeitig vorzuhalten und zu vergleichen, mit Datei-Header-Signatur-Suchen und ungetesteten Signaturdefinitionen zu experimentieren u. ä.

5.5 Fallprotokoll (Aktivitätsprotokoll)

Wenn in den Falleigenschaften eingestellt, protokolliert X-Ways Forensics alle Benutzeraktivitäten mit, solange der Fall offen/aktiv ist. Das erlaubt es, die Schritte, die Sie zu einem bestimmten Ergebnis geführt haben, auf einfachste Weise nachzuvollziehen, zu reproduzieren und zu dokumentieren, zu Ihrer eigenen Information oder für ein Gerichtsverfahren o. ä.

Folgende Daten werden aufgenommen:

- wenn Sie einen Menübefehl angewählt haben, der Titel des Befehls (oder zumindest seine Identifikationsnummer) und der Name des aktiven Editierfensters, falls kein Asservat, mit vorangestelltem Schlüsselwort „Menu“,
- wenn ein Meldungsfenster angezeigt wird, dessen Text und welchen Schalter Sie gedrückt haben (OK, Ja, Nein oder Abbrechen), mit vorangestelltem Schlüsselwort „MsgBox“,

- wenn ein kleines Fortschrittsfenster angezeigt wird, dessen Titel (wie etwa „Durchsuche Sektoren...“) und ob der Vorgang vollendet oder vorzeitig abgebrochen wurden, mit vorangestelltem Schlüsselwort „Operation“,
- ein Bildschirmfoto eines jeden angezeigten Dialogfensters mit allen gewählten Optionen für einen ggf. folgenden komplexen Vorgang, vorangehend der Titel dieses Fensters,*
- das ausführliche Protokoll, das von Datenträger klonen und Dateien retten nach Typ erzeugt wird,
- Ihre eigenen Einträge (freier Text), die Sie mit dem Menübefehl „Protokolleintrag“ hinzufügen können, entweder zu dem Fall als ganzes oder zu einem speziellen Asservat.

Der Ausgabepfad einer jeden mit dem Verzeichnis-Browser-Kontextmenü kopierten/wiederherstellten Datei, zusammen mit ausgewählten Metadaten wie Originalname, Originalpfad, Größe, Zeitstempel, wird in einer separaten Datei names „copylog.html“ oder „copylog.txt“ im Unterverzeichnis „_log“ mitprotokolliert.

Alle mitprotokollierten Aktivitäten werden mit Datum und exakter Uhrzeit erfasst, intern im Datenformat FILETIME mit einer Genauigkeit von 100-Nanosekunden. Aufzeichnungen von Aktivitäten werden standardmäßig mit dem Fall als Ganzes verknüpft. Aktivitäten, die sich auf ein Asservat beziehen, werden jedoch unterhalb des jeweiligen Asservats aufgezeichnet. Dies bestimmt, wo im Bericht die protokollierten Aktivitäten aufgeführt werden. Um das Aktivitätsprotokoll einzusehen, lassen Sie den Fallbericht ausgeben. Bildschirmfotos werden separat als PNG-Dateien im Unterordner „_log“ eines Fallordners abgelegt.

*If the checkbox for case log screenshots in the case properties is half-checked, that means that no actual graphical screenshots of dialog windows will be taken, just a simple text representation will be stored in the log (the same that you get when via Ctrl+C). These details are included in a special way in the HTML output, so that they do not detract too much from the main log entries. Either they are output in a smaller font and gray color (if "With screenshots" in the report options is fully checked) or simply as a pop-up when hovering with the mouse cursor over a space-saving placeholder rectangle (if half checked) or not at all (if not checked). The placeholder rectangle and pop-up work best when viewed in Google Chrome, as that browser does not truncate the text if lengthy and even shows a preview of the first line in the placeholder rectangle. If you have X-Ways Forensics take conventional (graphical) screenshots of dialog boxes in the log, pixels with the gray background color can be changed to pure white, to save toner/ink in case you are going to print your log at some time (anyway, please think twice and save paper).

5.6 Fallbericht

Sie können einen Bericht mit dem entsprechenden Befehl im Dateimenü des Falldaten-Fensters erzeugen. Der Bericht wird als HTML-Datei gespeichert und kann daher in einer Vielzahl von Applikationen angezeigt und geöffnet werden. Z. B. können Sie ihn mit Ihrem bevorzugten Internet-Browser ansehen oder in MS Word öffnen und weiterverarbeiten. Die Anwendung, in der der Bericht angezeigt werden soll, kann in Optionen | Viewer-Programm definiert werden. Wenn kein solches Programm angegeben ist, wird die Berichtsdatei in der Anwendung geöffnet, die mit der Dateinamenserweitung auf Ihrem Computer verknüpft ist. Mit dem Befehl „Bericht öffnen“ können Sie eine beliebige existierende Datei auswählen und in der definiert bzw.

verknüpften Anwendung öffnen.

Der Bericht kann die folgenden Bestandteile haben:

- **Hauptteil**: Beginnt mit einer optionalen Berichtsüberschrift, einem optionalen Logo, optionalen Vorbemerkungen (die HTML-Code enthalten dürfen), dem Titel und den Details des Falls, gefolgt von einer Liste von Hyperlinks zu den einzelnen Asservat-Sektionen. Zu jedem Asservat gibt der Bericht wiederum Titel, Beschreibung und technischer Detailbericht, Ihre Kommentare und Anmerkungen. Wenn nur halb gewählt, werden technische Details über die Asservate nicht mit den Bericht aufgenommen, nur eine Auflistung der Asservate. Es gibt eine Option, um interne Informationen wie Name des Fallbearbeiters, Pfade der Falldatei und der Sicherungen u. ä. im Fallbericht nicht auszugeben, falls der Bericht für externe Leser gedacht ist, die keinen Einblick in Ihre interne Organisation erhalten sollen. Eine weitere Option verhindert die Anzeige des technischen Detailberichts von Asservaten. Das kann nützlich sein, um z. B. vor Gericht unnötige Diskussionen mit Computerlaien zu meiden darüber, was etwa eine Sektorgröße ist o. ä..

- **Berichtstabellen**: Alle Dateien mit ausgewählten Vermerken werden in Form von sog. Berichtstabellen in dem Bericht ausgegeben, mit den gewünschten Metadaten wie Dateiname, Pfad, Zeitstempel und Kommentaren. Dateien können optional aus dem Asservat für die Einbindung im Bericht herauskopiert werden, in ein Unterverzeichnis des Verzeichnisses, in dem der Bericht gespeichert wird. Dann werden diese Dateien vom Bericht aus verlinkt. Es können entweder alle Dateien oder nur Bilder herauskopiert werden. Wenn nur Bilder, dann wird für Videos zumindest das erste Einzelbild (sofern extrahiert) kopiert, um das Video im Bericht zu repräsentieren. Bilder werden standardmäßig direkt in der HTML-Berichtsdatei angezeigt und nicht bloß verlinkt. Sie werden auf die von Ihnen angegebene Maximalgröße zurechtgestutzt, wobei ihr Seitenverhältnis erhalten bleibt. Wenn Sie als Maximalgröße 0×0 angeben, werden die Bilder doch nur verlinkt, wie andere Dateien. Wenn Sie es vorziehen, mehrere Dateien in einer Zeile auszugeben (zum Beispiel um die Anzahl der benötigten Seiten beim Drucken zu minimieren), bietet sich die Möglichkeit an, besonders lange Dateinamen und Pfadangaben nach einer benutzerdefinierten Anzahl von Pixel umbrechen zu lassen, damit die Seitenbreite nicht überschritten wird.

  Es gibt eine Möglichkeit, nur von markierten Dateien eine Kopie zum Einbinden in den Fallbericht anzufertigen statt von allen oder gar keinen. Nützlich, wenn Sie alle relevanten Dateien in Ihrem Bericht zumindest erwähnen, aber nur einen Teil davon zeigen möchten. Files of certain supported types can be converted to PDF format, for recipients of the report that otherwise would not have suitable applications to view the files. You can define the file types that do not need to be converted, e.g. those that can easily be displayed by a web browser or with Windows tools. If a conversion is not possible, the original file will be copied unconverted.

  Dateien können entweder gruppiert nach Asservat ausgegeben werden (und innerhalb des Asservats aufsteigend nach interner ID) oder in der Reihenfolge, wie sie zum Zeitpunkt der Berichterzeugung im Asservat-Überblick aufgelistet sind, wo Sie die Reihenfolge

dank der bis zu 3 Sortierkriterien frei festlegen können. Wenn zum Zeitpunkt der Berichterzeugung gar keine Dateien im Asservat-Überblick aufgelistet sind (weil er nicht rekursiv erkundet wurde), steht die zweite Möglichkeit nicht zur Verfügung. Erkunden Sie den Asservat-Überblick zunächst rekursiv (per Rechtsklick), um die zweite Möglichkeit nutzen zu können. Beachten Sie, dass wenn Sie von der zweiten Möglichkeit Gebrauch machen, solche Dateien, die nicht im Asservat-Überblick aufgelistet werden, nicht ausgegeben werden, auch wenn sie Teil einer Berichtstabelle sind. Das bedeutet, dass sich die aktuellen Filtereinstellungen auch auf die Berichterzeugung auswirken können. Wenn Dateien ausgelassen werden, weil sie zum Zeitpunkt der Berichterzeugung nicht im Asservat-Überblicksfenster aufgelistet sind, werden Sie darüber im Bericht und von einem Meldungsfenster benachrichtigt.

Wenn das Kontrollkästchen zur Ausgabe von Berichtstabellen nur halb angekreuzt ist, wird lediglich die Anzahl der Objekte mit jenem Vermerk ausgegeben.

Viele verschiedene Einstellungen erlauben es, den Bericht für Ihren Geschmack genau passend anzupassen. Zum Beispiel können Sie ausgegebene Dateien nach ihrer eindeutigen ID benennen und damit sicherstellen, dass Dateienamen kurz ausfallen, eindeutig sind, rückverfolgbar und reproduzierbar, und das stellt auch sicher, dass wenn dieselbe Datei in mehreren Berichtstabellen enthalten ist, sie nur einmal in das Berichtsunterverzeichnis kopiert wird. Das spart Zeit und Speicher. Sie können Dateien auch nach ihren Hash-Werten oder diversen anderen mehr oder weniger eindeutigen Eigenschaften benennen. Falls diese mal leer seni sollten, wird doch wieder der ursprüngliche Name für die Benennung herangezogen.

"List each file only once" is a 3-state checkbox. If fully checked, no file will be referenced in the report by more than one report table. Note that you can still see all report table associations of a file when it is listed in its first report table in the report, if you output the field "Report table". If the checkbox is half-checked, that means that a file will still be referenced (listed) by additional report tables in the report if it has multiple associations, but copied only once and linked only from the first report table.

A special option allows to output the complete internal metadata from a file in the case report as known from Details mode, in HTML format, instead of the extracted subset in the Metadata column in plain text. Wenn Sie die Hash-Werte von Dateien in Ihrem Fallbericht ausgeben möchten, aber zuvor keine Hash-Werte berechnet wurden (bei der Erweiterung des Datei-Überblicks), dann können die Hash-Werte auch noch bei Erzeugung des Berichts berechnet werden.

Smaller versions of pictures can optionally be generated specifically for the report, to greatly reduce the memory requirements of the Internet browser or word processing application when loading the HTML report, and to accelerate loading. This can make a big difference for reports with many high-resolution photos. The JPEG compression factor is user-definable. The resolution depends on the specified "maximum dimensions of pictures". The checkbox that represents this option is a 3-state checkbox. If half checked, the smaller versions of the pictures are used only for the preview directly in the HTML report. If fully checked, even when clicking the picture in the report you will only see the smaller version, and the original larger file is not included in the report at all. This

can be beneficial if your main concern is the drive space requirement of your report with linked files, not the output quality of pictures.

The report can optionally also show previews/thumbnails of non-picture files, e.g. Office documents, e-mails, web pages, programming source code, etc. etc., similar to the gallery. You can shrink the preview representation slightly or a lot or not at all, to either be able to read some of the text right in the report without opening the document or to get a better impression of the overall formatting of the text and just see logos etc.

- **Suchtreffer**, die zum Einbinden in den Fallbericht ausgewählt wurden, können optional im Bericht ausgegeben werden, mit ihrem Kontext links und rechts. Suchtreffer innerhalb von Dateien werden in dem Abschnitt der zugehörigen Datei in der Berichtstabelle ausgegeben, im Anschluss an die sonstigen Metadaten, falls die Datei in einer Berichtstabelle enthalten ist und die Berichtstabelle auch tatsächlich in den Bericht aufgenommen wird. Andernfalls können Sie in dem Abschnitt über das Asservat gefunden werden, zu dem sie gehören. Rein physische eigene Suchtreffer (im Modus "Disk" oder "Partition" definiert, nicht im Modus "Datei"), landen immer im Abschnitt über das Asservat.

- **Fallprotokoll**

Standardmäßig wird der Bericht für den gesamten Fall erstellt. Optional kann er nur für ausgewählte Asservate erstellt werden. It is relatively easy to use CSS (cascading style sheets) for case report format definitions. In addition to defining the parameters for standard HTML elements, key elements of the report are assigned "class" parameters to simplify targeting those for formatting purposes. Example style sheets are available to use as a basis for further modification. The report options allow picking or editing a CSS file as part of the reporting process. The default is "Case Report.txt". The default look from v18.0 and earlier is still available as "Case Report Classic.txt".

You have the option to convert the HTML case report to PDF format. This cannot be used in conjunction with the option to split the report file after a certain number of files. If the box with the PDF option is fully checked, that means that you wil receive *only* a PDF version of the report. If half checked, that means that you you will receive both an HTML and a PDF version of the report. Please note that if you delete one of them in the Windows Explorer/File Explorer, this will automatically also deleted the corresponding subdirectory with the copied files if there is one, even if it is still needed for the respective other version of the report.

5.7 Vermerke

Im Verzeichnis-Browser eines Asservats kann man relevante Dateien mit Vermerken versehen. Ein Vermerk ist ein benutzerdefinierter (virtueller) Marker von Dateien, insbes. relevanten Dateien. Dateien mit Vermerken können leicht in den Fallbericht aufgenommen werden (mit all ihren Metadaten und einem Link zur Datei, Bilder sogar direkt), und Sie können in einer rekursiven Ansicht nach Vermerken filtern, um die betreffenden Dateien später leicht wiederfinden zu können (wie ein Lesezeichen). Der Filter kann Dateien in mehreren Vermerken

mit den Operatoren ODER, UND und NICHT verknüpfen und hat sogar eine Option, die zusätzlich die "Geschwister" von Dateien mit Vermerken mit ausgeben kann, d. h. Dateien im selben Verzeichnis. Das ist nützlich, insbes. wenn man rekursiv erkundet und nach Pfad sortiert, um zu prüfen, ob weitere relevante Dateien in der Nachbarschaft zu finden sind.

Z. B. könnten Sie Vermerke erstellen mit Beschreibungen wie "Verbindung zu Fa. X", "Beweise gegen Beschuldigten B", "Kipo", "zweifelhafte Betriebsausgabe", "an Kollege Müller weitergeben", "später noch ausdrucken", "übersetzen lassen" usw. Und später, wenn Sie alle Dateien systematisch durchgegangen sind, können Sie sich mit Hilfe des Vermerkfilters einen Überblick verschaffen (z. B. "Zeige mir alle Dateien, die eine Verbindung zu Fa. X nahelegen und zugleich als Beweise gegen Beschuldigten B eingestuft wurden."). Sie weisen Dateien also praktisch einer von Ihnen selbst definierten Kategorie zu. Zugleich erlaubt Ihnen einen Vermerk auch, Dateien bequem erneut aufzusuchen, um sie genauer unter die Lupe nehmen zu können.

Dateien mit speziellen Vermerken zu versehen ermöglicht es bspw. des Weiteren, sie in einem einzigen Durchgang später herauszukopieren oder in einer zusammenhängenden Galerie-Übersicht zu betrachten. Dieselbe Datei kann auch mit mehreren Vermerken versehen werden. Vermerke definieren Sie in dem Dialogfenster, das beim Aufruf des Befehls "Vermerke" im Kontextmenü des Verzeichnis-Browsers erscheint, für eine Datei oder mehrere ausgewählte Dateien auf einmal. Dieses Dialogfenster zeigt nicht bestehende Vermerke für die ausgewählte(n) Datei(en) an (das wäre für mehrere ausgewählte Dateien auf einmal auch schwierig, dafür statt dessen einfach in die Spalte "Vermerke" schauen), sondern erzeugt auf komfortable und benutzerkonfigurierbare Weise neue und/oder entfernt bestehende Vermerke. In der Voreinstellung beim nächsten Aufruf des Befehls sind die zuletzt ausgewählten Vermerkbezeichnungen automatisch wieder ausgewählt. Im selben Dialogfenster können Sie auch neue Vermerkbezeichnungen anlegen, bestehende umbenennen oder löschen, und existierende Vermerke für die ausgewählte(n) Datei(en) entfernen/ersetzen. Sie können für jede Vermerkbezeichnung einzeln festlegen, ob Sie typischerweise nur die ausgewählte Datei oder das ausgewählte Verzeichnis selbst mit dem Vermerk versehen möchte und/oder zugleich die Elterndatei einer Datei (falls sie eine hat) und/oder die Unterobjekte von Dateien/Verzeichnissen und/oder etwaige bekannte Duplikate der ausgewählten Datei in zu dem Zeitpunkt offenen Asservaten (anhand von Hash-Werten erkannte und in der Attributspalte entsprechend gekennzeichnete Duplikate, s. Kontextmenü, und außerdem harte Verweise außer in HFS+).

Eine weitere Option erlaubt das automatische Anwenden von Vermerken auf Geschwister der ausgewählten Dateien. Das ist z. B. nützlich beim Begutachten von Suchtreffern, wenn Sie relevante Suchtreffer im Anhang einer E-Mail finden und Sie sicherstellen wollen, dass etwaige andere Attachments derselben E-Mail auf dieselbe Weise weiterverarbeitet werden, auch wenn sie keine Suchtreffer enthalten.

Wenn Sie viele Dateien mit Hilfe von Vermerken kategorisieren möchten, können Sie auch Tastenkombinationen dazu nutzen. X-Ways Forensics ordnet Ihren Vermerkbezeichnungen automatisch die Tastenkürzel Strg+1, Strg+2, ..., Strg+9 zu. In dem Dialogfenster für Vermerke können Sie diese Tastenkürzel auch selbst vergeben, indem Sie die Tasten drücken während eine Vermerkbezeichnung ausgewählt ist. Ohne Verbindung mit der Strg-Taste können Sie auch einfach die entsprechende Taste im Nummernblock drücken, wenn Num Lock aktiv ist. In diesem Fall werden die Tastendrücke nicht als Eingabe in den Verzeichnis-Browser verstanden, obwohl die Strg-Taste nicht gedrückt ist. Die Alternative mit dem Nummernblock funktioniert evtl. nicht

auf allen Computern. Strg+0 entfernt alle Vermerke von den ausgewählten Dateien, außer solchen, die von X-Ways Forensics automatisch erstellt wurden und als Hinweise für den Benutzer dienen oder solchen, die erkannte Bildinhalte darstellen. Alt+1, Alt+2, ..., Alt+9 entfernt die Verknüpfung mit der betreffenden Vermerkbezeichnung von den ausgewählten Dateien.

Optional kann automatisch das nächste Objekte im Verzeichnis-Browser ausgewählt werden, nachdem das vorherige mit einem Vermerk ausgestattet wurde. Ein dreistufiges Kontrollkästchen entscheidet darüber, ob dies geschehen soll, und wenn ja, ob für alle Arten der Vermerksausstattung oder nur für den Einsatz von Tastenkombinationen.

Sie können freien Text als Beschreibung für jede Vermerkbezeichnung hinterlegen, wenn Sie den Schalter mit dem Eigenschafts-Icon im Dialogfenster für Vermerke anklicken. Diese Beschreibung wird im Fallbericht zu sehen sein, wenn Sie die Dateien mit dem Vermerk ausgeben lassen. Sie ist nützlich für Erklärungen zur Bedeutung des Vermerks und hilft, die Vermerkbezeichnung selbst, die an diversen Stellen in der Benutzeroberfläche erscheint, kürzer fassen zu können.

Vermerkbezeichnungen können in den Dialogfenstern fürs Filtern und Erstellen von Vermerken optional alphabetisch sortiert werden. Standardmäßig werden sie in der Reihenfolge angezeigt, in der sie angelegt wurden. Die Auflistung von Vermerkbezeichnungen, die vom Programm automatisch als Hinweise angelegt werden, ist optional, und diese Vermerkbezeichnungen werden eingerückt angezeigt. Sie können die Reihenfolge von Vermerken in den zuvor genannten Dialogfenstern ändern, wenn sie nicht alphabetisch sortiert sind, durch Klick auf die Pfeiltasten. Das Ändern der Reihenfolge dort wirkt sich auch umgehend auf die Reihenfolge aus, in der Vermerke in der Vermerkspalte im Verzeichnis-Browser aufgelistet werden. Sie können also sicherstellen, dass die für Sie wichtigsten Vermerke zuerst angezeigt werden.

Es gibt eine Option zum Erzeugen von Vermerken für Dateien anhand der Suchbegriffe, die sie laut Spalte "Suchtreffer" enthalten. Nützlich, wenn Sie die Informationen darüber, welche Datei welche Suchbegriffe enthält, auch nach dem Löschen der Suchtreffer behalten möchten, oder um sie in Datei-Containern zu konservieren.

Eine weitere option erlaubt es, erkannte Hash-Set-Zugehörigkeiten zu Vermerken zu machen. Das könnte z. B. nützlich sein, wenn Sie Ihre Hash-Datenbank von Grund auf neu aufbauen oder einfach nur löschen möchten, und Sie nicht nur die Kategorisierung bekannter Dateien im Datei-Überblick behalten möchten, sondern auch den exakten Namen des betreffenden Hash-Sets. Auch nützlich, wenn Sie Dateien einem Datei-Container hinzufügen und den Empfänger die erkannten Hash-Set-Namen wissen lassen möchten, nicht nur die Kategorisierung. Diese behelfsmäßigen Vermerkbezeichnungen werden in einer besonderen Farbe hervorgehoben, um sie von anderen Arten von Vermerkbezeichnungen unterscheiden zu können. Hash-Set-basierte Vermerke können auch nebenbei erzeugt werden, wenn Sie Dateien in einen Container kopieren.

Insgesamt gesehen gibt es wirklich eine Vielzahl verschiedener Vermerke: 1) Vom Benutzer kreierte Vermerke, die für Berichtszwecke oder andere Zwecke angelegt wurden, 2) von X-Ways Forensics erstellte Vermerke, die Benutzer über besondere Eigenschaften von Dateien in Kenntnis setzen sollen, 3) Vermerke, die die in einer Datei aufgefundenen Suchbegriffe repräsentieren, 4) Vermerke, die Hash-Sets repräsentieren, in denen eine Datei wiedererkannt

wurde, 5) Vermerke, die eine Gruppe von Duplikaten identifizieren und 6) Vermerke, die von Excire erkannte Bildinhalte identifizieren. Um eine starke Aufblähung der Liste von Vermerkbezeichnungen bei der Berichtserstellung zu vermeiden, werden Vermerkbezeichnungen in dem Dialogfenster nur dann angeboten, wenn die Vermerke wirklich für Berichtszwecke gedacht sind. Davon wird ausgegangen bei allen vom Benutzer erzeugten Vermerken. Sie können den Berichtszweck für jede Vermerkbezeichnung im Dialogfenster für Vermerke ein- und ausschalten, indem Sie das Sternsymbol zuweisen bzw. entfernen.

Es ist möglich, Listen von Vermerkbezeichnungen im Dialogfenster für die Erstellung von Vermerken zu laden und zu speichern. Das ist nützlich, um gleich mit einer Reihe von vordefinierten möglichen Vermerken zu starten, wie sie typischerweise in einer bestimmten Art von Fall bei Ihnen benötigt werden. Diese Datei ist per Texteditor bearbeitbar. Das Format ist eins der folgenden:
a) Eine Vermerkbezeichnung pro Zeile (wenn keine Beschreibung vorhanden ist). Leerzeilen sind nicht erlaubt.
b) Eine Vermerkbezeichnung nach dem Unicode-Zeichen U+25B8 (Black Right-Pointing Small Triangle), gefolgt von einem Zeilenumbruch und einer beliebigen Beschreibung. Beliebig oft wiederholbar.
In beiden Fällen muss die Datei in UTF-16 gespeichert sein, mit einem Byte-Reihenfolge-Marker am Anfang. Die maximale Anzahl von Vermerkbezeichnungen in einem Fall beträgt 1000.

Vermerke können über das Kontextmenü des Falldatenfensters aus Asservaten exportiert und wieder importiert werden. Siehe Weitere Möglichkeiten zur verteilten Auswertung.

Eine einfacher bedienbare, reduzierte Fassung des Dialogfensters zur Erstellung von Vermerken ist verfügbar, mit weniger Einstellungen, die neue Benutzer verwirren könnten, die in X-Ways Investigator voreingestellt und in X-Ways Forensics und X-Ways Investigator optional ist. Z. B. werden in der vereinfachten Fassung Vermerkbezeichnungen, die von der Anwendungen erzeugt wurden, um den Benutzer auf etwas aufmerksam zu machen, nicht aufgelistet.

Um Dateien mit einem bestimmten Vermerk in Form einer Berichtstabelle in einem Bericht auszugeben, verwenden Sie den Befehl "Bericht erstellen" im Falldatenfenster.

Wie zuvor erwähnt, werden Vermerke auch intern von X-Ways Forensics verwendet und automatisch erzeugt, um Sie, den Benutzer, auf Besonderheiten von Dateien hinzuweisen, getreu dem Motto "Melden macht frei". Inwieweit Sie solche Dateien genauer prüfen, bleibt Ihnen überlassen. Intern angelegte Vermerkbezeichungen werden eingerückt und farblich unterschiedlich dargestellt, um Verwechslungen auszuschließen. Typische Beispiele für solche Vermerke sind:

Ohne erkennbaren textuellen Inhalt
Text nicht decodierbar
Fehlermeldungen s. Metadaten
Erkunden fehlgeschlagen
Leeres Archiv?
Übergreifendes Archiv
Keine E-Mails gefunden
Pfad zu lang.

Large non-resident $EA
Animated GIF
Animated PNG
Multi-page TIFF
Multi-page JPEG marker
Phone screenshot?
Zip bomb? Not fully processed
Unexpected tail (SFX?) / Contains unknown segment (SFX?)
FSG Packer / PECompact / UPX / Unknown segment / Binder?
Enthält eingebettete Dokumente
Contains embedded object(s)
Contains embedded file
Contains hidden file
Hybrid-MS-Office-Dokument!
RAR hybrid
Contains embedded non-JPEG/non-PNG picture
Enthält ältere, nicht sichtbare Stände
Concatenated-PDF
Contains private chunk
Keine Bilder extrahiert
Absturzursache?
Unsupported file type variant
Ausgelassen
Nicht kopiert
Virenverdacht
Nicht lesbar
Not decompressed

5.8 Viewer-Funktionalität

Der interne Viewer kann mit dem Befehl „Einsehen“ im Menü Extras und im Kontextmenü des Verzeichnis-Browsers auf eine Datei angewandt werden, des Weiteren im Vorschau-Modus. Er zeigt mit Hilfe einer internen Bildanzeigebibliothek Bilddateien verschiedener Formate (JPEG, PNG, GIF, TIFF, BMP, WEBP (nur das erste Bild, wenn animiert), HEIC, einige DICOM-Varianten, PSD, HDR, PSP, SGI, PCX, CUT, PNM/PBM/PGM/PPM, ICO) sowie die innere Struktur von Windows-Registrierungsdateien, Windows Event Logs (.evt und .evtx), Windows-Shortcut-Dateien (.lnk), Windows-Prefetch-Dateien, $LogFile-Dateien, $UsnJrnl:$J, Ext3/Ext4 .journal, .ds_store, Windows Task Scheduler (.job), $EFS LUS, INFO2, Restore Point change.log.1, wtmp und utmp Log-In-Records, MacOS X kcpassword, MacOS X finder bookmarks (flnk), AOL-PFC, Outlook NK2 auto-complete, Outlook WAB address book, Internet Explorer travellog (a.k.a. RecoveryStore), Skype Chat Sync, MS Outlook Express DBX und vieler anderer Dateien mit eingebauten Mitteln an. Wenn Sie versuchen, eine Datei einzusehen, deren Format nicht vom internen Viewer unterstützt wird, wird stattdessen die separate Viewer-Komponente aufgerufen.

Es gibt eine zusätzliche, externe Dateibetrachtungskomponente, die nahtlos in WinHex und X-

Ways Forensics integriert werden kann und es ermöglicht, über 270 (!) Dateiformate (wie zum Beispiel MS Word, Excel, PowerPoint, Access, Works, Outlook; HTML, PDF, StarOffice, OpenOffice, ...) direkt und auf besonders bequeme Art und Weise einzusehen. Dieses Modul ist in X-Ways Forensics und X-Ways Investigator enthalten. Es kann unter Optionen | Viewer-Programme aktiviert werden, optional auch für Bilder, die schon die interne Bildanzeigebibliothek darstellen könnte. Weitere Informationen online. Der Ordner für temporäre Dateien der Viewer-Komponente wird von WinHex/X-Ways Forensics gesteuert, d. h. auf den vom Benutzer unter Allgemeine Optionen bestimmten gesetzt. Allerdings akzeptiert die Viewer-Komponente im Gegensatz zu X-Ways Forensics nicht stillschweigend ungeeignete Pfade etwa auf schreibgeschützten Datenträgern. Bitte beachten Sie, dass die Viewer-Komponente seit ihrer Version 8.2 Dateien im Windows-Profil des aktuell angemeldeten Benutzers erzeugt, um darin ihre Konfiguration und Einstellungen zu speichern. In früheren Versionen hinterließ sie bei tatsächlicher Verwendung (nicht beim bloßen Laden) stattdessen Einträge in der Windows-Registry.

Die Viewer-Komponente erlaubt es auch, bestimmte passwortgeschützte Dokumente einzusehen, sofern das Passwort bekannt ist. Nur bestimmte Verschlüsselungsvarianten von Microsoft-Office- und PDF-Dokumenten, Microsoft Outlook PST 97-2013 und Zip-Dateien werden unterstützt. Bei der Vorschau einer solchen Datei wird das Passwort aus der Metadaten-Zelle der Datei entnommen (wenn dort eintragen in einer Zeile, die mit "Password: " beginnt) oder alternativ werden alle Passwörter aus der Passwortsammlung des aktiven Falls automatisch ausprobiert und dann für künftige Verwendung und Ihre Information in der Metadaten-Zelle verewigt. Wenn beim Einsehen einer solchen Datei kein passendes Passwort gefunden wird, wird zusätzlich der Benutzer wiederholt nach dem Passwort gefragt, solange bis das richtige Passwort eingegeben wird oder der benutzer durch Klick auf Abbrechen signalisiert, dass er aufgibt.

Registry-Viewer

MS Windows führt eine interne Datenbank baumförmiger Struktur (die sogenannte System-Registrierung, engl. Registry), in der alle wichtige Einstellungen des Betriebssystems gespeichert sind. Die Daten sind permanent gespeichert in mehreren Dateien (sogenannte Hives), die eine bestimmte Struktur aufweisen. Vom Verzeichnis-Browser aus lassen sich Registry-Dateien im Registry-Viewer einsehen (Doppelklick oder Kontextmenü). Mit dem RegistryViewer können Hives angezeigt werden, ohne sie in die aktuellen Datenbankeinträge des eigenen Systems zu importieren. Unterstützt wird die Anzeige von NT/2K/XP/Va/7-Hives. Win9x- und WinMe-Hives können nur bis zur Version 15.9 von X-Ways Forensics geladen werden. Hives von NT/2K/XP/Va/7 befinden sich in der Datei "ntuser.dat" im Benutzerprofil und im Verzeichnis \system32\config.

Es können bis zu 32 Hives gleichzeitig im Registry-Viewer angezeigt werden. Der Registry-Viewer hat die Fähigkeit, gelöschte Schlüssel und Werte in Hives zu finden, die unbenutzten Speicher enthalten, und verwaiste Schlüssel und Werte in beschädigten und unvollständigen Hives. Wenn kein vollständiger Pfad für einen Schlüssel bekannt ist, wird er unterhalb eines virtuellen Schlüssels namens "Pfad unbekannt" aufgeführt.

Durch Klick mit der rechten Maustaste kann an jeder Stelle im Hauptfenster ein Menü aufgerufen werden, über das man die Befehle "Suchen" und "Weitersuchen" ausführen kann. Beim Suchen kann über einen Auswahldialog festgelegt werden, nach welchem Ausdruck gesucht werden soll,

und ob der Suchausdruck in den Schlüsselnamen oder in den Namen oder den Werten (oder in allem) gesucht werden soll. Die Suche beginnt immer ganz am Anfang im ersten geladenen Hive und erstreckt sich über alle geöffneten Hives. Mit "Weitersuchen" kann der nächste Treffer nach einem bereits gefundenen Treffer gesucht werden. Das zu der Zeit ausgewählte Element hat keinen Einfluss darauf, von wo aus weitergesucht wird. Die Option "nur als ganzes Wort suchen" funktioniert für Werte nicht garantiert.

Im rechten Fenster kann durch Rechtsklick im Menü weiterhin "Kopieren" ausgewählt werden, wodurch sich der Wert des ausgewählten Elements in die Zwischenablage kopieren lässt.

Wenn Sie einen Eintrag in einem geladenen Hive im Registry-Viewer anklicken und sich das Datenfenster mit dem Datenträger/Image, von dem aus der Hive geladen wurden, im Dateimodus befindet, springt der Cursor nun automatisch auf den jeweiligen Eintrag in der Registry-Datei im Dateimodus, und er wird automatisch in der Datei als Block ausgewählt. Dies erlaubt es einem, insbes. binäre Registry-Einträge sowohl hexadezimal als auch als Text zu sehen, und Binäreinträge leicht in Binärform oder als Text zu kopieren, nicht nur als Hex-ASCII.

The Export List command in the registry viewer context menu allows to export all values in the selected hive to a tab-delimited text file.

When selecting a value, an edit window in the lower right corner tells you the logical size of that value and the size of its slack. It also interprets registry values of the following types, as known from the registry report: MRUListEx, BagMRU, ItemPos, ItemOrder, Order (menu), ViewView2, SlowInfoCache, IconStreams (Tray notifications), UserAssist, Timestamps (FILETIME, Epoch, Epoche), MountedDevices, OpenSavePidlMRU, and LastVisitedPidlMRU. The edit window also displays the access rights/permissions of the registry keys if (Default) is selected.

$LogFile-Viewer

Grundsätzlich liefert der Parser Statements aus drei Kategorien:
1) Log-Operation: Die Daten auf dem Datenträger bei (LCN,Byte-Offset) sind im Falle einer Redo/Undo-Operation durch die hier angegebenen Daten zu ersetzten.
2) Das PAGE-Statement kennzeichnet den Beginn einer neuen Log-Seite (ist stets ein Vielfaches von 4 KB). Die LSN gibt die letzte in dieser Seite verwendete LSN an. Ein * markiert eine veraltete Seite.
3) Das CheckPoint-Statement gibt die LSN für den nächsten Restart an.
Jedes Statement beginnt mit einem Byte-Offset für die betreffende $LogFile-Datei.

Abkürzungen:
LSN=Logical Sequence Number
LCN=Logical Cluster Number
VCN=Virtual Cluster Number
FID=File ID

Beschränkungen:
Es werden nur Log-Operationen aufgeführt, die Ondisk-Strukturen betreffen. Andere Log-Operationen werden der Einfachheit halber weggelassen. FILE-Records und INDX-Puffer

werden nicht vollständig angezeigt, da das Ergebnis sonst unübersichtlich würde. Um an den vollständigen Inhalt dieser Records zu gelangen, folgen Sie dem Byte-Offset in die Log-Datei für die Sie interessierende Operation. Es können auch Kopien von Log-Dateien verarbeitet werden: Im Pfad einer solchen Datei muss dazu jedoch der Teilstring $LogFile an beliebiger Stelle enthalten sein.

5.9 Registry-Bericht

WinHex kann über den Befehl "Bericht erzeugen" im Rechts-Klick-Menü des Registry-Viewer für die geöffneten Hives einen Bericht im HTML-Format erstellen, der potenziell relevante Schlüssel aus der Registry mit ihren Werten auflistet. Die Registry-Dateien müssen ihren Originalnamen haben, sonst kann der Bericht u. U. nicht erstellt werden. Die zu extrahierenden Schlüssel sind in Textdateien wie den mitgelieferten „Reg Report *.txt“ definiert, die nach eigenen Bedürfnissen angepasst oder erweitert werden können.

Standard tables have 4 columns: description, extracted value, registry path (provided as a tooltip), and last modification date of the corresponding key. The dates are displayed in gray for values that are not the only values in their respective key, as a visual aid to remind the reader that they are not the modification dates of the values themselves.

Free space in registry hives can be analyzed with the report definition file "Reg Report Free Space.txt". The free space can be as large as several MB, especially as a consequence of the use of virus scanners and registry cleaning programs. Deleted registry values are now highlighted in the report in red color.

Also registry value slack has a relevant size in NTUSER.DAT hives. This fact is exploited with 2 measures:
1) If the slack contains text strings, it will be output in the registry report (in green). This new feature can optionally be turned off the registry viewer context menu.
2) For values that contain item lists (i.e. are binary) you can use the "Reg Report Free Space.txt" definitions to output registry report will output lists of filenames with timestamps in green. The first timestamps is an access date, the second one is a creation date. If no timestamps can be output, these are artifacts from "RecentDocs".

Das Format der Einträge in „Reg Report *.txt“

(*Typkürzel*) (*Tabulator*) (*Schlüsselpfad*) (*Tabulator*) (*Beschreibung*) (*Zeilenvorschub*)

Typkürzel:
?? Definition für beliebiges Windows
NT Windows bis einschließlich XP
VT Windows ab Vista
** Neue Funktion (ohne absolute Pfade)
FR Abfrage im freien Speicher des Hives

Schlüsselpfad:

Kompletter Pfad des Registrierungsschlüssels

HKLM entspricht HKEY_LOCAL_MACHINE
HKCU entspricht HKEY_CURRENT_USER

Wenn ein "*" als Platzhalter im letzten Teilpfad verwendet wird, werden alle Pfade auf dieser Verzweigungsebene und allen tieferen Verzweigungsebenen mit ihren Werten in dem Bericht mitaufgelistet.

Beispiel:
NT HKLM\Software\Microsoft\Windows\CurrentVersion* ges. Windows-Unterzweig

Wenn ein bestimmter Wert von Interesse ist, der in allen Unterschlüsseln eines bestimmten Schlüssels vorkommt, dann können die Unterschlüssel abermals durch ein "*" ersetzt werden und der konkrete Wert dahinter angegeben werden.

Der erzeugte Bericht enthält jeweils den Schlüsselpfad mit der zugehörigen Zeitangabe der letzten, den Dateinamen des Hives, aus dem dieser Schlüssel ist, die Beschreibung aus "Reg Report *.txt" und den Wert.

Das Feld „Beschreibung“ kann am Ende eine Anweisung enthalten, die mit einem %-Zeichen eingeleitet wird. Folgt dem Prozent-Zeichen eine Zahl *n*, wird im Bericht das *n*-te Element des Schlüsselpfades an die Beschreibung angehängt. Das kann sehr nützlich sein, wenn der Pfad und nicht der Wert (oder nicht nur der Wert) die relevanten Informationen enthält. Folgt dem Prozent-Zeichen ein Buchstabe, wird der Wert bevorzugt als der Datentyp interpretiert, für den der Buchstabe steht. Derzeit definiert sind

%f Windows FILETIME Zeitstempel
%e Epoche (Unix) Zeitstempel
%E Epoche8 (Unix) Zeitstempel als QWORD
%D Dezimalzahl
%T Windows Systemtime-Zeitstempel
%s ANSI-ASCII nullterminiert
%S UTF-16-Zeichenkette nullterminiert
%b binäre Daten nicht als Zeichen interpretieren (REG_BINARY)
%P Windows PIDL-Datenstruktur
%I ItemPos-Datenstruktur (für Shell Bag, Desktop-Shortcuts u. a.)
%B konditional: wenn Wert TRUE
%F konditional: wenn Wert FALSE
%- kein Empty-Mode
%+ Rekursion des Teilbaumes
%i Wert ohne Unterscheidung von Groß- und Kleinschreibung
%d nur gelöschte Werte

Man kann auch z. B. die Mischkonstruktion %10f verwenden. Die Zahl muss zuerst erscheinen.

// am Anfang einer Zeile bewirkt, dass sie bei der Auswertung ignoriert wird.
am Anfang einer Zeile gibt erläuternden Test in den Bericht aus.

Weitere Ausgaben

In einer zweiten Phase der Erzeugung des Registry-Berichts werden zusätzliche Daten ausgewertet und in übersichtlichen Tabellen am Ende der HTML-Datei ausgegeben. Die Vorgaben in der Definitionsdatei, die zu der zweiten Stufe gehören sind mit "Dummy" gekennzeichnet. Dies bewirkt, dass während der ersten Phase keine Ausgaben entstehen. Will man stattdessen nur die Ausgaben der ersten Stufe der Auswertung erhalten, muss die Bezeichnung des Definitionseintrags nur von "Dummy" auf etwas anderes geändert werden.

Die Tabelle "Attached devices by serial number" wird nach dem im Buch von Harlan Carvey in Kapitel 4 beschriebenen Algorithmus erstellt. Weiterhin gibt es die Tabellen "Partitions by disk signature", "Windows portable devices", "Drivers installed", "File systems installed", "Services installed", "Networks" und "Network cards".

Another table is called "Browser Helper Objects", compiled with data from the hives NTUSER.DAT and SOFTWARE, about browser usage. "External Memory Devices" is a table which can be retrieved from Software hives of Windows Vista and later that lists external media with access timestamps, hardware serial number, volume label, volume serial number and volume size (size often only under Vista). Select the definition file "Reg Report Devices.txt" to get the table.

5.10 Parallele Suche

Dieser Befehl im Suchen-Menü ist verfügbar für Inhaber von Specialist- und forensischen Lizenzen verfügbar, und bietet alle Optionen nur für Inhaber von forensischen Lizenzen. Diese Suche arbeitet parallel in dem Sinn, dass sie Sie nach nach einer praktisch unbegrenzt langen Liste von Suchbegriffen zugleich suchen lässt (1 pro Zeile). Die Vorkommnisse dieser Suchbegriffe werden entweder gespeichert und aufgelistet in der Suchtrefferliste eines Asservats (für forensische Lizenzen, beim Arbeiten mit einem Fall, notwendig um in den Genuss der vollen Funktionalität zu kommen) oder im allgemeinen Positions-Manager.

Standardmäßig werden Treffer zu identischen Suchbegriffen zusammengefasst und über denselben Eintrag in der Suchbegriffsliste zugänglich gemacht. Das ist nützlich z. B., wenn Sie Suchläufe nach denselben Stichwörtern oder regulären Ausdrücken inkrementell (in mehreren Schritten) auf unterschiedliche Asservate loslassen. Es gibt ein Kontrollkästchen dazu, das man auch abwählen kann. Dann wird jedes Mal beim Starten einer Suche ein neuer Eintrag in der Suchbegriffsliste erzeugt, auch wenn das Stichwort, nach dem Sie suchen, identisch ist zu einem in einem vorherigen Suchdurchlauf oder im selben Durchlauf verwendeten Stichwort. Das ist nützlich, wenn Sie die Suchen mit unterschiedlichen Einstellungen betreiben, z. B. dasselbe Stichwort gleichzeitig als ganzes Wort und als Teilwort, so dass Sie die jeweiligen Treffer später getrennt voneinander auflisten können.

Sie können die parallele Suche einsetzen, um systematisch mehrere Festplatten oder Image-Dateien in einem einzigen Durchlauf nach Wörter zu durchsuchen wie „Droge“, „Kokain“, (umgangssprachliches Synonym Nr. 1 für Kokain), (umgangssprachliches Synonym Nr. 2 für Kokain), (umgangssprachliches Synonym Nr. 3 für Kokain), (umgangssprachliches Synonym Nr. 3 für Kokain in alternativer Schreibweise), (Name von Händler Nr. 1), (Name von Händler Nr.

2), (Name von Händler Nr. 3) usw. Die Suchtreffer vermögen die Untersuchung einzuschränken auf eine Liste von Dateien, auf die Sie sich konzentrieren können.

Die parallele Suche kann physisch in Sektoren oder logisch in Dateien suchen, oder in einem zuvor erstellten Index. Physisch sucht sie alle Sektoren eines Datenträgers in der Reihenfolge Ihrer LBA-Nummerierung ab (es sei denn, Sie suchen aufwärts, dann wird die Reihenfolge umgekehrt). Wenn Sie WinHex die Treffer einer physischen Suche nicht auflisten lassen, können Sie die F3-Taste betätigen, um zum nächsten Treffer zu springen. Logisch geht die Suche dateiweise vor, was vorteilhaft ist, da viel mächtiger und sorgfältiger. Mehr über die logische Suche.

Sie können dieselben Suchbegriffe zugleich in bis zu 6 Codepages suchen. Die in Ihrem Windows-System aktive Standard-Codepage ist mit einem Sternchen kenntlich gemacht und anfangs voreingestellt. Z. B. auf Computern in Westeuropa und in den USA ist dies die Codepage 1252 ANSI Latin I. Die Codepages mit der Bezeichnung „ANSI“ im Namen werden in Microsoft Windows verwendet. „MAC“ zeigt eine Codepage des Apple Macintosh an. „OEM“ bezeichnet eine Codepage, die von MS-DOS und Windows-Kommandozeilenfenstern zum Einsatz kommt. Wenn ein Suchbegriff nicht in die ausgewählte Codepage umgesetzt werden kann, weil er Zeichen enthält, die in dieser Codepage unbekannt sind, wird eine Warnung ausgegeben. Codepage-unabhängige RegEx-Suchen nach exakten Byte-Werten sind möglich, wenn Sie in einer Pseudo-Codepage namens „Direkte byteweise Übersetzung für reguläre Ausdrücke“ suchen, die Byte-Werte ohne jede Anpassung für bestimmte Codepages oder Groß- und Kleinschreibung sucht. X-Ways Forensics erlaubt das Suchen in Little-Endian- und Big-Endian-UTF-16 sowie in jeder regionalen Windows-Codepage sowie UTF16 mit darübergestülptem MS Outlook Cipher (compressible encryption).

In X-Ways Forensics und X-Ways Investigator können Sie eine Zeichenersetzung vornehmen lassen. (Die Funktionsweise dafür ist intern etwas anders als bei der Indexierung.) Die Liste wird in einer Textdatei namens "Character Adjustment.txt" (vormals "indexsub.txt")codiert als UTF-16 erwartet. Diese wird optional auch bei der Indexierung verwendet. Sie beginnt mit dem Byte-Reihenfolge-Zeichen für Little Endian, gefolgt von eine Anweisung pro Zeile, mit einem Pfeil (Größer-als-Symbol) in der Mitte. Diese Anweisungen bilden ein Zeichen auf ein anderes ab. Sie können sie nach eigenem Ermessen für Suchen in Ihrer Sprache anpassen. Beispiele für Französisch: Die Zeile É>E bedeutet, dass der Buchstabe É in den zu durchsuchenden Daten (bei Wahl von geeigneten Codepages) als Variante von E in Ihren Suchbegriffen akzeptiert wird. Sie bräuchten also nur nach Edith Piaf zu suchen und würden dabei nicht nur Edith Piaf, sondern auch Édith Piaf finden. Intern werden beide Varianten gesucht. ç>c bewirkt, dass Sie bei Suche nach Francois sowohl Francois (die vereinfachte Schreibweise) als auch François (die französische Originalschreibweise) finden können. Sie finden das vielleicht vorteilhaft, wenn Ihre Tastatur die Erzeugung des Zeichens ç gar nicht so leicht erlaubt. Umgekehrt kann es auch Sinn ergeben: c>ç bewirkt, dass bei der Suche nach François (was Sie vielleicht bevorzugen, wenn Sie frankophil sind, oder wenn Sie den Namen direkt so von irgendwo herkopieren) sowohl François als auch Francois gefunden wird. (Diese Ersetzungsrichtung ist allerdings für die Indexierung nicht empfehlenswert.) Selbst wenn Sie gar nicht speziell daran interessiert sind, andere Schreibweisen mit zu erfassen, können Sie solche Ersetzungen einmal definieren (z. B. unter Zuhilfenahme von Copy & Paste), um die Sonderzeichen später nie wieder bei der Suche mit der Tastatur erzeugen zu müssen.

Die Nichtbeachtung von Groß- und Kleinschreibung setzt nicht auf die Zeichenanpassung auf. So wird bspw. bei aktiver Anpassung é>e eine Suche nach e ohne Beachtung von Groß- und Kleinschreibung sowohl e als auch é finden und auch E, aber nicht É. Dafür müssten Sie die Anpassung É>E hinzufügen. NB: Sie könnten theoretisch Ihre eigenen Regeln für Suchen ohne Beachtung von Groß- und Kleinschreibung definieren allein mit Hilfe der Zeichenanpassung. Das wäre aber wirklich nur etwas für Nerds. Bis zu 16 Zeichenabbildungen für dasselbe Zielzeichen werden unterstützt. Zeichenanpassungen funktionieren zusammen mit regulären Ausdrücken, aber nur für Zielzeichen, die keine besondere Bedeutung in regulären Ausdrücken haben, und nicht für Zeichen innerhalb von []-Alternativen.

Sie können definieren, welche Zeichen als Teil von Wörtern betrachtet werden sollen. Das ist nützlich, um falsche Treffer für kurze natürlichsprachliche Wörter in binären Mülldaten oder Base64-Code zu vermeiden und generell für Benutzer, die Zahlen als Teil von Wörtern ansehen (so wie in "GIF89"). Beispiel: Ein nicht wünschenswerter Treffer für "Band" in "ZsIF9BAND4TpkSb" kann verhindert werden, wenn Sie nur nach ganzen Wörtern suchen UND Sie das Alphabet so geändert haben, dass es auch die Ziffer 0-9 mit einschließt, d. h. so dass diese als Wort-Zeichen betrachtet werden.

Es ist möglich, eine (unvollständige) Suchtrefferliste bereits dann einzusehen, wenn die Parallele Suche noch nicht beendet ist. Sie können den Schalter für die Suchtrefferliste jederzeit anklicken und die vorläufige Trefferliste betrachten. Zusätzliche Suchtreffer, die sich aufgrund der weiterlaufenden Suche ansammeln, werden aufgelistet, wenn Sie die Suchtrefferliste aktualisieren, wie auch sonst durch einen Klick auf den Enter-Schalter in der Suchbegriffsliste. Dieses Vorgehen ist nützlich z. B. bei einer Einsichtnahme eines laufenden Rechners vor Ort, um herauszufinden, ob ein Datenträger möglicherweise relevante Dateien enthält und sichergestellt werden soll. Wenn nach Durchsuchen von 5% aller Daten und Betrachten der bis dahin gesammelten Suchtreffer diese Frage bereits mit Ja beantwortet werden kann, kann die Suche abgebrochen werden, und es wurde viel Zeit gespart.

5.11 Logische Suche

Mächtige Unterart der parallelen Suche. Erlaubt es, entweder alle Dateien, markierte Dateien oder (wenn vom Verzeichnis-Browser-Kontextmenü aus aufgerufen) ausgewählte Dateien zu durchsuchen. Die logische Suche hat gegenüber einer physischen Suche diverse Vorteile:

- Dateischlupf kann gezielt adressiert (für alle Dateien oder, wenn halb gewählt, nur für nicht ausgelassene Dateien) oder ignoriert werden. In X-Ways Investigator wird Schlupfspeicher durchsucht; das Kontrollkästchen dafür wird aus Gründen der Vereinfachung nur nicht angezeigt.

- Der Suchbereich kann auf bestimmte Dateien und Verzeichnisse eingeschränkt werden, per Markierung oder Auswahl. Bitte beachten Sie, dass eine etwaige im Dialogfenster angezeigte Datenmenge nur eine Schätzung ist und die tatsächlich zu durchsuchende Datenmenge wegen Schlupfspeicher abweichen kann.

- Die Suche in Dateien (üblicherweise = in den Clusterketten der jeweiligen Dateien) findet

Suchbegriffe auch dann, wenn der Suchbegriff zufällig physisch durch die Dateifragmentierung zerschnitten ist (passiert am Ende und am Anfang nicht zusammenhängender Cluster).

- Die Suche kann auch erfolgreich auf Dateien angewandt werden, die auf NTFS-Dateisystemebene komprimiert sind, weil diese für die Suche dekomprimiert werden. Dies gilt sogar für per Datei-Header-Signatur-Suche gefundene Dateien, sofern dabei NTFS-Kompression gesondert berücksichtigt wurde.

- Es gibt ein gesondertes Kontrollkästchen, mit dem Sie bestimmen können, ob bestimmte Schlupfbereiche von NTFS-Kompression gezielt durchsucht werden sollen. Das Kästchen ist nicht beschriftet, aber hat einen Tooltip. Wenn es ganz gewählt ist, wird der undefinierte Schlupfbereich am Ende einer jeden Kopmressionseinheit von NTFS-komprimierten Dateien im Rohzustand durchsucht (so wie die Daten gespeichert sind, ohne Dekompression). Wenn das Kästchen zumindest halb gewählt ist, wird der wohldefinierte Schlupf von Wof-komprimierten Dateien ins Visier genommen (ebenfalls im Rohzustand durchsucht, ohne Dekompression).

- Wenn die Inhalte von Archiven (Dateien in ZIP, RAR, GZ, TAR, BZ2, 7Z und ARJ, falls nicht verschlüsselt, nur mit forensischer Lizenz) und individuelle E-Mails und E-Mail-Anhänge in den Datei-Überblick aufgenommen wurden, können sie mit durchsucht werden.

- Der Text, der in Dateien enthalten ist, deren Format von der Viewer-Komponente unterstützt wird, z. B. PDF (Adobe), WPD (Corel WordPerfect), VSD (Visio), SWF (Shockwave Flash), kann automatisch decodiert und in Form von unformatiertem ASCII- oder UTF-16-Klartext extrahiert werden, der dann zusätzlich zum Original-Dateiinhalt verlässlich durchsucht wird. Suchtreffer könnten sonst u. U. übersehen werden, da diverse Dateitypen Text üblicherweise oder zumindest gelegentlich auf eine besonders codierte, verschlüsselte, komprimierte, fragmentierte oder anderweitig unlesbare Art speichern. Wichtig: Insbes. für HTML-, XML- und RTF-Dokumente sowie E-Mails, die verschiedene Methoden wie u. a. UTF-8 zur Codierung von Nicht-7-Bit-ASCII-Zeichen (z. B. deutsche Umlaute) heranziehen, kann das Decodieren nützlich sein, abhängig von der Sprache Ihrer Suchbegriffe/den in Ihren Suchbegriffen enthaltenen Zeichen. Wenn Sie eine Dateimaske zum Decodieren angeben, wird diese nicht nur auf die Namen einer jeden zu durchsuchenden Datei angewandt, sondern auch auf den wahren Typ, sofern dieser über eine Signaturprüfung herausgefunden wurde (siehe Erweiterte Datei-Überblicke). Diese Funktion benötigt eine aktivierte separate Viewer-Komponente für die Dekodierung und die Textextraktion. Der decodierte Text wird entweder in Latin 1 oder Unicode ausgegeben. Er kann optional gepuffert werden (s. Optionen | Viewer-Programme), was eine bequeme Kontextvorschau für Suchtreffer in decodiertem Text ermöglicht und künftige Suchvorgänge beschleunigt. Die voreingestellte Dateimaske für diese Option ist *.pdf;*.docx;*.pptx;*.xlsx;*.odt;*.odp;*.ods;*.pages;*.key;*.numbers;*.eml;*.wpd;*.vsd; *.onepkg;*.json. Es wird empfohlen, ;*.html;*.xml;*.rtf je nach gesuchten Zeichen zu ergänzen, sowie weitere Dateitypen je nach Ihren Anforderungen. Z. B. könnte auch *.doc eine gute Idee sein, wenn Sie sehr gründlich sein möchten, weil Text innerhalb von

MS-Word-Dokumenten fragmentiert sein oder abrupt von einem Zeichensatz in den anderen wechseln kann. Beachten Sie nur, dass die zusätzliche Decodierung und Suche mehr Zeit benötigt und i. d. R. zu doppelten Treffern führt (Suchtreffer sowohl im Originalformat als auch im Ergebnis der Text-Extraktion). E-Mails werden von X-Ways Forensics generell nicht decodiert, wenn ohnehin nur 7-Bit-ASCII-Zeichen darin gesucht werden. Die Dateimaske wird angewandt sowohl auf den Dateinamen als auch auf den erkannten wahren Dateityp. Um den Text zu sehen, der von dieser Funktion aus einem Dokument extrahiert wird, können Sie das Dokument bei aktivem Vorschau-Modus im Verzeichnis-Browser auswählen und beim Wechseln in den Roh-Modus die Umschalt-Taste gedrückt halten.

- Ability to find *numbers* and *dates* not only if stored literally as text, but also if numbers or dates are stored in binary form in certain spreadsheet files (e.g. in OLE2 compound file format) or in some other encoded form (e.g. dates encoded as textual integer numbers in XML), if the "decode text" option is on and if in Options | Viewer Programs the box "Convert binary storage of numbers/dates in spreadsheets to text" is checked. However, this is slower than the regular text decoding. Works pretty well with numbers in Excel and LibreOffice Calc spreadsheets, but can be tricky occasionally with the format of dates if the original Excel user has selected a custom date format instead of one of the standard date formats and also because of some specialties with certain Calc files where it's not 100% predictable that a date will be extractable in the expected format. This kind of search likely works with some other file types as well, e.g. older spreadsheet types like MS Works or Lotus 123. You can try and define the file types in Options | Viewer Programs if needed. To quickly see and double-check the extraction of numbers and dates from a particular file of interest, you select that file in the directory browser and switch from ordinary to raw preview mode with the Shift key pressed. Please feel encouraged to completely remove that file mask there for faster text decoding if you do not need to search for numbers and dates in spreadsheets.

  Some more details about number searches: Consider a cell in an MS Excel spreadsheet that contains the number 1234567. You can now find that number with the Simultaneous Search searching simply for "1234567" (without the quotation marks). Even if you just know part of the sequence of digits and search for "34567", you will get a search hit (unless the "whole words only" option is on). If the cell has the "number" format (not "general"), with digit grouping enabled, you can optionally get the number with digit grouping when the file is searched/indexed/decoded in that volume snapshot for the first time, using the digit grouping symbol that is defined in X-Ways Forensics in Options | Notation, but that is not generally recommended because you would have to search for the same number both with and without the grouping symbol if you don't know whether the original spreadsheet cells were formatted as "number" with or without digit grouping or as "general". Anyway, to give you another example, if you enable that option for digit grouping in number cells in Options | Viewer Programs and you live in an English speaking country, using a comma as the digit grouping symbol, you would thus search for "1,234,567" to find that number in a number cell. You can also search for just ",567" to find the digit group "567" at the end or in the middle of any longer number in that notation.

If the number that you are looking for is a floating point number, the same rules apply, and you can optionally enter the number with as many decimals as you expect to be visible in the cell in the original application (or less), with the same decimal symbol as in your notation settings in X-Ways Forensics (either a point or comma). If a floating point number is stored for example as 9.876 and formatted to show 2 decimals, it will be shown rounded as 9.88 in the original application and will also be searchable like that in X-Ways Forensics. The same rules apply to currency amounts. You can append or prepend the currency symbol if you know for sure that it was shown in the original formatting, and how (e.g. with or without space between currency symbol and number), or you just omit symbol.

You can search for dates in pure date cells using the notation that is active in X-Ways Forensics as the so-called simple date format. If your simple date format is MM/dd/YY, you would search for 12/31/19 to find the date Dec 31, 2019. Partial date searches are also possible, and make sense especially if you do not use American date styles. For example in ISO notation "yyyy-MM-dd" you can search for "2019-07-". Or in German notation "dd.MM.yy" you can search for ".07.19" to find any date in July 2019. Pure time cell searches are also possible (with partial or whole time expressions). Just make sure to use the separator that is active in X-Ways Forensics for the display of times. Searches for combined date and time values are supported, however, the delimiter between date and time that you can expect is not the delimiter defined in Options | Notation, but typically a single space, or an individual delimiter defined by the user of the spreadsheet.

If an Excel worksheet is embedded in a .docx, .pptx, or .odt file and the volume snapshot has been sufficiently refined, the worksheet will be processed and searched in the same way as if it was a separate file. If embedded in a .doc file, you would get a notification in the form of a Vermerk "Contains embedded document(s)", which is often useful to check manually anyway. The number search capabilities should prove very useful especially in forensic accounting, tax fraud investigations etc. Please note that the simple search function of the viewer component (Ctrl+F) in ordinary ("pretty") Preview mode or the View command cannot find numbers or dates in spreadsheets, no matter how you type them.

Eine alternative Methode, um Daten aus einer Tabellenkalkulation als Text zu extrahieren, ist unter Optionen | Viewer-Programme ein- und ausschaltbar. Diese Option ist etwas experimentell und erfordert, dass das Hauptfenster von X-Ways Forensics im Vordergrund bleibt. Sie gewährleistet eine originalgetreuere Textextraktion im Sinne von Reihenfolge und Anordnung von Zellen, normalisiert die Formatierung von Datumszellen im decodierten Text auf die Notationseinstellung, die in X-Ways Forensics aktiv ist (für verlässlichere Suchergebnisse) und sie erfasst mit Sicherheit auch ausgeblendete Zellen. Die Grenzen und ordinalen Nummern von Arbeitsblättern werden durch Trennzeilen markiert. Wenn Sie Zeichen beibehalten möchten, die Ihre aktive Windows-Codepage nicht unterstützt (z. B. chinesische Zeichen auf einem typischen Computer in Europa oder Amerika) weil Sie beabsichtigen, nach ihnen zu suchen, kreuzen Sie bitte ein weiteres Kästchen an ("Muss Unicode unterstützen"). Mit dieser Option braucht die alternative Extraktionsmethode Zugriff auf die Windows-Zwischenablage.

- Optische Zeichenerkennung (OCR) in Bildern.

- Wenn Sie sich nicht für jeden einzelnen Suchtreffer interessieren, sondern lediglich dafür, welche Dateien zumindest einen der spezifizierten Suchbegriffe enthalten, kann eine logische Suche stark beschleunigt werden, indem Sie X-Ways Forensics anweisen, nur maximal einen Treffer pro Datei aufzuzeichnen und dann gleich mit der nächsten Datei fortzufahren. Die sich daraus ergebende Suchtrefferliste ist dann systematisch unvollständig, und Sie können nicht davon ausgehen, dass der eine ausgegebene Treffer pro Datei gerade ein für Sie besonders nützlicher oder aussagekräftiger ist oder dass bei mehreren Suchbegriffen gerade ein Treffer für einen Ihnen besonders wichtigen Suchbegriff ausgegeben wird. Es ist allerdings gewährleistet, dass die Suchtrefferliste alle Dateien enthält, für die es mind. einen Treffer (mit irgendeinem der verwendeten Suchbegriffe) gab, und zwar jede Datei nur einmal. Eine solche Liste ist ausreichend (und effizient!), um die betroffenen Dateien manuell einzusehen, sie mit Kommentaren zu versehen, sie aus einem Image herauszukopieren, sie an andere Ermittler in Form eines Containers weiterzugeben usw. Beachten Sie, dass es natürlich nicht möglich ist, Suchbegriffe mit einem logischen UND zu verknüpfen, wenn nur 1 Treffer pro Datei gespeichert wird. Diese Konsequenz wird von arglosen Benutzern oft vergessen.

- Dateien, die aus der Hash-Datenbank bekannt sind (entweder nur bekanntermaßen irrelevante oder bekannte nicht kategorisierte Dateien oder, wenn voll gewählt, auch bekannte verdächtige Dateien) sowie Dateien, die vom Benutzer ausgeblendet wurden oder die von einem aktiven Filter herausgefiltert werden, können bei der logischen Suche gezielt ausgelassen werden, um Zeit zu sparen und die Anzahl irrelevanter Treffer zu verringern. Der Schlupf solcher Dateien wird dennoch durchsucht, wenn die entsprechende Option "Schlupf öffnen und durchsuchen" voll eingeschaltet ist, weil sie dann eine höhere Priorität hat. Ist sie nur halb gewählt, wird auch der Schlupf solcher Dateien ausgelassen.

- Die empfehlenswerte Datenreduktion dient der Zeitersparnis und der Vermeidung doppelter Treffer durch gezieltes Auslassen bestimmter Dateien. Dateiarchive der unterstützten Typen (ZIP, RAR usw.) werden nicht durchsucht, sofern die in ihnen enthaltenen Bestandteile dem Datei-Überblick hinzugefügt wurden. In diesem Fall werden *nur* diese Bestandteile (komprimiert gespeicherte Dateien) durchsucht, in ihrem natürlichen (nicht komprimierten) Zustand. Dies kann sinnvoll für die Suche nach Schlüsselwörtern und vor allem die Indexierung (für die die Verarbeitung von Base64-Code aufwendig ist) sein, u. U. aber nicht für technische Suchen nach Signaturen usw. Die Option stellt in jedem Fall einen Kompromiss dar. Der Schlupf solcher Archive wird jedoch durchsucht, wenn die entsprechende Option eingeschaltet ist, weil sie eine höhere Priorität hat.

  Eine Datei, die als umbenannt/verschoben gekennzeichnet ist, wird bei aktiver Daten-reduktion ebenfalls nicht durchsucht, sofern die Suche prinzipiell auf alle (und nicht nur markierte oder ausgewählte) Dateien angewandt wird, da die Datei dann auch bereits unter ihrem aktuellen Namen/in ihrem aktuellen Pfad durchsucht wird.

  Wenn *.docx;*.pptx;*.xlsx;*.odt;*.odp;*.ods;*.pages;*.key;*.numbers für die Suche decodiert werden, werden die darin enthaltenen XML-Dateien mit dem Hauptinhalt

(document.xml, content.xml, index.xml, ...) sowie im Fall von .pages etwaige Preview.pdf ebenfalls ausgelassen, um redundante Suchtreffer zu vermeiden.

Dateien mit rotem X als Icon werden nicht durchsucht, es sei denn, sie werden gezielt über Auswahl oder Markierung adressiert.

- In NTFS können Dateien mit "echten" harten Verweisen (also nicht nur trivialen SFN-Verweisen) optional nur einmal durchsucht und indexiert werden. Heutzutage existieren in Windows-Installationen oft zwischen 10.000 und 100.000 harte Verweise von System-Dateien, z. B. 27 Stück zu einer Datei wie "Ph3xIB64MV.dll" in Verzeichnissen der Art
  \Windows\System32\DriverStore\FileRepository\ph3xibc9.inf_amd64_neutral_ff3a566…
  \Windows\System32\DriverStore\FileRepository\ph3xibc2.inf_amd64_neutral_7621f5…
  \Windows\System32\DriverStore\FileRepository\ph3xibc5.inf_amd64_neutral_22703…
  \Windows\winsxs\amd64_ph3xibc9.inf_31bf3856ad364e35_6.1.7600.16385_none_a0…
  \Windows\winsxs\amd64_ph3xibc5.inf_31bf3856ad364e35_6.1.7600.16385_none_9e…
  \Windows\winsxs\amd64_ph3xibc12.inf_31bf3856ad364e35_6.1.7600.16385_none_64…
  usw.
  Indem nur ein einziger harter Verweis durchsucht wird, kann man typischerweise mehrere GB an doppelten Daten einsparen, und verpasst trotzdem nichts, wenn man in allen anderen Dateien sucht. Diejenigen zusätzlichen harten Verweise, die bei der Suche optional ausgeklammert werden, sind daran zu erkennen, dass die Anzahl der Verweise im Verzeichnis-Browser in grau angezeigt wird. Suchtreffer in dem einzigen durchsuchten harten Verweis werden in der Anmerk.-Spalte in Suchtrefferlisten mit dem Hinweis "→Verweise" versehen, um Sie an die anderen harten Verweise derselben Datei zu erinnern, falls die Suchtreffer relevant sind.

- Es besteht die Möglichkeit, logische parallele Suchen zusätzlich zu Datei-Inhalten gleichzeitig auch auf Zellen des Verzeichnis-Browsers (also Metadaten) anzuwenden, und zwar auf die Zelle jeder ausgewählten Verzeichnis-Browser-Spalte wie Name, Autor, Absender, Empfänger oder Metadaten. Das erspart Ihnen das Einfügen Ihrer Suchbegriffe in die Filterdialoge diverser Verzeichnis-Browser-Spalten. Diese Vorgehensweise ist auch gründlicher, weil jeglicher von diesem Feature adressierter Text in UTF-16 durchsuchbar ist, wohingegen dieselben Daten anderswo fragmentiert gespeichert sein können (z. B. Dateinamen, insbes. in FAT), speziell codiert (z. B. Absender und Empfänger in E-Mails als Quoted Printable), komprimiert oder in unerwarteten Codepages. Sie ist auch bequem, weil alle Suchtreffer in derselben Weise präsentiert und aufgelistet werden wie gewöhnliche Suchtreffer in Datei-Inhalten. Nur in der Spalte mit der Suchtreffer-Beschreibung werden solche Treffer mit dem Namen der Spalte, die den gefundenen Text tatsächlich enthält, gekennzeichnet, und die Suchtreffer werden in einer anderen Hintergrundfarbe hervorgehoben. Sie können nach Suchtreffern in Zellen des Verzeichnis-Browsers auch filtern.

  Wenn Sie einen Suchtreffer dieser Art auswählen, wird der automatisch im Modus Details gesucht und hervorgehoben, genau wie normale Suchtreffer in Datei-Inhalten im Vorschau-Modus gesucht und hervorgehoben werden.

  Beachten Sie, dass eine Suche in Zellen des Verzeichnis-Browsers keine etwaigen

zusätzlichen Zellinhalte in einer anderen Farbe durchsucht, wie etwa alternative Dateinamen und Datei-Anzahlen in der Namensspalte.

- Einige blinde Flecke, die logische Suchen in anderen Computerforensik-Programmen aufweisen, gibt es in X-Ways Forensics nicht. Spezielle Bereiche in Volumes werden von logischen Suchen gesondert adressiert. Der Übergang von Dateischlupf in direkt darauffolgenden freien Speicher sowie in NTFS und exFAT der Übergang von bekanntermaßen nicht initialisierten Endstücken von Dateien in darauffolgenden freien Speicher gehören dazu, ebenso wie RAM-Schlupf in NTFS-Kompressionseinheiten.

Sollte X-Ways Forensics während dieser Operation einfrieren, denken Sie daran, dass die interne ID und der Name der zuletzt bearbeiteten Datei in dem kleinen Fortschrittsanzeigefenster angezeigt werden. Wenn diese Operation auf ein Asservat angewandt wird und X-Ways Forensics währenddessen bei einer bestimmten Datei abstürzt, wird Ihnen beim Neustart des Programms die betreffende Datei mitgeteilt, und die Datei wird mit einem Vermerk versehen. Das hängt von den Sicherheitsoptionen ab. All dies geschieht, damit Sie eine solche Datei ggf. ausblenden und so bei einem nochmaligen Versuch auslassen können.

Eine Parallelisierungsmöglichkeit (derzeit noch im experimentellen Stadium) erlaubt es, mehrere Prozessorkerne besser zu nutzen, durch den Einsatz von mehreren Threads. Die hat nur dann einen Effekt, wenn Sie in Asservaten suchen, die Images oder Verzeichnisse sind, keine Datenträger. Je schneller die Datenträger sind, auf denen die Images/Verzeichnisse liegen, in Form von Seek Times und Datenübertragungsrate, desto mehr Zeit prozentual können Sie hierdurch einsparen. Unter perfekten Bedingungen kann die Geschwindigkeit der logischen Suche so mehr als verdoppelt werden. Wenn Sie keine zusätzlichen Threads für die logische Suche wählen, funktioniert die Suche wie in X-Ways Forensics vor Version 18.9. Wenn Sie 1 oder mehr Extra-Threads wählen, wird die Suche in zusätzlichen Worker-Threads durchgeführt, und der Haupt-Thread des Prozesses hat während dessen nichts zu tun, außer auf Benutzeraktivitäten in der Benutzeroberfläche zu reagieren, wodurch diese jederzeit blitzschnell ansprechbar bleibt. In X-Ways Investigator können bis zu 3 Worker-Threads verwendet werden, in X-Ways Forensics bis zu 16, in Abhängigkeit von der vorgefundenen Anzahl von Prozessorkernen.

5.12 Suchtrefferliste

Verfügbar nur mit einer forensischen Lizenz, beim Arbeiten mit einem Fall, für Asservate mit einem Datei-Überblick. (Ansonsten erfüllt der Positions-Manager diese Aufgabe.)

Der Verzeichnis-Browser kann zur Suchtrefferliste umfunktioniert werden. Um in diesen Anzeigemodus zu gelangen, klicken Sie den Schalter mit dem Fernglas und den vier waagerechten Linien an, zu finden in derselben Leiste wie die Modus-Schalter. Er ist nur für Asservate verfügbar. In diesem Modus gibt es vier zusätzliche Spalten: physische (absolute) Offsets von Suchtreffern, logische (relative) Offsets, Beschreibungen, die die Codepages angeben, in denen die Suchtreffer gefunden wurden, und Hinweise, wenn sie im Dateischlupf liegen, und die Suchtreffer selbst (normalerweise mit einer Kontextvorschau, sortierbar nach Suchbegriff, Kontextvorschau nicht korrekt für arabischen oder hebräischen Text und Treffer in

UTF-8). Die Gruppieroptionen des Verzeichnis-Browsers haben keine Wirkung, wenn nach einer dieser Spalten sortiert wird. Die Spalte mit der Beschreibung eines Suchtreffers bietet auch einen Filter an, der es Ihnen erlaubt, sich auf als wichtig markierte Treffer zu konzentrieren, in den Fallbericht aufzunehmende Treffer, eigene Suchtreffer, Treffer in einer bestimmten Codepage, Treffer im Text-Extrakt eines Dokuments sowie Treffer im Schlupfspeicher oder im nicht initialisierten Endteil von Dateien. Suchtreffer in allen Varianten von UTF-16, die nicht an geraden Offsets ausgerichtet sind, werden in der Anmerkungsspalte als „unaligned“ beschrieben. Dies ist ein kleiner erläuternder Hinweis dazu, warum Sie den Text zwar in der ausrichtungsunabhängigen Kontextvorschau der Suchtreffer-Spalte lesen können, aber nicht in der starren Textspalte.

Fast alle Befehle im Verzeichnis-Browser-Kontextmenü sind auch für Suchtrefferlisten verfügbar, insbes. Möglichkeiten zum Kopieren, Einsehen, Markieren und Kommentieren von Dateien. Die dynamischen Filter, die auf den regulären Verzeichnis-Browser-Spalten basieren, können in Verbindung mit Suchtrefferlisten zum Einsatz kommen, z. B. um sich auf Treffer in Dateien eines bestimmten Typs mit einem bestimmten Änderungsdatum zu konzentrieren.

Die Suchtrefferliste basiert auf der Position und der Ebene im Verzeichnisbaum, die Sie anklicken, so dass Sie z. B. alle Suchtreffer in Dateien im Verzeichnis \Dokumente und Einstellungen sowie all dessen Unterverzeichnissen einsehen können, und sogar Suchtreffer von allen Asservaten des gesamten Falls auf einmal, wenn Sie den Asservatüberblick verwenden. Es ist außerdem möglich, bequem einen oder mehrere Suchbegriffe für das Einsehen der Treffer auszuwählen, in der Such*begriffs*liste unten im Falldatenfenster. Dadurch ist es auch einfach, schnell herauszufinden, wie viele Suchtreffer es für einen gegebenen Suchbegriff gibt, für jede beliebige Ebene im Verzeichnisbaum, weil diese Zahl in der Überschriftszeile Verzeichnis-Browsers je nach Befüllung mit Suchtreffern angezeigt wird.

Suchtrefferlisten sind nicht statisch, sondern werden dynamisch zusammengestellt, abhängig von gewählten Suchbegriffen, erkundetem Pfad, aktuellen Filtereinstellungen und basierend auf den Einstellungen der Suchbegriffsliste (logischen UND-Kombinationen und der Option "Nur 1 Treffer pro Objekt").

Sie können Suchtreffer über den Filter der Suchtreffer-Spalte filtern, z. B. basierend auf ihrem Kontext oder abhängig davon, ob Sie Suchtreffer als wichtig gekennzeichnet habe. Alle Filteroptionen können mit einem logischen ODER oder einem logischen UND verknüpft werden, und Sie können sich auf Suchtreffer konzentrieren, die die definierten Bedingungen entweder erfüllen oder NICHT erfüllen.

Suchtreffer können als wichtig gekennzeichnet werden (so dass links eine gelbe Glühlampe angezeigt wird), mit Hilfe des Verzeichnis-Browser-Kontextmenüs sowie durch Drücken der Leertaste. Mit der Leertaste können Sie solche Kennzeichnungen auch wieder aufheben. Sie können mehrere ausgewählte Suchtreffer auf einmal entmarkieren, indem Sie die Umschalt-Taste beim Aufruf des Kontextmenü-Befehls "Als wichtig kennzeichnen" gedrückt halten. Another context menu command allow to unmark all search hits in the evidence object(s) represented by the current data window as notable. This allows for incremental filtering. Example: You filter for search hits whose context contains the word "Hello". Then you mark those hits as notable (Ctrl+A plus context menu command). Then you filter for search hits that are notable AND contain the word "Hey". Then you unmark all search hits (even those that are currently not listed!),

which has no immediate effect on the presented list, and mark those that are listed as notable again. The result is that all search hits that contain both "Hello" and "Hey" in their context are now marked as notable.

Wenn Sie bestimmte Suchtreffer nicht mehr benötigen, können Sie sie auswählen und löschen. Z. B. weil es doppelte Suchtreffer geben könnte oder weil Sie eine Suche nach denselben Suchbegriffen in denselben Dateien nochmal mit leicht anderen Einstellungen laufen lassen möchten. Wenn Sie keinen der Suchtreffer für bestimmte Suchbegriffe mehr benötigen, können Sie diese Suchbegriffe in der Suchbegriffsliste auswählen und sie mitsamt all ihrer Suchtreffer löschen.

Die Kontextvorschau direkt in der Suchtrefferliste um einen Suchtreffer herum kann über das Kontextmenü ein- und ausgeschaltet werden im Fall von Problemen wie extremer Langsamkeit oder Instabilität.

Another context menu command allows to reposition search hits, with a relative offset change (+/-), and to resize search hits, with either an absolute new size or with a positive or negative relative size adjustment (click the arrow button to toggle). You can resize multiple search hits at the same time with the same settings.

5.13 Suchbegriffsliste

Die Suchbegriffsliste befindet sich unten im Falldatenfenster, wenn man sich im Modus zum Einsehen von Suchtreffern befindet (den Schalter mit dem Fernglas und den vier horizontalen Linien angeklickt hat). Die Suchbegriffsliste enthält alle Suchbegriffe, die jemals in dem Fall verwendet wurden, sofern nicht vom Benutzer gelöscht. The search terms can optionally be sorted alphabetically in ascending order or by the listed search hit count in descending order, via the context menu of the search term list, to make it easier to locate a certain search term in lengthy lists.

Wenn Sie Suchbegriffe in der Suchbegriffsliste auswählen und den Enter-Schalter anklicken, erhalten Sie eine Auflistung aller Treffer zu diesen Begriffen im aktuell gewählten Pfad, ggf. beeinflusst durch Filter, in einer Suchtrefferliste. Sie können mehrere Suchbegriffe auswählen, indem Sie die Umschalt- oder Strg-Taste gedrückt halten, wenn Sie sie anklicken. Benutzen Sie die Entf-Taste, um gewählte Suchbegriffe und all deren Suchtreffer permanent zu löschen.

Um eine Suchtrefferliste zu reduzieren auf eine Liste von Dateien, die mind. einen Suchtreffer aufweisen, kreuzen Sie „Nur 1 Treffer pro Objekt auflisten“ an. Dies kann sich als sehr nützlich erweisen, wenn Sie all solche Dateien einzeln durchsehen möchten, weil es gewährleistet, dass jede solche Datei dann nur noch genau einmal aufgelistet wird. Sie können allerdings nicht davon ausgehen, dass der eine übrigbleibende Treffer pro Datei gerade ein für Sie besonders nützlicher oder aussagekräftiger ist oder dass bei mehreren ausgewählten Suchbegriffen gerade ein Treffer für einen Ihnen besonders wichtigen Suchbegriff übrigbleibt. Die Reduktion ist nicht destruktiv; sobald Sie das Kreuz bei dieser Option entfernen und den Enter-Schalter wieder anklicken, erscheint wieder die komplette Suchtrefferliste.

The option to list 1 search hit per item only does not filter out search hits in slack space or in uninitialized parts of files (in the part exceeding the so-called valid data length). This is useful because the slack of a file is typically not related to the contents of that file, so any search hits in these special areas would likely have a totally different context than search hits in the logical portion of the file (and especially search hits in the uninitialized part of a file may reside in data from various different sources) and thus they need to be reviewed additionally. Please note that it is still necessary to unselect the "1 hit per item" option to separately check out search hits in conglomerates such as pagefile.sys and the virtual "Free space" file, which contain data from totally different sources. The "1 hit per item" option is most useful for documents, for which you can often tell after one quick look in Preview mode whether that particular file is relevant or not.

Es ist möglich, die Anzahl von Suchtreffern zu ausgewählten Suchbegriffen in der Suchbegriffsliste abzulesen und über den Befehl „Liste exportieren“ im Kontextmenü auch zu kopieren. Diese Zahlen basieren auf den aktuellen Einstellungen für die auf dem Bildschirm aufgelisteten Suchtreffer und hängen ab von Filtern, dem erkundeten Pfad, etwaigen UND-Verknüpfungen von Suchbegriffen usw. It is the numbers of hits that are actually listed, not the numbers of hits that have been recorded/saved. To see the total numbers of hits, deactivate any filter and select all search terms. Note that the "List 1 hit per item only" option also functions like a filter for search hits.

Sie können Suchbegriffe im Kontextmenü der Suchbegriffsliste umbenennen, so dass z. B. bestimmte lange reguläre Ausdrücke generell ersetzt werden durch kürzere, sprechendere Namen wie "IP-Adressen", "Kreditkartennummern", "E-Mail-Adressen" usw. These names can be remembered by the program such that future searches for the same expressions will immediately add entries in the search term list with the more easily recognizable friendly names. Friendly names and corresponding regular expressions are stored in the text file "Regular Expressions.txt", which you can share with your colleagues and from which you can easily copy and paste regular expressions when needed. The file can be opened from within the Simultaneous Search dialog window by clicking on the button with the yellow lightbulb (lightbulb for "ideas" for expressions to search for). You can edit the file directly with any text editor. Just keep the structure intact: Always 1 friendly name followed by 1 regular expression, 2 lines for each such pair, in UTF-16.

Es bestehen zwei verschiedene Möglichkeiten, mehrere Suchbegriffe mit Booleschen Operatoren logisch zu verknüpfen:

1) Standardmäßig werden mehrere ausgewählte Suchbegriffe mit einem logischen ODER verknüpft. Um einen Suchbegriff zu erzwingen, wählen Sie ihn aus und drücken die „+“-Taste. Um einen Suchbegriff auszuschließen, wählen Sie ihn aus und drücken die „-“-Taste. Um einen Suchbegriff auf normale ODER-Kombination zurückzusetzen, drücken Sie die Esc-Taste. Sie können für all dies auch das Kontextmenü der Suchbegriffsliste verwenden. Die folgenden Beispiele beschreiben die Auswirkung des Auswählens der Suchbegriffe A und B in Abhängigkeit ihres „+“- bzw. „-“-Status’.

A
B
= Suchtreffer für A und Suchtreffer für B in beliebigen Dateien (normale ODER-Kombination)

+A

B
= Suchtreffer für A und Suchtreffer für B in Dateien, die A enthalten

+A
+B
= Suchtreffer für A und Suchtreffer für B in Dateien, die sowohl A als auch B enthalten (UND)

A
-B
= Suchtreffer für A in Dateien, die nicht B enthalten

2) Um eine logische UND-Kombination zu erreichen, wenn die Suchbegriffe *nicht* mit „+“ oder „-“ versehen sind, verwenden Sie den kleinen Rollbalken, der erscheint, wenn Sie mehrere Suchbegriffe auswählen. Erlaubt es Ihnen, nur Suchtreffer in solchen Dateien zu sehen, die alle gewählten Suchbegriffe *zugleich* enthalten. Sie können bis zu 7 Suchbegriffe auf diese Weise verknüpfen. Wenn Sie mehr als 2 Suchbegriffe auswählen, können Sie auch weniger streng vorgehen und nur eine *Minimalzahl* von verschiedenen Suchbegriffen angeben, die in derselben Datei vorkommen muss, z. B. fordern, dass von den Suchbegriffen A, B, C und D eine beliebige Kombination von zweien in derselben Datei ausreicht, z. B. (A und B) oder (A und C) oder (B und D) usw. (unscharfe/flexible UND-Kombination).

Zusätzlich zur "Min. *x*"-Einstellung gibt es auch ein die Möglichkeit zu "Max. 1", wenn mehrere Suchbegriffe ausgewählt sind und nicht mit einem + erzwungen oder mit einem - ausgeschlossen werden. "Max. 1" listet Suchtreffer nur dann auf, wenn sie in Dateien enthalten sind, die keinen der anderen ausgewählten Suchbegriffe enthalten. Wenn Sie bei z. B. bei 3 Suchbegriffen auf anderem Weg dasselbe Ergebnisse sehen wollten, müssten Sie die Suchtreffer zu Suchbegriff A auflisten lassen bei Ausschluss von B und C, dann die Suchtreffer zu B beim Ausschluss von A und C, und dann die Suchtreffer von C bei Ausschluss von A und B, was natürlich längst nicht so elegant und komfortabel ist und all solche singulären Suchtreffer nicht gleichzeitig zeigt.

Wenn 2 Suchbegriffe in der Suchbegriffsliste ausgewählt sind und mit einem logischen UND verknüpft werden (egal mit welcher der beiden verfügbaren Methoden), können Sie zusätzlich einstellen, dass Suchtreffer zu den Suchbegriffen „nahe beieinander“ (NEAR) vorkommen müssen, um aufgelistet zu werden, um mit höherer Wahrscheinlichkeit relevante Kombinationen beider Suchbegriffe in derselben Datei zu finden, genau wie mit einer Umgebungssuche. Die maximale Entfernung zwischen den Suchtreffern, die noch als „nahe beieinander“ gewertet werden soll, können Sie in Bytes definieren. Eine NEAR-Kombination kann auch auf mehr als 2 ausgewählte Suchbegriffe angewandt werden. Die Wirkung ist, dass ein Suchtreffer nur dann aufgelistet wird, wenn *irgendein* anderer der ausgewählten Suchbegriffe in der Nähe vorkommt.

Die dem zugrundliegende linguistische Annahme ist, dass die Anordnung von Wörtern in naher Nachbarschaft in einem Dokument eine Beziehung zwischen den Wörtern impliziert. Given that authors of documents try to formulate sentences which contain a single idea, or cluster related ideas within neighboring sentences or organized into paragraphs, there is an inherent, relatively high, probability within the document structure that words used together are related. Whereas, when two words are on the opposite ends of a book, the probability there is a relationship between the words is relatively weak. By limiting search results to only include matches where the words are within the specified maximum proximity, or distance, the search results are assumed to

be of higher relevance than the matches where the words are scattered. (Abschnitt zitiert von wikipedia.org)

Des Weiteren bietet die Suchbegriffsliste eine "NOT NEAR"-Option an (abgekürzt NTNR), zusätzlich zu "NEAR". Bei 2 ausgewählten Suchbegriffen stellt NTNR sicher, nur solche Suchtreffer aufgelistet werden, die *nicht* in der Umgebung eines Suchtreffers des jeweils anderen Suchbegriffs liegen. Bei mehr als 2 ausgewählten Suchbegriffen ist das Resultat derzeit undefiniert.

5.14 Besonderheiten der Trefferzahl in Suchbegriffslisten

Question: Why when all the search terms are selected with "List 1 hit per item only" are the counts returned different from when I click on each search term individually with the same setting? Answer: Because the option is "List 1 hit per item only", and not "List 1 hit per search term per item only". Many users do not understand that. Imagine if in the same file there is 1 hit for search term A and 1 hit for search term B, and you select both A and B with that option enabled, then only 1 hit is listed, either the one for A or the one for B (up to X-Ways Forensics to decide). So the displayed hit count is 1 for one search term and 0 for the other one. If then you select the other search term only and click "Enter", the count for that search term will change from 0 to 1 because that is now the only possible search term from which hits can be listed, and up to 1 search hit is listed per file, so that 1 hit is listed.

Noch eine weitere Erklärung mit Beispiel: Datei 1 enthält die Suchbegriffe A und B, Datei 2 enthält die Suchbegriffe A, B und C. In der Suchbegriffsliste wählen Sie alle drei Suchbegriffe aus (A, B und C) und klicken auf "Eingabe". Dabei ist "Nur 1 Treffer pro Objekt" angekreuzt. Das hat zur Folge, dass von Datei 1 nur maximal ein Suchtreffer zur Anzeige ausgewählt wird und von Datei 2 auch nur maximal einer. Welche das sind, kann X-Ways Forensics sich aussuchen. Vielleicht nimmt es von Datei 1 den Suchtreffer zu Suchbegriff A und von Datei 2 den Suchtreffer zu Suchbegriff C. D. h. Als Anzahl der Treffer wird für Suchbegriff A in Klammern 1 angezeigt und für Suchbegriff C in Klammern auch 1. "What you see is what you get." Für B wird in Klammern 0 angezeigt, denn wenn der Benutzer nur 1 Treffer pro Datei haben will, braucht er Treffer für B ja gar nicht mehr. Er schaut sich die beiden Dateien ja sowieso schon an, wegen der Treffer für A und C.

Wenn Sie dann aber in der Suchbegriffliste NUR noch B auswählen und A und C gar nicht mehr, weil Sie sich im Moment nur für B interessieren, hat X-Ways Forensics keine Wahl mehr, dann muss es Ihnen den Treffer für B in Datei 1 und den in Datei 2 anzeigen. Auch hier gilt "Nur 1 Treffer pro Objekt". Dann wird für A und C in Klammern eine 0 angezeigt, denn die Suchtreffer für A und C werden zur Erfüllung von "Nur 1 Treffer pro Objekt" nicht benötigt. Und für B wird nun in Klammern eine 2 angezeigt, weil ja 2 Suchtreffer für B in der Suchbegriffsliste angezeigt werden, einer in Datei 1 und einer in Datei 2. Dass bei B vorher eine 0 stand, heißt nicht, dass es keine Suchtreffer für B gibt, sondern nur dass sie zu dem Zeitpunkt nicht angezeigt und zur Erfüllung des Wunsches "Nur 1 Treffer pro Objekt" auch nicht benötigt wurden. Die 0 signalisiert, dass das Auflisten etwaiger vorhandener Suchtreffer für Suchbegriff B keine Dateien zu Tage fördern, die Sie nicht ohnehin schon im Blickfeld haben dank der bereits aufgelisteten Suchtreffer zu A und C.

Wenn Sie sich in Wirklichkeit doch für ALLE Suchtreffer interessieren, dann ist es ein Fehler Ihrerseits, "Nur 1 Treffer pro Objekt" anzukreuzen. Oder vielleicht glauben Sie, dass "Nur 1 Treffer pro Objekt" in Wirklichkeit "Nur 1 Treffer pro Suchbegriff pro Objekt" bedeutet und nur falsch beschriftet ist. Das ist aber auch nicht der Fall. Wenn X-Ways Forensics 1 Suchtreffer zu einem beliebigen Suchbegriff liefert, hat es der Option genüge getan. Weitere Suchtreffer zu anderen Suchbegriffen in derselben Datei fallen unter den Tisch. Sie sind bei "Nur 1 Treffer pro Objekt" ja offenbar ausdrücklich nicht erwünscht.

5.15 Ereignislisten

Verfügbar nur mit einer forensischen Lizenz, beim Arbeiten mit einem Fall, für Asservate mit einem Datei-Überblick.

Beim Extrahieren von Metadaten (Teil des Erweiterns des Datei-Überblicks), kann X-Ways Forensics eine Liste von Ereignissen zusammenstellen aus Zeitstempeln. die auf Dateisystem-ebene gefunden werden sowie intern in Dateien und im Hauptspeicher. Denkbare Quellen sind Verläufe von Internet-Bowsern, Event-Logs von Windows, Registry-Hives von Windows, E-Mails usw. Eine Ereignisliste funktioniert genau wie eine Suchtrefferliste und wird angezeigt, wenn Sie einen Schalter anklicken, der sich direkt neben dem Schalter für Suchtrefferlisten befindet, an einem Uhrensymbol zu erkennen. Genau wie eine Suchtrefferliste kommt eine Ereignisliste mit weiteren Spalten daher: Zeitstempel des Ereignisses, Ereignistyp, Ereignis-kategorie, und einige Ereignisse haben eine individuelle Beschreibung/zusätzlichen Text, z. B. Ereignisse in der Windows-Registry und in Internet Explorer index.dat-Dateien verzeichnete Ereignisse

Wenn eine Ereignisliste chronologisch sortiert ist, nach Zeitstempeln, dann funktioniert sie wie eine Zeitleiste, anhand der Sie leichter eine Folge von Ereignissen ablesen können, die an unter-schiedlichen Orten gespeichert sind (z. B. E-Mail empfangen, Anhang abgespeichert, Anwendung gestartet, Dokument gedruckt, Datei gelöscht), die Sie sonst nicht untereinander im Zusammenhang sehen könnten. Wie üblich können Sie im Asservat-Überblick Ereignisse von verschiedenen Asservaten auf einmal sehen, rekursiv oder verzeichnisweise erkunden, nach Ereignistyp sortieren oder nach Ereigniskategorie sowie tagesgenau nach bestimmten Zeitspannen filtern.

Sie können Ereignisse genau wie Suchtreffer als wichtig kennzeichen. Nach als wichtig gekennzeichneten Ereignisse lässt sich über die Zeitstempel-Spalte filtern.

Ereignisbasierte Auswertung anstelle von dateibasierter Auswertung ist ein progressiver neuer Ansatz mit völlig anderer Perspektive, der zu Wissen über von Computern aufgezeichnete Aktivitäten führen kann, das auf andere Weise nur schwerlich gewonnen werden könnte. Sie können u. U. Zusammenhänge erkennen (in Verbindung mit Aktivität *x* stehende andere Aktivität), die ansonsten leicht übersehen wird, und die Logik hinter dem, was passiert ist, besser erklären.

Die Quellen von Ereignissen, die von der Metadaten-Extraktion in dieser Version ausgewertet

werden, umfassen alle unterstützten Dateisysteme (d. h. alle auch in den Zeitstempel-Spalten des Verzeichnis-Browser zu sehenden Zeitstempel; Änderung, Record-Änderung und letzter Zugriff werden ausgelassen, wenn sie identisch zur Erzeugungszeit sind), Prozesse in unterstützten Hauptspeicher-Dumps, extrahierte oder verarbeitete E-Mails sowie Dateien der folgenden Typen:
index.dat
Internet browser SQLite databases
.firefox (~55) fragments
_CACHE_001_ and _CACHE_002_
.lnk shortcuts
.automaticDestination-ms
.chrome Chromium cache data_1, data_2
.usnjrnl fragments
Registry hives*
Windows .evt event logs
Windows .evtx event logs (Most extracted events come with a description that includes the event source, the event ID and the record number. The record number allows you to quickly search for the record in the HTML preview if you need further details about that particular event.)
DataStore.edb (MS Windows operating system update events)
.hbin Registry hive fragments
.doc (last printed)
.msg
rp.log XP restore point
INFO2 XP recycle bin
.recycler Vista recyle bin
.snapprop Vista volume shadow copy properties
.cookie
.gthr;.gthr2 Gatherer and Gatherer fragments
.pf prefetch
attach timestamps from EDB
signing date from EXE/DLL/SYS/...
boot time from ETL (event trace log) files
OLE2 last modification
last saved in Office documents and RTF
Skype main.db (chats, calls, file transfers, account creation, ... - you can read entire chats if sorted chronologically)
Skype Chat Sync
internal creation from miscellaneous file types, including Exif timestamps from photos
JPEG GPS
Unix/Linux/Macintosh system logs (These events are practically of significance especially for USB device history examinations.)

* Weitere, speziellere Ereignisse als nur Standard-Registry-Zeitstempel werden optional ausgegeben, wenn man einen Registry-Bericht erzeugt, in Abhängigkeit von den verwendeten Berichtsdefinitionen.

The event type is displayed in gray if the timestamp is a previously valid timestamp, for example such as those found in NTFS in 0x30 attributes or index records of INDX buffer slack or in $LogFile.

Timestamps from 0x30 attributes in NTFS file systems are output as events only if actually different from their 0x10 counterparts and not identical to the 0x30 creation timestamp. They are marked as "0x30" in the Event Type column. Malware might give itself harmless looking timestamps after deployment, so that it does not seem to be related to the time of intrusion/infection. The 0x30 attribute timestamps, however, remain unaltered (except if the file is renamed or moved later), and that is the reason why some examiners are interested in them. If the time frame of intrusion/infection is known, related files would be found in the event list thanks to the original 0x30 attribute timestamps.

0x30 timestamps are marked in the Event Type column with “> 0x10” if they are later than the corresponding 0x10 timestamps, which seems unnatural and in some rare cases might be the result of backdating by the rightful users of the computers themselves. Under certain circumstances, backdating documents is seen as fraudulent and illegal. However, much more commonly 0x10 timestamps predating 0x30 timestamps is just the work of installation programs or the result of copying a file or moving a file from one volume to another or extracting a file from a zip archive, where Windows or other programs artificially apply the original creation time of the source file to the destination once copying turns out to be successful (internal programmatic backdating).

The selections in the event type filter are not remembered by the program from one session to the next.

Please see the description of the timestamp columns for more information.

5.16 Als Laufwerksbuchstabe einbinden

Verfügbar in X-Ways Forensics und WinHex Lab Edition. (Für Datei-Container mit nicht mehr als 1.000 Objekten mit jedem Lizenztyp für WinHex verfügbar, sogar kostenlos in der Evaluationsversion.)

Erlaubt es, die von aktiven Datenfenster repräsentierte Partition im eigenen Windows-System als Laufwerksbuchstaben einzubinden. Entweder vollständig (beim Aufruf über das Specialist-Menü oder über das Falldatenfenster-Kontextmenü für ein ganzes Volume) oder ausschnitthaft (wenn über das Kontextmenü des Verzeichnis-Browsers oder das Falldatenfenster-Kontextmenü auf ein Verzeichnis oder eine Datei mit Unterobjekten angewandt). So erhalten Sie bei Bedarf mit externen Programmen bequem und schnell Zugriff auf alle Dateien, ohne diese erst mit dem Befehl Wiederherstellen/Kopieren herauskopieren zu müssen. Sehr effizient insbes., wenn Sie eine ganze Partition oder ein Verzeichnis mit einem Virenscanner überprüfen möchten. Das Einbinden funktioniert für alle unterstützten Dateisysteme, für alle unterstützten Partitionierungsmethoden und alle unterstützten Image-Typen (in X-Ways Forensics: Roh-Images, .e01, VDI, VMDK, VHD, und selbstverständlich Datei-Container), sogar für Images innerhalb von anderen, auch für Partitionen von physisch angeschlossenen Datenträgern, die mit einem Dateisystem formatiert sind, das Windows unbekannt ist. Der Zugriff auf alle Dateien ist ein vollständig schreibgeschützter Zugriff. Das Mounten von Images oder Datenträger-Partitionen ändert nichts in dem Image bzw. auf dem Datenträger. Um das Einbinden als

Laufwerksbuchstabe zu beenden, rufen Sie den Menübefehl einfach erneut auf und klicken dann auf den Abbrechen-Schalter.

Sie können wahlweise alle existierenden und/oder alle bekannten ehemals existierenden Dateien des Volumes im eingebundenen Laufwerk sehen, genau dieselben Dateien wie im außerordentlich gründlichen Datei-Überblick von X-Ways Forensics selbst. Dessen Vollständigkeit hängt bekanntlich davon ab, ob er bereits erweitert worden ist oder nicht. Optional können herausgefilterte Dateien auch in den Verzeichnissen des eingebundenen Laufwerks von der Auflistung ausgenommen werden. D. h. in anderen Worten, die internen Filter von X-Ways Forensics können auch extern wirken. Unterobjekte von Dateien (Dateien in Dateien) werden ebenfalls optional nach außen dargestellt, als Dateien in einem künstlichen Unterverzeichnis, das denselben Namen hat wie die Elterndatei, lediglich um ein einziges Zeichen ergänzt, damit der Name eindeutig wird, wie Sie es evtl. vom Wiederherstellen/Kopieren-Befehl kennen. Standardmäßig ist dieses Zeichenanhängsel unsichtbar, d. h. ein Unicode-Zeichen ohne eigenen Breite, damit der Pfad des Unterobjekts so original wie möglich aussieht. Sie können das Zeichen allerdings durch ein anderes ersetzen, z. B. einen Unterstrich, wenn Sie etwas mit einem alten externen Programm auf die Dateien zugreifen, das nicht unicodefähig ist. Dazu müssen Sie das unsichtbare Zeichen zunächst aus dem Editierfeld entfernen, z. B. durch Anklicken und Drücken der Rücksetz-Taste. Das funktioniert auch dann, wenn es scheinbar keinen sichtbaren Effekt hat. Danach können Sie ein beliebiges anderes Zeichen einfügen.

Ehemals existierende Objekte werden optional aufgelistet, und wenn dies der Fall ist, werden Sie extern mit dem Attribut "versteckt" dargestellt, so dass sie auch im Windows Explorer optisch von existierenden Objekten unterscheidbar sind. Virtuelle Verzeichnisse werden auf dieselbe Art präsentiert. (Natürlich werden versteckte Dateien in Windows nur dann angezeigt, wenn Sie angeben, dass Sie sie sehen möchten, s. Extras | Ordner-Optionen | Ansicht). Existierende Dateien werden ebenfalls optional aufgelistet (aber existierende Verzeichnis zwangsweise, weil sie u. U. benötigt werden, um zu ehem existierenden Dateien überhaupt navigieren zu können). Virtuelle Dateien in einem Datei-Überblick sowie interne Dateien von Dateisystemen (wie $MFT in NTFS und Catalog in HFS+) werden ebenfalls nur optional eingebunden. Dasselbe gilt für die Originalnamen und -Orte von belanntermaßen umbenannten/verschobenen Dateien. Besondere Objekte wie alternative Datenströme, extrahierte E-Mails, Video-Standbilder, eingebettete Miniaturansichten, Ausschnitte usw. usf. werden im eingebundenen Laufwerk wie normale Dateien dargestellt. Dateischlupf wird nicht nach außen zugänglich gemacht. Dateien mit identischem Namen im selbem Verzeichnis (z. B. eine existierende Datei und eine ehem. existierende Dateien, bis zu 16) sind kein Problem für das Einbinden als Laufwerksbuchstabe. Solche Dateien können extern über den Laufwerksbuchstaben so geöffnet werden, als hätten sie eindeutige Namen.

Eine Option namens "Rekursiv anwenden" ist verfügbar, um die Dateien aus allen Unterverzeichnissen des aktuell aktiven Asservats bzw. des ausgewählten Verzeichnisses in einer flachen Liste anzuzeigen. Nützlich, wenn Sie vorhaben, viele dieser Dateien in einem externen Programm zu öffnen und zu dem Zweck nicht durch die diversen Verzeichnisse navigieren wollen. Wenn Sie diese Option benutzen, werden die int. IDs der Dateien in deren Namen eingefügt, um die Dateien für X-Ways Forensics besser identifizierbar zu machen.

Diese Funktion erfordert Windows 7 oder neuer sowie die Installation einen Treibers. Letztere

wird automatisch in Angriff genommen, wenn Sie einen beliebigen der Menübefehle zum Einbinden zum ersten mal aufrufen. Weiterhin wird das Microsoft Visual C++ 2013 Redistributable Package benötigt, das in Windows standardmäßig nicht enthalten ist und u. U. separat heruntergeladen werden muss). Das bedeutet, dass dieser spezielle Teil von X-Ways Forensics nicht portabel ist, aber das Einbinden als Laufwerksbuchstabe ist ohnehin keine für die Vorab-Einsichtnahme von laufenden Systemen vor Ort typische Funktion.

Interaktivität: Das Löschen einer Datei in einem von X-Ways Forensics bereitgestellten Laufwerksbuchstaben in Windows löscht natürlich nicht die Datei im Image oder auf dem Datenträger, aber kann unter Windows 7 eine der folgenden Aktionen im Datei-Überblick auslösen:
1) Datei im Datei-Überblick ausblenden
2) Datei als bereits eingesehen kennzeichnen
oder
3) Datei mit einem Vermerk Ihrer Wahl versehen.
Die dritte Option ist besonders dann nützlich, wenn Sie die Partition zum Überprüfen auf Malware mit einem Virenscanner als lokales Laufwerk einbinden. Sollte der Virenscanner eine Datei löschen oder in Quarantäne verschieben, wird X-Ways Forensics das bemerken und diese Datei mit dem gewählten Vermerk versehen. Beachten Sie, dass wenn Sie eine Datei aus dem Laufwerk heraus verschieben dieselbe Aktion ausgelöst wird, denn ein solches Verschieben ist identisch mit Kopieren gefolgt von Löschen. Das Verschieben einer Datei innerhalb des von X-Ways Forensics bereitgestellten Laufwerksbuchstabens ist nicht erlaubt.
Wenn Sie eine Datei in einem eingebundenen Laufwerk in Windows umbenennen, so wird auch die Datei im Datei-Überblick von X-Ways Forensics umbenannt. (Der Originalname wird ebenfalls aufbewahrt und im Verzeichnis-Browser zusätzlich angezeigt.)

5.17 File Type Categories.txt

Diese vom Benutzer anpassbare Datei definiert, aus welchen Dateitypen sich Kategorien zusammensetzen. Dem Namen einer Kategorie gehen drei Sternchen und ein Leerzeichen voraus (***), um ihn besonders kenntlich zu machen. Ihm folgt eine Liste von Dateitypen, die zu dieser Kategorie gehören, und zwar ein Dateityp pro Zeile. Solche Zeilen beginnen entweder mit einem „+“ oder „-“, wobei „+“ einfach nur bedeutet, dass der Dateityp im Dateitypfilter mit einem Häkchen versehen ist. Darauf folgt die typische Dateinamenserweiterung, dahinter ein Leerzeichen, und dann eine Beschreibung des Dateityps. Großbuchstaben in der Erweiterung sind nicht zu verwenden. Derselbe Dateityp/dieselbe Dateiendung darf mehreren Kategorien zugeschlagen werden (Einschränkungen s. Beschreibung der Kategoriespalte).

Alternativ zu Dateinamenserweiterungen werden auch ganze Dateinamen unterstützt. Dies ist nützlich für bestimmte Dateien mit einem wohldefinierten Namen, deren Endung allein nicht spezifisch genug ist oder die keine Dateiendung haben. Vollständige Dateinamen müssen durch umschließende Semikolons kenntlich gemacht werden. Beispiele:
-;index.dat; Internet Explorer history/cache
-;history.dat; Mozilla/Firefox browser history
-;passwd; Existing users

Es gibt eine virtuelle Kategorie „Anderer/unbekannter Typ“, die nicht speziell in der Datei definiert wird und einfach alle Dateien umfasst, die nicht zu einer der anderen, definierten Kategorien gehören.

File types are **rank**ed by importance/relevance and you may filter by this rank. For example, filtering out those file types ranked #0 will exclude font files, cursors, icons, themes, skins, clip arts, etc. Files with a low rank are of importance just in very specific investigations, for example source code, in which you would not be interested when looking for office documents or pictures for example, but definitely when hunting a virus programmer. Higher ranked file types are relevant in more cases. Generally the rank is useful in simple cases where you can expect to find what you are looking for in file types that are fairly well known. As another idea, you could make it a habit to only index files with higher ranks.

You also have the option to assign file types to a so-called **group**, a concept that is not identical to a file type category. Useful for example if your standard procedure is to let examiner A check out pictures and videos, examiner B documents, e-mail, and other Internet activity, and examiner C operating system files of various kinds, because of their specializations. You can give these groups meaningful names and filter for them, also using the Type Status dialog window. The groups are displayed in the Type filter.

All the definitions about file type ranks and file type groups are made in the "File Type Categories.txt" file. Suggestions for ranks and an example of a group of files that may deserve special attention are already predefined. Both ranks (from 0 to 9, where missing means 0) and groups (letters from A to Z) can be optionally specified following a tab at the end of a line, in any order, for example as "2P" or "DI3". So up to 10 rank levels are possible, but it is not necessary to fully utilize this range. Up to 26 groups are possible. You do not have to start alphabetically. The case of the letters is ignored. You may also define ranks and groups for an entire category, following a tab in a category line. File types that have no rank and group inherit both from the category to which they belong.

To give a group a more descriptive name than just a single letter, insert group definition lines at the end of the text file that start with a equal sign, e.g.
=P=Photos and videos for image group
=D=Docs, e-mails and Internet
=I=File types to index

You may store additional custom definitions of file types and categories in a separate file named "File Type Categories User.txt", which will be read and maintained in addition to the standard definitions in "File Type Categories.txt" and has the same structure and is not overwritten by updates of the software if contained in the installation directory, so that you can easily continue to use it even when overwriting your installation with a new version.

5.18 Hash-Datenbank

Funktionalität nur mit forensischer Lizenz verfügbar. Eine interne Hash-Datenbank besteht, sofern einmal erstellt, aus 257 binären Dateien mit der Endung .xhd (X-Ways Hash Database).

Der Speicherordner dafür kann im Dialogfenster „Allgemeine Optionen“ festgelegt werden. Eine solche Hash-Datenbank ist auf sehr effiziente Weise organisiert, so dass die Performanz beim Abgleich von Hash-Werten maximiert wird. Sie selbst entscheiden, auf welchem Hashtyp die Datenbank aufbauen soll (MD5, SHA-1, SHA-256, ...), und Sie selbst sind für das Befüllen der Hash-Datenbank mit Hash-Sets und Hash-Werten zuständig. Entweder Sie erzeugen in X-Ways Forensics selbst Hash-Sets, oder Sie importieren Hash-Sets aus anderen Quellen. Die Hash-Datenbank kann von mehreren Benutzern/Instanzen gemeinsam gleichzeitig verwendet werden, wenn derselbe Speicherort (dasselbe Verzeichnis) eingestellt ist. Dieselbe Hash-Datenbank kann aber nicht *aktualisiert* werden, wenn sie gerade von anderen Benutzern/Instanzen verwendet wird.

It is possible to maintain two separate hash databases at the same time, databases based on the same hash type or different hash types. Useful for example if you receive hash sets from different sources with different hash types (e.g. some with MD5 and some with SHA-1 values) and wish to use them simultaneously. The second hash database may be stored on a different drive. Useful if for example the primary hash database for general use is shared with colleagues on a network drive and the user wishes to create or import new hash sets, either for temporary use only or while the primary hash database is locked by other users, into a locally stored second database.

Jeder Hash-Wert in der Datenbank gehört zu einem oder mehreren Hash-Sets. Jedes Hash-Set gehört entweder zur Kategorie „bekanntermaßen irrelevant“ / „harmlos“ / „gutartig“ oder „verdächtig“ / „beachtenswert“ / „relevant“ / „bösartig“ oder kann im Zustand "nicht kategorisiert" verbleiben (noch nicht entschieden oder ungewiss).

In der Hash-Datenbank können Sie Hash-Sets schnell miteinander zu einem einzigen Hash-Set verschmelzen. Beachten Sie, dass doppelte Hash-Werte im resultierenden Hash-Set nicht sofort entfernt werden, sondern erst das nächste Mal, wenn Sie ein Hash-Set hinzufügen. Beachten Sie auch, dass Sie nicht gewarnt werden, wenn Sie Hash-Sets unterschiedlicher Kategorien verschmelzen.

Hash-Werte von Dateien können berechnet und mit der Hash-Datenbank abgeglichen werden, wenn Sie den Datei-Überblick erweitern. Die optionalen Spalten „Hash-Set“ und „Kategorie“ im Verzeichnis-Browser zeigen dann an, welche Dateien zu welchen Hash-Sets und welcher Kategorie gehören, was es Ihnen ermöglicht, nach diesen Aspekten zu sortieren/filtern und irrelevante Dateien einfach zu ignorieren bzw. sich auf relevante Dateien zu konzentrieren. Wenn der Hash-Wert einer Datei in mehreren ausgewählten Hash-Sets enthalten ist, gibt das Programm all diese Hash-Sets an und zeigt die Kategorie eines dieser Hash-Sets. Es prüft auch, ob alle zugehörigen Hash-Sets derselben Kategorie zugeordnet sind, und sollte das nicht der Fall sein, wird eine Warnung ausgegeben.

Eine optionale zweite, separate Hash-Datenbank mit *Block*-Hash-Werten (statt normalen Datei-Hash-Werten), gespeichert in einem separaten Verzeichnis, erlaubt es, nach unvollständigen Überresten bekannter Dateien, die von entscheidender Bedeutung sind, blockweise auf anderen Datenträgern zu fahnden. Sie können die Blockgröße für Block-Hash-Datenbanken selbst festlegen. 512 Bytes ist die Voreinstellung und empfohlen, es sei denn, Sie wissen genau, was Sie tun. Blöcke von 4 KB z. B. können kompatibel sein mit Volumes/Partitionen, die eine Clustergröße von 4 KB aufweisen, und Festplatten mit einer Sektorgröße von 4 KB physisch und logisch, aber würden eine Suche nach bekannten Daten vereiteln, wenn diese im Zieldateisystem

aus Sicht des Asservats nicht an 4-KB-Grenzen ausgerichtet sind. Das könnte z. B. passieren, wenn das Dateisystem einen irregulär großen Vorspann vor dem ersten Cluster hat (wie FAT) oder wenn Sie das blockweise Hashen (nur) auf der Ebene eines partitionierbaren Datenträgers anwenden, in dem die Partitionen nicht an 4-KB-Grenzen ausgerichtet sind. Die gute Nachricht ist aber, dass das blockweise Hashen genau wie eine Datei-Header-Signatur-Suche in X-Ways Forensics gezielt auf Partitionen angewandt wird, wenn Partitionen auf einem partitionierbaren Datenträger (oder einer Sicherung davon) bekannt sind, und nur der Bereich außerhalb von bekannten und erkundbaren Partitionen auf der Ebene des partitionierbaren Datenträgers verarbeitet wird.

Das über das Extras-Menü erreichbare Dialogfenster zum Verwalten der aktiven Hash-Datenbank(en) erlaubt es,

- mit einer neuen, leeren Datenbank die Arbeit zu beginnen (und die ggf. schon bestehende aktuelle Hash-Datenbank zu verwerfen, über den Befehl "Initialisieren, wobei auch ein neuer Hash-Typ ausgewählt werden kann),
- eine Liste der in der Hash-Datenbank enthaltenen Hash-Sets einzusehen,
- Hash-Sets umzubenennen,
- Hash-Sets miteinander zu verschmelzen (beachten Sie, dass doppelte Hash-Werte im resultierenden Hash-Set nicht sofort entfernt werden, sondern erst das nächste Mal, wenn Sie ein Hash-Set hinzufügen, und beachten Sie auch, dass Sie nicht gewarnt werden, wenn Sie Hash-Sets unterschiedlicher Kategorien verschmelzen),
- Hash-Sets zu löschen,
- die Kategorie jedes Hash-Sets zu ändern,
- die Integrität der Hash-Datenbank zu überprüfen,
- ausgewählte Hash-Set-Dateien zu importieren*,
- alle Hash-Sets in einem bestimmten Verzeichnis und dessen Unterverzeichnissen zu importieren (dito), optional in ein einziges internes Hash-Set, dessen Namen Sie angeben können,
- ausgewählte Hash-Sets zu exportieren (z. B. wenn Sie individuelle Hash-Sets mit anderen Ermittlern austauschen möchten, aber nicht die gesamte Hash-Datenbank)
- und zwischen der Verwaltung der normalen Datei-Hash-Datenbank und der Block-Hash-Datenbank hin- und herzuwechseln.

*Textdateien der Formate NSRL RDS 2.x, HashKeeper und ILook werden unterstützt, sowie Hash-Sets im JSON/ODATA-Format-Layout von Project Vic (Versionen 1.0, 1.1, 1.2 oder 2), wie in der Hubstream-Inbox zu finden. NSRL RDSv3 werden nicht direkt unterstützt, aber Instruktionen zur Erzeugung einer universellen Hash-Set-Textdatei aus der NSRL-RDSv3-SQLite-Datenbank sind verfügbar. Ein weiteres Import- und das Export-Format ist eine sehr einfache und universelle Hash-Set-Textdatei, in der die erste Zeile einfach den Hash-Typ angibt (z. B. "MD5") und alle weiteren Zeilen jeweils Hash-Werte in ASCII-Hex sind (bzw. im Fall von SHA-1 alternativ in Base32-Notation), 1 pro Zeile. Das Zeilenende-Zeichen ist 0x0D 0x0A.

When importing hash values from NSRL RDS 2.x, if you categorize the hash set as irrelevant, hash values marked as special or malicious will be ignored (not imported). If you categorize the hash set as notable, only hash values that are marked as malicious will be imported. If you set the hash set to the uncategorized state, only hash values that are marked as special or have an unknown flag will be imported. If you wish to import all hash values, you can import the same

NSRL RDS 2.x hash set file three times, with different categorizations, and all hash values will end up in suitably categorized internal hash sets.

Der Befehl „In Hash-Datenbank aufnehmen“ im Kontextmenü des Verzeichnis-Browsers erlaubt es Ihnen, Ihre eigenen Hash-Sets in den internen Hash-Datenbanken zu erstellen. Beim Importieren/Erzeugen von Hash-Sets werden doppelte Hash-Werte innerhalb desselben Hash-Sets eliminiert. Beim Importieren der NSRL-RDS-Hash-Datenbank prüft X-Ways Forensics auf Datensätze mit den Flags "s" (special) und "m" (malicious), so dass diese Hash-Werte nicht fälschlicherweise in das gleiche interne Hash-Set aufgenommen werden, das als irrelevant klassifiziert werden sollte. Die Hash-Datenbank kann bis zu 65.535 Hash-Sets verwalten.

Duplicate hash values that are already contained in the hash database can optionally be either removed from a newly created or newly imported hash set or from all existing hash sets, to keep the hash database more compact/less redundant if so desired.

There is a way to efficiently delete individual hash values from an existing hash set, by importing a hash set file (simple 1-column format, 1 hash value per line), where the hash values to delete must be listed first and must be prepended with a minus sign ("-"). The file must have the same name as the existing hash set in the database that you wish to update (additional filename extension allowed).

There is an option to unload the hash database if loaded at the moment when all data windows are closed (the moment when the last open data window is closed), to save main memory or to specifically allow other concurrent users or instances to *change* the hash database.

The rather simple CRC32 algorithm is supported in ordinary hash databases. Creating a hash database based on CRC32 is useful (only) if you really only know the CRC32 values of files that you are looking for, no more advanced hash values and not the full original file contents, for example from encrypted zip archives as such archives have the CRC32 values of the unencrypted data in the metadata. If you find CRC32 matches and the file size is the same as known from the metadata in such an encrypted zip archive, then it is very likely that you have found an unencrypted copy of the very same file. If you wish to import CRC32 hash values from a text file (with "CRC32" in the first line, followed by one checksum in hex ASCII per line), please note that their hex ASCII values are expected in big-endian ("human-readable") byte order, as displayed in software like 7-Zip and WinZip and also X-Ways Forensics itself, which unlike MD5, SHA-1 etc. is not the byte order in which they are stored in binary, in X-Ways Forensics internally as well as in zip files themselves and presumably elsewhere.

5.19 Hash-Kommentare

Zusätzlich zu den zwei regulären Hash-Datenbanken, einer Block-Hash-Datenbank, einer FuzZyDoc-Datenbank und (sofern berechtigt) einer PhotoDNA-Hash-Datenbank, können Sie jetzt zusätzlich eine Datenbank anlegen für wiederkehrende Dateien, für die Sie eine Beschreibung hinterlegt haben. Dies kann beispielsweise nützlich sein, wenn Sie in Ihren Fallberichten für das Gericht Beschreibungen der illegalen Bildinhalte beifügen müssen. Wenn dieselben Bilder in mehreren Fällen wiederkehren, kann Ihnen diese neue Datenbank Aufwand

ersparen, da Sie die Bilder nicht erneut sichten und kommentieren müssen. Was Sie als Kommentar eingeben, kann zusammen mit dem Hash-Wert der Datei in der Datenbank gespeichert werden. Um dies zu veranlassen, wählen Sie die betreffenden Dateien aus und rufen im Kontextmenü des Verzeichnis-Browsers "In Hash-Datenbank aufnehmen" auf. Ob für die gewählten Dateien bereits Hash-Werte berechnet waren, ist nicht entscheidend. Diese werden ggf. automatisch berechnet, falls nicht. Sie können dieselben Kommentare in einem anderen Fall automatisch wieder vergeben lassen, wenn Sie in dem anderen Fall beim Datei-Überblick Erweitern den Hash-Wert-Abgleich mit dieser Hash-Datenbank durchführen lassen.

Die Datenbank ist in der Datei "Hash Comments.txt" gespeichert. Sie können die Datenbank durch bloßes Weiterreichen dieser Datei mit anderen teilen. Die Datei ist von den übrigen Hash-Datenbanken unabhängig, was bedeutet, es spielt keine Rolle, wer welche regulären Hash-Datenbanken mit Hash-Sets aus welchen Quellen auch immer verwendet. Sie brauchen genau genommen überhaupt keine reguläre Hash-Datenbank, um eine Datei "Hash Comments.txt" zu erzeugen, oder um die Hash-Werte in Ihrem Fall mit der Datei "Hash Comments.txt" von jemand anderem abzugleichen. So ist die "Hash Comments.txt" universell einsetzbar und auch unter verschiedenen Organisationen austauschbar.

Sie können die Textdateien aus verschiedenen Quellen in der Benutzeroberfläche verschmelzen lassen: Öffnen Sie Extras | Hash-Datenbank und klicken Sie auf den Schalter "Importieren". Sollte X-Ways Forensics Einträge mit demselben Hash-Wert feststellen, wird abhängig von der gewählten Option im Import-Dialog entweder der bisherige Kommentar beibehalten oder der neue übernommen. Bitte behalten Sie das im Hinterkopf, wenn Sie Kommentare von anderen übernehmen. Die Regel betrifft auch Mehrfacheinträge in derselben Textdatei, wenn diese beispielsweise manuell zusammenkopiert worden sind.

Da es sich bei der Datei um eine schlichte Textdatei handelt, können Sie die "Hash Comments.txt" aus verschiedenen Quellen leicht in einem einfachen Text-Editor manuell zusammenfügen, oder die Beschreibungen nach Bedarf bearbeiten, automatisch übersetzen lassen, etc. Stellen Sie nur sicher, dass das vorgegebene Format von einem Hash-Wert + Beschreibung pro Zeile erhalten bleibt. Die erste Zeile (Titelzeile) in der Datei "Hash Comments.txt" muss aus der Bezeichnung des Hash-Typs ASCII (z. B. "MD5" oder "SHA-1") gefolgt von den ASCII-Buchstaben "Cmt" bestehen, wobei Groß-/Kleinschreibung von Bedeutung ist. Alle folgenden Zeilen beginnen mit einem Hash-Wert in Hex-ASCII (wobei sowohl Groß- als auch Kleinbuchstaben erlaubt sind), gefolgt von einem Tabulator-Zeichen und der Beschreibung in UTF-8. Sowohl Windows- als auch Unix-/Linux-Zeilenumbrüche sind erlaubt.

Es gibt ein unbeschriftetes, aber mit Tooltip ausgestattetes Kontrollkästchen, das erlaubt, vorhandene Kommentare für Dateien automatisch zu ersetzen, wenn Treffer für Hash-Werte in den Hash Comments gefunden werden. Das bedeutet natürlich, dass vorhandene Kommentare verloren gehen, wenn es für dieselbe Datei in der "Hash Comments"-Datenbank bereits einen Kommentar gibt.

Eine weitere Option erlaubt das automatische Voranstellen der Initialen "[HC] " vor Kommentare, die automatisch aus der "Hash Comments.txt" vergeben wurden, um sie von Kommentaren unterscheiden zu können, die manuell eingegeben wurden.

5.20 PhotoDNA

Aus Gründen der Lizenzierung kann die PhotoDNA-Funktionalität **nur Strafverfolgungsbehörden** zugänglich gemacht werden, als separater Download. Diese Behörden dürfen PhotoDNA verwenden zur Verhinderung der Verbreitung von Kindesmissbrauchsinhalten und für Ermittlungen, die das Ziel haben, die Verbreitung und den Besitz solcher Inhalte zu stoppen. Weitere Details über PhotoDNA finden Sie in dieser technischen Erläuterung und dieser Pressemitteilung.

X-Ways Forensics kann den sog. PhotoDNA-Hash-Algorithmus auf Fotos anwenden. Dank der Robustheit des Algorithmus' und seiner Spezialisierung auf Fotos kann er Bilder normalerweise auch dann automatisch wiedererkennen, wenn sie wiederholt einer verlustbehafteten Kompression unterworfen wurden (JPEG), wenn sie in einem anderen Dateiformat gespeichert wurden oder vergrößert oder verkleinert wurden, wenn die Bildschärfe herauf- oder herabgesetzt wurde, wenn Bildteile verpixelt wurden, wenn die Farben oder Kontraste angepasst wurden usw. Anders als Hash-Werte von konventionellen, zu allgemeinen Zwecken für Daten generischer Art entwickelten Algorithmen, sind PhotoDNA-Hashes resistent gegen diverse Bildoperationen oder ändern sich nur leicht. Optional können Fotos auch dann wiedererkannt werden, wenn sie gespiegelt wurden. Aus Zeitersparnisgründen und wegen vermuteter Irrelevanz werden Bilder mit einer Höhe oder Breite von weniger als 50 Pixeln nicht mit PhotoDNA untersucht.

Wenn die PhotoDNA-Funktionalität in X-Ways Forensics verfügbar ist, kann eine Hash-Datenbank mit PhotoDNA-Hash-Werten von Fotos (Bilddateien) erzeugt und verwaltet werden, und andere Bilddateien können mit dieser Hash-Datenbank in X-Ways Forensics und X-Ways Investigator abgeglichen werden, um bekannte Inhalte automatisch zu identifizieren.

Strafverfolgungsbehörden können eine eigene Sammlung solcher Hash-Werte anlegen, basierend auf Bildern früherer Fälle, und mit anderen Benutzern teilen. Oder sie können eine existierende umfangreiche Sammlung von Project Vic importieren (JSON/ODATA-Format Version 1.0, ab v18.1 von X-Ways Forensics auch Version 1.1, ab v18.2 von X-Ways Forensics auch Version 1.2). Sie können auch PhotoDNA-Hash-Datenbanken anderer X-Ways-Benutzer importieren (wählen Sie dazu die Datei "RHDB" aus!), nicht mehr benötigte Hash-Kategorien löschen und Kategorien in der Datenbank verschmelzen und umbenennen. Beim Importieren der Datenbank eines anderen Benutzers werden Kategorien mit gleichem Namen verschmolzen. PhotoDNA-Hash-Werte können auch aus Textdateien importiert werden, wenn diese in der ersten Zeile den Ausdruck "PhotoDNA" enthalten, gefolgt von 1 PhotoDNA-Hash-Wert pro Zeile in Hex-ASCII oder Base64.

Hash-Werte von Bildern im Datei-Überblick eines Asservats können der PhotoDNA-Hash-Datenbank auf dieselbe Weise hinzugefügt werden wie konventionelle Hash-Sets zu einer konventionellen Hash-Datenbank, über den Befehl “In Hash-Datenbank aufnehmen” im Verzeichnis-Browser-Kontextmenü. Die Datenbank ist eine der zahlreichen Datenbanken, die über den Befehl Extras | Hash-Datenbank verwaltet werden können. Die PhotoDNA-Hash-Datenbank wird in einem Verzeichnis gespeichert neben dem Verzeichnis für Hash-Datenbank Nr. 1.

Wenn Sie PhotoDNA-Hash-Sammlungen importieren oder die PhotoDNA-Hash-Werte von

ausgewählten Dateien direkt in X-Ways Forensics in die Datenbank aufnehmen, werden die hinzuzufügenden Einträge untereinander und mit den in der Datenbank bereits bestehenden Einträgen abgeglichen, um Redundanzen und sich widersprechende Kategorisierungen aufzudecken und die Datenbank so kompakt, schnell und nützlich wie möglich zu halten. This is recommended, but optional, and if you skip this step and if the data set is very large, you potentially save hours of time, at the cost that matching pictures against the database during volume snapshot refinement will take more time, and that for variations of the same picture you may get different classifications returned. You may define the import strictness separately to define how similar hash values have to be to warrant a re-classification of existing values (to keep the database consistent) and to define how similar hash values have to be to overwrite (replace) an existing value with new value (to keep the database compact and less redundant). The latter strictness must not be less than the former. Ein Hash-Wert kann entweder ein existierender, alter Hash in der Datenbank sein, ein neuer Hash, der gerade erst von der laufenden Import-Operation hinzugefügt wurde, oder ein noch hinzuzufügender Hash.
1) Wenn ein hinzuzufügender Hash-Wert Y absolut identisch ist zu einem alten oder neuen Hash-Wert X, wird Y ausgelassen. Wenn Y und X bloß ähnlich sind, wird Y hinzugefügt. Wenn Y und X nahezu identisch sind, wird X direkt durch Y ersetzt (überschrieben).
2) Wenn Y und X identisch oder ähnlich sind, aber zu verschiedenen Kategorien gehören, und X neu ist, dann bedeutet das, dass die Qualität der Importdatei gering ist. Sie sehen dann eine Warnung. Im Fall eines Imports von ProjectVic, wenn die beiden Kategorien die relativ ähnlichen Kategorien "Child Abuse" und "Child Exploitation" sind, wird nichts Besonderes gemacht. Falls die beiden betroffenen Kategorien nicht diese beiden sind: Wenn entweder X oder Y zur Kategorie "Non-pertinent" gehört und das Bild größtenteils einfarbig ist, wird X der Kategorie "Non-pertinent" zugeordnet. Ansonsten werden die sich widersprechenden Kategorisierungen aufgelöst, indem X der Kategorie "Uncategorized" zugeschlagen wird.
3) Wenn Y und X identisch oder ähnlich sind, aber zu verschiedenen Kategorien gehören, und X alt ist, wird X derselben Kategorie wie Y zugeordnet, unter der Annahme, dass die vorherige Kategorisierung falsch oder veraltet ist und die Importdatei korrekte/neue Informationen enthält. Das ist von Vorteil z. B. bei Einträgen mit einer Kategorisierung, die im Ausland vorgenommen wurde (z. B. Project Vic) und die aufgrund hiesiger anderer Gesetzgebung oder Rechtsprechung angepasst werden muss. Oder auch einfach aufgrund von Kategorisierungsfehlern oder unterschiedlicher Interpretation. Was in Land A als Kipo angesehen wird, wird in Land B evtl. anders eingestuft (Beispiel: computergenerierte Bilder). Die Umkategorisierung erfordert jedoch, dass Sie Kopien derselben Bilder in Ihrer Sammlung haben (nicht notwendigerweise die exakt gleichen Dateien) oder wissen, welcher Hash-Wert zu genau welchem Bild gehört.

Die Project-Vic-Standardkategorien der USA sind in einer benutzereditierbaren Textdatei namens PVicCat.txt vordefiniert. Benutzer bei Strafverfolgungsbehörden in Großbritannien und Kanada können ihre Definitionen herunterladen aus dem PhotoDNA-Download-Bereich unseres Web-Servers und die PVicCat.txt file in ihren Installationen ersetzen. Benutzer in anderen Ländern können ihre Kategorien bei Abweichungen gern mit uns teilen.

Beim Aufnehmen von PhotoDNA-Hash-Werten in die interne PhotoDNA-Hash-Datenbank mit dem entsprechenden Kontextmenü-Befehl haben Sie jetzt die Möglichkeit, Ihre Kommentare zu den ausgewählten Dateien in diese Datenbank als Beschreibungen aufnehmen zu lassen. Diese Beschreibungen können automatisch wieder als Kommentare übernommen werden, wenn beim nächsten Mal dieselben Bilder in einem anderen Fall gefunden werden. Diese können bestehende Kommentare in dem anderen Fall ersetzen oder (falls das entsprechende Feld nur halb angekreuzt

ist) zu bestehenden Kommentaren hinzugefügt werden. Dies ist insbesondere für Benutzer bei der Polizei in Deutschland von Vorteil, die aufgrund eines BGH-Urteils (2 StR 279/07) für jedes kinderpornographische Bild für gerichtliche Zwecke eine Textbeschreibung bereitstellen müssen, um ihnen zumindest die wiederholte Eingabe der Beschreibung bereits bekannter Bilder zu ersparen. Ebenfalls nützlich, um Informationen wie z. B. bekannte Identitäten der Personen in einem Bild, frühere Fallnummern, etc. für zukünftige Verwendung zu hinterlegen, falls dieselben Bilder nochmal woanders gefunden werden.

Die Beschreibungen in der Hash-Datenbank können mit Ihren Kommentaren aktualisiert werden, indem man einfach die PhotoDNA-Hash-Werte derselben Dateien erneut durch den entsprechenden Befehl in die interne Datenbank aufnehmen lässt. Wenn Sie die interne Hash-Datenbank eines Kollegen importieren (durch Auswahl deren RHDB-Datei), stellen Sie sicher, dass Sie nicht nur die entsprechende RHCN-Datei (mit den Kategorie-Namen) im selben Verzeichnis haben, sondern auch die neuen Unterverzeichnisse, die die Beschreibungen enthalten, falls vorhanden, falls Sie auch diese Beschreibungen mit importieren möchten.

Um all diese internen Beschreibungen zu löschen, können Sie schlicht die "D*" genannten Unterverzeichnisse des PhotoDNA-Hash-Datenbank-Verzeichnisses löschen. Oder falls Sie Ihre Datenbank anderen Benutzern ohne die Beschreibungen weitergeben möchten, fügen Sie die D* Unterverzeichnisse einfach nicht bei. Sie können auch einzelne Beschreibungen in den Text-Dateien in den D* Unterverzeichnissen jederzeit manuell löschen oder aktualisieren. Beschreibungen, die Sie bereits in Ihrer Datenbank haben, werden durch das erneute Importieren der gleichen Hash-Werte aus anderen Quellen nicht verloren gehen; sie werden aber überschrieben, falls es sich bei der anderen Quelle um eine PhotoDNA-Hash-Datenbank von X-Ways Forensics handelt, die Beschreibungen für dieselben Bilder enthält.

Bei der Erzeugung eines PhotoDNA-Hash-Sets aus ausgewählten Bildern können Sie alternativ das Hash-Set nicht in die interne Datenbank aufnehmen, sondern stattdessen eine separate Text-Datei mit PhotoDNA-Hash-Werten erzeugen lassen. Kreuzen Sie zu dem Zweck "Speichern unter..." an. Solche Dateien können an andere Nutzer weitergegeben werden, falls diese die angegebenen Hash-Werte zu ihren Datenbanken hinzufügen möchten, oder selbige entfernen wollen.

Es ist möglich, eine PhotoDNA-Hash-Datenbank um ungewollte Hash-Werte zu bereinigen. Dafür gibt es einen Schalter im Verwaltungs-Dialogfenster für die PhotoDNA-Datenbank. Die zu entfernenden Hash-Werte werden als einfache Text-Datei übergeben, mit einem Hash-Wert in Hex-ASCII-Notation pro Zeile und "PhotoDNA" in der ersten Zeile. Die angegebenen Hash-Werte betreffen sowohl exakte Übereinstimmungen in der Datenbank als auch kleine Abweichungen (dieselbe Abweichung ist erlaubt wie für den Abgleich eingestellt). Es kann notwendig werden, die PhotoDNA-Hash-Datenbank zu bereinigen, wenn Sie Hash-Sets aus einer fremden Quelle importiert haben, deren Inhalte teilweise Ihren Anforderungen nicht entsprechen, was offenkundig wird, wenn Sie falsche Treffer erhalten, falls Sie dennoch nicht das ganze Hash-Set entfernen wollen, oder falls Sie selbst versehentlich das falsche Bild in Ihre Hash-Datenbank aufgenommen haben.

There is a button that allows to export selected hash collections into text files to share them with other users or to check which hash values are contained/which ones were deduplicated etc. Another function (the button with the magnifying glass) will help you to check the database for the

presence of a specific hash value, specified in Hex ASCII or Base64 notation. If there is a hit, you will be shown the name of the hash collection that contains the hash value. If the matching entry in the database has a textual description, that description will be shown as well. Up to 19 matches are returned, and for each you will see how precise the match is (the higher, the more precise; same basic scale as the user-specified strictness for matching, i.e. level 1 means very rough match). You have the option to narrow down the result list to more precise matches by enforcing a higher minimum strictness level, which is useful if there are more matches than can be listed.

There is a function to mark selected PhotoDNA categories as "preferred", with a black star. That way they will get priority if for a picture in the volume snapshot matches are found with hash values in different categories. Such preferred categories will be reported as a match even if alternative matches with non-preferred categories are much closer matches. That is useful for example if you have categories in your database that you trust to be accurate and suitable and others that you trust less, for example because they are known to contain errors (e.g. the same picture classified as CP and non-pertinent at the same time) and/or because they are from a foreign source and based on different laws and jurisdiction.

Der Abgleich ist Teil der Operation "Bildanalyse und -verarbeitung" in Specialist | Datei-Überblick erweitern. Wenn es beim Abgleich zum selben Bild mehrere Treffer in verschiedenen Kategorien der Datenbank gab, können Sie dies im Verzeichnis-Browser erkennen: Der Name der Kategorie mit der exaktesten Übereinstimmung wird angezeigt gefolgt von einem Komma und drei Punkten. In den seltenen Fällen, in denen dies passiert, kann es wichtig sein, solche Bilder noch einmal gezielt anzusehen und die endgültige Entscheidung über deren Relevanz für den Fall zu treffen. Sie können auch nach Bildern filtern, die in mehr als einer Kategorie gefunden wurden. Solchen Bildern sollte evtl. genauso viel Aufmerksamkeit zuteilwerden wie doppelten Hash-Werten in konventionellen Datenbanken, die gleichzeitig zur Kategorie "irrelevant" und "verdächtig" gehören und die normalerweise auf eine inkonsistente Befüllung der Datenbank hindeuten, etwa versehentliche Fehlkategorisierung oder korrekte Kategorisierungen durch Benutzer in unterschiedlichen Rechtsräumen. Wenn die zurückgemeldete am besten passende Kategorie zu einem Bild Ihrer Ansicht nach falsch ist, können Sie dies heilen, indem Sie den PhotoDNA-Hash-Wert des Bildes der Datenbank erneut hinzufügen, unter Angabe der korrekten Kategorie.

5.21 Optische Zeichenerkennung in Bildern (OCR)

The OCR capabilities of the software package Tesseract can be utilized from within X-Ways Forensics and X-Ways Investigator. The package can be downloaded from our web server. Updated download instructions are available from the same place as always. If Tesseract is found in the subdirectory \Tesseract of the installation directory when X-Ways Forensics is first run, Tesseract will be activated automatically. Otherwise please go to Options | Viewer Programs to indicate the path.

OCR can be applied as part of logical searches or indexing to suitable files such as document scans or digitally stored faxes in TIFF format or PDF documents that contain only graphic content. The file mask for that is matched against the filename as well as Type column (which is

quite reliable and standardized after file type verification). By default, it includes even *.jpg, however, whether applying OCR to every JPEG file in a case is a little excessive or necessary is up to you to decide, and you have full control over the scope of the search using various means anyway. Please be aware that high-resolution photos cost a lot of time to check of text. Digital photos in JPEG and HEIC format will be rotated according to the instructions in the Exif metadata to restore the correct orientation and thus hopefully allow OCR of text that was originally photographed roughly horizontally. If the ordinary text decoding is already successful for a given file of a type that is contained in both file masks (*.pdf), OCR will not be applied additionally. The option "Store decoded text for context preview and future searches" will also keep text derived from OCR stored in the volume snapshot.

All hits returned by the logical search in OCR-derived text are identified as such in the Descr. column and highlighted in a different color. The Descr. filter allows you to list only such OCR search hits or not OCR hits. Older versions of X-Ways Forensics can see OCR search hits when opening the same case, but won't know that they are OCR search hits.

You can select up to two languages for text recognition at the same time, after clicking the ... button for this in Options | Viewer Programs. However, there is a trade-off if you select Chinese/Japanese and a Western language at the same time. This will deteriorate the recognition of the Asian characters. You may want to select *only* Chinese/Japanese for much better recognition in that language. English (actually Latin) letters can still be recognized in that case, even if English is not expressly selected, at reduced quality. Select both Chinese/Japanese and a Western language at the same time only if correct recognition is more important to you in the Western language.

Preview mode now has a separate submode in addition to Raw submode, called Text mode, in which pure text from non-picture files is extracted, just like for the logical search with the decode option. That submode can also be useful to better understand how text is extracted from various document types, in particular from spreadsheets, for which different extraction options exist that may differ in output, especially in formatting.

If the ordinary text extraction/decoding in Text submode does not return any result or if the previewed file is a picture file, and if Tesseract is available and active, OCR will be applied. This allows you to better understand how well OCR will work in searches for the kind of files that you are dealing with. You can also experiment with different languages selected and compare the quality of the results. The submode button is named "Text" by default, but will change its label to "OCR" to make you aware that OCR is or was employed to retrieve the text. OCR can be time-consuming for multi-page TIFF and PDF files, but can be interrupted by the user if necessary. If a logical search or indexing has applied OCR to a file before and the result was stored in the volume snapshot, then the OCR-based preview will be available instantly and OCR will not be re-applied from scratch.

Both submodes Raw and Text in Preview mode remain active until you leave Preview mode or select a file of a different type. If you prefer to make either of these submodes more persistent, so that it remains active even when previewing files of different types, you can hold the Shift key while clicking the respective submode button.

The Tesseract package that is downloadable from our web server already has support for the

following languages integrated, in alphabetic order:
ara: Arabic
chi_sim: simplified Chinese (horizontal writing only)
chi_tra: traditional Chinese (horizontal writing only)
deu: German
eng: English
fra: French
heb: Hebrew
ita: Italian
jpn: Japanese (horizontal writing only)
kor: Korean (horizontal writing only)
nld: Dutch
pol: Polish
rus: Russian
spa: Spanish
swe: Swedish
tur: Turkish
Other languages can be added if you can find .traineddata files for them at https://github.com/tesseract-ocr/tessdata_fast. Such files simply need to be put into the \tessdata subdirectory of Tesseract. Or you can visit https://github.com/tesseract-ocr/tessdata_best to download higher quality OCR engines for any of the supported languages. (Please note that OCR takes considerably more time with them.)

Supported file types are generally the following: PDF, PostScript (PS), TIFF, JPEG, HEIC, PNG, GIF, BMP, nicht animierte WEBP, AutoCAD DXF, Photoshop PSP, and maybe more.

5.22 Excire Forensics: Bildanalyse mit KI

Teil der Erweiterung des Datei-Überblicks. Verfügbar nur in X-Ways Forensics, und nur in einem 64-bittigen Windows 10, Windows 11, Windows Server 2016, Windows Server 2019 und Windows Server 2022. Excire Forensics weist folgende drei Fähigkeiten auf (lokal, nicht in der Cloud!):

• Fotos werden automatisch analysiert und ihr Bildinhalt wird erkannt: Objekte wie etwa bestimmte Arten von Gebäuden, Fahrzeugen, Tieren und Pflanzen, Strände, Berge, Menschen unterschiedlichen Alters, Nacktheit und Pornographie, Handfeuerwaffen, Drogen, Text, ... (vollständige Liste). Es werden auch dominante Farben erkannt und besondere Bildeigenschaften. Die Ergebnisse werden in Form von Vermerken oder Kommentaren ausgegeben, so dass Sie sich konzentrieren können auf Fotos mit bestimmten relevanten Inhalten (kombiniert mit UND oder ODER) oder aber Fotos mit für Sie irrelevanten Inhalten oder Eigenschaften herausfiltern können. Bei Ausgabe in Form von Vermerken erhalten auch Videos diese Labels, wenn die aus ihnen extrahierten Einzelbilder verarbeitet werden.

• Das Auffinden von aus Sicht der künstlichen Intelligenz ähnlichen Bildern, zu einer von Ihnen bereitgestellten Sammlung von typischen relevanten Bildern aus früheren Fällen oder sonstigen Vorlagenbildern (in den Formaten JPEG, PNG, Bitmap oder TIFF, 224x224 Pixels Minimum).

• Gesichter bestimmter Personen können in Fotos in neuen Fällen wiedergefunden werden. Sie werden von X-Ways Forensics aufgefordert, Gesichter in JPEG-, PNG-, Bitmap- oder TIFF-Bildern in einem von Ihnen speziell dafür bereitgestellten Verzeichnis zu markieren. Sie können dabei die Esc-Taste drücken, um die Verarbeitung abzubrechen.

X-Ways Forensics verarbeitet Bilder mit Excire, die in einem der folgenden Formate vorliegen: JPEG, PNG, Bitmap, TIFF, nicht animierte WEBP, GIF, HEIC. Sie bestimmten dabei, Bilder welcher Mindestauflösung verarbeitet werden sollen. Die Zahl der Fehlerkennung steigt in Bildern mit niedrigerer Auflösung, wie etwa Miniaturansichten.

Bilder können automatisch als irrelevant oder beachtenswert kategorisiert werden. In der umfangreichen Hierarchie identifizierbarer Objekte können Sie individuelle Schlagwörter oder ganze Teilbäume auswählen, die ein Bild für Sie mit hoher Gewissheit irrelevant erscheinen lassen, z. B. diverse Tierarten, Pflanzen, Sportarten, Musikinstrumente usw. Sie können auch festlegen, was ein Bild aus Ihrer Sicht beachtenswert macht, z. B. unbekleidete Menschen ("Akt"), Kinder, Fahrzeuge, Text usw. Im Zweifelsfall erhält die Kategorisierung als "beachtenswert" immer Vorrang vor "irrelevant", z. B. wenn Sie in einem bestimmten Fall mal Hunde für beachtenswert halten, aber Tiere ansonsten immer noch als irrelevant markiert sind. Logische UND-Kombinationen werden unterstützt bei der Einstufung als beachtenswert. Einige solche UND-Kombinationen sind vordefiniert, die bei der Ermittlung in Sachen Kinder-pornographie unterstützen sollen. Die berechnete Relevanz von Bilddateien kann automatisch adjustiert werden anhand des erkannten Bildinhalts, je nachdem, was für Sie als verdächtig oder irrelevant gilt, entweder stark, mäßig, leicht oder gar nicht.

Anwendungsbeispiele für Excire können Sie u. U. auch finden, indem Sie probieren, was in bekanntermaßen relevanten Bildern früherer Fälle erkannt wird. Z. B. könnten abfotografierte Dokumente mit „Text“ und/oder „Papier Textur“ erkannt werden, auch wenn sie zerknüllt sind oder handschriftlicher Natur sind und OCR keinen Text mehr erkennt.

Beschreibungen von Bildinhalten sind derzeit verfügbar auf Deutsch, Englisch, Französisch, Spanisch und Italienisch.

5.23 Zeitzonen-Konzept

Folgendes gilt für WinHex mit Specialist-Lizenz oder höher sowie X-Ways Investigator und X-Ways Forensics.

X-Ways Forensics bedient sich nicht der Windows-Logik, sondern seiner eigenen Logik, um UTC-Zeitstempel für die Anzeige im Verzeichnis-Browser, in Berichtstabellen und in exportierten Listen in eine frei wählbare Ortszeit umzurechnen. Es zeigt Zeitstempel unabhängig von der in der Windows-Systemsteuerung des Untersuchungssystems eingestellten Zeitzone an. Die Anzeige von Zeiten in X-Ways Forensics und Windows kann sich unterscheiden, weil Windows Zeitangaben in der Sommerzeit nicht basierend auf Sommerzeit anzeigt, wenn zum Zeitpunkt der Anzeige Winterzeit gilt.

Beim Arbeiten mit einem Fall gilt die für diesen Fall eingestellte Zeitzone global für das gesamte Programm (wählbar in den Falleigenschaften), ansonsten die Zeitzone, die in den „Allgemeinen Optionen“ eingestellt ist. Beim Arbeiten mit einem Fall ist es optional möglich, unterschiedliche Zeitzonen für verschiedene Asservate einzustellen, so dass Sie immer Ortszeiten sehen selbst für Datenträger, die in unterschiedlichen Zeitzonen verwendet wurden, wenn Sie dies vorziehen. Beachten Sie, dass die Zeitstempel nur für die *Anzeige* umgerechnet werden. Das heißt, in einer rekursiven Ansicht im Asservat-Überblick, der mehrere Datenträger enthält, hängt eine etwaige *Sortierung* nach Zeiten immer noch von absoluten UTC-Zeiten ab. Optional können Sie direkt im Verzeichnis-Browser bei jeder Zeitangabe sehen, wie viele Stunden tatsächlich für die Umrechnung in Ortszeit zu UTC addiert oder von UTC subtrahiert wurden (s. Verzeichnis-Browser-Optionen)

Zeitstempel auf FAT-Partitionen werden nie umgerechnet, da diese nicht in UTC gespeichert sind, sondern auf einer oder mehreren unbekannten lokalen Zeitzonen basieren. Zeitstempel aus Dateisystemen, die die Zeitzone explizit speichern, werden intern in UTC umgerechnet und dann zum Zweck der Anzeige von UTC in eine Ortszeit.

Die Definition der Zeitzonen kann bei Bedarf angepasst werden. Bitte beachten Sie, dass das Ändern der Definitionen egal in welchem Dialogfenster die Definition der Zeitzonen im gesamten Programm betrifft.

WinHex und X-Ways Forensics verwenden noch immer die Standard-Windows-Umrechnungslogik, die von der Zeitzone abhängt, die in der Systemsteuerung des Benutzers eingestellt ist, ...

- in Datei | Eigenschaften, wo Zeitstempel von Dateien auf dem System des Benutzers selbst abgefragt und geändert werden können,
- für die Protokollierung der Fallbearbeiten,
- allgemein, wenn nicht mit Specialist- oder forensischer Lizenz betrieben, und
- wenn ohne die Datei „timezone.dat“ betrieben.

Dass eine der beiden letzten Bedingungen zutrifft, können Sie daran sehen, dass der Schalter „Anzeige-Zeitzone“ im Dialogfenster „Allgemeinen Optionen“ nicht sichtbar ist oder grau angezeigt wird.

5.24 Datei-Container

Nur mit forensischer Lizenz verfügbar. Das Specialist-Menü erlaubt es, einen neuen Datei-Container anzulegen, einen existierenden zum weiteren Befüllen zu öffnen und den aktiven Datei-Container wieder zu schließen. Befüllt werden kann ein Container mit ausgewählten Dateien über das Kontextmenü des Verzeichnis-Browsers.

Wenn Sie ausgesuchte Dateien (auch von verschiedenen Asservaten) mit besonderer Relevanz für einen Fall gesammelt und bequem an andere Beteiligte des Verfahrens weitergeben möchten (z. B. spezialisierte Ermittler), die irrelevante Dateien nicht zu sehen brauchen oder sogar nicht sehen dürfen, empfehlen sich Datei-Container. Darin bleiben die allermeisten Metadaten aus dem Dateisystem (Name, Pfad, Größe, Attribute/Filemode, Zeitstempel, Löschzustand, Klassifikation

als alternativer Datenstrom oder virtuelle Datei oder E-Mail oder Datei-Anhang, ...) und insbes. natürlich der Inhalt der kopierten Dateien erhalten. Auch wenn ein konventionelles (physisches, sektorweise erstelltes) Image übertrieben und zu zeitaufwendig wäre, weil Sie nur einige ausgewählte Dateien zu sichern brauchen und keine kompletten Datenträger, bieten sich Datei-Container an. Datei-Container enthalten ein spezielles Dateisystem (XWFS), das die meisten Metadaten aus konventionellen Dateisystemen der Windows-, Linux- und Apple-Welt aufnehmen kann.

Datei-Container lassen sich wie andere Image-Dateien auch interpretieren, einem Fall hinzufügen und bequem untersuchen. Container können insbes. auch in X-Ways Investigator [CTR] eingelesen werden, der stark vereinfachten Version von X-Ways Forensics für Ermittler, die nicht auf EDV spezialisiert sind, sondern in anderen Gebieten wie Bestechung, Rechnungswesen, Kinderpornographie, Baurecht, usw. Der Empfänger eines Containers kann den Container zu seinem eigenen Fall hinzufügen, die darin enthaltenen Dateien genau wie in einer Festplattenpartition oder einem konventionellen Image einsehen, Stichwortsuchen laufen lassen, Kommentare zu Dateien eingeben, Dateien mit Vermerken versehen, Berichte erstellen usw. Vermerke können sogar exportiert und in den Originalfall wieder importiert werden, über Befehle im Kontextmenü des Fallbaums. Dies erlaubt es, den großen Analyseaufwand in größeren Verfahren auf mehrere Ermittler, die parallel arbeiten, zu verteilen, und deren Ergebnisse auch wieder zusammenzuführen.

Das aktuelle Container-Format kann von diversen Computerforensik-Tools verstanden werden, die nicht von X-Ways stammen. Ältere Versionen von WinHex (mit Specialist-Lizenz oder höher), X-Ways Forensics und X-Ways Investigator können es ebenfalls verstehen. All diese Tools können die Datei-Inhalte und die grundlegendsten Metadaten lesen (z. B. Dateiname, Pfad, diverse Attribute, die meisten Zeitstempel, existierend oder gelöscht). Um die größtmögliche Menge von Metadaten aus einem Container zu importieren, verwenden Sie aber bitte WinHex/X-Ways Forensics/X-Ways Investigator 16.3 oder neuer. Weitere Informationen. Ein Roh-Datei-Container (d. h. nicht im .e01-Format) kann in WinHex mit jedem Lizenztyp interpretiert und als Laufwerksbuchstabe eingebunden werden, so dass andere Tools, die das Container-Format nicht nativ verstehen, auf die enthaltenen Dateien zugreifen können. (Wenn solch ein Container nicht mehr als 1.000 Objekte enthält, kann auch die Evaluationsversion von WinHex das erledigen.)

Container können theoretisch bis zu 1 Milliarde Objekte aufnehmen. Es wird automatisch verhindert, dass Sie dieselbe Datei versehentlich zweimal in den gleichen Container kopieren (eine bestimmte Datei vorgefunden an einem bestimmten Ort). Wenn Sie den Inhalt des Containers während des Befüllens im Auge behalten möchten, so ist dies kein Problem. Sie können den Container demselben Fall dazu vorübergehend als Asservat hinzufügen, während er zum Befüllen geöffnet ist. Sie brauchen ihn nicht aus dem Fall zu entfernen oder das Asservat zu schließen, um den Container weiter zu befüllen. Nach jedem Befüllungsschritt können Sie den Datei-Überblick des Containers neu einlesen, um den vollständigen aktuellen Inhalt zu sehen. Und wenn Sie am Ende mit dem Befüllen des Containers fertig sind, können sie ihn aus dem Fall entfernen, da er darin wahrscheinlich nicht mehr benötigt wird.

Um die Quelle von Dateien im Container, die aus verschiedenen Asservaten stammen, deutlich zu machen, können die jeweiligen Asservatnamen als oberste Verzeichnisebene im Container aufgenommen werden. If the option to insert an artificial top directory level is only half selected, that means that only the names of partition evidence objects are included that have a physical

evidence object as a parent. Useful if the parent evidence object name is very long and redundant to include because you will fill your entire container only with files from that physical evidence object and will reference that object's name in the container name already.

Beim Erstellen eines Containers wählen Sie zwischen der normalen direkten Füllmethode und einem indirekten Weg. Indirekt heißt, Datei-Inhalte werden dem Container über den Umweg der eigenen Festplatte hinzugefügt werden. Sie werden nicht direkt in den Container kopiert, sondern zunächst in das Verzeichnis für temporäre Dateien (s. Allgemeine Optionen), und dann erst von dort in den Container. Das hat den Vorteil, dass ein aktives Virenschutzprogramm die Gelegenheit hat, die Dateien abzufangen, d. h. zu prüfen, unschädlich zu machen, umzubenennen, zu verschieben, zu löschen, zu sperren usw. Es kann so verhindern, dass die Dateien in den Container gelangen. Der Container bleibt dann mit hoher Gewissheit virenfrei und kann in verantwortlicher Weise in einer Umgebung mit höheren Sicherheitsanforderungen/größerem Schutzbedürfnis weitergegeben werden. Wichtig: Bitte überzeugen Sie sich testweise mittels bekannter Malware davon, dass Ihr Virenscanner bei auf diese Weise erzeugten Dateien tatsächlich anschlägt.

Eine optionale interne Bezeichnung (bis zu 31 Zeichen) kann angegeben werden. Diese wird als Volume-Label des XWFS-Dateisystems verwendet. Eine optionale Beschreibung kann auch in den Container integriert werden (bis zu 60.000 Zeichen). Diese wird beim Hinzufügen des Containers in einen Fall importiert und ist dann in den Kommentaren zu dem Asservat sichtbar. Die im Container gespeicherte Beschreibung kann auch später noch hinzugefügt oder bearbeitet werden.

Einem im Hintergrund aktiven (d. h. geöffneten oder gerade neu erstellten) Datei-Container können Sie im Verzeichnis-Browser ausgewählte Dateien per Kontextmenü hinzufügen. Entweder man kopiert dann den logischen Datei-Inhalt, den logischen Inhalt und den Schlupf separat, nur den Schlupf, nur einen im Datei-Modus ausgewählten Block oder sogar nur die Metadaten des Dateisystems. Sie können des Weiteren angeben, ob Unterobjekte gewählter Dateien mit kopiert werden sollen, auch wenn sie nicht selbst ausgewählt sind, und zwar entweder Unterobjekte jeglicher Art (wenn ganz gewählt) oder nur Datei-Anhänge von E-Mails (wenn die Option halb gewählt ist).

Optional können Container die Daten/Inhalte von Verzeichnissen selbst transportieren, d. h. abhängig vom Dateisystem Verzeichniseinträge, INDX-Puffer usw. Dies ist nützlich, wenn der Empfänger des Containers technisch bewandert ist und sich für Zeitstempel oder sonstige Metadaten in diesen Datenstrukturen interessieren könnte. Falls Sie sich entscheiden, Verzeichnisdaten in einen Container aufzunehmen, wenn Sie ihn erzeugen, hat das direkte Auswirkungen nur auf Verzeichnisse, die selbst ausgewählt sind. Es hat einen Effekt auf das jeweilige direkte Elternverzeichnis von gewählten Objekten nur dann, wenn Sie eine weitere Option einschalten („Daten/Inhalte direkt übergeordneter Objekte aufnehmen“). Diese weitere Entscheidung ist erforderlich, weil die Verzeichnisdaten sonst unbeabsichtigt Namen und sonstige Metadaten von Dateien enthüllen könnten, die z. B. aus Datenschutzgründen bewusst nicht in den Container aufgenommen wurden.

Sie können Objekte in den Container mit oder ohne ursprünglichen Pfad aufnehmen. Wenn Sie diese Option nur halb wählen, wird nur ein Teilpfad aufgenommen, nämlich alles unterhalb des Verzeichnisses, von dem aus Sie kopieren / das Sie erkundet haben. Dieses Verhalten liegt

Computer-Benutzern sehr nahe, weil auch der Windows File Explorer ausgewählte Dateien und Verzeichnisse so kopiert. Wenn Sie Dateien, die Unterobjekte anderer Dateien sind, incl. Pfad kopieren, wird die übergeordnete Datei zumindest als leere Hülle (ohne Daten) in den Container aufgenommen, damit das Unterobjekt mit dem korrekten ursprünglichen Pfad im Container erscheint und klar ist, woher sie stammt. Beispiele sind eine E-Mail, zu der der ausgewählte Datei-Anhang gehört, ein Zip-Archiv, das die ausgewählte Datei enthält, oder ein Dokument, in dem das ausgewähltes Bild eingebettet ist. Bei eingeschalteter Option „Daten/Inhalte direkt übergeordneter Objekte aufnehmen“ wird auch der Inhalt einer ggf. übergeordneten Datei automatisch mit kopiert, selbst wenn die übergeordnete Datei gar nicht selbst zum Kopieren ausgewählt war. Künstliche Verzeichnisse können optional in Containern angelegt werden, um Unterobjekte von Dateien aufzunehmen, zur besseren Kompatibilität mit Tools, die Dateien nicht als Unterobjekte von anderen Dateien akzeptieren. WinHex/XWF/XWI brauchen keine solchen künstlichen Verzeichnisse.

Einem Container kann jede Datei hinzugefügt werden, der Teil eines Datei-Überblicks sind, also z. B. auch einzelne extrahierte E-Mails. Einmal hinzugefügte Dateien können nicht wieder physisch entfernt, aber permanent ausgeblendet werden. Es gibt die Möglichkeit, automatisch Vermerke für Dateien zu erzeugen, die zu einem Datei-Container hinzugefügt wurden.

Optional können Hash-Werte von den kopierten Dateien im Container gespeichert werden. Dies erlaubt es, die Integrität der Datei später zu überprüfen, wenn der Container einem Fall hinzugefügt wurde, durch das Erweitern des Datei-Überblicks. Die Hash-Werte werden direkt für die Daten berechnet, wie sie vom Original-Quelldatenträger gelesen werden (wenn Sie nicht nur Metadaten in den Container übertragen), oder aus dem Datei-Überblick übernommen, sofern verfügbar.

Optional kann die Person, die einen Container erstellt, Vermerke (entweder alle oder nicht solche von X-Ways Forensics automatisch erstellten) und/oder Kommentare zu den in den Container zu kopierenden Dateien mit weitergeben. Dies ist nützlich, wenn nicht nur eine Sammlung von Dateien an andere Ermittler weitergegeben werden soll, sondern auch weitere fallspezifische Informationen und bereits gewonnene Erkenntnisse. Z. B. könnte der Kommentar den Grund dafür angeben, aus dem eine Datei zur Weitergabe im Container überhaupt ausgewählt wurde. Passing on internal file metadata in evidence file containers is a 3-state check box. If half checked, only extracted senders and recipients of e-mails will be passed on and not general metadata as known from the Metadata column. Please note that transferring extracted metadata to the container is not recommended if the recipient would like to work with an event list because events are not transferred to the container and events derived from within file contents will not be added to the event list if a file is marked as already metadata-processed.

Vorgang bei Lesefehler abbrechen: This option allows to abort copying files into an evidence file container upon a read error and to not include affected files partially. Useful when acquiring files from a network location and the connection might be interrupted, if you assume that if that happens you will get the connection back and will be more successful when you try again, to avoid having incomplete files in the container, which cannot be replaced with a complete copy retroactively. Available only when not filling containers indirectly.

Beim Schließen eines im Hintergrund geöffneten Containers wird dem Benutzer angeboten, den Container zu komprimieren, zu verschlüsseln und/oder in kleinere Segmente aufzuteilen. Das

Aufteilen ist nützlich, wenn der Container vollständig befüllt wurde, relativ groß geraten ist und z. B. auf CDs oder DVDs verschickt werden soll. Sie finden vielleicht auch einen überprüfbaren Hash-Wert für den gesamten Container nützlich, der bei dieser Gelegenheit berechnet und in den Zielcontainer eingebettet werden kann. Des Weiteren gibt es eine Option zum Einfrieren des Dateisystems in dem Zielcontainer, den Sie im .e01-Evidence-File-Format erzeugen, so dass er nicht weiter befüllt werden kann, auch nicht nach Rückumwandlung ins Roh-Image-Format.

5.25 Zugehörige Objekte

Nur mit forensischer Lizenz verfügbar.

Dateien/Verzeichnisse, zu denen es eine "zugehörige" Datei bzw. ein "zugehöriges" Verzeichnis im Datei-Überblick gibt, sind im Verzeichnis-Browser links neben ihrem Icon mit einem kleinen, blauen, nach unten zeigenden Pfeil markiert. Ein zusätzlicher Tooltip erscheint für Dateien mit einer "zugehörigen" Datei, wenn man den Mauszeiger über deren Icon hält. Dieser zeigt Ihnen komfortablerweise den Pfad und Namen der zugehörigen Datei an, z. B. das Ziel eines symbolischen Links. Es gibt vier verschiedene Arten von zugehörigen Objekten:

1) When taking a volume snapshot of Unix-based file systems, symbolic links are connected to their targets in the volume snapshot as so-called related files, so that you can conveniently navigate to the target by pressing Umsch+Backspace. Also one of potentially several symlinks pointing to a certain target will become the related file of the target, so that you can conveniently navigate to the symlink or quickly see that one or more symlinks exist that point to a certain target, since any file that has a "related" file in the volume snapshot is marked with a tiny blue arrow next to its icon. Also the same arrow will tell you whether the target of a symlink can actually be found in the file system. If a symlink links to other symlinks, those are not recursively linked. If resolving symlink takes to long because there are many symlinks in a volume, you may safely abort that step at any time.

2) When taking a snapshot of volumes with Windows installations, certain reparse points (a.k.a. junction points) are connected to their targets in the volume snapshot just like as symlinks in Unix-based file systems, so that you can conveniently navigate to the target by pressing Umsch+Backspace. Also there will be a back-reference to one reparse point, so that you can conveniently navigate to that reparse point or quickly see that one or more reparse points exist that link to a certain directory, since any directory that has a "related" directory in the volume snapshot is marked with a tiny blue arrow next to its icon. Forensic license only. Reparse points that do not get connected with their target directories will still show a comment that advises you of the target path as in earlier versions of X-Ways Forensics.

3) Harte Verweise in HFS+ verweisen auf die zugehörige sogenannte indirekte Knoten-Datei (iNode*-Datei). iNode*-Dateien verweisen zurück auf eine der verhartlinkten Dateien, so dass es sehr bequem ist, zumindest einen der harten Verweise mit seiner tatsächlichen Verwendung und seinem tatsächlichen Ort zu finden. Um weitere harte Verweise zur selben iNode*-Datei zu finden, können Sie z. B. nach der Spalte "1. Sektor" sortieren.

4) In NTFS in Schattenkopien gefundene Dateien, die auf ihre Trägerdatei zeigen, und

Schattenkopie-Trägerdateien, die auf ihre zugehörige Snapshot-Eigenschaften-Datei (in der Typspalte snapprop genannt) zeigen.

5.26 Generator-Signaturen

Die Generator-Signatur ist ein Konzept, mit dem verbreitete Dateitypen wie JPEG, Videos und PDF in Untertypen aufgeteilt werden können, die bestimmten Geräten (Scanner, Kamera) oder Anwendungen (z. B. Photoshop) zugeordnet werden können. Die JPEG-Generator-Signatur basiert auf der JPEG-Quantisierungstabelle und einigen anderen invarianten Eigenschaften, die bei jeder JPEG-Datei immer vorhanden sind. Die Generator-Signatur wird bei den Metadaten einmal als 32-Bit Wert in hexadezimaler Form ausgegeben gefolgt von einer Beschreibung, die aus der Datei „Generator Signatures.txt“ stammt.

607AE169 (IJG Library 94 / Paint)

In diesem Beispiel handelt es sich um die Signatur einer Datei, die mit Microsoft Paint erzeugt wurde. Die Zahl 94 gibt hier die Qualitätsstufe (1..100) an, die bei Paint fest voreingestellt ist.

Die JPEG-Signaturen können in drei Hauptgruppen aufgeteilt werden. Die erste Gruppe heißt Standard (identisch mit IJG Library). Hier werden die Quantisierungstabellen verwendet, so wie sie im JPEG Standard beschrieben sind. Es gibt hier genau 99 Qualitätsstufen. Die zweite Gruppe heißt Extended. Hier wird eine Qualitätsstufe in etwa 100 Zwischenstufen aufgeteilt, wobei die Quantisierungstabellen des Standards interpoliert werden. Solche Signaturen gehören i. d. R. zu günstigen Kameraeinsteigermodellen, die nach der Komprimierungsmethode „size-priority“ arbeiten.

D3D8AD02 (Extended 95.10 / 10 MP camera)

Die Qualitätsstufe wird sowohl in der Signatur als auch bei den JPEG-Details unter DQT-Marker mit zwei Nachkommastellen angegeben. Ob eine bestimmte Kamera nach size-priority arbeitet, kann man bei den Exif-Metadaten i. d. R. an dem Feld CompressedBitsPerPixel ablesen.

Die dritte Gruppe heißt Custom. Hier werden herstellerspezifische Quantisierungstabellen benutzt. Auch hier wird die Qualitätsstufe zwischen 0 und 100 mit zwei Nachkommastellen angegeben. Ausnahmen davon bilden Photoshop mit den Stufen 0 bis 12, Apple Quicktime 1 bis 1024 und LEAD Technologies 2 bis 255.

53631B67 (LEAD Technologies 2 / Scan)

Im zweiten Teil der Beschreibung, hier Scan, kann außerdem noch Facebook, WhatsApp oder MsPhoto stehen. MsPhoto bedeutet hier, dass die Datei mit Micosoft Photo Gallery bearbeitet wurde.

Die Generator-Signaturen werden intern als Grundlage für die Berechnung der generischen Relevanz benutzt. Zusätzlich werden sie auch bei der Datei-Header-Signatur-Suche in X-Ways Forensics zur Benennung von aus Sektoren ausgegliederten JPEG-Dateien eingesetzt, wenn keine

„besseren“ Metadaten vorhanden sind (z. B. Kameramodell und Zeitstempel aus den Exif-Daten). Wenn die Metadaten-Extraktion keine „besseren“ Metadaten findet, kann immer noch die Generator-Signatur ausgegeben werden, und diese erlaubt es Ihnen zumindest, Gruppen zusammengehöriger Dateien zu identifizieren, die wahrscheinlich dieselbe Herkunft haben. Wenn Exif-Metadaten vorhanden sind, können Sie überprüfen, ob Generator-Signatur und Exif-Metadaten miteinander konsistent sind, und das kann zeigen, ob ein Bild bearbeitet und erneut gespeichert wurde.

Insbesondere erlaubt die Generator-Signatur es, JPEGDateien zu erkennen, die von Scannern erzeugt wurde, da nur eine handvoll Generatoren in Scannern üblich sind. D. h. damit kann man eingescannte Bilder als solche auch dann erkennen, wenn sie nicht schwarz-weiß sind und nicht zu 100% nur Graustufen-Farben enthalten. Mit Hilfe der PDF-Generator-Signaturen können auch PDF-Dokumente als eingescannt identifiziert werden.

PDF-Generator-Signaturen stehen immer zur Verfügung, auch wenn sonst keine Metadaten vorhanden sind oder keine extrahiert werden können. Mit etwa 4.700 Signaturen (Stand v19.0) können mehr als 99% der PDF-Dateien zugeordnet werden. Bei der dokumentenorientierten Analyse kann auch die Kategorie „Reporting/Records“ in der Datei „Generator Signatures.txt“ von Interesse sein. Die Signaturen in dieser Kategorie gehören etwa zu Kontoauszügen oder Rechnungen.

Die Datei „Generator Signatures.txt“ enthält die Zuordungen von bestimmten Signaturen zu den dazugehörigen Beschreibungen und zusätzlich einer Rang-Angabe für die Berechnung der generischen Relevanz. Diese Datei ähnelt vom Aufbau her den anderen bei X-Ways Forensics mitgelieferten Textdateien und kann wie diese vom Benutzer für seine Ziele angepasst werden. Anstatt die Bewertung einer jeder einzelnen Signatur anzupassen kann man auch die Bewertung einer Kategorie z. B. „JPEG/Scan“ insgesamt anpassen. Das ist die Zahl hinter dem Tabulatorzeichen in der Zeile, die mit *** beginnt. Der Rang für eine bestimmte Signatur muss zwischen 0 und 9 liegen. Für den Rang der Kategorien gilt diese Beschränkung nicht.

The model designations of known scanning devices can be manually extended in the section "KnownScanner" of "Generator Signatures.txt". Identification by model name can help to identify scanned images if they contain Exif data or were edited. Generally the detection as scanned images is based on 1) generator signature, 2) generic properties of the Exif metadata (FileSource, Density, ...) and 3) the KnownScanner list.

The prefix "Reporting::" in generator signature definitions allows for easier filtering for the category reporting/records.

The structure of the separate file "Video Signatures.txt" is the same as that of "Generator Signatures.txt", but it deals with signatures of video files of the QuickTime format family only. It currently consists of two subcategories: Original and Generic. You may insert newly found signatures (as shown in Details mode) in the Original section if you are certain that the video has not been edited, otherwise in the Generic section.

5.27 Schnittstelle für externe Analyse

Über den Menübefehl "Datei-Export zur Analyse" im Falldatenfenster können Sie Dateien (z. B. alle Dateien aus dem gesamten Fall, die zu einer bestimmten Kategorie gehören) zur weiteren Analyse an ein externes Programm übergeben. Dieses Programm muss auf die unten beschriebene Schnittstelle ausgelegt sein. Erfordert X-Ways Forensics oder X-Ways Investigator oder WinHex mit forensischer Lizenz.

Das Ergebnis der Analyse kann zurück in X-Ways Forensics importiert werden, über den Befehl zum Importieren von Vermerken im Falldatenfenster. (Klicken Sie dazu z. B. rechts auf den fettgedruckten Falltitel.) Dies erstellt für die von der externen Software kategorisierten Dateien Vermerke (und erstellt datz ggf. neue Vermerkbezeichnungen), was es Ihnen erlaubt, nach diesen Dateien leicht zu filtern oder sie in einem Bericht auszugeben.

Technische Beschreibung der Schnittstelle

All files or files in a certain category or all tagged files or all non-hidden files are copied into a subfolder of the output folder specified by you. The subfolder is named with a CRC in hexadecimal characters that is unique for the active case. The files are named with unique IDs (64-bit integer numbers). One additional file named "Checksum" is created that contains 4 bytes with the same CRC, 4 bytes with the handle of the main window of X-Ways Forensics (or X-Ways Investigator, for that matter), 8 reserved bytes, and 128 bytes with the case title in UTF-16. When the files have been copied, X-Ways Forensics executes the external analysis program and specifies the complete path of the subfolder in quotation marks as a parameter.

The external program can now perform the analysis. It can classify files by creating one .rtd file for each classification.

When finished, the program can optionally check whether the X-Ways Forensics main window still exists and, if so, make X-Ways Forensics aware of the availability of the results, by sending a WM_SETTEXT messages to the main window, where the text starts with "Import: ", followed by the path of the directory where to find the .rtd files, without quotation marks. This will trigger the import automatically. Alternatively, the user can import the result as described above.

Die Namen der .rtd-Dateien (report table definition files) wird als Vermerkbezeichnung verwendet. Eine .rtd-Datei beginnt mit einer 4 Byte langen Signatur (0x52, 0x54, 0xDE, 0xF0), der 4 Byte großen Prüfsumme (s. o.), gefolgt von den 64-Bit Datei-IDs (Integer-Zahlen), die die Dateien identifizieren, die mit dem betreffenden Vermerk ausgestattet werden sollen.

6 Datei-Überblick

6.1 Allgemeines

Ein Datei-Überblick ist eine Datenbank vom Inhalt eines Volumes oder physischen Datenträgers (Dateien, Verzeichnisse, ...) zu einem bestimmten Zeitpunkt. Der Verzeichnisbaum und der Verzeichnis-Browser erlauben Einblicke in diese Datenbank. Basierend auf den zugrundeliegenden Dateisystem-Datenstrukturen besteht ein Datei-Überblick aus einem Datensatz pro Datei und Verzeichnis und speichert praktisch alle Metadaten (Name, Pfad, Größe, Zeitstempel, Attribute, ...), nur den *Inhalt* der Dateien und die Daten von Verzeichnissen nicht.

Ein Datei-Überblick referenziert gewöhnlich sowohl existierende als auch vormals existierende (z. B. gelöschte) Dateien, auch virtuelle (künstlich definierte) Dateien, wenn diese für computer-forensische Untersuchungen von Nutzen sind (so dass z. B. auch unbenutzte Bereiche eines Datenträgers abgedeckt werden). Operationen wie logische Suchen, Indexierung und alle Befehle im Kontextmenü des Verzeichnis-Browsers werden auf die Dateien und Verzeichnisse angewandt, wie sie im Datei-Überblick abgelegt sind. Wegen komprimierten Dateien und weil gelöschte Dateien und die virtuelle Datei "freier Speicher" mit denselben Clustern eines Dateisystems mehrfach verknüpft sein können, kann die Summe aller Dateien und Verzeichnisse in einem Datei-Überblick leicht die gesamte physische Größe des Datenträgers/der Partition übersteigen.

Ein Datei-Überblick wird entweder gespeichert in Form einer Handvoll Dateien des Namens Volume*.dir, im Ordner für temporäre Dateien oder (wenn mit einem Fall verbunden) in Dateien namens „Main 1“, „Main 2“, „Main 3“, „Names“, ..., im Metadaten-Verzeichnis des Asservats.

6.2 Erweiterung auf Volume-/Sektor-Ebene

Das Specialist-Menü erlaubt es, den Standard-Datei-Überblick auf verschiedene Weisen zu *ergänzen*, zu *erweitern*, so dass er mehr enthält als das Dateisystem regulär referenziert. Erfordert eine Specialist- oder forensische Lizenz. Volle Funktionalität nur mit forensischer Lizenz.

6.2.1 X-Tensions ausführen

X-Tensions sind DLLs, die Sie selbst programmieren können, um die Funktionalität von X-Ways Forensics zu ergänzen oder für Ihre eigenen Zwecke automatisiert zu nutzen. Weitere Informationen.

6.2.2 Dateisystem-Datenstruktur-Suche besonders intensiv:

Das intensive Suchen nach Dateisystem-Datenstrukturen ist eine potenziell lang andauernde

Operation, abhängig von der Größe der Partition, und aus diesem Grund nicht Teil der Standardprozedur beim Erzeugen des Datei-Überblicks.

FAT12/FAT16/FAT32: Sucht nach verwaisten Unterverzeichnissen, also Unterverzeichnissen, die von keinem anderen Verzeichnis mehr referenziert werden.

Ext3/Ext4: Ähnliches Vorgehen wie bei FAT. Prüft die gesamte Partition auf ehem. existierende Verzeichnisstrukturen, deren Inhalte nicht von ihren zugehörigen Inodes her bekannt sind (solche würden bereits beim Erzeugen des ursprünglichen Datei-Überblicks gefunden). Auf diese Weise gefundene Unterverzeichnisse werden mit einem generischen Namen in den Datei-Überblick aufgenommen, normalerweise unterhalb von "Pfad unbekannt", aber möglicherweise im Stammverzeichnis, wenn sie dort angeordnet waren. (Das Stammverzeichnis stellt hierbei eine Besonderheit dar, weil es eine unveränderliche ID hat.). Optional können bestimmten ehem. existierende Dateien, die sonst nur mit Metadaten des Dateisystems dargestellt würden und ohne Inhalt, mit Hilfe des Ext3/Ext4-Journals doch Daten zugeordnet werden.

ReiserFS, Reiser4: Sucht nach gelöschten Dateien (die in einem Standard-Datei-Überblick überhaupt nicht enthalten sind).

UDF: Während die erste und die letzte Session auf einer Multisession-UDF-CD/-DVD automatisch aufgelistet werden, können weitere Sessions in der Mitte nur mit dieser Option gefunden werden.

CDFS: In den meisten Fällen werden alle Sessions auf Multisession-CD/DVDs automatisch gefunden. In Ausnahmefällen (z. B. wenn CDFS zeitgleich zu UDF existiert oder die Abstände zwischen den Sessions ungewöhnlich groß sind), können hiermit weitere Sessions hinter der ersten gefunden werden.

RAM (Hauptspeicher): Findet u. U. beendete Prozesse und Rootkits.

NTFS: Schattenkopien können optional ausgewertet werden, mit einer forensischen Lizenz. Existierende und ehemals existierende Schattenkopie-Trägerdateien werden auf wertvolle Informationen geprüft, die anderweitig nicht erhältlich wären, so etwa Dateien, die nicht mehr in der aktuellen $MFT gefunden werden können oder frühere Versionen von Dateien, deren Inhalt sich geändert hat. Those files will be reconstructed up to 1 GB in length according to the shadow copy. Processing of volume shadow copies, if any, occurs before all the other operations that are part of the particularly thorough file system data structure search (parsing $LogFile, optionally searching for FILE record outside of $MFT and outside of VSC, searching for index records in the slack of INDX buffers). If there are volume shadow copies, the caption of the small progress indicator window will tell you when they are being parsed. Volume shadow copy host files that you exclude before processing will be omitted.

Files found in volume shadow copies are specially marked with "SC #" in the Attr. column, or "SC #, prev. version" if they are previous versions of files that were known to the volume snapshot already before the thorough file system data structure search, so that it is easy to filter them in or out. # stands for the sequential number of the snapshot in which these files were found. Remember you can sort by ID to see the files they are a previous version of next to them. You can also easily navigate to the VSC host by using the command Navigation | Find related file in

the directory browser context menu, for example so that in Details mode learn more about that particular snapshot. You could then invoke the same command once more to navigate to the corresponding snapshot properties file, where in Details mode you learn even more, e.g. description and official creation date.

You may optionally avoid that previous versions of files in volume shadow copies are added to the volume snapshot if they are exact duplicates (identical file contents) so that it is much easier to focus on files for which actually previous data is still available. Time for that may be well invested because even if modification dates are different, the file contents are often the same for files installed by the operation system. If fully selected, X-Ways Forensics will compare files up to 128 MB, if half selected, only up to 16 MB, as to not waste too much time on this feature.

NTFS: Nach FILE-Records kann optional überall gesucht werden, in Sektoren, die nicht der MFT in ihrer aktuellen Größe und Lage angehören und auch nicht zu einer von der o. g. Operation behandelten Schattenkopie gehören. Solche FILE-Records können z. B. im freien Speicher gefunden werden, wenn eine Partition neu erstellen, neu formatiert, verschoben, vergrößert, verkleinert oder defragmentiert wurde. Kann auf großen Partitionen sehr lange dauern, daher optional (s. Optionen des Datei-Überblicks). Clusters belonging to certain virtual machine disk image types are skipped to avoid the inclusion of files in the file system of the virtual machine in the volume snapshot of the host machine's volume.

NTFS: Mit einer forensischen Lizenz kann die aktuelle $LogFile-Datei sowie frühere Versionen von $LogFile, die in verarbeiteten Schattenkopien gefunden wurden, ausgewertet werden. Die Inhalte gelöschter Dateien können dank den Informationen in $LogFile oft rekonstruiert werden. Überbleibsel von Index-Records können sowohl in $LogFile als auch im Schlupf von INDX-Puffern gefunden werden und enthüllen u. U. entweder frühere Namen oder Pfade von umbenannten/verschobenen Dateien/Verzeichnissen enthüllen, die im Datei-Überblick schon verzeichnet waren, oder gelöschte Dateien, die dem Datei-Überblick bis dato noch unbekannt waren (allerdings ohne zugehörige Datei-Inhalte). Geben Sie an, ob Sie an früheren Namen bzw. Pfaden von umbenannten/verschobenen Dateien und Verzeichnissen interessiert sind oder nicht, und ob Sie Dateien in den Datei-Überblick aufnehmen lassen möchten, für die nur Name, Größe, Zeitstempel und Attribute (aber keine Daten/Cluster) bekannt sind. Wenn das Kontrollkästchen für frühere Namen/Pfade halb angekreuzt ist, dann werden Sie über frühere Namen/Pfade von umbenannten/verschobenen Dateien über die Metadaten-Spalte informiert, und erhalten keine zusätzlichen Dateien im Datei-Überblick für jeden früheren Namen/Pfad.

Bei allen Unteroperationen für NTFS werden besondere Anstrengungen unternommen, um die Aufnahme redundanter (identischer) Dateien in den Datei-Überblick zu vermeiden. Wenn die einzige neue Information in alten Versionen von FILE-Records oder Index-Records ehemals gültige Zeitstempel sind, keine früheren Namen/Pfade/Inhalte von Dateien (oder nur frühere Namen/Pfade, Sie an diesen aber explizit kein Interesse zeigen), dann werden diese Zeitstempel nur als Ereignisse ausgegeben, sofern die Option "Zeitstempel aus diversen Quellen als Ereignisse bereitstellen" bei der Erweiterung des Datei-Überblicks gewählt ist.

NTFS: Sie können festlegen, ob Sie daran interessiert sind, dass Dateien in den Datei-Überblick aufgenommen werden, deren Cluster (und damit deren Daten) gänzlich unbekannt sind, nur mit Metadaten (z. B. Dateiname, Pfad, Größe, Attribute und Zeitstempel), wie in Index-Records in INDX-Puffern und in $LogFile zu finden. Wenn angekreuzt, werden alle ehem. existierenden

Dateien, von denen nur Metadaten bekannt sind, in den Datei-Überblick aufgenommen. Wenn nicht angekreuzt, werden solche Dateien ignoriert.

Andere Dateisysteme: kein Unterschied zum Standard-Datei-Überblick

6.2.3 Datei-Header-Signatur-Suche

Diese Option hilft, solche Dateien in den Datei-Überblick aufzunehmen, die im freien oder belegten Laufwerksspeicher nur noch anhand ihrer Datei-Header-Signatur gefunden werden können und nicht mehr von Dateisystem-Datenstrukturen referenziert werden. Dazu werden Sie gefragt, welche bestimmten Dateitypen erkannt werden sollen, welche Standardgröße verwendet werden soll, welcher Präfix für den Ausgabenamen verwendet werden sollen usw., wie von „Dateien retten nach Typ“ bekannt (Details s. dort und in den Dateityp-Definitionen). Dateien, die mit dieser Methode gefunden werden, werden nur dann in den Datei-Überblick aufgenommen, wenn es noch keine andere Datei im Datei-Überblick mit derselben Startsektornummer gibt (überschriebene Dateien zählen hierbei nicht), um Doppelungen zu vermeiden, um Doppellistungen zu vermeiden. Nicht an Sektorgrenzen ausgerichtete Dateien werden aus Performanzgründen einfach immer aufgenommen. Dateien werden mit dieser Methode mit einem generischen Namen und der Größe ausgegeben, wie sie vom Mechanismus in »Dateien retten nach Typ« erkannt werden. Wenn auf physische, partitionierte Asservate angewandt, werden nur unpartitionierte Bereiche und Partitionslücken nach Datei-Headern durchsucht, da die Partitionen als separate, zusätzliche Asservate behandelt werden.

Usually results of the file header signature search are output in a special virtual directory for carved files, which is a subdirectory of "Path unknown". However, there is an option to show resulting files as child objects of existing files, if the carved files were found within these other files.

6.2.4 Blockweise hashen und abgleichen

Verfügbar mit forensischer Lizenz. Block-wise hashing may allow to identify complete or incomplete remnants of known notable files that are still floating around in free drive space even if they were fragmented and the location of the fragments is unknown, to show with some or very high certainty that these files once existed on that medium. The hash values are computed when reading from the evidence object sector-wise, and that happens at the same time when running a file header signature search if selected, to avoid unnecessary duplicated I/O, with the same sector scope. Matches are returned as a special kind of search hits. Multiple matches for contiguous blocks are more meaningful than isolated individual matches, as they are even less likely the result of some coincidence, and they are usually combined in a single hit. The size of all such hits is shown when listing search hits. The larger the size, the higher the evidentiary value of the match. Please note that X-Ways Forensics does not verify itself that contiguous matching blocks are in the same order as in the original file(s), but that can be verified manually and for data that is as unique as compressed data that is most likely the case.

Most suitable for selected notable files larger than a few sectors, files that are ideally compressed

or at least not only sparsely populated with non-zero data and do not contain otherwise trivial combinations of bytes values that occur frequently. Good examples are zip-styled Office documents, pictures and video files. Very trivial blocks within a file that consist of mostly just 1 hash value are ignored and not hashed (the same already when creating the hash set). For quicker matching, ideally work with a small hash database and do not select a hash type stronger than MD5. The length of block hash matches is shown in the Size column. This is useful so that you can sort them by the lengths and review more important (larger) matches first.

Hash sets of block hashes can be created or imported in the same way as ordinary hash sets, i.e. for selected files using the directory browser context menu, but they are handled by a separate hash database for block hashes (as opposed to file hashes). That separate database is internally stored in a subdirectory of the main hash database directory. You can create hash sets consisting of the block hashes of 1 file at a time, or combined hash sets of multiple selected files. The block size is currently always 512 bytes and might be user-definable in a future version.

6.3 Erweiterung auf Datei-Ebene

Die u. g. Operationen werden *nach* den oben genannten Operationen auf Dateien angewandt, die bereits im Datei-Überblick enthalten sind, und zwar alle Operationen zusammen und dateiweise (d. h. erst alle Operationen auf eine Datei, dann alle Operationen auf die nächste Datei usw.) und die Dateien werden in der Reihenfolge der internen IDs abgearbeitet. Einige Operationen davon können weitere Dateien hervorbringen, die dann die nächsthöhere verfügbar interne ID erhalten. Ehemals existierende Dateien, deren erster Cluster bekanntermaßen überschrieben wurde oder gar nicht erst bekannt ist, werden nicht verarbeitet, es sei denn, Sie wenden die Operationen per Markierung oder Auswahl gezielt auf sie an.

Dateien, die aufgrund eines Hash-Wert-Abgleichs als irrelevant angesehen werden, können automatisch von allen weiteren Operationen ausgenommen werden, um Zeit zu sparen und potenziell noch weitere irrelevante Dateien zu vermeiden, die sonst ggf. noch aus ihnen extrahiert würden. Es ist auch möglich, nicht nur bekanntermaßen irrelevante Dateien von der weiteren Verarbeitung auszunehmen, sondern auch bekanntermaßen relevante Dateien. Das ist nützlich zum Beispiel in größeren Fällen, wenn Sie viele solcher Dateien vorliegen haben oder erwarten und wenn die Kenntnis über das Vorhandensein der Dateien für Sie ausreichend ist und Sie für diese Dateien keine internen Metadaten, Hautfarbenanteile, PhotoDNA-Hash-Werte usw. benötigen und auch keine darin eingebetteten Daten o. ä. Es gibt auch eine Option zum Auslassen von Dateien, die herausgefiltert werden. All diese Optionen sind insbesondere deshalb sehr mächtig, weil sie sogar im Voraus Dateien gezielt aussparen können, die noch gar nicht Teil des Datei-Überblicks sind, wenn dessen Erweiterung beginnt. Wenn z. B. die Datei-Header-Signatur-Suche dem Datei-Überblick weitere Dateien hinzufügt, können diese je nach Datei weiterverarbeitet (z. B. gehasht) werden oder nicht, je nachdem ob zum Zeitpunkt der Erweiterung des Dateiüberblicks ein Typ-Filter aktiv ist.

There is an option to omit additional hard links for the same file in NTFS/HFS+ from volume snapshot refinement just as from logical searches, to save time and reduce the number of redundant identical child objects etc. This can make a big difference on partitions with Windows installations that have a lot of hard links and HFS+ partitions with Mac OS X Time Machine.

Which hard links are considered the "additional" hard links internally can be seen in the "Link count" column (gray number means to be omitted) and also in the Description column, which identifies all hard links (i.e. files with a hard link count larger than 2) and the additional ones in particular textually. The hard link that is not marked as "optionally omitted" in the Description column is considered the "main" hard link internally.

Eine ehemals existierende Datei, deren erster Cluster laut Dateisystem neu verwendet wurde (dargestellt als "1. Cluster nicht verfügbar") kann im Rahmen der Erweiterung des Datei-Überblicks verarbeitet werden, wenn Sie das Häkchen bei dem dafür zuständigen Kontrollkästchen entfernen, das standardmäßig dafür sorgt, dass solche Dateien ausgelassen werden. Das bedeutet insbesondere, dass nicht mit der Datei in Verbindung stehende zufällig an selber Stelle vorgefundene Daten gehasht werden können und das Ergebnis als Hash-Wert dieser Datei ausgegeben wird, obwohl er mit größter Sicherheit nicht der Hash-Wert dieser Datei war. In früheren Versionen hätte X-Ways Forensics dem Verlangen des Benutzers nach einer Hash-Berechnung nur dann stattgegeben, wenn eine solche Datei gezielt durch Markierung oder Auswahl angegangen worden wäre. Wenn X-Ways Forensics gezwungen wird, Hash-Werte von unsinnigen Daten zu berechnen, werden diese im Verzeichnis-Browser in grauer Farbe dargestellt, um Benutzer daran zu erinnern, dass diese Hash-Werte nicht überinterpretiert werden sollten und dass man nicht erwarten kann, diese Hash-Werte auf anderen Datenträgern wiederzufinden.

6.3.1 Hash-Wert-Berechnung und Abgleich

Es können **Hash-Werte** für Dateien im Datei-Überblick berechnet werden. Hash-Werte werden nicht erneut berechnet, wenn die Operation erneut auf dieselben Dateien angewandt wird. Zusätzlich zur reinen Hash-Berechnung erlauben es forensische Lizenzen, Hash-Werte mit individuell ausgewählten (oder einfach allen) Hash-Sets in einer internen Hash-Datenbank **abzugleichen**. Der dynamische Filter kann dann anschließend eingesetzt werden, um bekanntermaßen irrelevante Dateien auszublenden. Mit Hilfe der Hash-Datenbank als irrelevant erkannte Dateien werden außerdem optional von der weiteren Bearbeitung bei der Erweiterung des Datei-Überblicks ausgeschlossen, was u. a. Zeit spart. Im Gegensatz zur Hash-Wert-Berechnung wird der *Abgleich* für dieselben Dateien auf Wunsch erneut durchgeführt. Ein erneutes Abgleichen entfernt die zuvor angezeigten Hash-Sets aus dem Hash-Set-Feld bei allen Dateien des Datei-Überblicks, es sei denn, Sie lassen gezielt nur für markierte Dateien erneut abgleichen (dann werden nur deren bisherige Hash-Set-Zuordnungen entfernt). Das Kategorie-Feld wird nur ggf. aktualisiert, nicht geleert.

It is possible to compute hash values of two different hash types at the same time when refining the volume snapshot, for general purposes or to match them against two hash databases with different hash types. If matching is selected, all hash values will be matched against any of the two hash databases whose hash type fits. That means even if the primary hash type in the volume snapshot is MD5 and the secondary is SHA-1, and hash database #1 is based on SHA-1 and #2 based on MD5, X-Ways Forensics will match the hash values accordingly. The hash types in the volume snapshot and in the hash databases do not have to be in the same order.

Eine forensische Lizenz erlaubt es, Hash-Werte, die bereits früher berechnet wurden oder aus

einem Container importiert wurden, zu überprüfen. Das Ergebnis wird ins Nachrichtenfenster ausgegeben. Dateien, deren aktueller Hash-Wert nicht mit dem ursprünglich berechneten übereinstimmt, werden mit einem besonderen Vermerk versehen, so dass man sie sich bequem auflisten lassen kann. Das erneute Ausführen der Hashing-Option beim Erweitern des Datei-Überblicks aktualisiert nie die Hash-Werte, die bereits zuvor für Dateien im Datei-Überblick berechnet wurden.

Child objects of files inherit the hash category "irrelevant" from their parents. That is possible because if an entire file is irrelevant, everything that can be extracted from that file must also be irrelevant. However, what is extracted from a "notable" file is not necessarily also notable, because perhaps only some parts or aspects of the parent file are notable. Of course, child objects of irrelevant parents will only be output if the user chooses to not omit irrelevant files from further processing in the first place.

When matching hash values against hash databases (ordinary hashes like MD5, SHA-1, SHA-256, ...), there is an option to make a local copy of the database and work with that copy. This can be helpful if you share the database with your colleagues and your colleagues want to update the database (e.g. add additional hash sets) while it's in use for matching, which otherwise would not be possible for the whole duration of volume snapshot refinement. It could also enhance performance if the database is large and does not fit into main memory and is stored on a remote network drive. The local copy is created in the directory for temporary files if it does not exist yet, and updated only if the master copy of the hash database has changed (all users should have v19.8 or newer to avoid unnecessary copying of an unchanged database).

Zusätzlich zu konventionellen Hash-Datenbanken können Sie die Hash-Werte von Dateien auch mit der Hash-Kommentar-Datenbank abgleichen, um Kommentare/Beschreibungen zurückzuerhalten, die bekannten relevanten Dateien zuvor in anderen Fällen zugeordnet wurden, von Ihnen selbst oder Kollegen.

MD5/2 ist einer der angebotenen Hash-Typen, und dieser bezieht sicht auf MD5-Hash-Werte "halber Länge". Die halbe Länge ergibt sich durch "Falten", d. h. die erste Hälfte wird mit der zweiten Hälfte ver-xor-t, was ein 64 Bit breites Ergebnis liefert. Dies ist als sparsamer Kompromiss gedacht zwischen CRC32 (32 Bit) und einem regulären MD5-Hash (128 Bit), um die relativ große Lücke zwischen den beiden zu schließen und Speicher sowie Datenträgerkapazität zu sparen, z. B. für Deduplikationszwecke.

Ein weiterer besonderer Hash-Typ ist EDRM MIH, ein eDiscovery-Standard. Solche Hash-Werte können berechnet werden für extrahierte E-Mails und Original-.eml- und -.emlx-Dateien (wenn sie vollständige Kopfzeilen enthalten), um nach E-Mails mit bekanntem MIH-Wert zu suchen, für Datenbank-Abgleiche oder für Zwecke der Deduplizierung. Wenn ein MIH einer .eml-Datei im Datei-Überblick zugeordnet wird und die .eml-Datei aus einer .msg-Datei extrahiert wurde, wird derselbe MIH automatisch auch der Eltern-.msg-Datei zugewiesen. Zwei Kopien derselben E-Mail können zwei unterschiediche reguläre Hash-Werte haben, aber denselben MIH, z. B. wenn das Dateiformat unterschiedlich ist (eine rohe .eml-Datei ggü einer OLE2-.msg-Datei) oder wenn das Format des Rumpfes sich unterscheidet (z. B. einmal HTML, einmal reiner Text) und/oder wenn der Inhalt anders gespeichert wurde. Wenn EDRM MIH als Hash-Typ ausgewählt ist, aber kein MIH berechnet werden kann, weil die adressierte Datei keine E-Mail eines unterstützten Typs ist, bleibt die Hash-Wert-Zelle leer. Als Kompromiss können Sie "MD5/MIH" als

Hash-Typ wählen: Dann wird ein MIH berechnet wird, sofern dies möglich ist, und andernfalls ein MD5-Hash-Wert. Es erhalten auf diese Weise also alle hashbaren Dateien einen Hash-Wert gleicher Länge, für Deduplikationszwecke oder zum Abgleich.

6.3.2 Datei-Typ-Prüfung

Eine forensische Lizenz erlaubt es, **Dateitypen u. a. anhand von Signaturen** (auch mit Hilfe weiterer Algorithmen) zu über**prüfen**, d. h. Dateinamens-/Dateityp-Unstimmigkeiten in allen Dateien im Datei-Überblick aufzudecken außer denen, deren ursprünglicher erster Cluster bekanntermaßen nicht mehr verfügbar ist. Wenn z. B. jemand ein belastendes JPEG-Bild durch Umbenennen in "Rechnung.xls" (falsche Dateiendung) versteckt hat, wird der erkannte Dateityp "jpg" in der Spalte "Typ" des Verzeichnis-Browsers angezeigt. Weitere Informationen finden Sie in den Beschreibungen der Spalten Typ und Status. Die Dateisignaturen und Namensendungen, die für die Erkennung von Unstimmigkeiten verwendet werden, sind in den begleitenden Dateityp-Definitionsdateien definiert, die Sie nach Ihren Bedürfnissen anpassen können. Es ist die gleiche Datenbank, die auch die Grundlage für die Datei-Header-Signatur-Suche ist. Bitte beachten Sie, dass die Verbindung zwischen den gegenwärtig in einem freien Cluster gespeicherten Daten und einer gelöschten Datei, die dort mal gespeichert war, und deren Namen schwach ist, so dass allein schon deshalb eine Divergenz zwischen Dateiendung und erkanntem Typ bestehen kann, weil einfach nur der erste Cluster einer gelöschten Datei in der Zwischenzeit für eine ganz andere Datei wiederverwendet wurde. Wenn Sie die Dateityp-Überprüfung wiederholen möchten, z. B. weil Sie die Dateityp-Signatur-Datenbank bearbeitet haben, müssen Sie die Option „Erneut“ wählen. Den Status der Typ-Spalte des Verzeichnis-Browsers können Sie an der Typstatus-Spalte ablesen.

Die allermeisten selbstextrahierenden .exe-Archive werden intern ebenfalls bei der Signaturprüfung erkannt. Sie werden klassifiziert als Dateityp „sfx“ und der Kategorie „Archives“ zugewiesen. Diese Dateien manuell zu überprüfen verhindert, dass komprimierte Dateien in solchen Archiven in einer Untersuchung völlig übersehen werden. .exe-Archive mit Zip-Kompression können im Vorschaumodus eingesehen werden. Andere selbstextrahierende Archive müssten aus dem Asservat herauskopiert und mit einem geeigneten Tool wie WinRAR oder 7-Zip geöffnet werden.

Die Signaturprüfung enttarnt auch MS-Office-Hybrid-Dateien, d. h. verschmolzene MS-Word- und MS-Excel-Dokumente, die in beiden Applikationen geöffnet werden können und jeweils unterschiedliche Inhalte zeigen. Ein Hinweis darauf wird im Nachrichtenfenster angezeigt, und alle detektierten Dateien werden mit einem besonderen Vermerk versehen. MS-Office-Hybrid-Dateien sind ein cleverer Versuch, den Inhalt eines der verschmolzenen Dokumente zu verstecken.

6.3.3 Aufbereitung interner Metadaten und Ereignisse

Erfordert eine forensische Lizenz.

a) Kann die Dateiformat-Konsistenz von Dateien der Typen EXE, ZIP, RAR, JPEG, GIF, PNG,

RIFF, BMP und PDF prüfen. Die Typstatus-Spalte zeigt das Ergebnis an, entweder "OK" oder "beschädigt".

b) Erlaubt das Extrahieren von intern gespeicherten Erzeugungszeitstempeln aus OLE2-Compound-Dateien (z. B. MS-Office-Dokumente vor Version 2007), EDB, PDF, MS Office HTML, EML, MDI, ASF, WMV, WMA, MOV, JPEG, THM, TIFF, PNG, GZ, GHO, PGP pubring.pkr keyring, ETL, SQM, IE Cookies, CAT, CER, CTL, SHD Drucker-Spool, PF Prefetch, LNK-Shortcut und DocumentSummary alternativen Datenströmen. Diese Zeitstempel werden in der Spalte „Interne Erzeugung“ des Verzeichnis-Browsers angezeigt. In manchem Fällen wird der Zeitstempel extrahiert, der am weitesten in der Vergangenheit liegt und damit dem ursprünglichen wahren Erzeugungsdatum am nächsten kommt.

c) Erlaubt die Übernahme bestimmter Metadaten in die Metadaten-Spalte, was es wiederum ermöglicht, Dateien anhand dieser Metadaten zu filtern, Metadaten mit dem Befehl „Liste exportieren“ zu exportieren oder in Form einer Berichtstabelle mit dem Fallbericht auszugeben. Metadaten können extrahiert werden aus allen im Details-Modus speziell unterstützten Dateitypen sowie aus Windows-Link-Dateien (.lnk) und Windows-Prefetch-Dateien (.pf). Nur eine Untermenge der Metadaten aus dem Details-Modus wird extrahiert. Dabei haben Sie die Möglichkeit, bestimmte Zeilen zu entfernen, so dass Sie sie nicht in der Metadaten-Spalte sehen, z. B. um dem Fallbericht oder die Ausgabe des Befehls "Liste exportieren" zum Ausdruck oder Betrachten auf dem Bildschirm kompakt zu halten, oder einfach nur deshalb, weil bestimmte Metadatenfelder für Sie nicht relevant sind. Sie können nicht erwünschte Metadatenfelder durch Teilworte identifizieren. So ein Teilwort kann entweder auf den Feldnamen zielen (z. B. "Focal Length") oder auf den Inhalt des Feldes (wenn Sie z. B. wissen, dass Sie an dem Feld "Author" kein Interesse haben, wenn der Autor eines Dokuments "Joe Huber" ist. Pro Zeile kann 1 Teilwort eingegeben werden. Teilwörter dürfen Leerzeichen enthalten. Sie können Ihre Definitionen mit anderen Benutzern teilen, indem Sie die Datei "Unwanted Metadata.txt" weitergeben.

Jump list hash values are translated to application names in the presented metadata of customDestinations-ms and automaticDestinations-ms jump list files, based on a new user-editable text file named "Jump List Names.txt". The translation table currently consists of around 500 entries. If you add entries, please make sure to insert them at the correct place such that all entries remain sorted by the CRC in ascending order. Leading zeroes in the CRC obviously must be preserved. There is a tab character between the CRC and the application name.

d) Allows to restore original file system metadata (such as filename, timestamps) when found in certain file types such as $I* recycle bin files and iPhone mobile sync backup indexes (Manifest.mbdx). Original filenames are typically much more meaningful than random names that are assigned just to guarantee uniqueness in a single directory for backup purposes. Examples of such random names are 3a1c41282f45f5f1d1f27a1d14328c0ac49ad5ae (for a file in an iPhone backup) or $RAE2PBF.jpg (Windows recycle bin). The current filename according to the file system can still be seen in square brackets in the Name column, as well as in Details mode, and the Name filter will find both the original and the current name, so that current filename is not completely lost.

Alternative names and timestamps are also extracted from Linux PNG thumbnails as known from Ubuntu and Kubuntu distributions, desktop manager MATE and GNOME ThumbnailFactory.

The name of the original file is shown in square brackets in the Name column and the recorded timestamp of the original file is shown as a "Content created" timestamp. The complete path of the original file can be seen in the Metadata column.

e) Befüllt die Spalten Absender und Empfänger für einzelne Original-E-Mail-Dateien (.eml, .emlx, .olk14msgsource). Extrahiert darüberhinaus die Betreffzeile solcher E-Mails und zeigt sie in der Namensspalte an, falls vom Dateinamen abweichend. Bewahrt den Originaldateinamen, sofern es sich nicht um eine gecarvete Datei handelt (d. h. mit einem künstlich erzeugten Dateinamen), auf und zeigt ihn in derselben Spalte weiterhin als alternativen Namen an.

f) Erzeugt Vorschauen für SQLite-Datenbanken von Internet-Browsern, was z. T. voraussetzt, dass die Dateien auf ihren wahren Typ hin geprüft wurde. Unterstützt Firefox History, Firefox Downloads, Firefox Form History, Firefox Sign-Ons, Chrome Cookies, Chrome Archived History, Chrome History, Chrome Log-In Data, Chrome Web Data, Chrome Sync, Safari Cache, Safari Feeds und Skype's main.db-Datenbank über Kontakte und Datei-Transfers. The Google Chrome history also displays the transition for each visited web site, making it easier to ascertain whether the visit was triggered by the user or by some other action like redirect. The duration of each visit is listed as well. Internet searches run from the address bar of Chrome are listed in a separate table and also added to the event list. Parses Google Chrome SNSS session files (Current/Last Session and Current/Last Tabs). The resulting session overview lists all open tabs and their browsing history. Erzeugt außerdem Vorschauen für Internet Explorer index.dat-Dateien (auch künstlich bei der Datei-Header-Signatur-Suche aus Einzel-Datensätzen zusammengesetzten), WebCacheV*.dat-Dateien von Internet Explorer 10 sowie von der Datei spartan.edb des Browsers Edge (all favorites and ReadingList entries will be added to the event list), auch von $UsnJrnl:$J, Windows Event Logs (.evt und .evtx) und Apple FSEvent-Logs. From iOS's sms.db all recorded conversations via SMS are extracted to individual chat files, and all messages are added to the event list, where they can be filtered based on phone number or email address. Rekonstruiert darüberhinaus einen Browser-Verlauf aus Safaris Icon-Datenbank. Diese alternative Quelle ist sehr interessant, weil sie die Besuchshistorie auch dann aufzeichnet, wenn Safari im Private Browsing Mode betrieben wird.

X-Ways Forensics kann spezifische Daten aus den Ereignissen in.evtx-Event-Logs extrahieren und diese direkt in der Ereignisliste darstellen. Das macht das Arbeiten mit Event-Logs deutlich mächtiger, weil man so schnell nach Benutzernamen, IP-Adressen von Anmelde- oder RDP-Ereignissen, Task- oder Service-Namen, PowerShell-Befehlen usw. Filtern kann. Es gibt dazu eine tabulatorseparierte Definitionsdatei namens „Event Log Events.txt“ im Installationsverzeichnis, die eine Liste von Ereignis-IDs enthält, (optional) die Namen der betreffenden Komponenten in Windows, die die Log-Einträge erzeugen, und eine Liste von individuellen Datenfeldern, die extrahiert werden sollen (kommasepariert) und (optional) einem Textkommentar, der zur Beschreibung eines Ereignisses in der Ereignisliste hinzugefügt wird. Die Definitionsdatei kann nach Ihren eigenen Bedürfnissen angepasst werden, auch in Form von Kommentaren, die Sie einfügen können, indem Sie einer Zeile ein Semikolon voranstellen. Die Ereignisse aus einer .evtx-Datei werden in einer tabulatorseparierten Tabelle (TSV-Datei) ausgegeben. Diese Tabelle enthält die kompletten Daten von jedem Ereignis. Sie kann idealerweise in MS Excel oder einer ähnlichen Anwendung eingesehen werden.

Die HTML-Repräsentation von index.dat-Dateien (Verwaltung von Browser-Cache und Verlauf des Internet Explorer) enthält eine Spalte, aus der man den Offset des Datensatzes innerhalb der

Datei ablesen kann, an dem dem die Daten der betreffenden Zeile gefunden wurden. Dieser Offset ist mit einem Link hinterlegt. Wenn Sie diesen anklicken, navigieren Sie automatisch zu dem Offset in der zugehörigen index.dat-Datei im Datei-Modus. Es ist als bequem, die von X-Ways Forensics aus dem dort gespeicherten Datensatz extrahierten Informationen selbst zu überprüfen. (Beachten Sie, dass dies nicht dann funktioniert, wenn der Link nicht in 2 Zeilen umgebrochen wurde, was in v8.4 der Viewer-Komponente passiert, aber nicht in v8.3.7. Man kann natürlich immer noch manuell zu dem Offset navigieren.)

Metadata and events are extracted from SRUDB.dat, i.e. the activity captured by the system resource usage monitor (SRUM). You can see the processes started over time, listed with their owners, and a lot of statistics. Network usage activity by each process is extracted as well. The extracted information can be useful to pinpoint the moment of a possible intrusion or the process that caused an intrusion. The information is presented in detailed HTML child object files and as events in the event list. Support is also included for iOS netusage.sqlite files, which record the data usage of apps. Besides the amount of data flowing in and out, they also provides approximate timestamps when apps were used for the first and last times. Appropriate events are extracted and an HTML preview is created containing all relevant information.

Die HTML-Unterobjekte, die erzeugt werden, können nicht nur intern von X-Ways Forensics zur Bereitstellung einer Vorschau des Elternobjekts verwendet werden. Sie können alle diese Tabellen auch in einem externen Programm betrachten, wie einem Internet-Browser oder in MS Excel, indem Sie die Unterobjekte an ein Programm Ihrer Wahl senden (Kontextmenü des Verzeichnis-Browsers).Sie können HTML-Tabellen nach einer beliebigen Anzahl von Zeilen aufsplitten lassen. Diese Zahl darf ruhig höher liegen, wenn Sie die HTML-Vorschauen extern mit einem Internet-Browser betrachten und nicht mit der Viewer-Komponente, die nicht mehr sehr großen Tabellen umgehen kann. Die Existenz von HTML-Unterobjekten mit durchsuchbarem Text für Browser-Daten, Event-Logs und weiteren Datenquellen erhöht auch die Effektivität von Suchen und Indexierung.

g) Extrahiert Tabellen aus diversen sonstigen SQLite-Datenbanken im TSV-Format und verwendet die erste davon jeweils als Vorschau der SQLite-Datenbank-Datei selbst.

h) Extrahiert den Originalzustand von bearbeiteten PDF-Dokumenten, sofern verfügbar, als Unterobjekt.

i) Stellt Zeitstempel aus dem Dateisystem als Ereignisse bereit, zur Analyse in einer Ereignisliste.

j) Stellt interne Zeitstempel in Dateien als Ereignisse bereit.

k) Eine generische Relevanz von Dateien kann eingeschätzt werden. Sie können Dateien in der Reihenfolge absteigender Relevanz begutachten, indem Sie nach der Relevanz-Spalte sortieren. Die Gewichtung, mit der die Aktualität und die Größe einer Datei einen Einfluss auf die berechnete generische Relevanz haben, ist benutzerdefinierbar. 100% bedeutet Standardgewichtung. 50% bedeutet nur halb so starke Gewichtung wie in der Voreinstellung. 0% bedeutet, dass der Faktor überhaupt keinen Effekt hat. Das Maximum ist 255%. The weight of the device type for the generic relevance judgement can be defined in the file Generator Signatures.txt. The weight factor can be found at the end of the *** line. It may be between 0 and 50. For pictures in the formats JPEG, PNG, GIF and WEBP the algorithm tries to put more

emphasis on intelligence value rather than news value, and to weigh evidential value higher than informational value. A relevance value of 3.0 is the base value defined for JPEG files in File Type Categories.txt. This value is also what you can expect from pictures that are just advertising. 3.2 = typical browser cache picture. 3.5 = typical for a picture from the system partition. 3.9 = social media. 4.1 = webcam. 4.2 = backup. 4.7 = photo as originally taken by a digital camera. Sorting picture by relevance achieves a grouping effect in the gallery because pictures from a similar context are sorted next to each other.

l) Die Strukturtyp-Spalte kann befüllt werden. Der Strukturtyp ist eine Weiterentwicklung des Generatorsignatur-Konzepts mit der Idee einer skalierbaren Typologie, die die Lücke zwischen Dateityp und Hash-Wert ausfüllt. Der Strukturtyp wird als 32-Bit-Integer in hexadezimaler Schreibweise präsentiert. Identische Werte identifizieren Bilder/Videos/Dokumente/Dateien, die zur selben Sequenz gehören (z. B. während einer Session aufgenomme Fotos). Der Strukturtyp wird berechnet für JPEG, PNG, GIF, WEBP, BMP, DOC, XLS, WAV, EML, MSG, GZIP, normale ZIP, TAR, MP3, HTML, PDF, Quicktime-Videos (MP4, MOV, 3GP, ...) und für DOCX, PPTX, XLSX. Bitte überprüfen Sie dabei gewonnene Erkenntnisse über Zusammenhänge zwischen den Dateien mit Zeitstempel und weiteren Metadaten. Sie können den Strukturtyp einer Dateien, die Ihr Interesse geweckt hat, kopieren und den Filter der Spalte dazu verwenden, um weitere Dateien mit diesem Strukturtyp ausfindig zu machen (oder direkt den dafür vorgesehenen Kontextmenü-Befehl "Nach Ähnlichem filtern" aufrufen). Der Strukturtyp kann auch ein nützliches Kriterium in der Funktion "Duplikate in Liste finden" sein.

m) Wenn der erzeugende Gerätetyp bestimmt wird für unterstützte Dateitypen, wird diese Information in der betreffenden Spalte ausgegeben, sofern die Gewissheit (oder Konfidenz) den von Ihnen angegebenen Wert übersteigt.

HTML-Berichtsdateien können automatisch für die Windows-Registry-Hive-Dateien NTUSER.DAT, SYSTEM, SOFTWARE, SECURITY und SAM als Teil der Metadaten-Extraktion erzeugt werden, basierend auf den “Reg Report *.txt”-Definitionsdateien, die Sie in Ihrem Installationsverzeichnis haben (von denen mehrere vorinstalliert sind). Die HTML-Dateien werden dem Datei-Überblick als Unterobjekte hinzugefügt. Der Vorteil ist, dass sie als menschenlesbare Vorschauen für ausgewählte interessante Werte dienen können, und sie enthalten einige codiert gespeicherte Texte als Klartext (insbes. sog. UserAssist-Einträge), so dass die logische Suche sie finden kann. Unmengen von Zeitstempeln aus den verarbeiteten Registry-Hives werden zeitgleich der Ereignisliste hinzugefügt. All dies geschieht, wenn der Benutzer HTML-Vorschauen von Browser-Datenbank usw. erzeugen lässt und/oder interne Zeitstempel in Dateien als Ereignisse ausgeben lässt.

6.3.4 Erkundung von Archiven

Mit einer forensischen Lizenz kann der Inhalt von **ZIP-, RAR-**, ARJ-, GZ-, TAR-, 7Z-, CAB- und BZIP-**Archiven** in den Datei-Überblick aufgenommen werden, so dass Dateien in solchen Archiven separat aufgelistet, eingesehen, nach Stichwörtern durchsucht werden können usw., in ihrem dekomprimierten Zustand, sofern die Archive nicht verschlüsselt sind. Theoretisch gibt es kein Limit für die Verschachtelungstiefe, die verarbeitet werden kann (also Archive in Archiven in Archiven...). Wenn die Dateien in einem Archiv verschlüsselt sind, werden sie mit einem „e“

in der Attributspalte gekennzeichnet und das Archiv selbst mit „e!“. Das ermöglicht es, solche Dateien effizient mit dem Attributfilter zu finden.

Dokument-Dateien von MS Office 2007/2010/2013, LibreOffice, OpenOffice und iWork sind technisch gesehen typischerweise ebenfalls Zip-Archive, und werden standardmäßig auf dieselbe Art verarbeitet. Sie können solche Dateien von der Verarbeitung ausnehmen, wenn Sie oder die Empfänger etwaiger von Ihnen erstellter Datei-Container die Dokumente lediglich als Ganzes einsehen möchten, und keine eingebetteten Bilder oder XML-Dateien einzeln, und auch keine Metadaten aus diesen XML-Dateien zu extrahieren brauchen und etwaige verschachtelte Dokumente (in Dokumenten eingebettete andere Dokumente) sofern gewünscht selbst erkennen können. Es gibt noch viele weitere Dateitypen, die technisch gesehen Untertypen von Zip sind und nur optional verarbeitet werden. Zip-Untertypen, deren Inhalte normalerweise irrelevant sind, sind z. B. .jar, .apk und .ipa, aber spezielle Interessengruppen wie Malware-Ermittler sehen das evtl. anders. Die Entscheidung liegt bei Ihnen.

Für jede "Familie" von Datei-Archiven (general purpose, Office, special interest, ...) können Sie festlegen, ob solche Archive in den Verzeichnisbaum des Falldatenfensters eingebaut werden sollen, sobald ihr Inhalt in den Datei-Überblick aufgenommen wurde, so als ob sie Verzeichnisse wären.

X-Ways Forensics versucht, Zip-Bomben sowie rekursive Zip-, GZ- und andere Archive zu erkennen und sich vor ihnen zu schützen. Der Schutz besteht darin, dass die Verarbeitung nach einer gewissen erreichten Verschachtelungstiefe abbricht, sobald die bösartige Natur des Archivs erkannt wurde. Auf diese Art erkannte Archive werden als bereits verarbeitet gekennzeichnet und mit einem speziellen internen Vermerk ausgestattet. Wenn Sie anschließend manuell noch in tiefere Ebenen vordringen möchten, ist das möglich, indem Sie das innerste erreichte Archiv als noch zu verarbeiten markieren (durch Drücken von STRG+ENTF) und dann den Erkunden-Befehl im Kontextmenü auf das Archiv anwenden.

Beachten Sie, dass Sie zur korrekten Verarbeitung von Dateinamen mit Nicht-ASCII-Zeichen in Zip-Archiven in den Falleigenschaften erst die richtige Codepage angeben müssen. Z. B. ist das für Zip-Archive, die unter Linux erstellt wurden, wahrscheinlich UTF-8. Für Zip-Archive, die unter Windows erstellt wurden, ist das i. d. R. eine regionale Codepage. In mehrere Einzeldateien aufgeteilte Zip-Archive im Stil von PKZIP/WinZip und 7-Zip werden unterstützt, außerdem aufgeteilte 7z-Archive, aber keine anderen Arten segmentierten/dateiübergreifenden Archive.

Extended timestamps from the extra field in zip records are extracted and presented in the time-stamp columns based on Apple specifications, which is not always how these timestamps were meant. An alternative interpretation can be seen for each zip record in Details mode when select-ing the zip archive. The latter interpretation shows these timestamps with the "UT" prefix and tries to recognize the actual format variant, for example that used in GrayKey collections, and from GrayKey collection also extracts an an additional type of timestamp (a record change time-stamp). The alternative interpretation of extended timestamps can also be made available in the directory browser. This is an option in Options | Volume Snapshot. That kind of processing needs some more time.

Zip-, RAR- und 7Z-Archive können auch verarbeitet werden, sofern das Passwort bekannt ist oder erraten werden kann. X-Ways Forensics probiert alle Passwörter aus, die in der

Passwortsammlung des aktuellen Falls aufgelistet sind. Die fallspezifische Passwortsammlung kann von den Falleigenschaften aus eingesehen und bearbeitet werden. Es handelt sich um eine Datei namens "Passwords.txt" im Fallverzeichnis, codiert in UTF-16. Praktisch alle Unicode-Zeichen werden unterstützt, incl. Leerzeichen, chinesische Zeichen usw. Bei Passwörtern macht Groß- und Kleinschreibung i. d. R. einen Unterschied. Wenn die Sammlung das richtige Passwort für eine bestimmte Datei enthält, merkt sich X-Ways Forensics dieses Passwort in den extrahierten Metadaten der Datei und entnimmt es künftig bei Bedarf direkt von dort statt aus einer Passwortsammlung, um Dateien in dem Archiv zu lesen. Alternativ können Sie das Passwort für eine bestimmte Datei auch manuell hinterlegen, indem Sie die extrahierten Metadaten der Datei bearbeiten. Sie müssen dazu lediglich wissen, dass vor das Passwort das Wort "Password: " gestellt werden muss (mit Doppelpunkt und Leerzeichen). Dateien in verschlüsselten Datei-Archiven werden nicht als verschlüsselt dargestellt ("e"-Attribut) und gehandhabt, wenn das richtige Passwort zu dem Zeitpunkt, wenn die Dateien dem Datei-Überblick hinzugefügt werden, verfügbar ist. Die Archive selbst werden immer noch mit dem "e!"-Attribut gekennzeichnet. RAR- und 7Z-Archive, in denen nicht nur die Datei-Inhalte, sondern auch die Dateinamen verschlüsselt sind, werden derzeit nicht unterstützt.

6.3.5 E-Mail-Extraktion

Eine forensische Lizenz erlaubt es, **E-Mails und Dateianhänge** von E-Mails einzeln aufzulisten und zu untersuchen, die enthalten sind in Dateien folgender Formate: Outlook Personal Storage (.pst), Offline Storage (.ost), Exchange (.edb, Exchange 2010 und älter unterstützt, 2010 noch in der Testphase), Outlook Message (.msg), Outlook Template (.oft), Outlook Express (.dbx), bestimmte Datenbanken von Microsoft Outlook for Mac (.olm), Kerio Connect (solche store.fdb-Dateien, die wie gewöhnliche PST/OST verarbeitet werden können), AOL-PFC-Dateien, Mozilla Mailbox (inkl. Netscape und Thunderbird), Generic Mailbox (mbox, Unix mail Format), MHT Web Archive (.mht), winmail.dat = TNEF-Dateien. Standardmäßig versucht X-Ways Forensics, E-Mails aus solchen Dateien zu extrahieren, deren Typ in dieser Liste erscheint:
pst,ost,edb,dbx,pfc,mbox,eml,emlx,mht,mim,msg,olk14msgsource,olk14message,olk14msgattach,olk15msgattach,olk15msgsource,olk15message,oft,mbs,tnef,olm

E-Mails werden i. d. R. in Form von .eml-Dateien extrahiert. Um bequem alle extrahierten E-Mails aus allen E-Mail-Archiven (und auch verarbeitete ursprüngliche .eml-Dateien) aufzulisten, wird empfohlen, rekursiv zu erkunden und den Attribut-Filter zu verwenden (nicht den Typ- oder Kategorie-Filter). Tief verschachtelte E-Mails (E-Mails, die als Attachment weitergeleitet wurden und deren Elter auch selbst wieder als Attachment weitergeleitet wurden) werden im Fall von MBOX-Archiven aus technischen Gründen direkt als Unterobjekte der Haupt-E-Mail dargestellt. There is an unlabelled, but tooltipped checkbox that will make X-Ways Forensics name MSG files after the e-mail subject when extracting e-mail messages and attachments from them. That could be useful when dealing with generically named MSG files.

Absender und Empfänger werden für extrahierte E-Mails sowie deren Datei-Anhänge in den entsprechenden Spalten des Verzeichnis-Browser angezeigt. Sie können sowohl nach Erzeugungs- und Änderungsdatum als auch Absender und Empfänger filtern.

If e-mail messages have a Sender: line in addition to a From: line, then the sender according to

the Sender: line is shown in the Sender column of the directory browser additionally, after the From: sender, if actually different. They are delimited by spaces and a pipe (|). For example, an English language MS Outlook shows such e-mails as having been sent "on behalf of" someone else (by the Sender: sender on behalf of the From: sender). You can filter for such e-mails by entering a pipe as a substring for the Sender column. Analogously, different kinds of recipients (To:, Cc:, and Bcc:) are delimited by pipes in the Recipient column.

Alle Datei-Anhänge und eingebettete Dateien werden, sofern im E-Mail-Archiv gefunden (Ausnahme z. B. AOL PFC), ebenfalls extrahiert, und werden im Datei-Überblick normalerweise zu Unterobjekten der jeweils enthaltenden E-Mail. Alle extrahierten E-Mails und Anhänge liegen tatsächlich im Metadaten-Verzeichnis des Asservats und benötigen u. U. viel Plattenplatz.

Die E-Mail-Extraktion aus PST kann passwortgeschützte PST-Dateien ohne Angabe des Passworts verarbeiten! Sie unterstützt die folgenden Codepages für codierte PST-Dateien: ISO8859-1, ISO8859-2, ISO8859-3, ISO8859-4, ISO8859-5, ISO8859-6, ISO8859-7, ISO8859-8, ISO8859-9, ISO8859-10, ISO8859-11, ISO8859-13, ISO8859-14, ISO8859-15, ISO8859-16, koi8-r, koi8-u, 1250, 1251, 1252, 1253, 1254, 1255, 1256, 1257, 1258, 874, UTF16, UTF32, UTF8.

In älteren AOL-PFC-Dateien können Bilder auf eine besondere Weise in E-Mails eingebettet sein. Dann wird die E-Mail zwar mit einer Büroklammer gekennzeichnet, aber das Bild wird nicht separat als Datei extrahiert. Solche Bilder, wenn JPG oder PNG, kann man aber finden, indem man X-Ways Forensics JPGs und PNGs auch aus *.pfc extrahieren lässt.

Some advantages of the .eml format for output: E-mail messages output as .eml files are represented as simple and as authentic and universal as it gets. They are easy to understand, clearly structured into header and body, and extremely easy to completely view in a variety of simple programs (e.g. text editor, word processing, Internet browser, free e-mail clients like Thunderbird and Windows Mail). No commercial software like MS Outlook needed is needed to view .eml files. .eml is the "natural" format of e-mail, just like a raw image is the natural format of a disk image, if you even want to call it a "format" (actually it has no additional format specifications, it's just a plain representation of the data that it should represent). An .eml file contains the complete original metadata of the e-mail message, fully intact, exactly as it was sent and delivered. You have complete control over the file if you copy it out for someone else, can see all data, can verify that no unintended data made it into the file. You can easily redact any text in the body manually with a simple text editor, redact any metadata in the header, easily retroactively remove any attachment using a simple text editor if needed, all of which is impossible to do with a complex proprietary binary file format such as MSG. The general format of .eml files can be understood by anyone, and it is simply a text file. The format of MSG files can be understood only with a computer science or programming background, and learning it takes a lot of time. Redacting e-mail data hidden in MSG files is difficult.

A side task of e-mail processing is to extracted files from e-mail related MIM archives and make them accessible as child objects in the volume snapshot in plain binary form.

6.3.6 Eingebettete Dateien aus diversen Dateitypen hervorholen

Forensische Lizenz. Hiermit können Sie Dateien diverser Typen, die in Dateien diverser anderer Typen eingebettet sind, automatisch "herausmeißeln" (carven), durch eine auf Byte-Ebene durchgeführte Datei-Header-Signatur-Suche innerhalb von bestimmten Dateien. Dies ist gut machbar, wenn die äußere Datei (die Trägerdatei) intakt ist und die eingebettete Datei in der Trägerdatei nicht fragmentiert gespeichert ist. Ansonsten erscheinen die extrahierten Dateien u. U. als defekt. Insbesondere sucht diese Funktion JPEG- und PNG-Bilder, sogar JPEG-Bilder in anderen JPEG-Dateien (solchen, die Miniaturansichten von sich selbst enthalten). Auf diese Weise gefundene Dateien erhalten einen generischen Namen (»Embedded 1...jpg«, »Embedded 2...png«, o. ä.). Miniaturansichten in HEIC-Dateien werden im JPEG-Format ausgegeben.

Diese Funktion extrahiert außerdem .emf-Dateien, die in mehrseitigen Ausdrucken (.spl-Spool-Dateien) enthalten sind. .spl-Dateien, die nur eine einzige .emf-Datei enthalten, können direkt mit der Viewer-Komponente eingesehen werden. Des Weiteren auf diese Weise extrahiert werden .lnk-Verknüpfungen aus Jump-Lists der Art .customdestinations-ms.

Spezielle interne Algorithmen extrahieren ordentlich, d. h. unter Beachtung der Datenstrukturen im jeweiligen Dateiformat und sogar wenn fragmentiert, .lnk-Verknüpfungen aus Jump-Lists der Art .automaticdestinations-ms, Dateien jeglichen Typs aus .doc/.ppt-OLE2-Verbundsdateien, Browser-Cache-Dateien von Safari, Firefox (basierend auf “_CACHE_MAP_”-Dateien, Norton-Backup-Dateien (N360 backup, .nb20) sowie Windows.edb-Datenbanken (aus letzteren oft sogar E-Mails), und als Base64 eingebettete Bilder aus VCF-Dateien (elektronische Visitenkarten).

Browser-Caches von Google Chrome werden basierend auf den "index"-Dateien verarbeitet, with support for multiple streams of the same cache entry: The HTTP response (named .chrome1) is output as well as, if present, as are compiled JavaScript entries (.js1). If a no-cache directive was sent by the web server, at least the HTTP response is still cached. In Preview mode you can see a special representation of HTTP responses. Chrome caches can now also be processed if their index is not available, for example if cache fragments have been carved or if the cache was partially deleted or corrupted. It may be possible in some cases that a better extraction result can be achieved without the index, even if it is present. To try that, if the index has not been processed before, you can have the uncover function process "data_4" files and omit the index. data_4 is part of the optional "special interest" group.

Außerdem Miniaturansichten aus thumb*.db-Dateien, Google's Picasa 3 image organizer and viewer software (thumbindex.db and related files), Photoshop thumbnail caches (Adobe Bridge Cache.bc), Canon ZoomBrowser thumbnail collections (.info), and Paint Shop Pro caches (.jbf). Thumbnails in bestimmten alten "thumbs.db"-Dateien können nicht korrekt angezeigt werden. Solche thumbs.db-Dateien werden mit dem Vermerk "Unsupported thumbs.db" versehen und können z. B. mit dem frei verfügbaren Programm "DM Thumbs" von GreenSpot Technologies Ltd. eingesehen werden. Thumbcache*.db files of Windows Vista and later are targeted indirectly if thumbcache_idx.db is in the mask and if that file is available in the same directory. That speeds up the extraction and avoids the output of numerous duplicate thumbnails (only the highest available resolution is output). If thumbcache_idx.db is in the mask, that also means that thumbcache*.db files that are specifically selected or tagged for processing are not processed unless the thumbcache_idx.db file is also selected/tagged.

Außerdem from PDF documents any kinds of files that are marked as embedded plus JPEG and JPEG 2000 plus Acrobat form files in XML format plus JavaScript objects (the latter may make it easier to determine whether a PDF file should be considered malware), individual cookie files from Firefox and Chrome SQLite databases, also data blocks embedded as Base64 in XML-formatted PLists (.plist) and raw data blocks embedded in binary PLists (.bplist) are extracted as separate child objects when refining volume snapshots. It is recommended to verify file types at the same time so X-Ways Forensics can distinguish between traditional (XML-formatted) PLists and binary PLists (BPLists). Many PLists do not have a .plist extension and need to be identified as PLists first. Since the type of the embedded data is not identified by the PList as such, the output also benefits from a simultaneous file type verification. Nested PLists (PLists embedded in PLists) will also be identified and processed recursively. Another child object created for PLists represents parsed text in a human-readable way and serves as a preview of the PList itself.

Also reconstructs e-mail messages and extracts contact and account information from the Livecomm.edb database, which is used by the Windows Mail client (Windows 7 and newer), and contacts from Windows Live Mail contacts.edb database, also contacts from Windows Live Messenger's contacts.edb database.

You can also uncover various potentially relevant resources in 32-bit and 64-bit Windows PE executables (programs and libraries) as child objects, in particular RCDATA, named objects, bitmaps, icons and manifests. Useful for example for malware analysis. This does not happen automatically, only if you specifically target executable files via a suitable series of file masks.

Fully Base64-encoded files in the volume snapshot, provided that they have "b64" in the Type column can be automatically decoded, and the result is output in binary as (surprise) a child object.

Nicht zuletzt kann diese Funktion auch noch hiberfil.sys-Dateien von Windows XP bis Windows 7, 32 und 64 Bit, dekomprimieren und das Ergebnis automatisch dem Fall als Roh-Speicher-Dump hinzufügen. Schlupf von hiberfil.sys-Dateien (komprimierte Daten von der vorherigen Verwendung der Datei, wie sie nahe am Ende der Datei gefunden werden können, wenn die letzte Verwendung eine höhere Kompression erzielt hat als die vorherige Verwendung) wird in dekomprimierter Form als Unterobjekt bereitgestellt.

Generell werden alle von dieser Funktion produzierten Dateien dem Datei-Überblick in Form von Unterobjekten der jeweiligen Trägerdatei hinzugefügt, in der sie gefunden wurden. Dateien, die kleiner sind als 65 Bytes, werden aus Zeitersparnisgründen nicht angefasst.

Two separate file masks are maintained for uncovering embedded data in various file types. The second mask is optional and labelled as "special interest". For example malware investigators may choose to also process executable files that way when needed. You may prepend any element of a mask with a colon to temporarily exclude it, but keep it in the list for future reference. E.g. :*.jpg means *not* files with jpg as the extension or type.

In Dateien eines Typs, für den kein spezieller interner Extraktionsalgorithmus existiert, wird per Carving nach eingebetteten Dateien der Typen gesucht, die in “File Header Signatures Search.txt” mit dem Flag “e” gekennzeichnet sind. Das bedeutet, dass Sie aus noch viel mehr

Dateitypen Daten hervorholen können als den voreingestellten!

Extra precautions are taken to not produce duplicates of files that were already carved by the file header signature search. More precisely, the output of this function will replace corresponding carved files in the volume snapshot. The internal IDs of the carved files will remain the same, but additional metadata may become available (such as path/representation as a child object of the parent file, presumed original filename, more correct file size etc.). With the usual settings, this affects a considerable number of sector-aligned files.

Datei-Header-Signatur-Suche in nicht obig behandelten Dateien

A separate sub-operation optional allows you to freely carve any kind of file within any file that is not processed by the first sub-operation. By default, file types with the "e" flag are selected for that. Use great caution to avoid delays and copious amounts of garbage files (false positives) and duplicates. Please apply this new function very carefully and only with a good reason to specifically targeted files only, such as swap files or storage files in which backup application concatenate other files without compression, not blindly to all files or random files. Remember with great power comes great responsibility.

Signatures marked with the "E" flag (upper case) are never carved within other files, to prevent the worst effects, for example MPEG frames carved within MPEG videos, zip records carved within zip archives, .eml, .html and .mbox files carved within e-mail archives, .hbin registry fragments carved within registry hives. If you know what you are doing, of course you could remove the E flag.

There is an option to apply the carving procedure recursively, that means to files again that were already carved within other files. This can lead to many duplicates if the outer file at level 1 is carved too big so that files can be carved in it that were also carved at level 0 (the original file).

For situations where you want to carve embedded files that are not aligned at 512-byte boundaries in the original file, you may make use of the extensive byte-level option. Files are never carved in $MFT.

The default settings will make X-Ways Forensics conduct a file header signature searches at the byte level within pagefile.sys files, to find e-mail fragments, .lnk shortcut files, pictures, etc.

An unlabeled checkbox at the bottom allows you to turn on the verbose report mode that makes you aware of files that were previously carved at the general partition/volume level (i.e. by the File Header Signature Search) and that were output in the virtual directory for carved files, that have since been turned into child objects of other files because they seem to logically belong to them and are contained in them.

6.3.7 Standbilder aus Video erzeugen

Eine forensische Lizenz erlaubt es, **vereinzelte Standbilder aus Video**-Dateien im JPEG-Format

zu **erzeugen**. Dies geschieht entweder in einem benutzerdefinierten Zeitabstand (z. B. alle 20 Sekunden), die dynamisch von der Spieldauer der Videos abhängen kann, oder Sie können sich für eine fixe Anzahl von Standbildern pro Video entscheiden (1-255), egal wie lang die Spieldauer des Videos ist. While fixed-length intervals result in number of stills that grows proportionally with the play length, the fixed absolute number limits your workload if you are going to look at all stills in the gallery, and also decreases the time to process long videos, but of course at the cost of being less thorough and an increased risk of missing something should any suspect hide relevant content somewhere within an innocuous video. X-Ways Forensics versucht eine fixe Anzahl von Standbildern gleichmäßig aus dem Video zu extrahieren, um einen ausgewogenen und repräsentativen Eindruck von ihm zu vermitteln.

Diese Funktionalität wird angewandt auf Dateien, deren Typ auf die angegebene Reihe von Dateimasken passt. Erfordert ein externes Programm (MPlayer), und kann nur auf Asservate angewandt werden. Bilder können aus allen Video-Formaten und Codecs extrahiert werden, die von MPlayer unterstützt werden. Nützlich, wenn Sie viele Videos auf unangemessenen oder illegalen Inhalt hin überprüfen müssen (z. B. Kinderpornographie, ideologische Hetze oder terroristische Anleitungen). Dank der Zeitintervalle verpassen Sie keine relevanten Teile, die in der Mitte von Urlaubs- oder Geburtstagsfeier-Videos versteckt wurden.

Das Extrahieren von Bildern reduziert die Datenmenge erheblich, und das Betrachten der Bilder in der Galerie ist viel schneller, effizienter und bequemer als ein Video nach dem anderen anzusehen. Der potenziell zeitaufwendige Extraktionsprozess kann unbeaufsichtigt ablaufen, z. B. über Nacht, vor der Begutachtung durch den Ermittler.

Auch nützlich, wenn Sie extrahierte Bilder in einem Bericht unterbringen möchten. Das erste extrahierte Bild kann optional gleichzeitig als Vorschau für das Video im Vorschaumodus und in der Galerie dienen. ASF/WMV-Videos, die mit DRM geschützt sind, können nicht verarbeitet werden und werden konsequenterweise in der Attributsspalte mit e! gekennzeichnet. Dass Sie während der Extraktion gelegentlich kurz Sound aus den Videos hören, ist normal. Bitte schalten Sie die Tonwiedergabe Ihres Computers ab, wenn Sie dies vermeiden möchten. Beachten Sie, dass Sie bei einem kleinen Zeitintervall nicht notwendigerweise zusätzliche Bilder erhalten. Das hängt von der Art der Codierung/Kompression des Videos ab. If for example one particular video was encoded in such a way that it contains an I-frame (full image) only every 8 seconds and all the frames in between just describe the changes to reduce data, then you can expect no smaller still intervals than 8 seconds. That's because this function is meant to work fast and does not reconstruct exact frames at exact time indexes. If you need more detail, you can export all frames using the directory browser context menu. Identische Standbilder werden bei der Extraktion mit MPlayer nicht in den Datei-Überblick übernommen.

Once JPEG pictures have been exported from videos, the videos can optionally be dynamically represented in the gallery, with all extracted stills, showing them stills in a loop, to give a much more complete impression of the contents of videos without further user interaction (without having to explore them). Thus an alternative efficient way to review a large number of videos is this: Explore recursively, filter for videos, sort in descending order by number of child objects (so that videos with a similar number of stills are shown together), and activate Gallery mode. Watch the various video stills for each video. Proceed to the next gallery page when you are confident that no incriminating videos are represented on the current page, for example when all stills have been shown, which you will know is the case when the gallery has rotated back to the first still

for each video.

A small amount of metadata is extracted from videos when exporting stills, usually coding/compression format, resolution, bits per pixel, frames per second, data rate per second for video data. That is in addition to the metadata that is provided by the regular metadata extraction.

6.3.8 Bildanalyse und -verarbeitung

Des Weiteren ermöglicht es eine forensische Lizenz, den **Hautfarben**anteil in Bildern in Prozent zu berechnen sowie **Schwarz-Weiß-Bilder** zu **erkennen**. Dies kann für die Dateitypen JPEG, PNG, GIF, TIFF, BMP, PSD, HDR, PSP, SGI, PCX, CUT, PNM/PBM/PGM/PPM, ICO geschehen. Wenn ein Ermittler nach Spuren von Kinderpornographie suchen muss, kann das Sortieren aller Bilder nach Hautfarbenanteil (HFA) absteigend die Arbeit stark beschleunigen, weil es das Prüfen der großen Masse von Bildern mit 0-9% HFA (z. B. zig tausende kleine Grafiken im Browser-Cache) und die am wahrscheinlichsten belastenden Bilder ganz oben in der Liste angezeigt werden. Bitte beachten Sie, dass es falsche Treffer geben kann, also hautartige Farben auf einer Oberfläche, die keine Haut ist. Das Erkennen von Schwarz-Weiß- und Graustufen-Bildern ist nützlich, wenn nach elektronisch gespeicherten Faxen und eingescannten Dokumenten gesucht werden soll. Bilder, die nicht erfolgreich auf ihre Farbzusammensetzung überprüft werden können, da z. B. zu groß oder defekt, werden mit einem Fragezeichen aufgelistet. Besonders kleinformatige Bilder (Höhe oder Breite nicht größer als 8 Pixel, oder Höhe *mal* Breite nicht größer als von Ihnen angegeben) werden als unerheblich klassifiziert, basierend auf der Annahme, dass sie weder belastenden pornographischen Inhalts noch Dokumente sein können.

For large JPEG, PNG, GIF and TIFF files, at the same time when analyzing the colors in the pictures during volume snapshot refinement, X-Ways Forensics can optionally also create thumbnails in advance for much quicker display updates in Gallery mode later. Internal thumbnails are only created if no original thumbnails are embedded in the files and extracted at the same time, and they are actually utilized for the gallery only if auxiliary thumbnails are enabled (see Options | General). It is possible to specify your preferred resolution (maximum width or height in pixels) and quality (JPEG compression factor) of the thumbnails. However, the maximum amount of data that can be stored in the volume snapshot for a thumbnail is limited, to 64 KB, so if a generated thumbnail gets larger than that, X-Ways Forensics will automatically reduce the user-defined resolution accordingly. To discard all internal thumbnails, but keep the computed skin color percentages, you may delete the file "Secondary 1" in the "_" subdirectory of an evidence object behind X-Ways Forensics' back, i.e. when the evidence object is not currently open.

Excire: Bildanalyse mit künstlicher Intelligenz (separates Kapitel)

Es gibt einen kleinen Schalter auf der rechten Seite, der eine Hand zeigt. Ein Klick auf diesen Schalter zeigt die Steuerungsmöglichkeiten für PhotoDNA, auch wenn diese Funktionalität für Sie nicht verfügbar ist, um Ihnen eine Vorstellung davon zu geben, wie dieses Modul verwerdet werden kann. PhotoDNA wird Benutzern in Strafverfolgungsbehörden kostenlos zur Verfügung gestellt.

If you have an internal PhotoDNA hash database, known photos can be recognized automatically even if visually altered. If you select more strict matching (allow less variation in a picture), the process can be noticeably faster in huge databases. Resulting matches can be seen and filtered in the combined Analysis column (only 1 match per file). Multiple matches for the same picture can optionally be output as labels. This is useful if you need to see *all* matches and/or if you wish to see PhotoDNA matches in the same place as ordinary hash database matches, which can also be output as labels. Please note that photos that are recognized via PhotoDNA already are not additionally checked for the amount of skin tone. PhotoDNA hash values are computed and matched only if the picture contains a total number of pixels that is larger than a user-defined minimum (width times height). This avoids database look-ups that can be time-consuming in very large PhotoDNA hash databases and typically have no benefit for small garbage pictures. The minimum dimensions allowed as a condition are 50x50 pixels. The PhotoDNA algorithm intrinsically requires a certain minimum number of pixels to provide meaningful results. If you select the lowest possible strictness level for matching (level 1), you will be asked whether you are really certain, as that level is known to occasionally deliver false matches. That level is offered in X-Ways Forensics only because it is provisionally suggested by the original developers of PhotoDNA. The recommended and default level in X-Ways Forensics is level 3.

It is possible to more conveniently match pictures against the PhotoDNA hash database again, for example after having added some hash values to the database or after having assigned hash values to different categories, thanks to a checkbox simply labelled "Again". You can still uncheck the "Already done?" check box for the whole picture analysis and processing operation to also discard the results of the skin color computation and precomputed thumbnails and regenerate both plus the PhotoDNA matches from scratch. Please note that with the "Again" option when re-using previously computed PhotoDNA hashes, changes to the state of the check box "Recognize pictures even if mirrored" have no effect. That means if previously unchecked when hash values were computed for the first and stored in the volume snapshot, checking it later when re-using the stored hash values won't do any good.

Matching pictures against the PhotoDNA hash database another time is much faster if during a previous run you have X-Ways Forensics store the computed PhotoDNA hashes in the volume snapshot. Saves the time to read the files from the disk/image again and to decode/decompress the JPEG data or other formats again (time-consuming for high-resolution photos) and to recompute the hash values. Please note that PhotoDNA hashes require considerably more drive space than ordinary hashes. Also, more than one PhotoDNA hash may be required for just one picture. It is recommended to store the hash values in the volume snapshot for future fast re-matching only if you expect your PhotoDNA hash database to change during processing of a case, for example if it is likely that you or your colleagues discover further relevant pictures in that case, forcing you to search for other copies of these pictures. Files that got their PhotoDNA hash value(s) stored in the volume snapshot have more information in Details mode: The actual hash value(s) can be seen, as well as all the matches along with their respective accuracies.

When computing PhotoDNA hash values and storing the hashes for deduplication and fast re-matching, X-Ways Forensics now also automatically compares embedded thumbnails to their parent files. If the difference is noticable, that will be brought to the user's attention with two Vermerken, "Thumbnail discrepancy" and "Thumbnail notable (data corrupt/incomplete)", where the latter means that there is a difference most likely just because the parent file is corrupt or incomplete. (The thumbnail, which requires little storage space and is located near the start of the

file, could be unaffected and therefore helpful.) The former could indicate that someone has retroactively altered /redacted the full resolution picture and left the embedded thumbnail as it was.

To discard stored hash values you can either take a new volume snapshot, or alternatively you may delete the file "PDNA" in the "_" subdirectory of the evidence object, where the volume snapshot is internally stored.

Wenn beim Hash-Abgleich sowohl Treffer mit einer herkömmlichen Hash-Datenbank als auch mit der PhotoDNA-Hash-Datenbank erzielt werden, die unterschiedliche Kategorisierungen haben, erhält die "schwerwiegenderen" Kategorie Vorrang bei der Kategorisierung der Datei: unbekannt < irrelevant < unkategorisiert < verdächtig. The option to mark a file as already viewed when it gets categorized as irrelevant is now applied to the combined result of ordinary hash database and PhotoDNA hash database matching.

6.3.9 Dokumente über FuzZyDoc identifizieren

The so-called **FuzZyDoc™** technology can help you to identify known documents (word processing documents, presentations, spreadsheets, e-mails, plain text files, ...) with a much more robust approach than conventional hash values. Even if a document was stored in a different file format (e.g. first PPT, then PPTX, then PDF), it can still be recognized. Internal metadata changes, e.g. after a "Save as" or or after printing (which may update a "last printed" timestamp), do not prevent identification either. Very often even if text was inserted/removed/reordered/revised, a document can still be recognized. This is achieved by using fuzzy hashes.

FuzZyDoc hash values are stored in yet another hash database in X-Ways Forensics. Hash sets based on selected documents can be added to the FuzZyDoc database exactly like hash sets can be created in ordinary hash databases, and the FuzZyDoc hash database can also be managed in the same dialog window as the other hash databases. For each selected document you can create 1 separate hash set, or you can create 1 hash set for all selected documents. Up to 65,535 hash sets are supported in a FuzZyDoc hash database. You have the option to export, import and merge FuzZyDoc hash sets. The result of the export can be used with the import function or alternatively is also valid as a stand-alone database by itself.

FuzZyDoc is available to all users of X-Ways Forensics and X-Ways Investigator (i.e. not only law enforcement like PhotoDNA). FuzZyDoc should work well with documents in practically all Western and Eastern European languages, many Asian languages (e.g. Chinese, Japanese, Korean, Indonesian, Malay, Tamil, Tagalog, ..., but not Thai, Divehi, Tibetan, Punjabi, ...), and Middle Eastern languages (e.g. Arabic, Hebrew, ..., but not Pashto, ...). Note that numbers in spreadsheet cells are not exploited by the algorithm, only text. Note that only files with a confirmed or newly identified type will be matched against the FuzZyDoc hash database. For that reason, file type verification is applied automatically when FuzZyDoc matching is requested.

Documents whose contents are largely identical (e.g. invoices created by the same company with the same letterhead) are considered similar by the algorithm even if important details change (billing address, price, product description), depending on the amount of identical text. That

means that if you have 1 copy of an invoice of a company, matching against unknown documents will easily identify other invoices of the same company. For every document that is matched against the database, up to 4 matching hash sets are returned, and the 4 best matching hash sets are picked for that if more than 4 match. For every matching hash set, X-Ways Forensics also presents a percentage that roughly indicates to what degree the contents of the document match the hash set. Two different percentage types are available. A percentage based on the total text in the processed document gives you an idea of how much of the text in the document is known/was recognized, whereas a percentage based on the text represented by the hash set gives you an idea of how closely a document resembles the original document that the hash set is based on (makes sense only if you generate 1 hash set per document, i.e. do not combine multiple documents in 1 hash set). The matching percentage does not count characters one by one, and it works only on documents that actually make sense, not on small test files that only contain a few words.

Before matching files against the FuzZyDoc hash database (a new operation of Specialist | Refine Volume Snapshot), you can specify which types of files you would like to analyze, and you can unselect hash sets in the database that you are temporarily not interested in. Note that processing less files (e.g. by specifying less file types in the mask) of course will require less time, proportionally, but selecting less hash sets for matching as such does not save time. You may specify a certain minimum percentage that you require for matches (15% by default) to ignore insignificant minor similarities. That option is not meant to save time either.

In order to re-match all documents in the volume snapshot against the FuzZyDoc hash database, please remove the checkmark in the "Already done" box first. Otherwise the same files will not be matched again, for performance reasons. Re-matching the same files may become necessary not only if you add additional hash sets to your FuzZyDoc database, but also if you delete hash sets, as that invalidates some internal links (if that happens, it will be shown in the cells of the result column).

Matches with the FuzZyDoc database are presented in the same column as PhotoDNA matches and skin color percentages, called "Analysis". A filter for FuzZyDoc matches is available. FuzZyDoc should prove very useful for many kinds of white collar crime cases, most obviously (but not limited to) those involving stolen intellectual property (e.g. software source code) or leakage of classified documents.

6.3.10 Verschlüsselungsdetektion

Eine forensische Lizenz erlaubt es, optional **dateiformatspezifische und statistische Verschlüsselungstests** durchzuführen. Mit einem Entropietest werden alle existierenden Dateien, die mind. 256 Byte groß sind, darauf geprüft, ob sie vollverschlüsselt sind, d. h. vom ersten bis zum letzten Byte. Wenn der Test positiv ist (die Entropie einen bestimmten Schwellwert überschreitet), wird die betreffende Datei mit dem Hinweis „e?“ in der Attributsspalte versehen, um anzuzeigen, dass sie möglicherweise besondere Aufmerksamkeit verdient. Typisches Beispiel: Verschlüsselte Container-Dateien, die von Verschlüsselungsprogrammen wie TrueCrypt, PGP Desktop, BestCrypt oder DriveCrypt als Laufwerksbuchstabe geladen werden können. Der Entropietest wird nicht angewandt auf Dateien vom Typ ZIP, RAR, TAR, GZ, BZ, 7Z, ARJ, CAB, JPG, PNG, GIF, TIF, MPG oder SWF, von denen bekannt ist, dass sie intern komprimiert sind und damit

eine ähnlich hohe Entropie aufweisen wie Zufallsdaten und verschlüsselte Daten. Dieser Test wird nicht benötigt, um festzustellen, dass Dateien auf NTFS-Dateisystemebene oder innerhalb von Archiven verschlüsselt sind.

Der zweite Test prüft Dateien mit den Endungen/Typen .doc (MS Word 4...2003), .xls (MS Excel 2...2003), .ppt, .pps (MS PowerPoint 97-2003), .mpp (MS Project 98-2003), .pst (MS Outlook), .docx (MS Word 2007...2010), .xlsx (MS Excel 2007...2010), .pptx, .ppsx (MS PowerPoint 2007-2010), .odt (OpenOffice2 Writer), .ods (OpenOffice2 Calc) und .pdf (Adobe Acrobat) auf dateiformatspezifische Verschlüsselung; MS-Office-Dokumente auch auf Schutz durch angewandtes digitales Rechtemanagement (DRM). Wenn der Befund positiv ist, werden diese Dateien mit dem Hinweis „e!“ in der Attributsspalte versehen. Dieser Test erfordert, dass die separate Viewer-Komponente aktiv ist. X-Ways Forensics probiert auch automatisch die Passwörter in der Passwortsammlung des aktuellen Falls auf solche Dateien anzuwenden und merkt sich das passende Passwort, sofern gefunden, in der Metadaten-Zelle der Datei, für die künftige Verwendung beim Einsehen oder der Vorschau der Datei und zu Ihrer Information.

Zusätzlich detektiert der Verschlüsselungstest mit eCryptfs (dem Enterprise Cryptographic File System für Linux in den Implementationen für Ubuntu 8.10, 9.04, 9.10 und 10.04). Solche Dateien werden in der Attributspalte mit „E“ gekennzeichnet, genau wie EFS-verschlüsselte Dateien in NTFS.

6.3.11 Indexierung

Verfügbar nur mit forensischer Lizenz. In der Informatik ist der Plural von Index Indexe, und nicht Indizes. Das zugehörige Verb heißt indexieren, und nicht indizieren. Die Indexierung erfasst die Daten mit derselben Logik wie eine logische Suche, mit den gleichen Vorteilen (s. dort).

Erstellt Indexe aller Wörter in allen oder bestimmten Dateien im Datei-Überblick, basierend auf den von Ihnen angegebenen Zeichen, basierend auf dem Unicode-Zeichensatz und/oder bis zu zwei von Ihnen anzugebende Codepages. Es ist möglich, bis zu drei solcher Indexe pro Asservat zu haben (z. B. kyrillische Zeichen indexiert in Unicode und zwei kyrillischen Codepages). X-Ways Forensics erlaubt Ihnen, bequem die Zeichen von mehr als 22 Sprachen für die Indexierung auszuwählen. Derzeit sind die meisten europäischen und viele asiatische Sprachen vordefiniert, z. B. Deutsch, Spanisch, Französisch, Portugiesisch, Italienisch, skandinavische Sprachen, Russisch, südslawische Sprachen, osteuropäische Sprachen, Griechisch, Türkisch, Hebräisch, Arabisch, Thailändisch und Vietnamesisch. Sie können jedes Zeichen einzeln angeben, oder Intervalle (z. B. a-zA-Z) wenn das Editierfeld mit "range:" beginnt. Hinter den Intervallen können wieder einzelne Zeichen folgen (z. B. a-zA-Zäöüß). Um den Bindestrich selbst mit zu indexieren (nicht empfohlen), geben Sie ihn als allerletztes Zeichen an.

Das Indexieren kann ein lang andauernder Prozess sein und ggf. viel Plattenplatz benötigen (grobe Faustregel mit Voreinstellungen bei üblichen Daten: 5-25% der Originaldatenmenge). Dafür erlaubt es Ihnen der Index, weitere Suchvorgänge äußerst schnell und spontan durchzuführen. Die Index-Dateien werden in Unterverzeichnissen des Metadaten-Ordner des betreffenden Asservats gespeichert. Die zu indexierende Datenmenge können Sie gezielt steuern.

Beachten Sie, dass der Index auf partitionierten Datenträgern wie z. B. physischen Festplatten ausschließlich die unpartitionierten Bereiche abdeckt, weil jede Partition ihren eigenen Index haben kann.

Wörter, die kürzer als ein von Ihnen bestimmtes unteres Limit sind, werden ignoriert. Je größer die Minimallänge von Wörtern in Zeichen, desto kleiner wird der Index und schneller die Indexierung. Voreinstellung als Minimum sind 4 Zeichen. Häufig vorkommende irrelevante Wörter kann man durch die Ausnahmeliste mit vorangestelltem Minuszeichen aus dem Index ausschließen (z. B. -und, wenn schon 3 Zeichen akzeptiert werden), was den Index verkleinert und das Indexieren beschleunigt. Je größer Sie die Spanne akzeptierter Wortlängen wählen, desto größer wird der Index und desto langsamer die Indexierung. Relevante Wörter mit 3 Buchstaben können Sie in die Ausnahmeliste mit vorangestelltem Pluszeichen aufnehmen (z. B. +xtc), so dass diese trotz Unterschreiten des Standard-Limits von 4 mit indexiert werden. Die Ausnahmeliste muss nicht alphabetisch sortiert sein. Wörter in der Ausnahmeliste, die länger als das von Ihnen angegebene obere Limit sind, werden im Index abgeschnitten. Die Ausnahmeliste kann keine Ausnahmen von der angegebenen Auswahl an zu indexierenden Zeichen definieren.

Groß- und Kleinschreibung wird bei der Indexierung optional unterschieden. Dies kann z. B. dann nützlich sein, wenn Sie den Index deswegen erstellen, um später eine Wortliste zum Zweck eines individuellen Wörterbuchangriffs auf ein Passwort zu exportieren.

Wenn Sie X-Ways Forensics Teilwörter in den Index mit aufnehmen lassen, verlangsamt das die Indexierung (um den Faktor 3-5) und bläht den Index auf. Allerdings wird Sie das in die Lage dazu versetzen, verlässlich und schnell z. B. "Rechnung" in "Berechnung" und "Verrechnung" sowie "Gesellschaft" in "Aktiengesellschaft" zu finden. Allerdings können Sie auch wenn Sie den Index nicht speziell für die Teilwortsuche auslegen später nach Teilwörtern suchen, jedoch wird die Suche dann langsamer sein und das Ergebnis unvollständig. Bitte beachten Sie, dass es in der Verantwortung des Benutzers liegt, die Teilwortindexierung einzuschalten, wenn die Wörter der zu indexierenden Sprache nicht durch Leerzeichen voneinander getrennt sind (wie z. B. im Chinesischen, Japanischen, Thailändischen, ...).

Das Indexieren ist unnötig langsam, wenn die zu indexierenden Daten auf demselben Datenträger liegen wie Ihr Fall, in dem der Index erzeugt wird. Vermeiden Sie es, mit aktiver Internet-Verbindung zu indexieren, wenn Ihr Windows-System für automatische Updates konfiguriert ist und nach der Installation von Updates den Computer evtl. selbständig neu startet.

Optional kann der Text in bestimmten Dateitypen zur Indexierung decodiert werden (s. Logische Suche), und es ist möglich, Indexe für ausgewählte mit einem Fall verbundenen Datenträger/Images in einem einzigen Durchgang zu erstellen. Sie können gleichzeitig in bis zu sechs verschiedenen Codepages indexieren.

Es ist möglich, eine Zeichenersetzungsliste in Unicode zu definieren, die bewirkt, dass bestimmte Buchstaben als andere Buchstaben indexiert werden (z. B. „é“ wie „e“). Das erlaubt es Ihnen, Varianten in der Schreibweise mit einer einzigen Index-Suche abzudecken, z. B. sowohl den Namen „René“ mit Accent also auch „Rene“ ohne. Diese Liste muss die Struktur
é>e
è>e
à>a

...
aufweisen (d.h. 1 Ersetzung pro Zeile) und in einer Unicode-Textdatei namens „Character Adjustment.txt“ gespeichert sein, die mit dem LE-Unicode-Zeichen 0xFF 0xFE beginnt. „Character Adjustment.txt“ ist eine optionale Datei. Sie wird im Installationsverzeichnis von X-Ways Forensics erwartet.

Sie erhalten eine Warnung, wenn Sie das Leerzeichen als Teil von Wörtern definieren. Und zwar darum, weil der Zweck von Leerzeichen ist, Wörter voneinander zu trennen. Sie sind nicht selbst Teil von Wörtern. Wenn ein Leerzeichen als Teil von Wörtern definiert wird, dann bedeutet das, dass ein ganzer Satz wie "Kai Möller hat seine Kreditkarte verloren." als ein einziges Wort betrachtet wird.

Sie können alle Indexe eines Asservats löschen, indem Sie das Häkchen im Kontrollkästchen „Bereits erledigt?“ im Dialogfenster „Datei-Überblick erweitern“ entfernen. Dies löscht auch die individuelle Kennzeichnung der Dateien im Datei-Überblick als indexiert (sichtbar in Form eines kleinen „i“).

Suche in Index: Nach dem Indexieren von Dateien können Sie den Index sehr schnell nach Schlüsselwörtern durchsuchen, mit der Parallelen Suche. Wählen Sie "Suche im Index" in der aufklappbaren Liste am unteren Rand des Dialogfensters. Buchstaben in Suchbegriffen, die über die für die Indexierung verwendete Maximalwortlänge hinausragen, werden bei der Suche ignoriert (damit "Tortenheber" auch dann im Index gefunden wird, wenn das Wort im Index im Fall einer Maximallänge von 7 Buchstaben nach "Tortenh" abgeschnitten wurde). Groß- und Kleinschreibung wird nicht unterschieden, es sei denn, Sie haben den Index mit dieser Option erzeugt. Wenn das Auflisten der Suchtreffer zu lange dauert, z. B. weil Sie nur ein einziges Zeichen oder ein sehr häufiges kurzes Wort eingegeben haben, können Sie jederzeit Esc drücken oder den Fortschrittsanzeigefenster schließen, um den Vorgang abzubrechen. In einer von einer Index-Suche gefüllten Suchtrefferliste sind physische Offsets nicht verfügbar.

Sie können bequem Nicht-RegEx-Index-Suchen nach Suchbegriffen durchführen, die Leerzeichen enthalten, genau wie in der konventionellen Suche. Das ist sehr wichtig für Namen (z. B. "Hans Mustermann" oder "Brandner Bau GmbH") und für Doppelwörter im Englischen (z. B. "bank account" oder "credit card limit"), und zum Teil auch im Deutschen, dank Deppenleerzeichen. Das funktioniert auch dann, wenn die Bestandteile des Doppelworts für sich genommen die maximal indexierte Wortlänge (standardmäßig 7 Zeichen) überschreiten, so dass Sie problemlos Wörter wie "basketball positions" (10+9 Buchstaben) oder "skyscraper architecture" (10+12 Buchstaben) finden. Aber wie immer werden die Bestandteile nur bis zur indexierten Wortlänge gefunden, was kein Problem ist, weil es nicht viele andere Wörter als "basketball" und "skyscraper" gibt, die mit "basketb" bzw. "skyscra" beginnen. Tatsächlich werden neben Leerzeichen auch andere nicht indexierte Worttrennzeichen gefunden, wenn Sie nach Begriffen mit Leerzeichen suchen, z. B. Bindestriche, so dass Sie auch "Spider-Man" und "Lebkuchen-Herz" finden, wenn Sie nach "spider man" und "Lebkuchen Herz" suchen, oder Unterstriche wie in "konto_nummer" (könnte in einem Dateinamen wie "konto_nummer.html" vorkommen) oder Pluszeichen wie in "credit+card" (z. B. üblich in Such-URLs von Google, wenn man nach englischen Doppelwörtern mit Leerzeichen sucht) oder Punkte wie in "Interview.pdf". Daher sind in dieser Hinsicht Index-Suchen noch mächtiger als konventionelle Suchen. Leerzeichen als Teil von Wörtern zu definieren ist falsch.

6.4 Wissenswertes zur Erweiterung des Datei-Überblicks

Sollte X-Ways Forensics während der Verarbeitung einer bestimmten Datei einfrieren, beachten Sie, dass die interne ID und der Name der zuletzt bearbeiteten Datei in den kleinen Fortschrittsanzeigefenster angezeigt werden. Wenn die Erweiterung des Datei-Überblicks auf ein Asservat angewandt wird und X-Ways Forensics währenddessen bei einer einzigen bestimmten Datei abstürzen, wird Ihnen beim Neustart des Programms die betreffende Datei mitgeteilt, und die Datei wird mit dem Vermerk "Absturzursache?" ausgestattet. Das hängt von den Sicherheitsoptionen ab. All dies geschieht, damit Sie eine solche Datei ggf. ausblenden und so bei einem nochmaligen Versuch auslassen können. Es ist unschädlich, die Erweiterung des Datei-Überblicks für dasselbe Asservat nochmal von vorne anzustoßen, d. h. das führt nicht zu doppelten Unterobjekten und kostet kaum erneut Zeit, weil bereits verarbeitete Dateien schnell übersprungen werden, bis zu dem Punkt, an dem der Erweiterungsfortschritt das letzte Mal gespeichert wurde, was vom Auto-Save-Intervall des Falls abhängt. Der Datei-Überblick merkt sich für jede Datei einzeln, welche Erweiterungsoperationen bereits auf sie angewandt wurden, so dass dieselben Operationen normalerweise nicht erneut auf dieselbe Datei angewandt werden.

Wenn der Hash-Wert für eine problematische (absturzverursachende) Datei berechnet wurde, werden diese Datei und etwaige Kopien automatisch ausgelassen, wenn Sie den Datei-Überblick (weiter) erweitern und Hash-Werte mit berechnen lassen (zumindest, wenn der Schutz vor Duplikaten von Absturz-Dateien in den Falleigenschaften eingeschaltet ist). Um den Fall Informationen über vorherige Dateien, die Abstürze verursachen, vergessen zu lassen, klicken Sie auf den zugehörigen Löschen-Schalter in den Falleigenschaften. Übersprungene Dateien bekommen ebenfalls den zuvor genannten Vermerk ab.

The file processing part of volume snapshot refinements supports multiple threads (only if not applied to a selection). Depending on the selected suboperations and the types of the files in the volume, and depending on I/O speed, this can double, triplicate or even quadruplicate the performance. The faster your mass storage solution (HDD, SSD, RAID) in terms of seek times and data transfer speed, the more time you save percentage-wise. This parallelization feature is still considered experimental and not complete yet, but the potential time saving in one of the most important and most time-consuming functions of the program is enormous. Selecting multiple extra threads has an effect only when searching in evidence objects that are images or directories, not disks. If you select 0 extra threads, it will work as in X-Ways Forensics versions before 19.0. If you select 1 or more extra threads, processing is done in additional worker threads (as many as you select), and the main thread of the process will be idle, which means the GUI will remain highly responsive. In X-Ways Investigator up to 3 worker threads may be used, in X-Ways Forensics up to 16, if your CPU supports that. If multi-threaded processing crashes, next time when you restart the program it probably cannot tell you which file exactly presumably caused the crash. File-wise processing conducted by X-Tensions (through calls of XT_ProcessItem or XT_ProcessItemEx) are also parallelized if the X-Tensions identifies itself as thread-safe. Processing of files in file archives is currently excluded from parallelisation internally.

Sie können automatisch eine Sicherung des Datei-Überblicks anlegen lassen nach dessen Erweiterung, so dass Sie zu diesem Zustand bei Bedarf leicht zurückkehren können statt den Datei-Überblick neu einzulesen und neu zu erweitern. Das könnte nützlich sein, wenn Ihnen bei der Begutachtung von Dateien ein Fehler unterläuft oder wenn der Datei-Überblick irgendwie

beschädigt wird. Wenn das Kontrollkästchen hierzu ganz statt nur halb gewählt ist, wird auch schon nach dem Zwischenschritt 1 (Operationen auf Datenträger-/Partitionsebene) eine Sicherung angelegt. Der Menübefehl zum Wiederherstellen von Datei-Überblick-Sicherungen kann im Kontextmenü des betreffenden Asservats im Falldatenfenster gefunden werden.

Sie können eine direkt nach der Erweiterung des Datei-Überblicks auszuführende parallele Suche im Voraus einplanen.

6.4.1 Wechselseitige Abhängigkeiten

Es gibt verschiedene Interdependenzen zwischen all diese Operationen. Z. B., wenn die Inhalte eines Archivs in dem Datei-Überblick aufgenommen werden, können sich unter diesen Dateien Bilder befinden, die auf Hautfarben geprüft werden sollen, oder Dokumente, die auf Verschlüsselung zu testen sind. Sie können mit der Prämisse arbeiten, dass wenn im Rahmen von „Datei-Überblick erweitern“ eine zusätzliche Datei in den Datei-Überblick aufgenommen oder ihr wahrer Typ erkannt wird, auch alle sinnvollen anderen Operationen auf diese Datei angewandt werden, *sofern sie gewählt sind*. Das, was eine Operation produziert, wird automatisch in andere Operationen (oder sogar nochmal dieselbe) wieder hineingesteckt, sofern geeignet.

Es könnte jemand auf die Idee kommen, ein belastendes JPEG-Bild zu verbergen, indem er es in ein MS-Word-Dokument einbettet, diese .doc-Datei umbenennt in .dll, sie in einem Zip-Archiv komprimiert, das Zip-Archiv in .dll umbenennt, das falsch benannte Zip-Archiv in ein weiteres Zip-Archiv packt, dieses wiederum in .dll umbenannt und diese .dll-Datei als E-Mail-Attachment per MS Outlook verschickt. Wenn die jeweiligen Optionen in „Datei-Überblick erweitern“ alle gewählt sind, macht X-Ways Forensics Folgendes: Es extrahiert den E-Mail-Anhang aus dem PST-E-Mail-Archiv. Es erkennt, dass die .dll genannte Datei eigentlich ein Zip-Archiv ist. Dann nimmt es den Inhalt dieses Archivs in den Datei-Überblick auf, nämlich eine Datei mit der Endung .dll. Diese Datei wird als ein weiteres Zip-Archiv erkannt. Konsequenterweise wird auch dieses Archiv erkundet, und die .dll-Datei darin als MS-Word-Dokument erkannt. Bei der Suche nach eingebetteten Bildern findet X-Ways Forensics die JPEG-Datei in der .doc-Datei und kann sie, wenn gewünscht, sofort auf Hautfarben überprüfen. All dies geschieht in einem *einzigen* Schritt.

6.4.2 Zusatzinformationen

X-Ways Forensics merkt sich komfortablerweise, welche Operationen schon auf welche Dateien angewandt wurden, so dass bei einem erneuten Durchlauf (Erweitern des Datei-Überblicks) Zeit gespart wird und keine Unterobjekte doppelt erzeugt werden usw. Es merkt sich aber nicht die im einzelnen verwendeten Unteroptionen zu jeder Operation (z. B. ob bei der Metadaten-Extraktion auch „Vorschau für Browser-Datenbanken erzeugen“ ausgewählt war) und kann diese nicht separat nachholen. Die einzigen Operationen, die immer wiederholt durchgeführt werden, sind Indexierung und Abgleich von Hash-Werten mit konventionellen Hash-Datenbanken. Sollten Sie aus irgendeinem Grund eine andere Operation noch ein weiteres Mal auf dieselbe Datei anwenden wollen (z. B. dann mit anderen Unteroptionen oder nach Anpassung der Dateisignatur-

Datenbank zur Typprüfung), können Sie evtl. ein mit dem Wort "Erneut" bezeichnetes Kontrollkästchen finden und nutzen oder ansonsten die Datei auswählen und durch Drücken von Strg+Entf komplett auf den Zustand "noch zu bearbeiten" zurücksetzen. Dies löscht auch etwaige bereits berechnete Hautfarbenanteile, extrahierte Metadaten, Hash-Werte, Ergebnisse des Hash-Abgleichs usw. usf. Diese Funktion entfernt jedoch keine bereits extrahierten Unterobjekte aus dem Datei-Überblick. Dies muss ggf. vom Benutzer separat erledigt werden, sofern gewünscht, durch Ausblenden und Entfernen dieser Unterobjekte. Ebenso wenig entfernt die Funktion etwaige, bei einer vorangegangenen Erweiterung des Datei-Überblicks ausgegebene Ereignisse. Ein weiteres Tastenkürzel, STRG+ UMSCH+ENTF, erlaubt es, Zuordnungen von Dateien im Datei-Überblick mit normalen Hash-Sets, FuzZyDoc-Hash-Sets und PhotoDNA-Kategorien zu entfernen. Diese bleiben sonst bestehen, auch wenn die Hash-Sets aus der Datenbank gelöscht werden. Strg+Umsch+Entf entfernt außerdem die Kennzeichnung "Duplikate gefunden" in der Beschreibungsspalte.

Ob eine Datei bei der Erweiterung des Datei-Überblicks verarbeitet werden soll oder nicht, wird vom Programm erst dann entschieden, wenn diese Datei an der Reihe ist, nicht im Voraus, wenn Sie die Operation starten. Das bedeutet, wenn Sie im Programm weiterarbeiten, während die Erweiterung läuft, and Filter aktivieren/deaktivieren/ändern oder Dateien markieren/entmarkieren oder Dateien ausblenden/einblenden, kann sich das noch auf den Erfassungsbereich der Operation auswirken, je nach gewählten Optionen und je nachdem, ob die Datei, die Sie markieren/entmarkieren/ausblenden/einblenden/... schon verarbeitet wurde oder nicht. Wenn Ihnen eine Operation gefühlt zu viel Zeit in Anspruch nimmt, können Sie daher immer noch Filter strenger einstellen oder bestimmte große Dateien entmarkieren o. ä., ohne den laufenden Prozess abzubrechen.

When volume snapshot refinement is in the stage of processing individual files, then the progress percentage is simply the internal ID of the currently processed file divided by the total number of items in the volume snapshot. X-Ways Forensics doesn't know beforehand which files need a lot of time to process, only when actually reading from the file it will be decided what should be done with the file and discovered how much data is embedded etc. File type verification and potentially hash database matching may change the decision about what to do with the file, if anything at all. If an entire evidence object consists of just 1 file, e.g. if you added a single files to the case, then the progress percentage will not advance. The progress is 0% initially and 100% for a fraction of a second when done. The displayed percentage does not reflect the sub-progress within a given large file.

An unlabelled (but tooltipped) check box in the volume snapshot refinement dialog window can now make X-Ways Forensics reveal which suboperation is currently applied to the currently processed file. A 3-digit abbreviation will be displayed with the following meaning:
Sig: file type verification
Hsh: hashing
Vid: capture sporadic still images from videos
Idx: preprocessing original file contents for indexing
Dec: text decoding for indexing
IdX: preprocessing decoded text for indexing
Emb: search for embedded data
PDN: PhotoDNA database matching
Pic: other picture analysis steps

Eml: e-mail extraction
Fuz: FuzZyDoc database matching
Met: metadata extraction
Enc: file format specific encryption test
Ent: entropy check
Arc: inclusion of files in archives into the volume snapshot
This may be helpful for educational reasons, to give users a better idea of how computationally expensive certain suboperations are and how much time could be saved by not selecting them if not absolutely necessary. It may also prove useful for debugging purposes. Whether this option may slow down processing on certain computers has not been tested.

Gewisse ehem. gültige Zeitstempel von Dateien werden während diverser Unteroperationen der besonders intensiven Dateisystem-Datenstruktur-Suche in NTFS als Ereignisse ausgegeben, abhängig von der Option "Zeitstempel aus diversen Quellen als Ereignisse bereitstellen". Diese Option wirkt sich auch auf andere Operationen aus, deren Hauptzweck nicht das Ermitteln von Zeitstempeln/Ereignissen ist.

7 Ausgewählte Grundkonzepte

7.1 Editier-Modi

Der Modus, in dem eine Datei oder ein Datenträger im Programm geöffnet ist, wird in der grauen Informationsspalte angezeigt. Deren Kontextmenü enthält einen Befehl, um den Modus des aktuellen Fensters selektiv zu ändern.

Nur-Lesen-Modus: Empfohlener Modus für computerforensische Untersuchungen. Dateien und Datenträger, die im Lese-Modus geöffnet werden, können nicht (absichtlich oder versehentlich) editiert/verändert, sondern nur eingesehen werden. Sie werden also »schreibgeschützt« geöffnet. Um den strengen forensischen Anforderungen zu genügen, ist dies der einzige Modus, der in X-Ways Forensics verfügbar ist für Datenträger und als Datenträger interpretierte Sicherungen, auch für Dateien, die Sie von Laufwerksbuchstaben aus öffnen, die geschützt sind (s. Sicherheitsoptionen), so dass Sie immer noch Dateien verarbeiten (decodieren, konvertieren, entschlüsseln, ...) können, die im Verzeichnis des aktuellen Falls oder im allgemeinen Ordner für temporäre Dateien gespeichert sind.

Standard-Editiermodus: Im Standard-Editiermodus werden Änderungen, die Sie an einer geöffneten Datei oder einem Datenträger vornehmen, in einer temporären Datei gespeichert. Diese wird dynamisch verwaltet. Erst beim Speichern oder Schließen werden die Änderungen dann nach Rückfrage in die Originaldatei bzw. auf den Datenträger übertragen.

In-Place-Modus: Verwenden Sie diesen Modus mit Vorsicht. *Sämtliche* Änderungen (Tastatureingaben, Füllen/Entfernen des Blocks, Schreiben des Zwischenspeichers, Ersetzen-Vorgänge, ...) werden direkt in die Originaldatei bzw. auf den Datenträger („in-place“) geschrieben. Dies geschieht dynamisch, spätestens aber dann, wenn das Editierfenster

geschlossen wird, ohne weitere Rückfragen. Es ist daher nicht erforderlich, den Menüpunkt „Speichern“ im Dateimenü aufzurufen, es sei denn, Sie möchten sicherstellen, dass alle Änderungen zu einem bestimmten Zeitpunkt geschrieben werden, wenn das Editierfenster noch geöffnet ist.

Dieser Modus empfiehlt sich, wenn das im Standard-Editiermodus obligate Übertragen von Daten aus der Originaldatei in die Temporärdatei und umgekehrt zu zeitaufwendig wäre und zu viel Festplattenspeicherplatz verbräuchte. Dies kann z. B. dann der Fall sein, wenn in großen Dateien viele Änderungen vorgenommen werden sollen. Da im In-Place-Modus keine Daten in temporären Dateien gespeichert werden, ist dieser Editiermodus generell schneller als der Standard-Editiermodus. Der In-Place-Modus ist der einzige Modus, in dem der Arbeitsspeicher-Editor benutzt werden kann. Hinweis: Auch im In-Place-Modus muss eine temporäre Datei angelegt werden, wenn die Größe der Originaldatei verändert wird.

Wenn Sie Dateien über das Betriebssystem öffnen (z. B. über Datei | Öffnen, von irgendeinem Laufwerksbuchstaben, der gerade in Windows zugeordnet ist), werden Datei-Schreibbefehle des Betriebssystems verwendet, um eine Datei zu ändern. Es ist aber in WinHex auch möglich, Dateien direkt auf einem Datenträger/in einem Roh-Image zu editieren, in jedem von WinHex unterstützten Dateisystem, auch wenn Windows nicht bekannt, auch wenn Windows die Dateien nicht sehen kann (z. B. weil gelöscht), ohne die Zeitstempel oder Attribute zu ändern, im In-Place-Modus. Für diese Editierfähigkeit muss die Datei aus dem bereits geöffneten Dateisystem heraus geöffnet werden, das es enthält, entweder über den Öffnen-Befehl im Kontextmenü des Verzeichnis-Browsers oder im Datei-Modus (nur mit forensischer Lizenz). Komprimierte Dateien und generell Dateien innerhalb anderer Dateien (z. B. E-Mails und Datei-Anhänge in E-Mail-Archiven) können nicht editiert werden, außer innerhalb eines Datei-Containers, wenn sie selbst dediziert vom Original-Datenträger oder Image dort hineinkopiert wurden. Beachten Sie, dass Dateien auf die neue Weise nicht gekürzt oder verlängert werden können und dass nur allozierte Bereiche einer Datei geändert werden können. Das Editieren von Dateien, die wie oben beschrieben direkt aus Datenträgern/Images heraus geöffnet werden, ist nur in WinHex möglich, nicht in X-Ways Forensics oder X-Ways Investigator, wo Schreibzugriff auf Sektor-Ebene (in das alle Datei-Schreibzugriffe der neuen Art intern übersetzt werden) ausgeschlossen sind und wo der einzige verfügbare Modus für Datenträger und interpretierte Images und für darin geöffnete Dateien nach wie vor der Schreibschutz-Modus ist. X-Ways Forensics lässt sich auch als WinHex betreiben (einfach .exe-Datei umbenennen).

In der Computerforensik und IT-Sicherheit kann die Editiermöglichkeit hilfreich sein beim manuellen Redigieren (z. B. Überschreiben mit XXX) von spezifischen Daten, die nicht untersucht/weitergegeben/eingesehen werden sollen oder um bestimmte Bereiche in einer Datei sicher zu überschreiben (z. B. als Block definieren und diesen dann füllen). Beachten Sie, dass Datei-Container Roh-Images sind, wenn sie nicht ins .e01-Evidence-File-Format konvertiert worden sind, und daher nachträgliches Editieren von Dateien erlauben, was aber natürlich begleitende Hash-Werte ungültig macht. Es ist sogar möglich, Verzeichnisse zu editieren, also die Cluster mit Verzeichnisdaten, wie z. B. INDX-Puffer in NTFS, z. B. wenn Sie darin vorkommende Namen bestimmter Dateien unlesbar machen müssen.

7.2 Scripte

Ein Teil der Funktionalität von WinHex kann in automatisierter Weise verwendet werden, z. B. um wiederkehrende Routineaufgaben zu erledigen oder um bestimmte Tätigkeiten an nicht beaufsichtigten Computern im Netz ferngesteuert auszuführen. Die Möglichkeit, andere als die mitgelieferten Beispielscripte auszuführen, ist Besitzern von professionellen und höheren Lizenzen vorbehalten. Scripte können vom Start-Center oder von der Kommandozeile aus gestartet werden. Wenn ein Script ausgeführt wird, können Sie die Esc-Taste drücken, um es abzubrechen.

WinHex-Scripte sind Textdateien mit der Namensendung „.whs“. Sie können mit jedem Texteditor bearbeitet werden und bestehen einfach aus einer Folge von Befehlen. Es wird empfohlen, pro Zeile nur einen Befehl einzugeben, um die Übersichtlichkeit zu wahren. Abhängig vom jeweiligen Befehl müssen dahinter ggf. Parameter angegeben werden. Die meisten Befehle wirken sich auf die Datei oder den Datenträger im aktuell aktiven Editierfenster aus.

In Anhang B finden Sie eine Beschreibung aller gegenwärtig unterstützten Scriptbefehle.

7.3 X-Tensions API

Automate investigative tasks and extend the functionality of X-Ways Forensics with *X-Tensions*: The X-Ways Forensics X-Tension API (application programming interface) allows you to use many of the advanced capabilities of the X-Ways Forensics computer software programmatically and extend them with your own functionality. For example, you could implement some specialized file carving for certain file types, automated triage functionality, alternative report generation, or automatically filter out unwanted search hits depending on your requirements etc.

Among other things, X-Tensions allow you to:
- read from a disk/partition/volume/image
- retrieve abundant information about each file and directory in the volume snapshot
- read from any file
- create new objects in the volume snapshot
- Vermerke erstellen
- add comments to files
- process, validate and delete search hits
- and do practically *everything else that is possible with a Windows program*! (thanks to the Windows API)

You can use your programming language of choice, e.g. C++, Delphi, or Visual Basic, and do not have to learn any new programming language. You can use your compiler of choice, for example Visual Studio Express (freeware).

Since an extension is not an interpreted script, but regular compiled executable code that is running in the address space of the application itself, you can expect highest performance, the same

as with internally implemented functionality. X-Tensions give you easy and direct access to crucial and powerful functions deep inside X-Ways Forensics.

When X-Tensions functions can get called:
- when refining the volume snapshot
- when running a simultaneous search
- via the directory browser context menu
- via the search hit list context menu

The X-Tension API also allows the development and use of so-called Disk I/O X-Tensions. These are snap-ins that sit between all analysis functionality and the user interface of X-Ways Forensics on the one hand and a disk/image/RAID/partition/volume from which sectors are read on the other hand. They can for example deal with full disk encryption and decrypt the data in all sectors read by X-Ways Forensics on the fly when needed, so that all relevant functions only get to see the decrypted data and can deal with it as if it was a normal disk/volume.

The user may open a selected evidence object through such a Disk I/O X-Tension using a new command in the context menu of the Case Data window. After selecting the intended X-Tension DLL, if the DLL signals that it can successfully deal with the data in that evidence object, the case will remember which DLL that was chosen and automatically apply it next time when opening the same evidence object. Note that as always partitions count as evidence objects themselves. That way full disk encryption can be tackled as well as volume level encryption.

Once completely run, the user is prompted whether or not stubborn C# X-Tension DLLs should be completely unloaded after execution. Programmers may prefer to do that when debugging their own X-Tensions, but apparently this can prevent usage the same DLL a second time in the same session of X-Ways Forensics, so ordinary users better choose No.

You may distribute your X-Tension DLLs that you compile and/or your source code free of charge or even for a fee, under whatever license terms you see fit.

For more information please see http://www.x-ways.net/forensics/x-tensions/api.html.

7.4 Disk-Editor

Im Extras-Menü finden Sie den Befehl zum Öffnen von lokal angeschlossenen physischen Datenträgern sowie die von Laufwerksbuchstaben repräsentierten Volumes auf Sektorebene. Wenn Sie einen physischen, partitionierten Datenträger öffnen, können Sie anschließend von dem Datenträger aus per Doppelklick die auf diesem Datenträger erkannten Partitionen öffnen. Die auf diese Weise erreichte Darstellung einer Partition enthält Volume-Schlupfspeicher (überschüssige Sektoren, die keinen weiteren ganzen Cluster mehr ergeben), der beim Öffnen des logischen Laufwerksbuchstabens fehlt.

The list of logical volumes can optionally include volumes that are active in Windows, but not currently associated with any drive letter. Active volumes that are not ordinary volumes are displayed with a special icon and a special description, e.g. "TrueCryptVolumeX". Useful so that

on a live system that you wish to preview, examine or acquire you can quickly see which volumes may need to be addressed separately (in additional to physical storage devices) because it would be difficult to reconstruct or unlock them later based on the data on the physical storage device. If volumes without connected drive letter are listed, that also includes volumes that have been mounted within Windows as a junction point in another volume. Such volumes are listed with a special link icon, and the junction point is displayed between volume label and volume size. The list of volumes that do not have drive letters may now also include volumes that were previously active in Windows. Those are marked with a crossed out red circle icon. For example a previously mounted TrueCrypt volume that was dismounted might be shown in this fashion. Such volumes cannot be opened any more, they are just listed for informational purposes, which is useful when working on a live system that needs to be examined.

Gewöhnlich ist es vorteilhafter, mit einem Volume statt einem physischen, partitionierten Datenträger zu arbeiten, weil dann mehr Features zur Verfügung stehen. Beispielsweise sind »Cluster« vom Dateisystem definiert, die Zuordnung von Clustern zu Dateien (und umgekehrt) ist WinHex bekannt, »freier Speicher« und »Schlupfspeicher« haben eine Bedeutung. Wenn Sie Sektoren editieren möchten, die außerhalb eines logischen Laufwerks liegen (etwa der Master Boot Record), wenn Sie etwas auf allen Partitionen einer Festplatte auf einmal suchen möchten oder wenn eine Partition beschädigt oder mit einem Windows unbekannten Dateisystem formatiert ist, so dass Windows sie nicht als Laufwerksbuchstaben zugänglich macht, empfiehlt es sich, den physischen Datenträger zu öffnen. Von dem Fenster aus, das einen physischen Datenträger repräsentiert, können Sie auch etwaige definierte Partitionen einzeln öffnen, die i. d. R. im Verzeichnis-Browser in diesem Fenster aufgelistet werden, durch Doppelklick. WinHex versteht konventionelle MBR-Partitionierung, GPT (GUID Partition Type), Apple-Partitionierung, Superfloppy-Format, Windows' dynamische Platten, die vom LDM (Logical Disk Manager) verwaltet werden (MBR und GPT) und LVM2 (MBR und GPT) und PC-kompatible BSD-Disklabel. Alle Typen dynamischer Volumes werden unterstützt: simple, spanned, striped und RAID 5. Das gedrückt Halten der Strg-Taste beim Öffnen von Festplatten unterdrückt die Erkennung und spezielle Behandlung von dynamischen Platten und stellt sicher, dass Festplatten so interpretiert werden, als wären sie auf konventionelle Weise partitioniert worden. Einige der vorgenannten Partitionierungstypen werden nur für Specialist- und forensische Lizenzen unterstützt.

Es gibt einen optionalen Roh-Zugriff für optische Laufwerke, der es ermöglicht, von Audio-CDs zu lesen und auch die kompletten 2352-Byte-Sektoren auf Daten-CDs (CD-ROM und Video-CDs), die Fehlerkorrektur-Informationen enthalten. If a physical storage device is treated as offline or read-only in Windows Disk Management, that information is displayed in all disk selection dialog windows. Offline disks can be opened for reading/imaging/analysis, but they are write-protected.

Bitte beachten Sie die folgenden Einschränkungen bzw. Voraussetzungen:

- Um auf Datenträger sektorweise zugreifen zu können, sind Administrator-Rechte erforderlich. Unter Windows Vista und neuer muss man das Programm dazu explizit als Administrator ausführen. Einfach nur als Administrator angemeldet zu sein ist *nicht* ausreichend.
- Auf Netzlaufwerke kann nicht sektorweise zugegriffen werden.
- In X-Ways Forensics lassen sich Datenträgersektoren oder Sektoren in interpretierten Image-Dateien prinzipiell nicht editieren, nur in WinHex.

- WinHex kann auf CD-R(OM)s und DVDs nicht schreiben.
- Unter Windows Vista und neuer kann WinHex Sektoren nicht schreiben, die in der Partition mit der aktiven Windows-Installation liegen oder in der Partition, von der aus WinHex ausgeführt wird.

Im Anhang C dieses Handbuchs finden Sie die Spezifikationen des Master Boot Record einer Festplatte, der mit dem Disk-Editor editiert werden kann.

Auf Disk schreiben: Entspricht dem Befehl „Speichern“ für Dateien und befindet sich beim Benutzen des Disk-Editors an dessen Stelle im Menü. Schreibt die von Ihnen vorgenommenen Änderungen auf den Datenträger. Bitte beachten Sie, dass Sie damit einen äußerst kritischen Eingriff in die Integrität des Datenträgers vornehmen. Sofern die entsprechende Rückgängig-Option eingeschaltet ist, wird von den betroffenen Sektoren vor dem Überschreiben eine Sicherung angelegt. *Die Funktion ist nur in der Vollversion verfügbar.*

7.5 Arbeitsspeicher-Editor/-Analyse

Im Extras-Menü finden Sie die Funktion „Speicher öffnen“. Der Arbeitsspeicher-Editor ermöglicht es, den physischen Arbeitsspeicher/RAM und den logischen Arbeitsspeicher eines in der Ausführung befindlichen Programms (= eines Prozesses) eines laufenden Systems direkt einzusehen. Für letzteres werden alle von dem Prozess belegten Seiten im Arbeitsspeicher als zusammenhängender Speicherbereich abgebildet. Ungenutzte (leere oder nur reservierte) Blöcke im Speicher werden von WinHex standardmäßig ignoriert, optional aber mit erfasst und mittels „?“-Zeichen angezeigt. Ohne diese Lücken können Sie in Dateien geschriebene Speicherdumps exakt miteinander vergleichen (absolute und virtuelle Adressen sind identisch), um etwa den Stack oder Heap zu beobachten oder Computerviren zu verfolgen.

Wenn Sie aus der Liste aller laufenden Prozesse einen Prozess auswählen, können Sie entweder den sog. Primärspeicher oder den Gesamtspeicher eines Prozesses öffnen, oder einzelne von diesem Prozess geladene Module (DLLs). Als Primärspeicher wird derjenige Bereich bezeichnet, der im Adressraum unterhalb der System-DLLs liegt und von den meisten Programme vorrangig für verschiedenste Zwecke genutzt wird, für Stack und Heap. Zumindest das Hauptmodul eines Prozesses (die EXE-Datei) ist i. d. R. ebenfalls im Primärspeicher enthalten. Der Gesamtspeicher umfasst alle allozierte Seiten im gesamten logischen Adressraum eines Prozesses.

Mit der 64-Bit-Edition von WinHex/X-Ways Forensics können Sie geladene Module oberhalb der 4-GB-Grenze in 64-Bit-Prozessen aufgelistet bekommen, und Speicher in solchen Adressbereichen öffnen und editieren. Unicode wird für Prozess- und Modul-Namen sowie Pfade im Speicher-Editor unterstützt. Seitengrenzen werden durch horizontale Linien gekennzeichnet. Grenzen, die Lücken zwischen zusammenhängend allozierten Bereichen kennzeichnen, werden von dunkleren horizontalen Linien repräsentiert. Die Informationsspalte zeigt jetzt mehr Details an, wie z. B. die höchste repräsentierte Adresse und die Zahl der Lücken im zugewiesenen Speicher (=Zahl der zusammenhängenden zugewiesenen Speicherbereiche -1) wie auch den Schutz-Status und Typ der aktuell dargestellten Seite.

Bitte beachten Sie die folgenden Einschränkungen:

- Zugriff auf *physischen* RAM nur unter Windows XP (32-Bit), nur bis 4 GB, und nur mit Administratorrechten
- Das Editieren ist nur im In-Place-Editiermodus möglich.
- Achtung: Rückgängig gemacht werden können bei Verwendung des Arbeitsspeicher-Editors *ausschließlich* Tastatureingaben!
- Die Evaluationsversion erlaubt generell nur den Nur-Lesen-Modus.

Beachten Sie bitte die Optionen „Auf Änderungen im Speicher prüfen“ (Optionen | Sicherheit) und „Logische Adressen im Speichereditor“ (Optionen | Allgemein).

Hauptspeicheranalyse

Erfordert eine forensische Lizenz. Wenn Sie den lokalen physischen Arbeitsspeicher öffnen (über Extras | RAM öffnen, nur unter Windows XP) oder einen Hauptspeicher-Dump als Datei öffnen (und diese Datei genau wie ein Datenträger-Image interpretieren) oder einen Speicher-Dump einem Fall hinzufügen, werden die Prozesse im Verzeichnis-Browser aufgelistet, auch versteckte Prozesse, mit ihren Zeitstempeln und Prozess-IDs, und ihr jeweiliger Speicheradressraum kann individuell im Modus "Process" eingesehen werden, wobei die Seiten in korrekter logischer Reihenfolge hintereinander dargestellt werden, wie sie aus Sicht jedes Prozesses angeordnet sind. Die "intensiven Dateisystem-Datenstruktur-Suche" ist signaturbasiert, dauert ein bisschen länger als das Erstellen des standardmäßigen Datei-Überblicks und kann Spuren von weiteren beendeten Prozessen aufdecken. RAM kann auch über ein Netzwerk hinweg gesichert werden mit Hilfe von F-Response (Extras | Datenträger öffnen). Die Analyse wird unterstützt für die meisten (aber nicht alle) Varianten (Service-Packs) von Windows 2000, Windows XP, Windows 2003 Server, Windows Vista, Windows 2008 Server und Windows 7, 32-Bit und (weniger vollständig) 64-Bit. Unterstützt werden nur 1:1-Abbilder des RAM, d. h. auch die vom BIOS und PCI-Geräten benutzten Speicherbereiche sollten enthalten sein.

Datenstrukturen des Windows-Kernels und benannte Objekte werden bequem in einem Baum im Datei-Überblick unter „Objects“ aufgelistet. Geladenen Module werden unter „Modules“ aufgeführt. Das ermöglicht es X-Ways Forensics einerseits, deren Speicherseiten im RAM-Modus den Modulen zuzuordnen, und andererseits Hash-Werte zu berechnen, um Module über spezielle Hash-Sets identifizierbar zu machen. Zum Hashen ist es empfehlenswert, nur den nicht veränderlichen Header von geladenen Modulen anzeigen zu lassen (s. Optionen des Datei-Überblicks).

Der technische Detailbericht gibt einerseits wichtige systemweite Parameter aus und andererseits die aktuellen Adressen wichtiger Kernel-Datenstrukturen sowie geladene Kernel-Module. Im Details-Modus finden sich zu jedem Prozess die Adressen von prozessbezogenen Datenstrukturen und die ID des übergeordneten Prozesses. Im RAM-Modus wird zu jeder Speicherseite in der Informationsspalte ggf. ein zugehöriger Prozess und der Verwaltungszustand angezeigt.

Mit dem entsprechenden Hintergrundwissen kann diese Funktionalität benutzt werden, um mehr zu erfahren über den aktuellen Zustand der Maschine und der Prozesse, Sockets, geöffnete Dateien, geladene Treiber und angeschlossene Datenträger, um Schadsoftware zu identifizieren,

um die entschlüsselte Version von verschlüsselten Daten zu finden, um etwas in der Vorfallanalyse Netzwerk-Spuren zu analysieren, und um weitere Erkenntnisse im Bereich der Speicherforensik zu gewinnen.

7.6 Editieren mit Schablonen

Eine Schablone („Template“) ist ein Dialogfenster, das die Mittel zum Editieren maßgeschneiderter Datenstrukturen zur Verfügung stellt. Im Vergleich zum reinen Hex-Editieren ist das Editieren mit Schablonen komfortabler und weniger fehleranfällig. Hier werden Änderungen in getrennten Editierfeldern vorgenommen und mit der ENTER-Taste bestätigt (oder beim Schließen der Schablone). Die zu editierenden Daten können von einer Datei, von Datenträger-Sektoren oder aus dem virtuellen Arbeitsspeicher stammen. Insbesondere beim Editieren von Datenbanken empfiehlt sich das Benutzen von Schablonen aufgrund des leichteren Datenzugriffs. Sie finden den Befehl zum *Drucken* einer Schablone im Systemmenü, und ebenso einen Befehl, der den Inhalt einer Schablone als tabulatorseparierten Text in die Zwischenablage kopiert. Das Systemmenü ist bekanntlich das Menü, das erscheint, wenn Sie die obere linke Ecke eines Fensters anklicken.

Die Variablen in einer Schablone können auch in Form von Einträgen im Positions-Manager ausgegeben werden (entweder dem allgemeinen Positions-Manager oder, falls das Datenfenster ein Asservat repräsentiert, dem Positions-Manager dieses Asservats), ebenfalls über das Systemmenü. Das bedeutet auch, dass sie direkt in der Hex-Editor-Anzeige visuell hervorgehoben und mit einem erklärenden Tooltip ausgestattet werden. Option kann das Schablonenfenster aus komplett übersprungen werden, so dass die Ausgabe direkt im Positions-Manager erfolgt. Dazu halten Sie beim Anwenden der Schablone die Umschalt-Taste gedrückt.

Eine *Schablonen-Definition* wird als Textdatei mit der Endung .tpl (für „Template“) gespeichert. Der *Schablonen-Editor* ermöglicht es Ihnen, solche Definitionen zu verfassen und deren Syntax zu prüfen. Eine Schablonen-Definition enthält hauptsächlich Variablen-Deklarationen, ähnlich wie die in Programmiersprachen. Die Syntax finden Sie in Anhang A im Detail erläutert. Zu den unterstützten Datentypen gehören alle geläufigen Integer-, Gleitkomma- und Boolean-Varianten, Datumstypen, Hex-Werte, Binärwerte, Zeichen und Strings. Man kann Arrays (Felder) sowohl von einzelnen Variablen als auch von ganzen Blöcken definieren.

Die Möglichkeit, beim Interpretieren von Daten mit einer Schablone die aktuelle Position frei zu bestimmen machen das Editieren mit Schablonen besonders flexibel:

- Dieselbe Variable kann in Form von unterschiedlichen Typen interpretiert und manipuliert werden.
- Irrelevante Datenbereiche können übersprungen werden.

Der *Schablonen-Manager* listet alle Textdateien im WinHex-Verzeichnis, die Schablonen-Definitionen enthalten, auf. Er zeigt die Bezeichnung der Schablone, eine Beschreibung, den Dateinamen und den Zeitpunkt der letzten Änderung an. Klicken Sie auf den „Anwenden“-Schalter, um unter Verwendung der ausgewählten Schablonen-Definition eine Schablone zum Editieren der Daten im aktuellen Editorfenster an der aktuellen Position anzuzeigen. Sie können im Schablonen-Manager auch neue Definitionen erstellen oder vorhandene Definitionen löschen

oder mit dem Schablonen-Editor bearbeiten.

WinHex ist werkseitig mit mehreren Beispiel-Schablonen ausgestattet.

8 Datenrettung

8.1 Datenrettung mit dem Verzeichnis-Browser

Gelöschte Dateien und Verzeichnisse, die im Verzeichnis-Browser aufgelistet werden, können besonders einfach und selektiv über das Kontextmenü des Verzeichnis-Browsers gerettet werden. Sie navigieren zu einem Verzeichnis (oder erkunden das Stammverzeichnis rekursiv), wählen die wiederherzustellenden Dateien aus und benutzen den Befehl „Wiederherstellen/Kopieren“ im Kontextmenü. Siehe Kapitel „Verzeichnis-Browser“. Idealerweise erweitern Sie natürlich vorher erst den Datei-Überblick, so dass mehr ehemals existierende Dateien gefunden und im Verzeichnis-Browser aufgelistet werden.

8.2 Dateien retten nach Typ/Datei-Header-Signatursuche

Datenrettungsfunktion im Extras-Menü und auch eine Strategie zum Auffinden ehemals existierender Dateien als Teil der Befehls „Datei-Überblick erweitern“. Erkennt Dateien an bestimmten Header-Signaturen, also an einer für den jeweiligen Dateityp charakteristischen Bytewert-Folge. Wird auch als „File Carving“ bezeichnet. Aufgrund dieses Ansatzes ist File Carving nicht vom Vorhandensein von funktionierenden Dateisystemstrukturen abhängig.

Dateien retten nach Typ: Wenn anhand einer Signaturdefinition gefunden, werden die Dateien in einem von Ihnen angegebenen Ausgabeordner auf einem Ihrer eigenen Laufwerke gespeichert. Optional werden Dateien jedes Typs in einem separaten Unterordner abgelegt (...\JPEG, ...\HTML, usw.). Die vermuteten Inhalte der Dateien werden tatsächlich kopiert.
Datei-Header-Signatursuche: Die gefundenen Dateien werden nirgendwo gespeichert, sondern lediglich in einem virtuelle Verzeichnis des Datei-Überblicks *aufgelistet*. Nur ein Verweis auf jede Datei wird gespeichert, mit einem künstlich erzeugten Namen (basierend auf einer laufenden Nummer oder der Startsektornummer), vermuteter Größe, und Start-Offset. Der Datei-Inhalt wird ad hoc vom ursprünglichen Datenträger/Image gelesen, wenn er zum Einesehen/Kopieren der Datei benötigt wird. Optional können Sie die Dateien mehrerer Durchläufe von Datei-Header-Signatur-Suchen in separaten Unterverzeichnissen ausgeben, so dass sie leichter voneinander unterschieden werden können, wenn hilfreich.

Beachten Sie, dass das Ausgliedern von Dateien aus Sektoren anhand von Datei-Header-Signaturen (File Carving) generell annimmt, dass die folgenden zugehörigen Cluster physisch zusammenhängend sind, also im Fall von ursprünglich fragmentiert gespeicherten Clusterketten inkonsistente Dateien ausgibt. Folgende Ausnahme ist definiert: Wenn die Datei-Header-Signatur-Suche in einem unterstützten Dateisystem (außer Ext2/Ext3) den Anfang einer Datei im

freien Speicher findet, an einer Cluster-Grenze, wird standardmäßig angenommen, dass die Daten um etwaige folgende im Dateisystem als belegt markierte Cluster herum gespeichert sind. Das rekonstruiert Dateien korrekt, die zeitlich nach anderen Dateien gespeichert wurden und um diese herum, und die dann gelöscht wurden, solange die dabei freigegebenen Cluster nicht anschließend nochmal wieder neu verwendet überschrieben wurden. Um das Ausgliedern von Daten in diesem Sinne rein aus dem freiem Speicher (unter Meidung von allozierten Clustern) zu verhindern, d. h. immer zusammenhängende Cluster anzunehmen, können Sie die Option „Dateien in freien Clustern allokationsavers ausgliedern“ *ab*wählen. Als Beispiel stellen Sie sich 9 aufeinanderfolgende Clusters in einer Partition vor: f1 f2 f3 b1 b2 b3 f4 f5 f6. Dies sind 3 freie Cluster, gefolgt von 3 benutzten Clustern und nochmal 3 freie Cluster. Das Ausgliedern aus dem freien Speicher unter Vermeidung allozierter Cluster kann eine Datei ergeben, die aus f1 f2 f3 f4 f5 f6 besteht. Ohne die „allokationsaverse“ Option können Sie eine Datei erhalten, die aus f1 f2 f3 u1 u2 u3 besteht.

Die Option „Ext2/Ext3-Block-Logik anwenden“ veranlaßt diese Wiederherstellungsmethode ebenfalls, von der Standardannahme nicht-fragmentierter Speicherung abzuweichen: Statt dessen folgt sie dem typischen Ext-Block-Muster, in dem beispielsweise der 13. Block ab dem Header der Datei als indirekter Block betrachtet wird, der selbst auf die folgenden Datenblöcke verweist. Diese Option zeigt keine Wirkung, wenn sie auf Partitionen angewendet wird, von denen WinHex weiß, dass sie ein anderes Dateisystem als Ext2 oder Ext3 haben oder wenn ein Header gefunden wird, der nicht an einer Block-Grenze ausgerichtet ist.

Sie können den gesamten Dateityp-Baum in diesem Dialogfenster per Schalter aufklappen oder einklappen. Das ist nützlich, weil Sie bei aufgeklapptem Baum komfortablerweise durch Eintippen der ersten paar Buchstaben einer Dateityp-Beschreibung automatisch zum ersten dazu passenden Eintrag im Baum springen können.

Da auf ein ggf. vorhandenes Dateisystem (funktional oder nicht) nicht zurückgegriffen wird, sind dieser Methode die Original-Datei*größen nicht bekannt*, und die Original-Datei*namen* auch nicht. Das ist der Grund, warum die resultierenden Dateien zumeist nach folgendem Muster benannt werden: Prefix#####.ext. "Prefix" ist ein von Ihnen angegebenes optionales Präfix. "#####" ist eine laufende Nummer pro Asservat. "ext" ist die Dateinamenserweiterung, die laut den Dateityp-Definitionen zu diesem Dateitype gehört. Das Präfix für den Ausgabedateinamen darf optional einen Platzhalter "%d" enthalten, der durch den Datenträgernamen ersetzt wird. Dies ist nützlich, wenn Sie "Dateien retten nach Typ" auf mehrere Datenträger auf einmal anwenden und später leicht erkennen können möchten, welche Datei von welchem Datenträger stammt.

Mit Specialist-Lizenzen oder höher gilt bei aktiver Option „aussagekräftige Benennung“: Exif-JPEG-Dateien werden optional automatisch nach dem Digitalkamera-Modell benannt, das sie erzeugt hat, sowie nach ihrem internen Zeitstempel, sofern verfügbar. Viele Windows-Registry-Hive-Dateien erhalten ihren ursprünglichen Namen, ebenso einige JPEG-Dateien, für die Photoshop einen Namen in den internen Metadaten hinterlegt hat. Bei JPEG-Dateien ohne bekannten Namen und ohne Exif-Metadaten, die jedoch von einem bekannten Generator erzeugt wurden, wird in Klammern eine Zusatzinformation an den Namen angehängt (s. Generator-Signatur). Thumbs.db-Dateien werden immer thumbs.db genannt, index.dat immer index.dat. Das o. g. Präfix wird nicht zusammen mit Originaldateinamen verwendet.

Es kommen intern diverse Algorithmen zur Anwendung, die versuchen, Dateien vieler

verschiedener Typen (u. a. JPEG, GIF, PNG, BMP, TIFF, Nikon NEF, Canon CR2 raw, PSD, CDR, AVI, WAV, MOV, MPEG, MP3, MP4, 3GP, M4V, M4A, ASF, WMV, WMA, ZIP, GZIP, RAR, 7Z, TAR, MS Word, MS Excel, MS PowerPoint, RTF, PDF, HTML, XML, XSD, DTD, PST, DBX, AOL PFC, Windows Registry, Prefetch, index.dat, SPL, EVTX, EML) in ihrer ursprünglichen, korrekten Größe wiederherzustellen, indem es deren Datenstrukturen untersucht. Das betrifft die Einträge in der Dateityp-Definitionsdatei, mit einem "~" in der Footer-Spalte. Die Einträge sollten nicht verändert werden, sonst funktioniert die Größen- und Typerkennung für diese Dateitypen u. U. nicht. Alternativ kann auch eine Footer-Signatur helfen, das Ende einer Datei zu finden. Dateien, für die kein interner Algorithmus existiert oder für die ein verfügbarer interner Algorithmus die ursprüngliche Größe nicht ermittelt und für die auch kein Footer gefunden wird, werden mit der in der Dateityp-Definitionsdatei angegebenen Normalgröße wiederhergestellt. Seien Sie eher „großzügig“ beim Angeben einer solchen Normalgröße, da „zu groß“ wiederhergestellte Dateien durchaus noch von ihren zugehörigen Anwendungsprogrammen geöffnet werden können, frühzeitig abgeschnittene unvollständige Dateien aber nicht. Der Versuch, die Originalgröße von Dateien bestimmter Typen herauszufinden durch Suche nach einem etwaigen definierten Footer wird begrenzt durch ein *Größenerkennungslimit*, das optional ebenfalls in der Definitionsdatei hinterlegt werden kann, hinter der Normalgröße und einem Schrägstrich. Ein solches Limit ist erforderlich, um zu verhindern, dass der Footer einer Datei in der gesamten Partition gesucht wird, was bei einer sehr großen Partition ziemlich zeitraubend wäre. Außerdem wird es immer unwahrscheinlicher, den richtigen Footer zu finden, je weiter entfernt vom Header man sucht, und selbst wenn er sehr weit entfernt gefunden wird, ist eine solche Datei wahrscheinlich fragmentiert oder teilweise überschrieben o. ä. Die Normalgröße wird, wenn nicht angegeben, als 1 MB angenommen. Die Maximalgröße, wenn nicht angegeben, beträgt das 64-fache der Normalgröße.

Datei-Header sind i. d. R. am Anfang eines Clusters zu finden, denn dort platzieren Dateisysteme i. d. R. Dateianfänge. Es ist allerdings gründlicher (und nicht langsamer), nach Dateiheadern auch an *Sektor*-Grenzen suchen zu lassen, um auch Dateien von einer früheren Partition mit einem anderen Cluster-Layout finden zu können, so dass dies das Standardverhalten ist. Wenn der Algorithmus auf einen physischen Datenträger oder eine einfache Datei angewandt wird, wo keine Cluster definiert sind, muss WinHex ohnehin an Sektorgrenzen suchen. Es gibt noch eine weitere Möglichkeit, die vollständige Suche auf *Byte*-Ebene. Diese ist erforderlich, wenn Sie versuchen, Dateien zu finden, die nicht verlässlich an irgendwelchen Sektorgrenzen ausgerichtet sind (z. B. Dateien in Backup-Dateien oder in Tape-Images oder sonstige in andere Dateien eingebettete Dateien) sowie für Datensätze/Einträge/Micro-Formate/Hauptspeicher-Artefakte usw. usf., d. h. nicht vollständige konventionelle Dateien. Damit kann allerdings eine erhöhte Zahl von fälschlicherweise erkannten Datei-Headern einhergehen, also Bytewertfolgen, die zufällig auf einem Datenträger vorkommen, aber dort nicht den Anfang einer Datei anzeigen. Individuelle Flags in der Dateityp-Definitionsdatei können je nach Dateityp für eine passende Behandlung sorgen, also Suche an Cluster-, Sektor- oder Byte-Grenzen.

Anfangssektoren von im Datei-Überblick bekannten Dateien werden zumeist von der Datei-Header-Signatur-Suche ausgeschlossen, um Duplikate zu vermeiden. Dies kann streng oder weniger streng erfolgen. Weniger streng bedeutet, wenn die Signaturdefinition oder die interne Dateigrößenerkennung stark genug ist, um anzudeuten, dass eine bekannte gelöschte Dateien mit einer neuen Datei überschrieben wurde, dann wird die vermutete neue Datei aus den Sektoren ausgegliedert, obwohl sie denselben Anfangssektor wie eine bekannte Datei aufweist. Eine generelle Ausnahme betrifft die Startsektoren von komplett uninitialisierten Dateien (d. h.

Dateien mit einer "valid data length" von Null), die immer so behandelt werden, als gäbe es keine dort bekannten Dateien. Außerdem wirken Anfangssektoren von bekannten Dateien, die nicht exakt an Sektorgrenzen ausgerichtet sind, ebenfalls nicht bei der Duplikatsverhinderung mit. (Die Anfangssektoren solcher Dateien sind keine saubere Art, solche Dateien zu identifizieren.)

If you intentionally abort the file header signature search or if the file header signature search causes X-Ways Forensics to crash, next time when you start a file header signature search in the same evidence object, you will find an option to resume it right where it was interrupted, or where it was when the volume snapshot was last saved before the crash occurred (depends on the auto-save interval of the case).

Sie können den Erfassungsbereich der Datenrettung wenn gewünscht auf einen ggf. ausgewählten Block einschränken und/oder auf belegten oder unbelegten Speicher (bei einem logischen Laufwerk oder einer Partition verfügbar). Um nur Dateien zu retten, die gelöscht worden sind, wählen Sie unbelegten Speicher. Dateien, die z. B. nur aufgrund von Dateisystemfehlern nicht mehr zugreifbar sind, können dagegen durchaus noch in als belegt gekennzeichneten Clustern gespeichert sein.

Die Auswirkungen von NTFS-Kompression auf Dateiinhalte können bei der Datei-Header-Signatursuche optional besonders berücksichtigt werden (nur mit forensischer Lizenz), in vielen Fällen erfolgreich. Wenn die Signatur einer NTFS-komprimierten Datei gefunden wird, wird die Datei als komprimiert gekennzeichnet, und es wird versucht, die Datei bei Bedarf automatisch zu dekomprimieren, mit einem ausgeklügelten Algorithmus, der sogar aus mehreren Kompressionseinheiten bestehende Dateien dekomprimieren kann.

8.3 Dateityp-Definitionen

„File Type Signatures *.txt“ sind durch Tabulatorzeichen in Spalten aufgeteilte Textdateien, die als Datenbank von Dateityp-Definitionen fungieren. Sie werden verwendet beim Erweitern des Datei-Überblicks und beim Befehl Dateien retten nach Typ.

WinHex ist werksseitig mit verschiedenen Dateityp-Signatur-Definitionen ausgestattet. Sie können diese Definitionen aber beliebig an Ihren Bedarf anpassen und erweitern, entweder in der Datei „File Type Signatures Search.txt“ oder in zusätzlichen Dateien desselben Formats, die „File Type Signatures *.txt“ heißen und ebenfalls geladen werden. Letzteres hat den Vorteil, dass solche Dateien nicht überschrieben werden, wenn Sie das nächste Mal ein Update installieren und einen nicht bereits verwendeten Dateinamen benutzen. Nur wenn der Dateiname das Wort „Search“ enthält, werden die in der Datei definierten Typen auch für die Datei-Header-Signatur-Suche benutzt, sonst nur für die Überprüfung des Typs von Dateien, die bereits im Datei-Überblick enthalten sind (nur mit forensischer Lizenz). Insgesamt werden bis zu 4096 Einträge unterstützt (1024 für die Suche).

Klicken Sie den Schalter „Typ-Definition“ bzw. „Signaturen“ an, um die Datei „File Type Signatures Search.txt“ zu editieren. Standardmäßig öffnet WinHex die Datei in MS Excel. Das ist bequem, weil die Datei aus Spalten besteht, die durch Tabulatorzeichen getrennt sind. Wenn Sie die Datei mit einem Text-Editor verändern, stellen Sie sicher, dass die Tabulatorzeichen erhalten

bleiben, denn WinHex verlässt sich beim Interpretieren der Datei auf deren Vorhandensein. MS Excel erhält sie automatisch. Nach dem Editieren der Dateityp-Definitionen müssen Sie das Dialogfenster schließen und erneut aufrufen, damit Sie die Änderungen in der Dateityp-Definitionsdatei sehen.

1. Spalte: File Type

Eine menschenlesbare Bezeichnung des Dateityps, z. B. "JPEG". Nur die ersten 19 Zeichen werden berücksichtigt.

2. Spalte: Extensions

Einer oder mehrere Dateinamenserweiterungen, die typischerweise für diesen Dateityp benutzt werden, z. B. "jpg;jpeg;jpe". Geben Sie die üblichste Erweiterung zuerst an, denn diese wird für die Benennung wiederhergestellter Dateien verwendet. Wird die erste Erweiterung außerdem in Großbuchstaben angegeben, wird sie bei der Typprüfung für die Typspalte verwendet, auch wenn die Datei eine der alternativen plausiblen Dateiendungen hat. Mehr 255 Zeichen unterstützt.

3. Spalte: Header

Eine eindeutige Header-Signatur, anhand derer Dateien dieses Dateityps erkannt werden können. Sie wird als regulärer Ausdruck angeben (Erläuterung unter Suchoptionen), so dass es möglich ist, variable Byte-Werte zuzulassen (z. B. bedeutet [\xE1\xE2]: "Der Byte-Wert könnte 0xE1 oder 0xE2 sein.") oder undefinierte Bereiche (.). Die Maximallänge der repräsentierten Signatur beträgt 48 Bytes. Um überhaupt geeignete charakteristische Dateiheader-Signaturen herauszufinden, öffnen Sie ein paar existierende Dateien des gewünschten Typs in WinHex und halten nach übereinstimmenden Byte-Werten nah dem Anfang der Dateien an identischen Offsets Ausschau.

4. Spalte: Offset

Der relative Offset innerhalb einer Datei, an dem die Signatur auftritt. Oftmals einfach 0. Die Signatur muss innerhalb der ersten 512 Bytes enthalten sein.

5. Spalte: Footer

Optional. Eine Signatur (Folge von Byte-Werten), die das Ende einer Datei verlässlich anzeigt, anzugeben als regulärer Ausdruck. Das kann Ihnen helfen, eine Rettung mit der korrekten Dateigröße zu erreichen. Reguläre Ausdrücke, die Daten variabler Länge repräsentieren, funktionieren u. U. nicht wie erwartet. Der Algorithmus sucht hinter dem Header nicht weiter nach Footern als durch die in Bytes angegebene maximale Dateigröße bestimmt.

Noch besser als eine Footer-Signatur ist die Verfügbarkeit eines intern in X-Ways Forensics implementierten Algorithmus, der das Dateiformat gut kennt und die korrekte Dateigröße normalerweise ermitteln kann, wenn die Datei nicht fragmentiert, unvollständig oder defekt ist. Solch ein Algorithmus wird in der Footer-Spalte mit einer Tilde (~) und einer ID-Nummer angegeben.

6. Spalte: Default size

Optional. Eine dateitypspezifische Normalgröße in Bytes, optional gefolgt von einem Schrägstrich und einer dateitypspezifischen Größenerkennungsgrenze.

7. Spalte: Flags

Optional. Flags können die Datei-Header-Signatur-Suche für bestimmte Dateitypen noch individueller und genauer gestalten, und sind ein weiteres Anzeichen dafür, wie ausgeklügelt und mächtig das Datei-Carving in X-Ways Forensics ist.

A: Means that a definition heavily depends on the associated algorithm (the one defined with the ~ character) and is too generic for identification without it.

b (kleingeschrieben): Die Signatur wird auf *B*yte-Ebene gesucht, wenn dies gemäß Einstellungen in der Benutzeroberfläche erlaubt wird. Hilfreich insbes. für Einträge/Datensätze/Mikroformate/ Speicher-Artefakte (d.h. keine vollständigen herkömmlichen Dateien), die typischerweise nicht an Sektor- oder Cluster-Grenzen ausgerichtet sind.

B (großgeschrieben): Verhindert die Suche auf Byte-Ebene nach einer bestimmten Signatur, um starke Geschwindigkeitseinbußen zu vermeiden.

c (kleingeschrieben): Wenn berücksichtigt (hängt von Einstellungen in der Benutzeroberfläche ab), werden Datei-Header ignoriert, wenn sie nicht an Cluster-Grenzen ausgerichtet sind. Dies kann für bestimmte Dateitypen hilfreich sein, um falsche Treffer zu reduzieren.

C (großgeschrieben): Kennzeichnet Dateityp-Signaturen, die nicht für die Suche nach NTFS-komprimierten Dateien berücksichtigt werden sollen, sofern der Effekt von NTFS-Kompression ausgeglichen wird, weil die Signaturen entweder zu schwach sind und zu viele falsche Treffer hervorrufen würden oder weil die Dateien des betreffenden Typs sowieso nicht komprimiert gespeichert würden.

d (kleingeschrieben, für "direkt"): Die Signatur wird wörtlich interpretiert, nicht als regulärer Ausdruck, Zeichen für Zeichen, als Byte-Werte gemäß der in Ihrem Windows-System aktiven Codepage. Useful for example if you are not very familiar with regular expressions or don't need them and just want to get all characters interpreted literally according to the code page that is active in your Windows system, without thinking much about whether the characters are considered special characters in regular expressions. For example, *<?xml version="1* is a valid signature for certain XML files, but it works only with the direct flag because the question mark has a special meaning, which results in a different byte value sequence for the signature internally if the entire expression is interpreted as a regular expression, and would not yield any matches if regular expression interpretation is active.

e: Steht für "eingebettet". Wenn ein Dateityp einen Tilde- (~) Algorithmus in der Footer-Spalte aufweist und mit diesem Flag gekennzeichnet ist, wird er voreingestellt für den Teil "Datei-Header-Signatur-Suche in nicht obig behandelten Dateien" bei der Suche nach eingebetteten Daten. Das "e"-Flag hilft lediglich dabei, die Häkchen für diese Option anfangs sinnvoll zu setzen. Letztlich ist es Sache des Benutzers, die Auswahl der Dateitypen für diese Operation in

der Benutzeroberfläche selbst festzulegen. Zusätzlich bestimmt das Flag, was für eingebettete Daten in Dateien gesucht werden, für deren Typ keine interne Extraktionsmethode eingebaut ist.

E: Wird niemals signaturmäßig eingebettet in anderen Dateien gesucht.

f (kleingeschrieben): Indicates that the specified *f*ooter signature is used to find data that is not part of the file any more and should excluded. Ordinary footers are included in the carved file. Useful for file formats that do not have a well defined footer, where the end of the file can be detected by the occurrence of data that does not belong to the file any more. That could be the same signature as the header (if files of that type occur typically in groups, back to back) or just \x00 (for file formats such as text files that do not contain zero-value bytes, where however \x00 can be expected with a high likelihood in the RAM slack). Such footer signatures should be marked as exclusive because the data matched by it is not part of the file itself.

F (großgeschrieben): Lässt X-Ways Forensics Treffer der Datei-Header-Signatur-Suche verwerfen, wenn kein zugehöriger *F*ooter gefunden werden kann, sofern eine Footer-Signatur in der Definition angegeben ist. Kann sinnvoll sein, um die Zahl der falschen Treffer zu reduzieren.

G (für "*g*ierig"): Dateien nehmen all die ihnen zugeordneten Sektoren exklusiv in Beschlag. Die Datei-Header-Signatur-Suche setzt ihre Suche nach weiteren Datei-Headern erst hinter dem mutmaßlichen Ende von solchen Dateien fort. Dieses Verfahren kann in besonderen Situationen sinnvoll sein, wenn die internen Algorithmen in X-Ways Forensics verifizieren können, dass keine andere Art von Daten innerhalb der beschlagnahmten Sektoren beginnen. Benutzer von Konkurrenzprodukten, die weniger Dateien als X-Ways Forensics finden, kennen das Überspringen von Sektoren (aber ungeprüft!) vielleicht als Standardfunktionsweise und halten es sowieso für normal. Wenn eine Datei im freien Speicher allokationsavers gecarvt wird, wird für die Fortsetzung der Datei-Header-Signatur-Suche nur ihr erstes Fragment übersprungen.

g (kleingeschrieben): Weaker version of the same flag. Only if an internal file size detection algorithm exists for a file type and if a file with the same start sector number exists already with the same file size as detected, the "g" flag will cause X-Ways Forensics to skip the affected sectors. This can help to prevent overlapping zip files and thereby avoid potentially many contained duplicate files.

h: Gibt an, dass die angegebene *H*eader-Signatur Daten findet, die nicht selbst Teil der Datei sind. Das bedeutet, dass der Header von der gecarvten Datei ausgeschlossen wird. Die gecarvte Datei beginnt dann nach dem Header. Verhindert außerdem allokationsaverses Ausgliedern von Dateien dieses Typs.

H: The definition is meant only for the signature *h*ighlighting feature, not for regular file header signature searches or for file type verification. Such definitions only require three pieces of information: The keyword or regular expression, the relative offset (typically 0) and the flag "H". The description at the start of the line is optional, but recommended because the color depends on the description, and for different descriptions you will likely see different colors. You could even create a dedicated text file, for example named "File Type Signatures Search Highlighting.txt", that defines various keywords or regular expressions that you are always interested in and would like to get highlighted immediately in every case even before running appropriate searches. Also useful if you analyze or reverse-engineer file formats, where for example records do not have a

fixed length (so that the record presentation option in WinHex is not applicable), but are identifiable by signatures.

L: Identifies links that merely link to other definitions. Useful for example to have an entry for OpenOffice files, which was missed by some users and whose absence could lead to the misconception that it is not possible to carve OpenOffice files. If the entry for OpenOffice is selected for carving, this internally automatically selects zip archives for carving, which makes sense because OpenOffice files technically are zip files and can be carved as such. The disadvantage is just that other zip archives that are not OpenOffice files are also carved. However, those files will be distinguishable thanks on the internal file type detection, for example based on the automatically assigned filename extension.

S: Marks signatures that are good enough for the file header signature search (probably in conjunction with a carving algorithm), but not for file type verification because of occasional misidentifications. This flag should be very rarely needed.

t: Signalisiert X-Ways Forensics, dass der *T*yp von gecarvten Dateien nicht sofort als bestätigt dargestellt werden soll. Nützlich z. B. für Dateiformat-Familien wie XML, damit der exakte Untertyp später bei der Dateityp-Prüfung bestimmt werden kann.

u (kleingeschrieben): Erlaubt es, Dateien nur in laut Dateisystem *u*nbenutzten Clustern zu carven.

U (großgeschrieben): Erlaubt es, Dateien nur in laut Dateisystem *u*nbenutzten Clustern zu carven, die außerdem nicht bekanntermaßen zu einer im Datei-Überblick befindlichen ehemals existierenden Datei gehören. Dies erfordert eine „Bereinigung“ des freien Speichers. Wenn diese in den Optionen des Datei-Überblicks abgewählt ist, funktioniert ein großgeschriebenes U genau wie ein kleingeschriebenes u.

W (großgeschrieben): Identifiziert Header-Signaturen, die zu schwach sind, um den Typ einer Datei neu zu erkennen, aber gerade noch gut genug sind, um den Typ, den bereits die Dateinamenserweiterung andeutet, zu bestätigen.

x: Identifiziert Dateitypen, für die es relativ normal ist, wenn die tatsächliche Dateinamenserweiterung von der Standarderweiterung abweicht, so dass Dateien eines solchen Typs nach der Typprüfung nicht als "anders erkannt" dargestellt werden, sondern lediglich als "neu erkannt", damit die Dateien nicht mehr Aufmerksamkeit auf sich ziehen als ihnen zusteht.

y: Identifiziert Dateitypen, die bekanntermaßen intern Verschlüsselung verwenden, so dass Dateien dieser Typen, die aus Sektoren ausgegliedert wurden, automatisch in der Attributspalte mit "e!" gekennzeichnet werden können.

8.4 Manuelle Datenrettung

WinHex bietet nicht nur verschiedene automatische Datenrettungsmechanismen an, es ist auch ein sehr mächtiges Werkzeug, um Daten manuell (von Hand) zu retten. Es ist möglich, verlorengegangene oder logisch gelöschte Dateien (oder allgemeiner: Daten), die nur im Dateisystem als

„gelöscht“ verzeichnet sind, aber nicht tatsächlich *physisch* gelöscht oder überschrieben wurden, zu retten.

Öffnen Sie das logische Laufwerk, auf dem sich die gelöschte Datei befand, mit dem Disk-Editor. Prinzipiell können Sie eine solche Datei wiederherstellen, indem Sie die Datenträger-Sektoren, die dieser Datei zugeordnet waren, als aktuellen Block auswählen und mit dem Menübefehl „Bearbeiten | Block kopieren | In neue Datei“ speichern. Allerdings kann es sich als schwierig erweisen, die Sektoren, in denen die Datei noch gespeichert ist, zu *finden*. Es gibt zwei verschiedene Möglichkeiten, dies zu bewerkstelligen:

1. Falls Sie einen kurzen Ausschnitt aus der Datei, die Sie suchen, genau kennen (z. B. die charakteristische Signatur im Header einer JPEG-Datei oder die Wörter “Sehr geehrter Herr Meier” in einem MS-Word-Dokument), suchen Sie diesen auf dem Datenträger unter Zuhilfenahme der diversen Suchfunktionen (u. a. „Text suchen“ oder „Hex-Werte suchen“). Dies ist eine sehr einfache und zuverlässige Möglichkeit.

2. Falls Sie nur den Namen der gesuchten Datei kennen, brauchen Sie etwas Hintergrundwissen über das Dateisystem auf dem Datenträger (FAT16, FAT32, NTFS, ...), um Spuren des ehemaligen Verzeichniseintrags oder einer sonstigen Datenstruktur der Datei zu finden und dadurch die Nummer des ersten der Datei zugeordneten Clusters zu ermitteln.

Möglicherweise stoßen Sie auf das Problem, dass die wiederherzustellende Datei fragmentiert ist, also nicht in aufeinanderfolgenden, zusammenhängenden Clustern gespeichert ist. In FAT-Dateisystemen kann der nächste Cluster einer Datei in der Dateizuordnungstabelle am Anfang des Datenträgers nachgeschlagen werden, aber diese Information geht beim Löschen einer Datei verloren.

9 Optionen

9.1 Allgemeine Optionen

1. Spalte:

- Unter Windows Vista und neuer kann es empfehlenswert sein, WinHex/X-Ways Forensics **immer als Administrator auszuführen**, wenn Sie sektorweisen Zugriff auf Datenträger benötigten. Dies kann in der Windows Registry automatisch in HKEY_CURRENT_USER unter \Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers vorgemerkt werden, wirkt sich aber nicht auf Installationen auf Wechseldatenträgern aus.

- Sie können WinHex auf Wunsch **mehrfach zugleich ausführen**. In der Voreinstellung ist die Option halb gewählt. Das bedeutet, dass Sie beim erneuten Ausführen der .exe-Datei gefragt werden, ob Sie eine neue Instanz starten möchten oder abbrechen. Sie können dann sogar versuchen, eine in einer Endlosschleife gefangenen vorherige Instanz wiederzubeleben. Z. B. sollte das passieren, während eine bestimmte Datei bei der Erweiterung des Datei-Überblicks

verarbeitet wird, hilft dies u. U. der laufenden Instanz, aus der Endlosschleife auszubrechen und mit der nächsten Datei fortzufahren. Die zweite Instanz zeigt auch einige technische Informationen darüber an, was die vorherige Instanz zu dem Zeitpunkt tut. Diese Analyse ist auch ohne Wiederbelebung der vorherigen Instanz möglich. Abbrechen stellt das Hauptfenster der vorherigen Instanz in den Vordergrund. Es ist auch möglich, eine vorherige Instanz sofort unsauber zu beendet. Das sollte normalerweise vermieden werden, da es mit Datenverlust einhergehen kann.

- Wenn mehrere Instanzen (Sessions, Prozesse) von WinHex/X-Ways Forensics zur selben Zeit auf demselben Computer laufen, werden diese Instanzen beginnend mit 1 durchnummeriert. Die Instanznummer kann nun nicht nur der sog. About-Box entnommen werden (das Fenster, das aufgeht, wenn Sie die Versionsnummer in der oberen rechte Ecke des Hauptfensters anklicken), sondern für zusätzliche Instanzen auch direkt in der Überschriftsleiste des Hauptfensters angezeigt werden, so dass es leichter fällt, die Instanzen in der Windows Task-Bar und im Windows Task-Umschalter voneinander zu unterscheiden. Dieses Verhalten hängt ab von einem neuen Kontrollkästchen im Dialogfenster mit den allgemeinen Optionen, oben links. Wenn das Kontrollkästchen zur Unterscheidung von Instanzen voll gewählt ist, haben die unterschiedlichen Instanzen zur besseren Unterscheidung ihre eigenen (frei wählbaren) Hintergrundfarben. Beachten Sie bitte noch: Wenn Sie ältere Instanzen beenden und neue starten, dann nehmen die neuen Instanzen wieder dieselben früheren Instanznummern beginnend mit 1 in Beschlag.

- Beim **Programmstart** kann WinHex optional das sog. **Start-Center** anzeigen oder die letzte **Fensteranordnung wiederherstellen** (alle Fenster mit ihren Größen und Positionen, wie Sie sie am Ende der vorhergehenden WinHex-Sitzung verlassen haben).

- Standardmäßig werden **Editierfenster** nicht **maximiert geöffnet**.

- Geben Sie die Zahl der **zuletzt geöffneten Dokumente** an, die WinHex sich **merken** und im Start-Center anzeigen soll (max. 255). Bis zu 9 davon werden gleichzeitig auch am Ende des Dateimenüs aufgeführt.

- Wenn die Option „**Dateidatum und -zeit beibehalten**“ aktiviert ist, werden Datum und Uhrzeit der letzten Änderung einer Datei beim Speichern mit Datei | Speichern (unter) auf dem Stand belassen, den die Datei zum Zeitpunkt des Öffnens hatte.

- **Weitere Kontextmenüs**: Wenn ganz gewählt oder wenn beim Rechtsklick auf ein Verzeichnis im Falldatenfenster die Umschalt-Taste gedrückt gehalten wird, erscheint ein Kontextmenü, mit dem Sie das rechts angeklickte Verzeichnis rekursiv erkunden können (ganz so wie wenn kein Kontextmenü bei einem Rechtsklick angezeigt wird), das Verzeichnis rekursiv markieren können (genau wie durch Drücken der Leertaste), das Verzeichnis rekursiv aufklappen können (genau wie beim Drücken der Multiplikationstaste im Ziffernblock), das Verzeichnis rekursiv einklappen können, einen Teilbaum als ASCII-Textdatei exportieren können oder den kompletten Pfad des Verzeichnisses in die Zwischenablage kopieren können. Wenn zumindest half gewählt oder die Umschalt-Taste beim Rechtsklick der Hex-Editor-Anzeige gedrückt gehalten wird, erscheint dort ebenfalls ein geeignetes Kontextmenü.

- **WinHex** kann sich **im Windows-Kontextmenü** eintragen. Das Kontextmenü (s. u.) sehen Sie, wenn Sie im Windows-Explorer oder auf dem Desktop mit der rechten Maustaste ein Objekt anklicken. Wenn Sie die Option nur halb aktivieren, gibt es keinen Kontextmenü-Eintrag für einzelne Dateien.

- Ein dreistufiges **Kontrollkästchen** kann optional das Starten von Windows-Bildschirmschonern verhindern und damit u. U. auch die Notwendigkeit, das Passwort der aktuell angemeldeten Benutzers erneut einzugeben. Dies wirkt sich entweder nur dann aus, wenn gerade länger andauernde Operationen laufen, die vom Fortschrittsanzeigefenster begleitet werden (wenn nur halb angekreuzt), oder aber während der gesamten Laufzeit des Programms (wenn ganz gewählt). Diese Optionen hat einen Effekt, egal ob das Hauptfenster sichtbar ist oder nicht und egal ob das Programm im Hintergrund oder Vordergrund läuft. Nützlich zum Beispiel beim Sichern eines laufenden Systems vor Ort, wenn Sie ungern die Kontrolle über das System verlieren würden während, die Sicherung läuft, oder einfach nur deshalb, weil Sie die Fortschrittsanzeige einer laufenden Vorgangs auf Ihrem eigenen Rechner von einer anderen Ecke Ihres Büro aus im Auge behalten möchten.

- Benutzer können ihre eigenen Tooltips definieren, für vier Arten von Steuerelementen in Dialogfenstern: Kontrollkästchen, Radioschalter, herunterklappbare Listen und gewöhnliche Schalter (außer "OK", "Abbrechen" und "Hilfe"). Das ist möglich, indem Sie solche Elemente bei gedrückt gehaltener Umschalttaste anklicken, und nützlich für individuelle Notizen und Ideen, so dass Sie Ihre bevorzugten Einstellung für verschiedene Situationen und ihre Bedeutungen beschreiben und sich daran besser erinnern können. Die Tooltip-Texte werden in einer Datei namens **Tooltips.txt** gespeichert und können auch mit anderen Benutzern ausgetauscht werden, z. B. innerhalb einer Organisation, um Ihre Kollegen darauf aufmerksam zu machen, welche Einstellungen gemäß den bei Ihnen definierten Konventionen verwendet werden sollen. Tooltip-Texte werden in Unicode gespeichert, dürfen bis zu 510 Zeichen lang sein und können zu Formatierungszwecken Zeilenumbrüche enthalten. Anhand eines grauen Sternchens links können Sie erkennen, dass für ein bestimmtes Steuerelement ein benutzerdefinierter Tooltip verfügbar ist. Eine englischsprachige Tooltips.txt-Datei ist im Download enthalten. Wenn Sie Tooltips aus der Datei laden möchten, stellen Sie bitte sicher, dass das Kontrollkästchen namens „Tooltips.txt“ mit einem Häkchen versehen ist.

- **Einstellungen in .cfg-Datei speichern**: If half checked, the settings are saved whenever the program terminates (cleanly). If fully checked, then every time when you click OK in any dialog window (could be useful if the program does not terminate cleanly, to avoid that you lose your later settings). If totally unchecked, the program settings will not be saved at all, except if you hold the Shift key when exiting the program, which is necessary once if you would like to save in the .cfg file the setting that from then on the settings should not be saved again.

- Festplatten-**Partitionen** werden standardmäßig basierend auf ihrer **Lage** durch**nummeriert**.

- Wenn die Option „**Gelöschte Partitionen erkennen**“ eingeschaltet ist, versucht WinHex, leicht zu findende gelöschte Partitionen zu entdecken, die sich in Lücken zwischen existierenden Partitionen befinden oder direkt am Anschluss an die letzte Partition im unpartitionierten Bereich, und zwar beim Öffnen physischer Festplatten. Solcherlei zusätzlich

erkannte Partitionen werden im Zugriffsschaltermenü mit aufgelistet und dort als gelöscht gekennzeichnet. Bitte beachten Sie, dass in Partitionslücken gefundene gelöschte Partitionen die Partitionsnummerierung beeinflussen. Z. B. wird eine Partition Nr. 3 zu Partition Nr. 4, wenn vor ihr eine gelöschte Partition erkannt wird.

- You can control whether opening volumes should include **volume slack**, i.e. those remaining sectors in a partition that don't add to another cluster. The data in that area, aside from a potential NTFS backup boot sector, does not belong to that volume logically and was stored there before the volume was created. It is not needed to parse the file system or to mount the volume (though some tools may output an error message if it's not included). Including such data in a volume image can be an IT security leak if only the regularly accessible part of the volume had been sanitized (wiped) before usage, not the entire partition or physical storage device.

- Wenn die Option „**Auf Überhangsektoren testen**“ ausgeschaltet ist, versucht WinHex nicht, beim Öffnen einer physischen Festplatten auf Überhangsektoren zuzugreifen. Diese Sektoren befinden sich am Ende der Festplatte, außerhalb der logischen C/H/S-Geometrie, weshalb sie vom Betriebssystem nicht benutzt werden. Falls zusätzliche Sektoren gefunden werden, speichert WinHex deren Erkennung für das nächste Mal, wenn Sie eine Festplatte physisch öffnen. Sie können dann aber immer noch einen erneuten Test erzwingen, indem Sie beim Öffnen die Shift-Taste gedrückt halten. Das Testen auf Überhangsektoren kann auf einigen Systemen *in Ausnahmefällen* sehr lange Wartezeiten mit sich bringen, merkwürdiges Verhalten des Windows-Systems oder sogar Schäden an der Betriebssystem-Installation hervorrufen.

- Die **alternative Plattenzugriffsmethode 1** für physische Festplatten kann Ihnen u. U. Zugriff ermöglichen auf Festplatten, die mit einer unkonventionellen Sektorgröße formatiert sind, oder andere Datenträger, auf die sonst nicht zugegriffen werden kann. Beachten Sie, dass diese Zugriffsmethode langsamer als die reguläre sein kann. Wenn die Verlangsamung beträchtlich ist, informiert Sie WinHex darüber und empfiehlt, zur Standardzugriffsmethode zurückzukehren. Die Wirkung der **Zugriffsmethode 2** beschränkt sich ebenfalls auf physische Festplatten. Bei Alternativmethoden erlauben es, einen Time-Out in Millisekunden anzugeben, nach dessen Ablauf Leseversuche abgebrochen werden. Dies kann nützlich sein beim Umgang mit Festplatten, die defekte Sektoren aufweisen, wenn das versuchte Lesen eines einzigen Sektors sonst zu einer Verzögerung von vielen Sekunden oder Minuten führt.

- „**Caching beim Lesen von Sektoren**“ beschleunigt den sequentiellen Datenträgerzugriff durch den Disk-Editor. Diese Option empfiehlt sich insbes. beim Durchsehen von CD-ROM- und Disketten-Sektoren, da sie die Zahl der erforderlichen physischen Zugriffe stark herabsetzt.

- Eine weitere Option ist es, den Benutzer beim Interpretieren von **Roh-Images** immer die **bevorzugte Handhabung** bestätigen zu lassen, d. h. von welcher Art von Image (Volume oder Disk) ausgegangen werden soll, welche Sektorgröße angenommen werden soll und in welchem Pfad ggf. weitere Image-Datei-Segmente gesucht werden sollen. Das ist genau das, was auch passiert, wenn Sie die Umsch-Taste gedrückt halten während des Interpretierens eines Images als Datenträger oder beim Hinzufügen eines Images zum Fall. Normalerweise

nicht nötig, wenn das Image von X-Ways Forensics selbst erzeugt wurde, aber dennoch, bestimmte Wechseldatenträger (USB-Sticks und Speicherkarten) können zu unterschiedlichen Zeiten sowohl als Volume als auch als partitionierter Datenträger formatiert und verwendet worden sein. In solchen Situationen kann das Interpretieren als Volume und als Disk unterschiedliche Dateisysteme zum Vorschein bringen, die einander überlappen.

- Das **Ersatzmuster für nicht lesbare Sektoren** wird in einem separaten Kapitel beschrieben.

2. Spalte:

- Ändern Sie wenn nötig den **Ordner**, in dem die **temporären Dateien** angelegt werden. Voreingestellt ist der Ordner, den die Umgebungsvariable „TEMP“ Ihres Systems angibt. Sie können statt eines absoluten Pfads auch einfach einen Punkt (.) eingeben. Dieser steht stellvertretend für das Verzeichnis, von dem aus WinHex/X-Ways Forensics ausgeführt wird. Oder .. für das übergeordnete Verzeichnis. Oder geben Sie einen relativen Pfad ein bezogen auf . oder .., z. B. .\temp oder ..\temp. Dieses Prinzip gilt auch für die folgenden Ordner.

- Ebenfalls wählen können Sie den **Ordner**, in dem die **Sicherungsdateien** (Images und WHX-Backups) angelegt und erwartet werden.

- Bestimmen Sie außerdem den **Ordner**, in dem **Fälle und Projekte** erzeugt und erwartet werden. Standardmäßig geschieht dies in dem Verzeichnis, in dem WinHex installiert ist.

- Außerdem definierbar ist der **Ordner**, in dem **Schablonen und Scripte** abgelegt werden.

- Bestimmen Sie ferner die **Ordner**, in denen die **internen Hash-Datenbanken** und die PhotoDNA-Hash-Datenbank verwaltet werden. The hash database of block hash values, if used at all, is stored in a directory at the same level as the first internal hash database, with the same base name plus " [block hash values]" appended.

In allen diesen Standardpfaden können Sie System- und Benutzerumgebungsvariablen verwenden, wobei der Variablenname mit Prozentzeichen zu umschließen ist, z. B. %TEMP%.

- **Oberfläche von X-Ways Investigator [CTR]/X-Ways Imager:** Verfügbar beim Betrieb mit einer forensischen Lizenz. Erlaubt das Umschalten auf die stark reduzierte Oberfläche von X-Ways Investigator [CTR], die für Ermittler gedacht ist,
  - die in Bereichen wie Wirtschaftskriminalität spezialisiert sind,
  - die kein profundes Wissen über Computerforensik benötigen,
  - die die technischen Einblicke, die WinHex und X-Ways Forensics bekanntermaßen gewähren, nicht brauchen,
  - die z. B. bequem zu handhabende X-Ways Datei-Container von versierten Computerforensik-Fachleuten erhalten mit ausgewählten Dateien verschiedener Quellen (z. B. „alle Dokumente, die die Schlüsselwörter x und y enthalten“), in denen irrelevante Dateien bereits herausgefiltert sind,
  - die Hunderte von elektronischen Dokumenten sichten müssen, relevante Dokumente erkennen, mit Kommentaren versehen, logische Strukturen und Verbindungen identifizieren und mit Hilfen von Kommentaren kenntlich machen, Dokumente drucken, und all das

möglichst mit wenigen Mausklicks, in einer einzigen Umgebung, die es ihnen erspart, jedes Dokument einzeln zu extrahieren und in der zugehörigen Applikation einzulesen,
- die möglicherweise in einer Umgebung arbeiten müssen, die von Systemadministratoren stark eingeschränkt wurde.
Der Oberfläche von X-Ways Investigator fehlen viele fortgeschrittene technische Funktionen, um Nicht-EDV-Fachleuten einen leichteren Zugang zum Programm zu gewähren. Lizenzen für X-Ways Investigator sind auf Anfrage zu 50% des regulären Preises zu erhalten. Eine optionale Datei "investigator.ini" steuert zusätzliche Vereinfachungen und administrative Sicherheitsvorkehrungen, z. B. dass Benutzer nur das Öffnen von Datei-Containern erlaubt wird, und nur solchen Containern, die als sicher klassifiziert sind.

- Windows settings for window text and background colors are adopted in WinHex/X-Ways Forensics since v20.0. Those settings can be reached with a few mouse clicks in the Control Panel in Windows XP, in Windows 7 they can still be found via Personalization | Window Color | Advanced appearance settings, and which in Windows 10 they can still be edited as raw RGB value with the Registry Editor in this key: HKEY_CURRENT_USER | Control Panel | Colors (followed by logging in and out). Black backgrounds for almost all parts of the user interface (main window, data window, Case Data window, ...) in particular are supported, which can be helpful when working in an environment with little ambient light, which generally benefits users who think they can work longer with a less bright screen, and which in general should reduce the disruption of melatonin production and the circadian rhythm among people who face screens emitting unnatural light. The viewer component respects those settings for most document types (but it does not or cannot respect them for PDF files for example). For the most complete dark screen experience you would change your entire Windows system to a dark theme. The easiest way to achieve that not only for "apps", but also real desktop applications, is to activate the black high contrast theme. In Windows 10 you would go to PC Settings | Personalization | Settings for high contrast | Activate high contrast | Contrast black. There is also an *internal* **dark mode**, which is readily available even without any of the above procedures or settings, which you can activate when needed for night time or generally, for health reasons or to attract less attention during secretive work in a dark adversary environment. It is not 100% complete, as for example it does not affect user interface elements such as window captions, pop-up menus, scrollbars, standard file selection windows or date selection boxes. For those dark mode support from Windows is needed (see above).

  Various meaningful colors in the graphical user interface have to be adjusted in X-Ways Forensics' own dark mode or when a black background color in Windows settings is detected and adopted, for example the color of file types depending on the type status. In the calendar, the grayscale coding of days with lots of activities is inversed if the background color is black. Color preferences for block selections, tag marks, "already viewed", modified bytes, and positions/search hits highlighting are remembered separately for normal mode and dark mode.

- A separate option useful in conjunction with dark mode is the ability to render pictures with the internal graphics viewing library as well as all thumbnails in the gallery darker. If that check box, which can be found next to the check box for dark mode, is half checked, that means the pixels will be darkened a little less.

- Sofern die Option „**Datei-Icons anzeigen**“ aktiviert ist, werden die in der aktuellen Datei

enthalten Windows-Icons unten in der Informationsspalte angezeigt. Enthält eine Datei keine Icons, so wird das dem Dateityp zugeordnete Icon dargestellt, wenn die Option „voll“ gewählt ist. Gilt nur für Dateien, die über Datei | Öffnen geöffnet werden.

- Bestimmen Sie außerdem das Aussehen der Dialog- und Meldungsfenster und Schalter in WinHex. Sie haben die Wahl zwischen mehreren verschiedenen Stilen.

- Im Unterdialog "Sleep(0) Frequency" besteht die Möglichkeit anzugeben, wie kooperativ sich X-Ways Forensics bei länger andauernden Operationen (wie Hashes, Suchen, ...) verhalten soll, wenn es mit anderen Prozesses um CPU-Zeit konkurriert, indem Sie UMSCH+STRG+F5 drücken. 0 ist dort die Voreinstellung (nicht außergewöhnlich kooperativ). Sie können Werte wie 10, 25, 50 oder 100 ausprobieren. 100 bedeutet maximale Bereitschaft, CPU-Zeit abzugeben. Dies ist nützlich, wenn X-Ways Forensics mehrfach zugleich von verschiedenen Benutzern auf demselben Server ausgeführt wird, damit die CPU-Zeit gerechter verteilt wird.

- Mit einer forensischen Lizenz können Sie längere Operationen von anderen Computern im selben Netzwerk aus überwachen, also sehen, ob sie noch andauern oder beendet wurden. Sie können **Fortschrittsbenachrichtigungen** über Textdateien erhalten (die in einem Verzeichnis auf einem Netzlaufwerk erzeugt werden) oder per E-Mail, in benutzerdefinierten Intervallen. Mehrere E-Mail-Empfangsadressen können einfach per Komma getrennt hintereinander angegeben werden. Der richtige SMTP-Port ist meist 25, manchmal auch 587. Die richtigen Einstellungen für den E-Mail-Versand erhalten Sie von Ihrem Administrator oder Internet-Provider.

3. Spalte:

- Entscheiden Sie, ob das Betätigen der **ENTER-Taste** Hex-Werte in die zu editierende Datei schreiben soll. In der Voreinstellung sind dies 0x0D 0x0A (=Zeilenende-Zeichen). Sie können bis zu vier zweistellige Hex-Werte angeben. Das Start-Center könnte dann immer noch mit **UMSCHALT+ENTER** geöffnet werden.

- Auf Wunsch können Sie mit der Tabulator-Taste auf Ihrer Tastatur das **Tabulator-Zeichen** erzeugen (0x09). Um dann vom Hexadezimal-Modus in den Text-Modus und umgekehrt zu wechseln, müssen Sie die Tabulator-Taste zusammen mit der Umschalt-Taste drücken.

- Nicht druckbare **Zeichen** mit einem Zeichensatzwert von kleiner als **0x20** in der Textanzeige in Form eines benutzerdefinierten anderen Zeichens repräsentiert werden. Dieses Ersatzzeichen kann auch für hohe Unicode-Werte eingesetzt werden. Es ist für das Auge angenehmer, wenn Zeichen aus anderen Sprachen als der eigenen nicht angezeigt werden, und Sie können es sich wahrscheinlich erlauben, sie nicht zu sehen, wenn Sie ohnehin nicht nach fremdsprachlichem Text (z. B. Chinesisch, Japanisch, Koreanisch) suchen. Wenn Sie nur reine 7-Bit ASCII-Zeichen brauchen (ausreichend für Englisch), in ANSI ASCII und allen UTF-16-Varianten, können Sie das Ersatzzeichen anwenden auf alle Werte oberhalb von 0x0080. Um wenigstens noch alle Buchstaben von westeuropäischen Sprachen wie Deutsch, Französisch und Spanisch zu sehen, wenden Sie es auf > 0x00FF an. Um auch noch osteuropäische Sprachen zu sehen, > 0x04FF.

- Die **Bytes** können **einzeln** als Zeichen **in der Text-Spalte** repräsentiert werden, oder WinHex kann versuchen, sie zu verbinden, was falls die in Windows aktive Codepage ein Doppel-Byte-Zeichensatz (DBCS) ist wünschenswert sein *kann*, um die richtigen Zeichen zu sehen (wenn 2 Bytes = 1 Zeichen), aber auch störend wegen der variablen Zeilenlänge. Hat nur dann einen Effekt, wenn Ansicht | Zeichensatz | *-ASCII gewählt ist, also die in Windows aktive Codepage sich auf WinHex auswirkt.

- Auf Wunsch können beim Benutzen des Arbeits**speichereditors** anstelle von Null-basierten linearen (lückenlos fortlaufend gezählten) Offsets **logische Adressen** im Speicher von Prozessen angezeigt werden. Dies geschieht grundsätzlich in hexadezimaler Schreibweise. Im Dialogfenster der Funktion »Offset aufsuchen« sind dann auch logische Adressen einzugeben.

- Es können **Seiten**- und Sektor**trennlinien angezeigt** oder ausgeblendet werden. Wenn diese Option nur halb gewählt ist, werden nur Sektortrennlinien angezeigt.

- Geben Sie an, wie viele **Bytes** in einem Editierfenster **pro Zeile** dargestellt werden sollen. Standardeinstellungen sind 16 oder 32 Bytes, je nach Bildschirmauflösung.

- Geben Sie an, wie viele **Bytes** als **Gruppe** zusammenhängend angezeigt werden sollen. I. d. R. empfiehlt sich eine Zweier-Potenz.

- There is an option to define the size of the extra gap between rows in the hex editor display in pixels, which together with the official height of the selected font defined the distance between the rows. The default value has always been 3 before v17.2, but now it can be decreased, to display more rows at the same time and see more data. For example with the Courier font the display still looks fine with an extra gap of 1, but you see 15% more data (based on font size 10). Even negative values are possible. With -1 you may see 35% more data than before.

- **Im Modus Datei Suchtreffer hervorheben:** Option, alle Suchtreffer in einer Datei zur gleichen Zeit im Datei-Modus farblich zu hinterlegen, entweder nur, wenn gerade eine Suchtrefferliste angezeigt wird (wenn halb gewählt) oder permanent, sobald die Suchtreffer eines Asservats geladen wurden, d. h. auch beim Arbeiten mit dem normalen Verzeichnis-Browser (wenn ganz ausgewählt). Suchtreffer werden geladen, wenn ein Asservat geöffnet wurde, sobald Suchtreffer aufgelistet werden. Diese Funktion betrifft eigene Suchtreffer genauso. Erfordert eine forensische Lizenz.

- **Automatische Einfärbung:** 1) Hebt die diversen Elemente von FILE-Records auf NTFS-Partitionen hervor, wenn Sie den blinkenden Cursor in einen solchen Record hineinbewegen, um das Navigieren und das Verständnis zu erleichtern. Erfordert eine Specialist- oder forensische Lizenz. Wenn nur halb gewählt, wird die Hervorhebung nur in Datenfenstern versucht, die NTFS-Volumes repräsentieren, nicht in anderen Dateisystemen oder auf partitionierten/physischen Datenträgern.

  2) Hebt ausgerichtete FILETIME-Werte in den Modi Disk/Partition/Volume und Datei farblich hervor. Nützlich beim manuellen Inspizieren diverser Microsoft-Formate, die u. U.

mehr Zeitstempel enthalten als automatisch extrahiert werden können (versuchen Sie z. B. index.dat, Registry-Hives, .lnk-Verknüpfungen usw. usf.). Wenn die untere Hälfte eines Datenfensters den Eingabefokus hat und FILETIME-Werte hervorgehoben erscheinen, können Sie auch den Mauszeiger über einen solchen Wert bewegen, um eine menschenlesbare Interpretation des Zeitstempels zu erhalten. Alternative können Sie diese natürlich wie immer auch vom Daten-Dolmetscher enthalten, wenn Sie das erste Byte eines solchen Werts anklicken. If auto-coloring for FILE records etc. is fully checked, FILETIME structures are now highlighted even if not aligned at a 4-byte boundaries.

3) X-Ways Forensics und WinHex Lab Edition: Hebt Datei-Header-Signaturen hervor, direkt in der Hex-Anzeige (X-Ways Forensics: Modi Disk/Partition/Volume und Datei). Die Identifikation erfolgt durch Anwenden der Signaturdefinitionen in "File Header Signatures Search *.txt" auf jeden einzelnen Offset in der aktuell sichtbaren Seite. Die "~"-Algorithmen, die oft falsche Treffer erkennen oder bei der Datei-Header-Signatur-Suche zwischen verschiedenen Untertypen unterscheiden können, kommen allerdings nicht zum Einsatz. Die farbliche Hervorhebung hilft Ihnen dabei, die Anfangspositionen von gut bekannten Daten-/Dateitypen mit bloßem Auge sofort zu erkennen, auch wenn sie in andere Daten eingebettet sind, z. B. Miniaturansichten in JPEG-Dateien, einzelne Datensätze in Zip-Archive, TIFF-Signaturen in Exif-Metadaten, Zertifikate in Windows-Registry-Hives u. v. a. m. Weitere Information erhalten Sie in der Erklärung des H-Flags der Signaturdefinitionsdatei. Wenn diese Option halb gewählt ist, werden Signaturen nur an 512-Byte-Grenzen gesucht und hervorgehoben.

- **Freien Speicher/Schlupfspeicher hervorheben:** Zeigt Offsets und Daten in weicheren Farben an (hellblau bzw. grau). Hilft, diese speziellen Laufwerksbereiche leicht zu erkennen. Erfordert eine Specialist-Lizenz oder höher.

- Sie haben die Möglichkeit, die **Hintergrundfarbe** des **Blocks** zu bestimmen.

- Wählen Sie die **Hintergrundfarbe** für jeden zweiten **Datensatz** in der Datensatz-Darstellung (s. Positions-Menü).

- Bestimmen Sie die Standardfarbe für neu aufgenommene Anmerkungen/Positionen/Lesezeichen.

- WinHex kann **veränderte Bytes**, also bereits editierte Bereiche einer Datei, eines Datenträgers oder des Arbeitsspeichers, in einer gesonderten Farbe Ihrer Wahl anzeigen, damit Sie Originaldaten von Ihren Änderungen unterscheiden können.

- Bestimmen Sie die Farbe für Schlupfspeicher und nicht initialisierten Speicher.

- Wählen Sie eine **Schriftart** für die Hex-Editor-Darstellung aus, und entscheiden Sie, ob Sie die Standard-GUI-Schriftart von Windows in den restlichen Teilen der GUI von WinHex/X-Ways Forensics verwendet sehen möchten (z. B. im Verzeichnis-Browser und im Falldatenfenster).

- Sie können die Größe der Standard-GUI-Schriftart anpassen. Eine positive Zahl von Pixeln

erhöht die Schriftgröße, eine negative Zahl verringert sie. Ein Neustart des Programms ist empfehlenswert, wenn Sie Anpassungen vornehmen. Generell ist es viel besser, bei Bedarf die DPI-Skalierung in Windows insgesamt anzupassen, weil das einen konsistenteren Effekt auf alle Elemente der GUI hat, incl. anklickbare Steuerelemente, nicht nur die Größe der Schrift in bestimmten Bereichen. Allerdings kann es Situationen geben, in denen es praktischer ist, die Schriftgröße direkt und speziell in X-Ways Forensics zu ändern, z. B. wenn Sie eine unter- oder überdurchschnittliche Sehkraft haben und Sie eine portable Installation von X-Ways Forensics öfter auf fremden Rechnern ausführen.

Die Voreinstellungen *sämtlicher* Optionen (programmweit) können durch Benutzen der Funktion „Initialisieren“ im Hilfe-Menü wiederhergestellt werden.

9.2 Notationseinstellungen

Es gibt *allgemeine* Notationseinstellungen (zu erreichen über die Allgemeinen Optionen) und separate, ggf. abweichende Einstellungen speziell für Ausgaben wie Fallberichte, den Liste-exportieren-Befehl und Wiederherstellen/Kopieren. U. a.:

- Wählen Sie Ihre bevorzugte Darstellungsweise für Datum, Zeit und Zahlen. Das ist besonders wichtig, um unabhängig zu sein von den Windows-Regionseinstellungen eines Live-Systems, das Sie ggf. einsehen, also an einem Computer, der nicht Ihr eigener ist. Jahreszahlen in Datumsangaben können optional zweistellig angezeigt werden.

- There is an option to output dates in the directory browser and in some other parts of the user interface in a nicer, longer and more locale-specific notation, which can include the weekday and the name of the month based in your language or in English. Also, that format is Unicode-capable, which allows for example for original Chinese notation of dates. Please see http://msdn.microsoft.com/en-us/library/dd317787%28v=vs.85%29.aspx for a complete explanation of what kind of notation is possible. Examples of how to represent the month (in English): MMMM = April, MMM = Apr, MM = 04, M = 4. Example of a complete format: d/MMM/yyyy (ddd) = 2/Apr/2014 (Wed).

- In Zeitangaben können optional **Sekunden**bruchteile angezeigt werden. Sie können die Anzahl der gewünschten **Dezimalstellen** angeben. Die Wirkung hängt ab von der verfügbaren Genauigkeit des ursprünglichen Zeitstempel-Formats und vom Speicherort des Zeitstempels. (Zeitstempel in Datei-Überblicken werden nur mit bis zu 4 Nachkommastellen angegeben, wobei die 4. Ziffer gerundet ist.) Die verfügbare Genauigkeit wird in jedem Fall für die Sortierreihenfolge herangezogen, auch wenn sie nicht angezeigt wird. All das ist nützlich z. B. für Dateisysteme wie NTFS, die in allen oder einigen Zeitstempeln sehr hohe Genauigkeiten unterstützen.

- Optional kann der **Abstand** von Zeitangaben **von** der **UTC-Zeit**zone direkt in dern Spalten für Zeitstempel mit angezeigt werden. Dieser Abstand hängt von der für die Anzeige gewählten Zeitzone und der Sommerzeit-Einstellung ab.

- Bestimmen Sie, ob die **Offsets** (Byte-Adressen) in **dezimaler** oder **hexadezimaler**

Schreibweise angegeben und zur Eingabe verlangt werden.

- **Hexadezimal**ziffern jenseits der 9 können entweder in Form von **Klein-** oder Groß**buchstaben** dargestellt werden (a-f, A-F).

- **Dateigrößen** können Sie optional **immer in Bytes** statt gerundet **anzeigen** lassen. Im mittleren Zustand des Kontrollkästchens betrifft das nur Größen von Objekten in Volumes, wenn vollständig gewählt auch Objekte auf physischen, partitionierten Datenträgern.

- **SHA-1- und TTH192-Hash**-Werte können optional in **Base32**-Notation im Verzeichnis-Browser **angezeigt** werden, wie in P2P-Programmen üblich.

- Wählen Sie aus drei verschiedenen Arten der **Darstellung** des **Existenz**zustands von Dateien und Verzeichnissen.

- Wählen Sie, welche Arten von **Vermerken** Sie in der Vermerk-Spalte überhaupt sehen möchten, und ob auf das Vorhandensein von Vermerken in der Namenszelle durch größere oder kleinere Dreiecke hingewiesen werden soll. Die Vermerkbezeichnungen können optional in der Vermerkspalte nach *x* Zeichen abgeschnitten werden, so dass mehr Vermerke in die Zellen des Verzeichnis-Browsers passen. Wenn diese Option halb gewählt ist, bedeutet dass, dass das Abschneiden durch drei Punkte kenntlich gemacht wird, ansonsten erfolgt es stumpf ohne Hinweis.

- Bestimmen Sie, welche Arten von Beschreibungen Sie in der Beschreibungsspalte sehen möchten. Einige „interne“ Flags können ebenfalls in der Bescheibungsspalte angezeigt werden, sofern gewünscht. Diese Flags identifizieren den Status einer Datei bezüglich Datei-Überblick-Erweiterung:
  [Emb]: wurde auf eingebettete Dateien geprüft
  [Arc]: Datei-Archiv auf Inhalte geprüft
  [Enc]: Verschlüsselungstest durchgeführt
  [Ext]: E-Mail(-Archiv) auf extrahierbare Inhalte geprüft
  [Met]: auf interne Metadaten geprüft
  [Xtn]: von einer X-Tension erzeugt

9.3 Verzeichnis-Browser

- Das **Gruppieren** von **Dateien** und **Verz**eichnisse im Verzeichnis-Browser ist optional. X-Ways Forensics merkt sich die Sortierkriterien und den Zustand dieser Option separat 1) für den normalen Verzeichnis-Browser eines Volumes, 2) für den normalen Verzeichnis-Browser eines partitionierten Datenträgers, 3) für Suchtrefferlisten und 4) für Ereignislisten. Standardmäßig ist dieses Kästchen nur halb angekreuzt. Das bedeutet, dass nur bei nichtrekursiver Erkundung gruppiert wird, also nur dann, wenn Verzeichnis für die Navigation benötigt werden und daher eine Position ganz oben in der Liste hilfreich ist/erwartet wird.

- Das **Gruppieren existent**er und **gelöscht**er Objekte im Verzeichnis-Browser ist optional. Es gibt zwei Möglichkeiten der Gruppierung: Wahlweise werden möglicherweise

wiederherstellbare Dateien (mit einem Fragezeichen versehen) und bekanntermaßen nicht wiederherstellbare Dateien (mit einem X versehen) zusätzlich intern gruppiert (dann gibt es also insgesamt drei Gruppen) oder nicht (nur zwei Gruppen). Ein kleines Symbol mit einer oder zwei horizontalen Trennungslinien zeigt an, ob die Liste in zwei oder drei Gruppen unterteilt ist, auch in dem Kopf der Spalte, die das Hauptsortierkriterium ist, als kleine Erinnerung daran, dass Sie beim Rollen im Verzeichnis-Browser und Suchen nach einer bestimmten Datei z. B. anhand ihres Namens in jeder Gruppe schauen müssen, weil die Sortierung nicht gruppenübergreifend ist sondern innerhalb jeder Gruppe stattfindet.

- Ein **Doppelklick** auf Verzeichnis **erkundet** dieses. Ein Doppelklick auf eine gewöhnliche Datei wendet den **Einsehen**-Befehl auf sie an. Diese Option steuert, ob Dateien mit Unterobjekten bei einem Doppelklick eingesehen oder erkundet werden. Wenn das Kontrollkästchen halb angekreuzt ist, werden Sie jeweils gefragt.

- Dateien können optional inklusive ihrem **Schlupf**speicher **geöffnet und durchsucht** werden. Der halb gewählte Status des Kontrollkästchens macht nur für die logische Suche einen Unterschied (s. dort).

- Ein „**..**“-Eintrag wird am oberen Ende des Verzeichnis-Browsers optional angezeigt, wenn man innerhalb eines Volumes von einem Verzeichnis in ein anderes navigiert. Sofern angezeigt, ist er am oberen Ende des Verzeichnis-Browsers fixiert und rollt nicht mit den anderen Einträgen aus dem sichtbaren Bereich heraus. Er zeigt die Details des Verzeichnisses, das er repräsentiert (dasjenige, zu dem Sie navigieren würden, wenn Sie den Eintrag doppelt anklicken), genau wie die anderen Einträge im Verzeichnis-Browser. Ein „**.**“-Eintrag wird ebenfalls optional angezeigt und repräsentiert das aktuell angezeigte Verzeichnis repräsentiert. Nützlich, falls Sie beispielsweise bestimmte Metadaten (z. B. Zeitstempel) des übergeordneten Objektes gleichzeitig mit den Metadaten der Unterobjekte sehen wollen. Und falls das von . oder .. repräsentierte Objekt eine Datei ist und Sie es auswählen, können Sie diese Datei im Datei-, Vorschau- oder Detail-Modus einsehen. Auch in der Galerie wird es mit angezeigt.

- Wenn mehrere Filter aktiv sind, werden sie normalerweise verUNDet. Das bedeutet, dass jede Datei den ersten aktiven Filter passieren muss UND auch jeden anderen aktiven Filter, um im Verzeichnis-Browser aufgelistet zu werden. Sie können Dateien aber auch mit einem logischen ODER filtern. Das bedeutet, dass jede Datei nur den ersten aktiven Filter ODER auch einen von den anderen aktiven Filtern zu passieren braucht, um aufgelistet zu werden. Wenn aktive Filter mit einem logischen ODER verknüpft werden, wird das in der Überschriftszeile des Verzeichnis-Browsers neben der Zahl der aktiven Filter vermerkt. Ein Klick auf die Anzahl der Filter oder auf das Word ODER wechselt zwischen UND- und ODER-Verknüpfung. Wenn mehrere Filter mit ODER kombiniert werden, kann das Beschreibungsfilter aber optional immer noch mit dem Ergebnis verUNDet werden, und das geschieht auch standardmäßig so, und Sie erkennen das anhand eines mit dem Wort UND beschrifteten Kontrollkästchens, das in solchen Situationen im Dialogfenster des Beschreibungsfilters sichtbar ist, und das Beschreibungsfilter wird dann separat gezählt und behandelt. Bitte beachten Sie, dass komplexe verschachtelte Filtereinstellungen mit ODER und UND durch Einsatz mehrerer .settings-Dateien realisiert werden können.

- Dass Filter auch auf Verzeichnisse angewandt werden, ist optional. Wenn aktiv, betrifft dies

aber nur tatsächlich geeignete Filter. Filter, deren Anwendung auf Verzeichnisse keinen Sinn ergibt (Typ, Typstatus, Hash, Hash-Set, Autor, ...) werden nicht angewandt.

- Das Auflisten von Unter**verz**eichnissen beim **rekursiven** Erkunden ist optional. Sie werden nicht für Navigationszwecke benötigt, wenn bereits Dateien aus allen Unterverzeichnissen aufgelistet werden und lenken eher ab, wenn Sie einfach nur alle aufgelisteten Dateien begutachten möchten. Standardmäßig ist diese Option halb gewählt. In diesem Zustand werden Verzeichnisse nur dann bei rekursiver Erkundung aufgelistet, wenn alle aktiven Filter auf Verzeichnisse anwendbar sind (Name, Zeitstempel, Besitzer, int. ID, Attribute, ...) und die Verzeichnisse auch tatsächlich durch den Filter gelassen werden.If for example both the Name filter and the Type filter are active at the same time, directories will not be listed, because even if they satisfy the Name filter, they cannot possibly satisfy the Type filter (directories do not have a file type). But if the Name filter is on and the filter for timestamps, then directories are listed if they match both filter conditions.

- Die **rekursive Auswahlstatistik** rechts unterhalb des Verzeichnis-Browsers (nur mit forensischer Lizenz) enthüllt, wie viele Unterverzeichnisse, Dateien und wieviel Daten ein Verzeichnis (oder eine Datei mit Unterobjekten) enthält, wenn es im Verzeichnis-Browser ausgewählt wird, es sei denn, es wird bereits rekursiv erkundet, unter Beachtung etwaiger aktiver Filter. Wenn diese Option nicht gewählt ist, wird nur eine Statistik über die direkte Auswahl im Verzeichnis-Browser angezeigt, nicht über ggf. indirekt mit ausgewählte Unterobjekte. Wenn die Option halb gewählt ist, berücksichtigt die Statistik nur Unterobjekte von Verzeichnissen, aber nicht Unterobjekte von Dateien.

- Das **Markieren** oder **Ausblenden** von Objekten im Verzeichnis-Browser kann **rekursiv** oder nicht-rekursiv erfolgen. Nicht-rekursiv bedeutet, dass das Markieren/Entmarkieren/Ausblenden/Einblenden einer Datei oder eines Verzeichnisses keine Auswirkung auf den Status von Eltern- und Unterobjekten oder übergeordneten oder Unterverzeichnissen hat. Nützlich z. B. wenn Sie eine Operation beim Erweitern des Datei-Überblicks auf alle Unterobjekte einer Datei anwenden möchten oder alle Unterobjekte einer Datei durchsuchen möchten, die Elterndatei selbst aber nicht. Bei rekursivem Vorgehen ist es nicht möglich, ein nicht markiertes Elternobjekt zu haben, desse Unterobjekte alle markiert sind. Im mittleren Zustand der Option erben Unterobjekte weiterhin die Markierung von ihrem Elter in dem Moment, in dem sie dem Datei-Überblick hinzugefügt werden, z. B. wenn Sie E-Mails und Datei-Anhänge aus markierten E-Mail-Archiven extrahieren. Ob Markieren und Ausblenden rekursiv funktioniert oder nicht, das können Sie auch durch Drücken der Umschalttaste steuern. Rekursives Markieren/Entmarkieren in großen Datei-Überblicken kann *sehr* langsam sein.

- **Erweitertes Sortieren**: Takes 4 to 6 times more time than the highly optimized standard Unicode sorting (noticeable when sorting millions of files), but has several useful settings and characteristics:
  - Language-specific character equivalence rules (treat ß like ss, treat é similar to e, ü similar to u etc.)
  - Linguistically improved case insensitivity
  - Special treatment of hyphens and apostrophes (they are treated differently from other non-alphanumeric characters to ensure that words such as "coop" and "co-op" stay together in a sorted list).

- Treat decimal digits as numbers, e.g. sort "2" before "10" (not useful for hexadecimal notation, available under Windows 7 and later only)
- Treat half-width and full-width characters the same (full-width characters are sometimes used by East Asians when writing English language letters)
- Ignore kana type (treat corresponding Japanese hiragana and katakana characters the same)
Advanced sorting depends on the regional settings of the currently logged on user. For example, if regional settings of a Nordic country are active, Å comes after Z, as defined in the alphabets of that region, otherwise near A, as perhaps expected by non-locals. Advanced sorting rules are also applied when sorting the search hits by the Search Hit column.

Es gibt eine Option zum Sortieren von Suchtreffern nach ihrem Inhalt und Kontext anstatt bloß des Suchbegriffes, zu dem sie gehören. Das ist nützlich für Stichwortsuchen (keine technischen Suchen, z. B. nach Hex-Werten). Das Sortieren auf diese Weise ist in der Tat langsamer, weil die Daten und der Kontext aller Suchbegriffe gelesen und in eine vergleichbare Codepage konvertiert werden müssen. Das Sortieren nach Daten in den Suchtreffern hilft bei regulären Ausdrücken, die auf variable Daten passen, denn für konstante Suchbegriffe sind die Suchbegriffe zu den Daten in den Suchtreffern identisch. Nach dem Suchen nach E-Mail-Adressen mit dem Ausdruck [a-zA-Z0-9_\-\+\.]{1,20}@[a-zA-Z0-9\-\.]{2,20}\.[a-zA-Z]{2,7} z. B. erkennen Sie durch Sortieren nach den Daten schnell etwaige vorhandene Gruppen von identischen E-Mail-Adressen und können diese schnell überspringen, oder sehen ähnliche Adressen (solche, die mit denselben Buchstaben anfangen), direkt untereinander. Das Fortsetzen des Sortierens anhand des Textes, der dem eigentlichen Suchtreffer folgt, sofern die Daten in den Suchtreffern identisch sind, präsentiert Ihnen identische oder ähnliche Textpassagen direkt untereinander und erlaubt ebenfalls ein zügigeres Durchsehen von Suchtrefferlisten. Sie können angeben, wie viele Zeichen in Daten und folgendem Kontext in das Sortieren einbezogen werden sollen. Je mehr Zeichen, desto mehr Speicher wird für das Sortieren benötigt. Das kann bei riesigen Anzahlen von Suchtreffern einen merklichen Unterschied machen.

- Optional kann das **Sortieren** direkt nach dem **Programmstart** ganz ausgeschaltet werden, so dass das Programm die beim letztem Gebrauch des Programms verwendeten Sortierkriterien vergisst, was einen Geschwindigkeitsvorteil haben kann. Ebenso wird dann beim Ausschalter aller Filter mit einem einzigen Mausklick nicht mehr sortiert, was sonst mit einer längeren Verzögerung verbunden sein könnte, wenn plötzlich wieder alle Dateien rekursiv aufgelistet werden.

- Ein 3-stufiges Kontrollkästchen bestimmt, ob das Anklicken/Auswählen einer Datei oder eines Verzeichnisses im Verzeichnis-Browser im Modus Disk/Partition/Volume die Daten aufsucht, die zu diesem Objekt gehören, oder die definierende Datenstruktur dieses Objekts im Dateisystem. Bitte bedenken Sie, dass ein schneller Sprung zu letzterem auch durch einen Klick auf die Zelle „Dateisystem-Offset“ ausgelöst werden kann, auch wenn ein Klick an anderer Stelle zu ersterem springt. Wenn das Kästchen gar nicht gewählt ist, findet in der unteren Hälfte des Datenfensters überhaupt kein Sprung statt. Dies kann nützlich sein, wenn Sie direkt auf einem physisch beschädigten Datenträger operieren, bei dem ein Zugriff auf bestimmte Sektoren oder Bereiche die Anwendung zum Hängen bringt oder das Betriebssystem zum Absturz.

- Verzeichnis-Browser-**Einstellungen** (insbes. Spaltenbreiten, Filtereinstellungen und Sortierungseinstellungen) können optional **in Fällen** ge**speichert** und beim Laden wieder aktiviert werden (sofern von einer kompatiblen Version gespeichert).

- **Dynamische E-Mail- & Datumsspalten** überlässt X-Ways Forensics die Entscheidung darüber, ob die Spalten „Absender“ und „Empfänger“ im Verzeichnis-Browser angezeigt werden sollen oder nicht. Wenn aktiv, werden sie genau dann angezeigt, wenn zumindest eine extrahierte E-Mail im sichtbaren Ausschnitt des Verzeichnis-Browsers enthalten ist. Dies ist nützlich, weil mehr Platz für andere Spalten bleibt, wenn die ausschließlich für extrahierte E-Mails gefüllten Spalten nicht benötigt werden. Die Spalten mit alternativen Zeitstempeln, incl. Erzeugung des Inhalts, können auch dynamisch angezeigt werden, nämlich dann, wenn Dateien, die solche Zeitstempel im Datei-Überblick haben, im sichtbaren Bereich des Verzeichnis-Browsers enthalten sind.

- The 1st sector column can optionally show physical start sector numbers for files in partitions (counted from the start of the physical disk or disk image) instead of logical start sector numbers, if the partition was opened from within the physical disk/disk image. In that case the column label contains a P in a circle (P for physical). Only for ordinary partitions, not Windows dynamic volumes or LVM2 volumes.

- Es gibt eine Option zum **Anzeigen** von **Dateityp-Rängen** in der Typstatus-Spalte, was auch ein **Sortieren** der Spalte nach diesen Rängen zur Folge hat. Ränge werden definiert in der Datei File Type Categories.txt.

- Die **Anzahl** der enthaltenen **Dateien** eines Verzeichnisses oder einer Datei mit Unterobjekten kann optional direkt hinter dem Namen angezeigt werden, entweder nur im Verzeichnis-Browser oder (wenn ganz angekreuzt) auch im Verzeichnisbaum im Falldatenfenster.

- Standardmäßig zeigt die Pfad-Spalte nur einen **Teilpfad** vom aktuellen Erkundungspunkt aus gesehen an, wenn man rekursiv erkundet. Das ist derselbe Pfad, den Sie mit Wiederherstellen/Kopieren erzeugt bekommen, wenn Sie dort nur einen Teilpfad wiederherstellen lassen. Nützlich z. B., wenn Sie eine Dateiliste inkl. Unterverzeichnisse an jemanden weitergeben möchten (Befehl "Liste exportieren), in der Dateien in unterschiedlichen Verzeichnissen voneinander unterscheidbar sein sollen, ohne den vollständigen Pfad der Dateien zu verraten (z. B. wenn auf Ihrem eigenen Datenträger gespeichert in einem Verzeichnis, dessen Name andere nichts angeht). Wenn ganz angekreuzt, beginnt ein Teilpfad mit dem Namen des jeweiligen Unterverzeichnisses. Wenn nur halb, wird dem ...\ vorangestellt, um die Auslassung kenntlich zu machen.

- A button with an arrow allows to right-align the path columns in case you are more interested in the end of the path and would like to keep the column width compact. The arrow points to where the paths will be aligned.

- A special file **icon** for **pictures** is available, very useful when your main focus is on such files. Depending on whether the check box is fully checked or half checked, symbols like question marks, arrows, scissors, hammers, etc. that further reveal the status of the file get superimposed additionally or not. If not, that is easier on the eye. You can still tell the exact

deletion status from the Description column, and the rough deletion/existence status is still obvious from the contrast of the icon.

- **Conditional cell** background **coloring** helps to draw your attention to items of interest without having to filter out all non-matching items. Matching items are found through a substring search in the cell contents of a selected column. Substring expressions may be up to 15 characters long. You may use an asterisk to match anything except blank cells. If a match is detected in a cell, either only the background of that particular cell can be colored (called "cell-targeted coloring") or the entire line. To color an entire column, regardless of the cell contents, activate cell-targeted coloring for that column and specify an empty condition string, i.e. no condition at all. If a cell matches multiple conditions, all of these conditions have an effect and contribute to the final color mix (the last one most), so that hopefully none of the targeted properties go unnoticed. For line-targeted coloring, only the first 255 characters in the respective cell are guaranteed to be searched.

  Conditions cannot be defined for search hit specific columns, but for event specific columns. That can prove useful when trying to identify patterns in events. For example, you could color all events of type "Program started" in red and log-in events in yellow and see more easily how far apart from each other they are. Conditional cell background coloring is case-specific if "Store directory browser settings in cases" is selected. The color settings are also stored in a file named "Conditional Coloring.cfg", and they are stored in and loaded from .settings files along with other directory browser settings. Up to 255 conditions may be defined.

Der Schalter „Alle Ausblendungen aufheben“ erlaubt es, alle ausgeblendeten Dateien und Verzeichnisse im Datei-Überblick des Asservats im aktiven Datenfenster wieder in den Normalzustand zu versetzen (einzublenden). Um selektiv nur die Ausblendung bestimmter Dateien aufzuheben, stellen Sie zunächst sicher, dass diese Dateien nicht herausgefiltert werden. Dann können Sie sie auswählen und die Ausblendung mit einem Befehl im Kontextmenü aufheben.

Es gibt einen weiteren Schalter, der es Ihnen ermöglicht, ausgeblendete Objekte aus dem Datei-Überblick gänzlich zu entfernen, wenn Sie irrelevant sind und nicht mehr benötigt werden, insbes. bedeutungslose Fehlfunde der Datei-Header-Signatursuche. Dies macht den Datei-Überblick kleiner, d. h. effizienter in der Handhabung, und spart Arbeitsspeicher. Nützlich auch, wenn Sie möchten, dass X-Ways Forensics bestimmte Dateien über die Datei-Header-Signatursuche noch einmal findet, sie dann aber z. B. mit einer anderen Standardgröße auflistet, weil die ursprünglich angegeben Standardgröße sich als inadäquat herausgestellt hat. Das Entfernen läuft schneller ab, wenn man vorher alle Suchtreffer löscht. Das Entfernen bringt es mit sich, dass die internen IDs durcheinandergewürfelt werden, d. h. nach dem Entfernen können Sie aus der internen ID nicht mehr auf die Reihenfolge schließen, in der die Objekte dem Datei-Überblick hinzugefügt wurden. Ausgeblendete Dateien, die nicht ausgeblendete Unterobjekte haben, werden nicht entfernt. Es wird sehr empfohlen, mit einer Kopie Ihres Falls zu arbeiten, wenn Sie diese Funktion nutzen, die sie z. B. mit dem Befehl „Speichern unter“ erzeugen.

Spalten

Es sind diverse Spalten im Verzeichnisbrowser verfügbar. Sie sind alle optional. Sie werden angezeigt, wenn sie eine Spaltenbreite von mehr als 0 Pixeln haben, oder versteckt, wenn ihre

Breite 0 Pixel beträgt. Eine Spalte kann auch alleine mit der Maus sichtbar gemacht oder versteckt werden, indem Sie den Spaltennamen im Dialogfenster anklicken.

Es ist möglich, die *Reihenfolge* der Spalten des Verzeichnis-Browsers anders festzulegen. Dies ändert auch die Reihenfolge der Felder im Fallbericht (d. h. in Berichtstabellen), auf Deckblättern beim Drucken, in exportieren Dateilisten und im separaten Protokoll für den Wiederherstellen/ Kopieren-Befehl. Sie können eine Spalte verschieben, indem Sie erst den der Spalte zugeordneten runden Auswahlschalter anklicken und dann den vertikalen Rollbalken, der oben erscheint. Sie ursprüngliche Standardreihenfolge der Spalten kann wiederhergestellt werden, indem Sie diese Spalte mit der *rechten* Maustaste anklicken.

9.4 Optionen des Datei-Überblicks

Diese Optionen greifen i. d. R. beim (Neu-)Einlesen eines Datei-Überblicks.

Link Hälfte des Dialogfensters

• Erweiterte Attribute (extended attributes) in NTFS werden optional in den Datei-Überblick als Unterobjekte desjenigen Verzeichnisses oder derjenigen Datei aufgenommen, zu dem/der sie gehören, mit dem Namen "$EA", und in der Attr.-Spalte "($EA)" gekennzeichnet, und zwar entweder alle solchen Attribute (wenn das Kontrollkästchen, das das steuert, ganz angekreuzt ist) oder nur die nicht-residenten (wenn halb gewählt, Voreinstellung). Wenn dies überhaupt nicht geschieht, werden Cluster, die zu nicht-residenten erweiterten Attributen von existierenden Objekten gehören, der virtuellen Datei „Diverse nicht-residente Attribute“ zugeschlagen. Hintergrundinformation: Microsoft verwendet erweiterte Attribute bei ausführbaren Dateien des System als Teil der Secure-Boot-Komponente. Angreifer haben in einigen aufsehenerregenden Fällen große erweiterte Attribute zum Verstecken von Malware genutzt. Große erweiterte Attribute werden automatisch mit einem Vermerk versehen, um sie leicht finden zu können, wenn es sie gibt.

• Das **Aufnehmen** von sog. „Logged Utility Streams“ (**LUS**) in **NTFS** in neu eingelesene Datei-**Überblicke** ist optional. Entweder werden *alle* LUS aufgenommen (wenn ganz gewählt) oder nur Nicht-$EFS-LUS (wenn halb gewählt) oder gar keine LUS. Nützlich für von Windows Vista geschriebene NTFS-Dateisysteme, wenn Sie sich nicht für $TXF_DATA-LUS interessieren.

• Aus dem Internet heruntergeladene Dateien in NTFS können bequem als solche erkannt werden, wenn ihr alternativer Datenstrom "Zone.Identifier" in Form eines Vermerks statt als Unterobjekt im Datei-Überblick abgebildet wird. Das bedeutet, dass Sie nicht zu dem Unterobjekt zu navigieren brauchen, um herauszufinden, um was für ein Unterobjekt es sich handelt. "ZoneId=3" als Vermerkbezeichnung identifiziert Dateien, die aus dem Internet heruntergeladen wurden.

• X-Ways Forensics has the ability to detect unusual or suspicious short filenames (SFNs, 8+3 character names) in NTFS. Such short filenames can optionally be output in the volume snapshot either as alternative names or as fully valid hardlinks themselves (i.e. like additional copies of the same files). They can also be labeled as "peculiar SFNs" to make you aware of them. Unexpected

SFNs that don't seem to match their corresponding LFNs could be interesting if they reflect previous names of files that have been renamed, or because they may have been specially engineered to replace sensitive files with fixed names (such as DLLs or configuration files), while their LFNs are different and perfectly innocuous. If you find that too many normal files are flagged that way, you can try UNchecking the box for "more strict matching", so that some of the less severe discrepancies are ignored.

• You can choose which copy of a FAT12/FAT16/FAT32 file allocation table to work with. This can be either a user-designated copy or the one that is defined as active in the boot sector (in case of FAT32). If neither the user selects a copy nor the boot sector defines a single copy as active, the first copy will be used, labelled as "FAT 1". The copy that was selected at the time when the volume snapshot was taken will be used for the whole lifetime of that volume snapshot, even if the settings are changed. It is displayed in the Info Pane. The Technical Details Report informs which copy or copies are considered active in the file system.

• Standardmäßig werden belegte (allozierte) Cluster in Dateisystemen vom Typ FAT12, FAT16, FAT32 und exFAT beim Lesen der Daten von gelöschten Dateien übersprungen. Das bedeutet, dass die Datei von gelöschten Dateien nicht notwendigerweise immer als zusammenhängend gespeichert angenommen werden. Es werden so viele freie Cluster vom Startcluster aus als zugehörig angenommen, wie es nötig ist, um die bekannte Dateigröße abzubilden, wobei Cluster, die im Dateisystem als von existierenden Dateien belegt markiert sind, umgangen werden. Wenn dabei das Ende des Volumes erreicht wird, wird der nächste freie Cluster vom Anbeginn des Volumes aus als nächster Cluster angenommen, so wie auch die eingebaute Logik von typischen FAT32-Dateisystem-Treibern arbeitet, die bei der Suche nach belegbaren Clustern durch das Volume rotierten. Diese Option ändert Annahmen über den Speicherort von Dateien, die bereits im Datei-Überblick enthalten sind. Daher führt eine An- oder Abwahl dieser Option auch dazu, dass sich Hash-Werte von Dateien ändern, wenn sie neu berechnet werden.

• Der zusätzliche Aufwand, den X-Ways Forensics betreibt, um gelöschte Objekte in FAT32-Dateisystemen korrekt in den Datei-Überblick aufzunehmen, ist optional. Wenn nur halb gewählt, wird nur für Unterverzeichnisse mehr Zeit investiert, nicht für Dateien.

• Wenn beim Erstellen des Datei-Überblicks auf einer CD/DVD Lesefehler auftreten (z. B. wegen Kratzern auf der Oberfläche), wissen Sie, dass nicht alle Sektoren mit den Datenstrukturen des Dateisystems lesbar sind. Das **Anzeigen** des **ISO9660**-Dateisystems auf CDs *zusätzlich* zu einem evtl. ebenfalls vorhandenen **Joliet**-Dateisystem kann nützlich sein, wenn der Joliet-Teil beschädigt ist, weil Sie dann eine zweite Chance haben, alle Verzeichnisse und Dateien aufgelistet zu bekommen, nämlich dann, wenn entsprechenden Datenstrukturen derselben Verzeichnisse im ISO9660-Bereich in *lesbaren* Sektoren liegen.

• In Ext file systems, more in-depth parsing of deleted directory entries during the initial creation of the volume snapshot is an option, covering even misaligned entries in relation to the existing directory entries. This might find additional previously existing files in Ext, at a likely manageable risk of finding some garbage entries as well.

• Eine vollständige Ausgabe von EA (erweiterten Attributen) in HFS+/APFS erfolgt standardmäßig nicht. Alle von X-Ways Forensics für relevant befundenen Attribute werden aber verarbeitet und entweder in der Metadaten-Spalte ausgegeben, wenn sie textueller Natur sind,

oder als Datei-Inhalt von residenten oder komprimierten Dateien oder als Verknüpfungen zu zugehörigen Verzeichnissen oder als Unterobjekte, die in der Attr.-Spalte mit (EA) gekennzeichnet sind. Wenn halb gewählt, werden zusätzlich "firstlink"- und "quarantine"-Attribute in der Metadaten-Spalte ausgegeben. Wenn ganz gewählt, werden sogar leere binäre PLists und gewöhnliche "Security"-Attribute als Unterobjekte ausgegeben.

• Output of simple extended attributes in Apple file systems as special lines in the Metadata column instead of child objects is optional. If included in the Metadata column, the Metadata field will also be shown in Details mode.

• Für bessere Ergebnisse beim Abgleichen mit speziellen Hash-Sets kann von geladenen **Modulen** bei der Hauptspeicher-Analyse optional jeweils nur der invariante **Header** angezeigt werden.

• Directory listings obtained from the operating system ("OS dir list"), which you get for example when adding a directory or a single file to a case as an evidence object, can be made to not show any timestamps from the file system or only the modification timestamp. That is useful if the timestamps of the files do not have the usual significance, e.g. if they reflect when you collected the files and not what timestamps they had originally at their original location.

• Wenn Sie einen Datei-Überblick erzeugen von Verzeichnissen (oder von ganzen Laufwerksbuchstaben ohne sektorweisen Zugriff), wobei nicht X-Ways Forensics selbst das Dateisystem ausliest, sondern Windows (was intern als Dateisystem "OS dir list" bezeichnet wird = operating system supported directory listing), dann können alternative Datenströme auch mit aufgenommen werden. Das können Sie abstellen, wenn ADS nicht von Interesse sind und/oder Sie Zeit sparen möchten.

• Es gibt eine Option zum schrittweisen Vervollständigen des Datei-Überblicks, wenn Sie mit Verzeichnis-Auflistungen des Betriebssystems arbeiten ("OS dir list"), wenn Sie ein Verzeichnis zum Fall hinzufügen. If selected, the volume snapshot initially just contains the contents of the top-level directory, and it is further completed only on demand, step-by-step when you manually explore subdirectories. This is exactly how the Windows Explorer/File Explorer in Windows works, and useful when dealing with slow and huge network drives that would take a long time up front to scan completely. But it's very different from the usual approach in X-Ways Forensics, and will obviously prevent you from getting a complete listing of all files when exploring recursively, simply because there is no guarantee that all files have been included in the volume snapshot yet until you have explored all subdirectories. If at any time you decide that you wish to include the contents of a certain directory in the volume snapshot recursively, you can use the "Expand all" command in the context menu of the Case Data window (right-clicking that directory) or unselect the option to complete the volume snapshot on demand and then explore that directory. Please remember that the most convenient way to expand an entire subtree is by clicking its root and pressing the multiplication key on the numeric keypad (standard feature in Windows). If the incremental completion option is active, directories that have not been explored yet are marked with an asterisk (*) in the Attr. column.

• When taking a volume snapshot of directories (or entire drive letters without sector-level access), where it's not X-Ways Forensics itself that parses the file system, but Windows (internally referred to as file system "OS dir list" = operating system supported directory listing),

alternate data streams can also be included. This can be turned off if you are not interested in ADS and/or wish to save time.

• In volume snapshots based on directory listings of the active operating system ("OS dir list"), write-locked files that are open in other processes and cannot be changed are optionally shown with an upper-case "L" in the Attr. column (for "locked"). Files that are merely kept option may be shown with a lower-case "o" if the box that represents this option is fully checked (for "open"). This could be useful when previewing or acquiring a live system, to find out which files are/were open in running processes or background services, or which executable files appear(ed) to be running/loaded. Please note that checking this for many files will take a long time. It may be practical only for specific directories of interest. This option has no effect on mapped network drives. It is possible to use the Attr. filter to quickly target open or write-locked files, and these files are higher in the sort order for the Attr. column.

• In Datei-Containern wird von v18.8 und neuer gezielt der Status der enthaltenen Dateien bzgl. Datei-Überblicks-Erweiterung (DÜE) vermerkt, d. h. ob bereits vereinzelte Standbilder zu Videos erzeugt wurden oder ob bereits eingebettete Daten gesucht wurden usw. usf. Wenn Sie sich dafür entscheiden, diesem Status zu trauen und ihn zu übernehmen, werden diese Dateien nicht erneut verarbeitet, wenn Sie sich dazu entschließen, den Datei-Überblick des Containers selbst zu erweitern. U. U. könnten Sie es bevorzugen, den DÜE-Status von Dateien in Containern nicht zu übernehmen, damit Sie nichts übersehen, wenn Sie vermuten, dass der ursprüngliche Bearbeiter keine so gründlichen Einstellungen für die Erweiterung verwendet hat wie Sie es vorhaben, oder wenn zuvor eine ältere, weniger mächtige Version von X-Ways Forensics zur Verarbeitung der Dateien eingesetzt wurde. Das Übernehmen des DÜE-Status ist eine Voraussetzung dafür, um in einem Container enthaltene Videos mit rotierend durchlaufenden repräsentativen Einzelbildern dargestellt zu bekommen.

Rechte Hälfte des Dialogfensters

• Ob **ehem. existierende Dateien** überhaupt in Datei-Überblicke aufgenommen werden sollen, ist etwas, das Sie entscheiden können. Wenn Sie an solchen Dateien nicht interessiert sind, weil Sie weder Datenrettung betreiben noch konventionelle gründliche Computerforensik, dann können Sie Zeit sparen, indem Sie solche Dateien auslassen.

• **Löschzustand vererben**: Bewirkt, dass gelöschte Partitionen ihren Löschzustand auf alles, was sie enthalten, übertragen (Dateien und Verzeichnisse), und dass gelöschte E-Mail-Archive ihren Löschzustand auf alle in ihnen enthaltenen E-Mails, Verzeichnisse und Datei-Anhänge übertragen. Das erscheint logisch, aber geht einher mit einem Verlust an Information, da je nach Bezugssystem *alles* als gelöscht angezeigt wird, selbst Dateien bzw. E-Mails, die aus Sicht des Dateisystems bzw. der E-Mail-Archivs nicht gelöscht waren, sondern noch existierten, als die Partition bzw. die Datei gelöscht wurden. Standardmäßig ist diese Option nicht aktiv, so dass X-Ways Forensics zwischen existierenden und gelöschten Dateien und E-Mails auch in gelöschten Partitionen/gelöschten E-Mail-Archiven unterscheidet, so dass mehr Informationen erhalten bleiben.

• Zusätzliche harte Verweise zur selben Datei in NTFS können optional überlesen werden, wenn Sie ein Datei-Überblick erzeugt wird. Das heißt, sie werden überhaupt nicht darin aufgenommen und werden nicht im Verzeichnis-Browser als zusätzliche Dateien aufgelistet. Das kann evtl. nützlich sein, wenn Sie versuchen, die Verteilung der Speicherplatznutzung zu verstehen, wobei das Mehrfachzählung derselben Datei keinen Sinn ergibt. Die Spalte "Verweise" zeigt dabei aber immer noch die wahre Anzahl von harten Verweisen an (die allerdings Dateinamen im reinen 8.3-Zeichenformat nicht mitzählt und die sich übrigens deutlich vom nicht besonders gut gepflegten Verweiszähler im FILE-Record unterscheiden kann).

• Neu ermittelte Namen (z. B. E-Mail-Betreffzeilen von Original-.eml-Dateien oder Namen von Dateien laut iPhone-Backups) können zu Hauptnamen im Datei-Überblick werden (und dadurch auch Teil des Pfades etwaiger Unterobjekte), so dass die Originalnamen laut Dateisystem zu Zweitnamen degradiert werden, oder sie werden selbst zu Zweitnamen und werden in hellerer Farbe hinter dem Hauptnamen in eckigen Klammern als Zusatzinformation angezeigt. In der Voreinstellung ist diese Option halb gewählt, was bedeutet, dass nur die neu erkannten Namen von Original-.eml-Dateien (d. h. deren Betreffzeilen) zu Hauptnamen werden in der Namensspalte werden und die potentiell weniger hilfreichen generischen Dateinamen laut Dateisystem als Zweitnamen aufbewahrt werden.

• **Bereinigung des freien Speichers**: Erlaubt es Ihnen, mit einer angepassten virtuellen Datei "Freier Speicher" zu arbeiten, die um diejenigen Cluster reduziert wird, die erkannt wurden als zugehörig zu ehemals existierenden Dateien, um den Speicherplatz in Dateisystemen zu minimieren, der für logische Suchen und zum Indexieren *doppelt* gelesen wird. Nach dem Ändern dieser Option und nach Entdeckung weiterer ehem. existierender Dateien wird die virtuelle Datei aktualisiert, wenn sie das nächste Mal geöffnet wird, z. B. beim Auswählen der Datei im Datei-Modus oder die Datei bei der logischen Suche an der Reihe ist. Relative Offsets der Suchtreffer in dieser virtuellen Datei werden u. U. falsch, wenn sie sich ändert (z. B. wenn weitere Cluster weiteren identifizierten ehemals existierenden Dateien zugeschlagen werden und der bereinigte freie Speicher kleiner wird), so dass sie nicht zum Navigieren zu Suchtreffern im Datei-Modus taugen. Nur physische Offsets von Suchtreffern, im Modus Partition bzw. Volume verwendbar, bleiben garantiert gültig. Die virtuelle Datei „Feier Speicher“ wird eingefroren und ändert sich nicht mehr, sobald sie indexiert wurde oder wenn sie Unterobjekte bekommt, also typischerweise Dateien, die manuell in ihr im Datei-Modus gecarvt wurden, denn diese sind abhängig von unveränderten relativen Offsets innerhalb der virtuellen Datei.

• Optional können **Dateien** auf den logischen Laufwerken A: bis Z: über das **Betriebssystem geöffnet** werden und nicht über die eingebaute Logik auf der Sektorebene. Bitte beachten Sie, dass dies forensisch einwandfrei nur auf schreibgeschützten Datenträgern ist. Auf beschreibbaren Medien aktualisiert (ändert, verfälscht) Microsoft Windows dabei u. U. den Zeitstempel des letzten Zugriffs bei Dateien, die Sie öffnen. Der Vorteil dagegen ist, dass der Zugriff auf die Dateien auf diese Weise in vielen Situationen merklich schneller ist, besonders auf langsamen Laufwerken wie CD/DVD, z. B. wenn Sie Hash-Werte oder Hautfarbenanteile für Dateien im Datei-Überblick berechnen lassen, weil Microsoft Windows im Voraus Daten liest und eine Datei-Caching-System unterhält. Dateien auf Multisession-CDs und -DVDs jedoch können nicht auf diese Weise gelesen werden.

• Bekanntermaßen nicht initialisierte Bereiche am Ende von Dateien in bestimmten Dateisystemen, in denen solche Umstände (gültige Datenlänge < logische Dateigröße) vermerkt

sind, werden von Windows gegenüber normalen Anwendungen, die Dateien regulär über das Betriebssystem öffnen statt Datei-Inhalte direkt aus den Sektoren des Volumes zu lesen, in Form von binären Nullen dargestellt. D. h. die Daten, die tatsächlich in den belegten Clustern gespeichert sind und i. d. R. älter sind und nichts mit der jeweiligen Datei zu tun haben, werden ignoriert. Dieses Verhalten von Windows wird optional reproduziert, für alle Leseoperationen, die nicht der logischen Suche oder Indexierung oder der Suchtreffer-Kontextvorschau dienen. Das ist z. B. nützlich, um Hash-Kompatibilität mit solchen Anwendungen zu erzielen (aber nicht, wenn Sie Datei-Hash-Kompatibilität mit Forensik-Programmen bevorzugen, die für die Hash-Berechnung wohl meist die auf dem Datenträger gespeicherten Daten heranziehen). Auch beim Herauskopieren von Dateien mit dem Wiederherstellen/Kopieren-Befehl greift diese Option. Die logische Suche und Indexierung arbeiten hingegen ungeachtet dieser Einstellung immer forensisch gründlich, d. h. die Cluster, die nicht initialisierten Bereichen zugeordnet sind, werden auf jeden Fall durchsucht und nicht ausgespart. Wenn die Option halb gewählt ist, wird die Darstellung in Form von Nullbytes auch auf in separaten Datenfenstern oder im Datei- oder Preview-Modus geöffnete Dateien angewandt. Das An- oder Abwählen dieser Option hat eine sofortige Wirkung, sogar auf bereits geöffnete Dateien, bei der nächsten internen Leseoperation. Schattenkopie-Trägerdateien werden so behandelt, als ob ihre Daten initialisiert/gültig wären, obwohl das im NTFS-Dateisystem anders vermerkt ist, um unnötige Komplikationen zu vermeiden.

• Es gibt eine Option, um **fragmentierte Dateien** und Verzeichnisse in neu erzeugten Datei-Überblicken besonders kenntlich zu machen. In Asservaten werden solche Objekte mit einem speziellen Vermerk versehen. Wenn man nicht mit einem Fall arbeitet, werden sie teilweise markiert. Die Identifikation kann nützlich sein zu Ausbildungszwecken (um Dateien zu finden, für die sich das Dateisystem nicht zusammenhängende Clusterketten in besonderen Datenstrukturen merken muss, und um besser zu verstehen, mit welcher Logik ein Dateisystemtreiber freie Cluster für Allokationen auswählt) oder um ein paar grobe Rückschlüsse auf die Verwendung des Dateisystems ziehen zu können (Dateien sind mit höherer Wahrscheinlichkeit fragmentiert, wenn sie später im Dateisystem erzeugt wurden, zu einer Zeit, als viele andere Dateien schon wieder gelöscht worden waren, aber andere noch existierten, so dass Allokationslücken entstanden sind).

• Sie können festlegen, ob Sie daran interessiert sind, dass Dateien in den Datei-Überblick aufgenommen werden, deren **Cluster** (und damit deren Daten) gänzlich **unbekannt** sind, nur mit Metadaten (z. B. nur Dateiname und Pfad und/oder Zeitstempel), in Ext*, XFS, Reiser* und NTFS. Die Datei-Überblicks-Option „Dateien mit unbekannten Clustern aufnehmen“ ist eine der berüchtigten Kontrollkästchen mit 3 Zustände. Wenn ganz angekreuzt, werden alle ehem. existierenden Dateien, von denen nur Metadaten bekannt sind, in den Datei-Überblick aufgenommen. Wenn gar nicht ausgewählt, werden solche Dateien komplett ignoriert. Wenn halb gewählt, werden nur Dateien, für die mehr als bloß der Name oder Zeitstempel bekannt sind aufgenommen, aber keine Verzeichnisleichen in den Dateisystemen Ext* und Reiser*. In NTFS kann es vorkommen,

• **Schneller Überblick ohne Cluster-Zuordnung** beschleunigt das Erzeugen des Datei-Überblicks für eine Partition (insbes. für die Dateisysteme Ext2, Ext3 und ReiserFS, und insbes. auch dann, wenn die Dateien mit dem Datei-Überblick über eine langsame USB-1.1-Schnittstelle oder ein Netzlaufwerk gespeichert werden), führt allerdings dazu, dass WinHex nicht mehr imstande ist, für jeden Sektor und jeden Cluster anzugeben, für welche Datei/welches

Verzeichnis er verwendet wird. Sie können die Funktion »Dateisystem neu einlesen« im Extras-Menü verwenden, um das Dateisystem auf einem Datenträger neu einzulesen (z. B. nach dem Ausschalten dieser Option).

• Wenn die Option »**Datei-Überblick aufbewahren**« eingeschaltet ist, bleiben die Informationen, die WinHex über geöffnete Dateisysteme gesammelt hat (Menü Disk-Tools und/oder Specialist-Menü), beim Beenden von WinHex im Ordner für temporäre Dateien erhalten. WinHex kann sie dann beim nächsten Programmstart wiederverwenden. Datei-Überblicke von Asservaten beim Arbeiten mit einem *Fall* werden grundsätzlich immer aufbewahrt, unabhängig von dieser Einstellung, und zwar im Metadaten-Unterverzeichnis dieses Asservats.

• Sie können optional **mehr Daten** des Datei-Überblicks **im Speicher halten**, damit z. B. das Sortieren nach Zeitstempeln viel schneller vonstattengeht.

• Zur Beschleunigung diverser Operationen (Erweiterung des Datei-Überblicks, logische Suche und insbes. die optionale dynamische Darstellung des Kontextvorschau von Suchtreffern in der Suchtrefferliste) werden optional mehr dekomprimierte Inhalte von **Datei-Archiven** im **Cache** des Datei-Überblicks **gehalten**. Die Option beschleunigt generell das erneute Öffnen von Dateien in Archiven nach dem ersten Mal, insbes. in verschachtelten Archiven. Der Cache des Datei-Überblicks kann auf diese Weise sehr groß werden. Er kann optional verworfen werden, wann immer Sie das Datenfenster schließen (nützlich, wenn Sie mit dem betreffenden Asservat oder dem ganzen Fall erstmal fertig sind), und das ist eine fallspezifische Einstellung in den Falleigenschaften. Wenn der Cache geleert wurde, können Dateien jederzeit erneut dort abgelegt werden, wenn sie erneut geöffnet werden, sofern die Option dafür aktiv ist. Wenn das Kontrollkästchen fürs Caching halb gewählt ist, bedeutet das, dass nur verschachtelte Archive im Cache gehalten werden, ähnlich wie in früheren Versionen komprimierte TAR-Archive gehandhabt wurden.

• Option to convert certain RTF-formatted e-mail bodies from Outlook e-mail archives to plain UTF-8 (when extracting e-mails) to be able to better view generated .eml files in external e-mail clients and to allow for the alternative .eml preview.

• The option for an alternative interpretation of extended timestamps has an effect when including the contents of file archives in the volume snapshot. S. Kapitel “Erkundung von Archiven”.

9.5 Viewer-Programme & Galerie-Optionen

Hier können Sie die separate Viewer-Komponente aktivieren und den Pfad angeben, wo sie zu finden ist. Standardmäßig und der Einfachheit halber sollten die Dateien der Viewer-Komponente aus dem Zip-Archiv schlicht in dasselbe Verzeichnis extrahiert werden, in dem das Hauptprogramm (X-Ways Forensics oder X-Ways Investigator) ausgeführt wird. Dafür geben Sie stellvertretend einen Punkt als Pfad ein. Kompliziertere relative Bezüge zu dem Verzeichnis, in dem X-Ways Forensics ausgeführt wird, sind auch möglich, z. B. „..\viewer“ verweist auf ein Verzeichnis namens „viewer“, das im übergeordneten Verzeichnis liegt. Absolute Pfade sind

natürlich auch möglich, z. B. „X:\Viewer854“.

Die Viewer-Komponente ist ein separater Download, weil Änderungen daran viel seltener sind als an X-Ways Forensics und weil man dieselbe Version und Kopie der Viewer-Komponente für mehrere verschiedene Installationen/Versionen von X-Ways Forensics gemeinsam verwenden kann. Es ist definitiv empfehlenswert, auf Ihrem eigenen Auswerterechner die Viewer-Komponente zu aktivieren, weil ihre Funktionalität benötigt wird u. a. zum Einsehen diverser Dateitypen und Decodieren von Text für Suche und Indexierung. Die Viewer-Komponente legt ihre Einstellungen in Form von Dateien im Windows-Profilverzeichnis des ausführenden Benutzers ab. Daher ist es evtl. ratsam, sie bei der Ausführung auf zu untersuchenden Live-System nicht zu verwenden, wenn dort möglichst wenig verändert werden soll.

Eingesehene Dateien merken: Mit einer forensischen Lizenz kann das Programm sich optional merken, welche Dateien bereits vom Benutzer eingesehen worden sind, und diese optisch mit einer grünen Hintergrundfarbe um das Markierungsfeld herum kenntlich machen. Das ist besonders nützlich, wenn Hunderte oder Tausende von Dokumenten oder Bildern über einen längeren Zeitraum hinweg begutachtet werden sollen, um zu vermeiden, versehentlich dieselben Dateien mehrfach anzuschauen. Eine Datei kann automatisch als bereits eingesehen gekennzeichnet werden, wenn sie im Vollfenstermodus oder im Vorschaumodus betrachtet wird, wenn Bilder in der Galerie zu sehen sind oder wenn eine Datei basierend auf der Hash-Datenbank als bekanntermaßen irrelevant identifiziert wird.
Beim Identifizieren von Duplikaten (doppelten Dateien) basierend auf Hash-Werten, wenn eine der Dateien als bereits eingesehen gekennzeichnet ist, können die Duplikate optional ebenfalls als bereits eingesehen gekennzeichnet werden. Optional zusätzlich andersherum, bei voll angekreuztem Kontrollkästchen: Wenn Dateien als Duplikate aufweisend gekennzeichnet sind und ihre Hash-Werte verfügbar sind, und eine von diesen Dateien eingesehen wird, werden sofort auch all deren Duplikate als bereits eingesehen gekennzeichnet (innerhalb der Datei-Überblicke aller offenen Datenfenster, und im Zshg. mit der Galerie kann dies langsam sein). Beim Einsehen werden dann auch weitere harte Verweise einer Datei (ebenfalls Duplikate) automatisch als bereits eingesehen gekennzeichnet, außer in HFS+.
Um eine Datei manuell als bereits eingesehen kenntlich zu machen, können Sie Alt in Kombination mit dem Pfeiltasten drücken. Alt+Links entfernt die Kennzeichnung. Sie können auch das Markierungsfeld einer Datei im Verzeichnis-Browser mit der rechten Maustaste anklicken um die Kennzeichnung zu setzen oder zu entfernen.
Ein Verzeichnis gilt als bereits eingesehen, wenn all seine Dateien und Unterverzeichnisse als solches kenntlich gemacht sind.

Wenn die interne Grafikanzeigebibliothek zum Einsehen von Bilder verwendet wird, nicht die Viewer-Komponente, kann das vorherige Einsehen-Fenster optional automatisch geschlossen werden, sobald ein neues Bild eingesehen werden soll (wenn "Mehrere Bilder zugleich einsehen können" nicht gewählt ist). In dem Fall ist auch eine "Auto Update"-Option verfügbar, die es erlaubt, automatisch das nächste Bild in das Einsehen-Fenster zu laden, sobald ein neues Bild ausgewählt wird, auf welche Weise auch immer, z. B. durch einen einfachen Mausklick oder die Pfeiltasten oder nach dem Setzen eines Vermerks für die vorherige Bilddatei. Das sollte vor allem bei der Arbeit mit mehreren Monitoren hilfreich sein, wobei das Einsehen-Fenster, das das Bild anzeigt, auf dem zweiten Monitor verbleibt. Wenn Bilder mit der internen Grafikanzeige-bibliothek eingesehen werden, dreht dies JPEG-Bilder automatisch passend so, wie es ggf. von den Exif-Daten vorgesehen ist.

Eine alternative E-Mail-Darstellung ist im Vorschau-Modus verfügbar (auch im Fallbericht). Datei-Anhänge werden von dieser Art der Darstellung im Vorschau-Modus noch nicht verlinkt. Optional können E-Mails im .eml-Format in der Vorschau (nicht im Roh-Modus) ohne Kopf (ohne die Header-Zeilen) angezeigt werden. Nützlich in der Standard-E-Mail-Darstellung, wenn Sie gern mehr vom Rumpf (Body) der E-Mail sehen möchten, ohne nach unten rollen zu müssen. Betreff, Absender, Empfänger und Zeitstempel werden ohnehin auch im Verzeichnis-Browser angezeigt, und zu etwaigen Datei-Anhängen können Sie auch im Verzeichnis-Browser navigieren.

Eine weitere Option ermöglicht es, dem dauerhaften Verbrauch von GDI-Schrifttyp-Objekten in der Viewer-Komponente zu begegnen. Um einen Absturz zu vermeiden, wenn z. B. Miniaturansichten von tausenden PDF-Dateien für den Fallbericht erzeugt werden, sollte diese Option aktiv sein. Standardmäßig ist sie halb gewählt. Voll gewählt bedeutet, dass die dafür notwendigen Prüfungen auf Handle-Lecks öfter durchgeführt werden.

Applying Exif orientation metadata in Preview mode, for the View command, in the gallery, for OCR and for Excire is optional and controlled by a 3-state checkbox. If fully checked, the Exif orientation is strictly applied. If half checked (default), it is not applied if X-Ways Forensics thinks it is most likely correct to *not* (further) rotate or flip the picture. Thumbnails and low-resolution alternatives embedded in JPEG files inherit the Exif orientation from their parent files.

Galerie-Optionen

Gallery screen space is utilized very efficiently because thumbnails are not forced to be squares. You can specify your preferred thumbnail width and height separately, in pixels. The specified dimensions will be dynamically adjusted (increased) to best fill the available screen space without partial thumbnails being visible. Since most photos and practically all videos are shot in landscape format, you may want to select width and height accordingly (width larger than height) when viewing pictures. Document thumbnails can often be freely adjusted to any rectangle shape, for example those representing word processing documents or spreadsheets, but not presentations. For most documents other than presentations, portrait format feels like a more natural way of representation. The aspect ratio of the width and height that you specify is displayed in the options dialog to quickly give you a rough idea how compatible the measures will be with ordinary photos, videos or documents.

- Wenn die Erzeugung von **Miniaturansichten** für **Bilder** in großen (z. B. soliden RAR-) **Archiven** für die Galerie-Ansicht zu langsam ist, können Sie diese ausschalten. Dies deaktiviert auch die Kontextvorschau in Suchtrefferlisten für Suchtreffer in Dateien in Archiven.

- Wenn große JPEGs eingebettet Miniaturansichten enthalten und diese bereits in den Datei-Überblick aufgenommen wurden, dann können sie optional als **Ersatz für Miniaturansichten** auch in der Galerie herhalten, um das Hauptbild zu repräsentieren. Ebenso intern von X-Ways Forensics selbst berechnete Miniaturansichten großer Bilder. Der Vorteil ist, dass diese natürlich viel schneller zu laden sind als das Hauptbild. Auch aus Videos exportierte JPEG-Bilder können behelfsmäßig das Video, zu dem sie gehören, in der Galerie repräsentieren,

sogar alle diese Bilder dynamisch rotierend, wenn diese Option ganz gewählt ist (wenn Sie das als störend empfinden, dann besser nur halb wählen).

- Die Galerie hat ihre eigene 3-stufige Option "Doppelklick=Einsehen statt Erkunden", analog zum Verzeichnis-Browser. In der Galerie bedeutet ein Doppelklick standardmäßig Einsehen.

- Es gibt eine Option, mit der man Dateien mittels eines einzigen Klicks in der Galerie einsehen kann, statt mittels eines Doppelklicks. Das ist nützlich z. B. dann, wenn Sie bestimmte Bilder auf einem separaten Monitor betrachten möchten und das Einsehen-Fenster nicht zu schließen brauchen, um die Galerie erneut zu sehen, wenn Sie die Bilder nicht ohnehin alle nacheinander einsehen möchten (wozu das Drücken der Tasten Bild auf und Bild ab effizienter wäre).

- Eine weitere Option erlaubt das Markieren einer Datei durch einen Klick an einer beliebigen Stelle innerhalb der Miniaturansicht, nicht nur im Markierungsquadrat. Das macht es bequemer, eine große Anzahl von Dateien zu markieren, und ist auch bequemer als das Auswählen vieler Dateien bei gedrückt Halten der Strg-Taste.

- Die Galerie kann optional Miniaturansichten für alle Dateitypen anzeigen, die von der Viewer-Komponente unterstützt werden, incl. Office-Dokumente, PDF, HTML, E-Mails sowie Bilder, die die internen Bildanzeigebibliothek nicht anzeigen kann (wie etwa .emf, .wmf, .jp2, ...). Sie können wählen zwischen normalen, leicht geschrumpften und stark geschrumpften Miniaturansichten von Dokumenten. Geschrumpfte Ansichten zeigen mehr Details und geben einen Eindruck vom ursprünglichen Layout von Dokumenten, aber auf Kosten der Lesbarkeit. Größere Schriftarten (besonders Überschriften) im ursprünglichen Dokument, wenn nicht zu stark verkleinert, bleiben typischerweise in der Miniaturansicht lesbar und können dem Betrachter bereits vermitteln, um was für eine Art von Dokument es sich handelt, auch wenn man es nicht einsieht, so dass er wahrscheinlich schneller die Dokumente findet, nach denen er Ausschau hält. Außerdem kann er bereits vorab sehen, welche Dateien überhaupt in der Viewer-Komponente hübsch dargestellt werden können. Es ist sehr empfehlenswert, in Windows Aero zu aktivieren, wenn man die Galerie mit der Option für Nicht-Bilder verwendet.

  Wenn die Option nur halb gewählt ist, werden nur Nicht-Bild-Dateien mit bestätigtem oder neu/anders erkannten Typ-Status so dargestellt, d. h. z. B. Dateien mit nicht identifizierbarem Zeichensalat als Inhalt eher nicht, mit Formatierung hübsch darstellbare Dokumente eher doch. Dateien, die größer als 16 MB sind, werden nicht mit einer Miniaturansicht dargestellt, aus Gründen des beschleunigten Galerieaufbaus. X-Ways Forensics versucht, die Erzeugung einer Miniaturansicht abzubrechen, wenn sie länger als ein paar Sekunden dauert. Wenn die Erzeugung fehlschlägt, sehen Sie evtl. Fehlermeldungen der Viewer-Komponente wie "Operation cancelled" in kleinen roten Buchstaben in der Miniaturansicht. Wenn die Erzeugung von X-Ways Forensics nicht mal versucht wird, sehen Sie nur den Dateinamen und ein Icon.

- Miniaturansichten von True-Color-Bildern können in der Galerie optional farblich angepasst werden. Diese Option ist für Benutzer in Strafverfolgungsbehörden gedacht, die massenweise Kinderpornografie sichten müssen, um die psychische Belastung und den Stressfaktor zu

reduzieren. Wenn das Kontrollkästchen hierfür voll gewählt ist, erscheinen Miniaturansichten in Graustufen. Wenn es halb gewählt ist, findet eine Farbersetzung statt, mit der menschliche Haut sehr unnatürlich aussieht. Miniaturansichten können auch bewusst unscharf/ verschwommen dargestellt werden, ein bisschen oder stärker, mit demselben Zweck. All diese Effekte können begrenzt werden auf die Bilder, die bereits als verdächtig erkannt wurden.

- Sie haben die Möglichkeit, ein benutzerdefiniertes Time-Out in Millisekunden festzulegen, nach dessen Ablauf das Laden von Bildern mit der internen Grafik-Anzeige-Bibliothek für die Galerie abgebrochen wird, z. B. bei defekten oder nicht unterstützten oder extrem großen Bilddateien. Timeouts for loading pictures for picture analysis and processing and for the XWF_GetRasterImage() API function and for the report are twice as long as defined for the gallery.

Text-Decodierung für logische Suche, Indexierung und Text-Untermodus der Vorschau

Crash-safe text decoding: If enabled, text extraction from certain file types for logical searches and indexing will be done by the viewer component in a separate process, such that if the viewer component crashes or becomes unstable, it does not render the main process (X-Ways Forensics) unstable or cause it to crash.

Es gibt eine Option, um Leerzeichen um geläufige chinesische Zeichen in decodiertem Text herauszufilter. Solche Leerzeichen können unerwarteterweise z. B. bei der Verarbeitung bestimmter PDF-Dokumente erscheinen und Stichwort-Suchen in Chinesisch vereiteln.

Buffer decoded text for context preview: If enabled, the result of the text extraction from certain file types for logical searches and indexing will be stored by X-Ways Forensics in the volume snapshot for reuse when searching/indexing again, to save time.

Externe Programme, benutzerdefinierte Betrachtungsprogramme

Sie können Ihren Lieblings-Text-Editor angeben und ein HTML-Betrachtungsprogramm. Letzteres kann etwa MS Word oder NVU sein, d. h. ein Programm, mit dem Sie HTML-Fallberichte, wie von X-Ways Forensics automatisch erzeugt, weiter bearbeiten können. Zum bloßen Ansehen und Ausdrucken ist der Internet Explorer zu empfehlen.

Sie können hier auch den Pfad der .exe-Datei von MPlayer angeben, einem Programm, das X-Ways Forensics das Extrahieren von Bildern aus Videos ermöglicht. Wenn mplayer.exe in einem Unterverzeichnis \MPlayer unterhalb des Installationsverzeichnisses von X-Ways Forensics gefunden wird, wird es automatisch als Videoextraktionsprogramm und auch als externes Betrachtungsprogramm eingestellt. Relative Pfade, die mit .\ oder ..\ beginnen, sind möglich, wobei . für das Verzeichnis steht, in dem X-Ways Forensics ausgeführt wird, und .. für dessen übergeordnetes Verzeichnis. Bitte beachten Sie, dass wir für externe Programme keine Unterstützung bieten können.

Es können auch bis zu 32 benutzerdefinierte Betrachtungsprogramme angegeben werden, die direkt aus X-Ways Forensics heraus über das Verzeichnis-Browser-Kontextmenü aufgerufen werden können. Des Weiteren können Sie angeben, welche Dateitypen Sie gern mit den

Programmen ansehen möchten, die in Ihrem Windows-System mit den jeweiligen Dateiendungen verknüpft sind, typischerweise Dateitypen, die die separate Viewer-Komponente nicht unterstützt. Eine Option namens „Abweichenden Typ als Namensänderung anhängen“ erleichtert es, Windows dazu zu bringen, das richtige Programm für falsch benannte Dateien, Dateien ohne Erweiterung, etc. zu starten. Die Pfade der externen Betrachtungsprogramme sind in einer separaten Datei namens "Programs.txt" gespeichert, so dass es leicht fällt, eine ganze Sammlung solcher Programme mit anderen Benutzern auszutauschen, oder die eigenen Pfade zu behalten, wenn man alle anderen Programmeinstellungen von jemand anderem übernehmen möchte. In der Textdatei kann man auch absolute Pfade zu relativen Pfaden machen (mit . oder ..), für Programme, die genauso portabel wie X-Ways Forensics selbst sind und die man auf einem USB-Datenträger mit X-Ways Forensics für Durchsuchungen vor Ort mitnehmen möchte. Wenn Sie externe Programme von X-Ways Forensics aus mit bestimmten Parameter zusätzlich zum Namen der zu öffnenden Datei aufrufen möchten, können Sie diese Parameter in derselben Zeile von Programs.txt angeben, vom Pfad der ausführbaren Datei getrennt mit einem Tabulatorzeichen. delimited from the path of the executable file with a tab. Der Name der zu öffnenden Datei wird automatisch am Ende angehängt, hinter Ihren eigenen Parametern, es sei denn, Sie fügen den Platzhalter %1 irgendwo in der Parameterliste ein. Dann wird dieser Platzhalter durch den Dateinamen ersetzt.

Tesseract: OCR

Per OCR erkannter Text wird ignoriert, wenn er nicht mindestens aus *x* zusammenhängenden nützlichen Zeichen besteht. Solche OCR-Ergebnisse werden nicht gespeichert, ausgegeben, kopiert, indexiert oder durchsucht. Das ist vorteilhaft, wenn Sie OCR auf unbekannte/wahllos herausgesuchte/normale Bilder anwenden (d. h. keine bekannten Textdaten), um die Anzahl der Dateien zu reduzieren, die später (irreführenderweise) auf den Beschreibungsfilter für Dateien mit per OCR ermitteltem Text reagieren oder für die (unnötigerweise) Unterobjekte erzeugt werden durch die Funktion "Kopieren: extrahierter Text" usw. Ein "nützliches" Zeichen ist hier definiert als ein Zeichen mit einem ASCII-/Unicode-Wert von 0x30 oder höher. Das bedeutet, dass sog. Whitespaces <=0x20 nicht zählen, und ebensowenig die druckbaren Zeichen !=#$%&'()*+,-.& (die Spanne 0x21-0x2F), weil einige davon gelegentlich zu Unrecht in zufälligen Pixel-Kombinationen erkannt werden. Alle echten Buchstaben in jeder Sprache zählen, und auch Ziffern ("0" bis "9").

9.6 Rückgängig-Optionen

Für den Befehl „Rückgängig“ stehen Ihnen folgende Optionen zur Auswahl:

Bestimmen Sie, wie viele nacheinander ausgeführte Aktionen ungeschehen gemacht werden können. Wichtig: Dies hat keinen Einfluss auf die Anzahl der umkehrbaren Tastatureingaben, die nur vom Arbeitsspeicher limitiert wird.

Um Zeit und Speicherplatz auf der Festplatte zu sparen, können Sie ein Dateigrößenlimit angeben, oberhalb dessen keine Sicherungen mehr durchgeführt werden, so dass der „Rückgängig“-Befehl nur noch nach Tastatureingaben zur Verfügung steht.

Automatisch angelegte Sicherungen für die Benutzung durch den „Rückgängig“-Befehl werden von WinHex selbständig beim Schließen der Datei gelöscht, falls die betreffende Option voll aktiviert ist. Ist sie nur halb aktiviert, werden sie erst bei Programmende gelöscht.

Geben Sie für alle Arten von Editiervorgängen an, ob sie rückgängig gemacht werden können.

9.7 Sicherheitsoptionen

- In der Voreinstellung müssen Sie das **Speichern von** Änderungen an existierenden **Dateien bestätigen**. Wenn Sie diese Option ausschalten, entfällt die Sicherheitsabfrage.

- Sollten die Operationen Datei-Überblick erweitern, logische Suche und Indexierung bei der Verarbeitung einer Datei abstürzen, kann X-Ways Forensics Ihnen beim nächsten Programmstart die wahrscheinlich für den Absturz verantwortlich Datei mitteilen, sofern sie **Info**rmationen **für** einen **Absturzbericht** haben **sammeln** lassen. Voll angekreuzt wird das Programm im Fall, dass die Erweiterung eines Datei-Überblicks das Programm zum Absturz bringt, beim Neustart auch angeben, welche Unteroperation genau auf das/die problematische(n) Datei(en) angewandt wurde, als das Programm abgestürzt ist. Es wurde bisher nicht getestet, ob diese erhöhte Genauigkeit beim Protokollieren eine erkennbare Verlangsamung nach sich ziehen könnte. Es kann mehrere Kandidaten für die problematische Datei geben, die die Instabilität verursacht hat, wenn zum Absturzzeitpunkt mehrere Threads aktiv waren.

- X-Ways Forensics hat die Fähigkeit, bestimmte Operationen auch nach einem **Absturz** (einem unfreiwilligen Programmende) ohne Eingriff des Benutzers **automatisch fortzusetzen**. Die derzeit unterstützten Operationen sind die Teilschritte "Datei-Header-Signatur-Suche" und "Individuelle Verarbeitung einzelner Dateien" der Erweiterung des Datei-Überblicks, bei Aufruf über das Hauptmenü oder über die Befehlszeile oder beim Hinzufügen von Asservaten zum Fall. Im Gefolge eines Absturzes werden diese Vorgänge automatisch fortgesetzt an einer Stelle, die davon abhängt, wann der Datei-Überblick zuletzt gespeichert wurde. (Das wiederum hängt vom Intervall fürs automatische Speichern in den Falleigenschaften ab, denn wann immer der aktive Fall gespeichert wird, wird auch der Datei-Überblick eines jeden offenen Asservats gespeichert. Sie können den Fall auch manuell speichern, während der Datei-Überblick erweitert wird.) Wenn es nicht klar ist, welche bestimmte Datei einen Absturz ausgelöst hat, weil Sie eine Operation mit zusätzlichen Threads haben laufen lassen, dann wird diese Operation zunächst ohne zusätzliche Threads fortgeführt. Mit etwas Glück, wird der Absturz dann gar nicht mehr auftreten. Wenn doch, wird die Operation abermals fortgesetzt, und wenn eine bestimmte Datei als Auslöser erkannt wird, wird diese automatisch übersprungen. Im Fall eines Absturzes bei der Datei-Header-Signatur-Suche wird der Sektor, an dem eine problematische Datei ausgegliedert wurde, übersprungen.

- Ausschließlich in Preview- und Beta-Releases können Sie Abstürze auf Wunsch simulieren, wenn Sie diese Neuerung beobachten, testen oder demonstrieren möchten, z. B. weil Sie sie sich zunutze machen möchten bei der mehr oder weniger automatisierten Ausführung von X-Ways Forensics mit Befehlszeilen-Parametern, wenn Sie auf die Situation reagieren müssen, dass eine Instanz von X-Ways Forensics verschwindet und sofort von einer weiteren Instanz

ersetzt wird, die Sie nicht selbst gestartet haben. Für die Simulation können Sie den Namen einer Datei angeben, die einen Crash in den unterstützten Operationen auslösen soll. Dieser Dateiname sollte natürlich möglichst eindeutig sein und idealerweise nur auf eine Datei passen, von der Sie wissen, dass sie im initialen Datei-Überblick enthalten ist oder deren Hinzufügen Sie bei der Erweitung des Datei-Überblicks erwarten. Groß- und Kleinschreibung im Dateinamen wird dabei beachtet. Bitte beachten Sie, dass wenn Sie X-Ways Forensics aus Sektoren ausgegliederten Dateien Namen mit fortlaufenden Nummern zuweisen, und Sie einen Absturz simulieren lassen mit einer Datei, deren Name erwartungsgemäß 012345.jpg wird, dass selbst wenn X-Ways Forensics erfolgreich lernt, den Sektor zu meiden, in dem die Datei bei der Datei-Header-Signatur-Suche gefunden wird, dass die nächste ausgegliederte Datei evtl. auch wieder 012345.jpg genannt wird (abhängig vom Dateityp) und somit noch einen weiter Absturz auslösen wird. Eindeutige Namen von ausgegliederten Dateien sind solche, die von der intelligenten Benennungsoption erzeugt werden (sowas wie "Canon DIGITAL IXUS 950 IS 2007-07-01 12:01:46.jpg") oder von der Option, Dateien nach Startsektor-Nummern zu benennen. Um einen zufälligen, nicht reproduzierbaren Absturz zu simulieren, können Sie X-Ways Forensics auch einfach mit dem Task-Manager von Windows terminieren.

- **Nachrichten über Ausnahmefehler**: Bestimmt, wie mitteilsam sich das Programm beim Auftreten von Ausnahmesituationen zeigt. Wenn ganz ausgeschaltet, werden Sie im Nachrichtenfenster nur über Ausnahmesituationen mit potenziell ernsten Auswirkungen (wie etwa merklich unvollständige Auswertungsergebnisse) informiert. Wenn ganz eingeschaltet, werden alle Ausnahmesituationen dort vermerkt, auch solche, die typischerweise nur mit defekten Dateien auftreten und keine negativen Auswirkungen auf andere Ergebnisse haben. Der mittlere Zustand des Kontrollkästchens ist ein Kompromiss. Unabhängig von dieser Einstellung werden Ausnahmesituationen immer in der Datei error.log vermerkt.

- Alle Hinweise und Warnungen, die im **Nachrichten**fenster ausgegeben werden, können optional automatisch in der einer Textdatei names „**msglog.txt**“ im Installationsverzeichnis mitgeschrieben werden. Wenn zum Zeitpunkt der Ausgabe ein Fall aktiv ist, wird der Text stattdessen in eine Datei gleichen Namens in das Log-Unterverzeichnis dieses Falls geschrieben. Voreingestellt ist, dass das Kästchen halb angekreuzt ist. Voll angekreuzt bedeutet, dass auch Nachrichten im Fortschrittsanzeigefenster (Beschreibungen von Vorgängen und die Namen von verarbeiteten Dateien) in die Log-Datei geschrieben werden. Das ist normalerweise etwas übertrieben.

- Die Option „**Auf Änderungen im Speicher prüfen**“ betrifft den Arbeitsspeicher-Editor. Sie sorgt dafür, dass WinHex vor jedem Lesen und Beschreiben des virtuellen Speichers erst prüft, ob sich dessen Größe und Zusammensetzung geändert hat. Ist dies der Fall, wird der Speicher in WinHex neu abgebildet und ein damit ein möglicher Lesefehler vermieden. Besonders unter Windows NT kann diese Einstellung den Arbeitsspeicher-Editor stark verlangsamen. Beim Editieren des *Gesamtspeichers* eines Prozesses wird unabhängig von der gewählten Einstellung nicht auf Änderungen geprüft.

- **Strenger Laufwerksbuchstabenschutz**: Nur mit forensischer Lizenz verfügbar. In X-Ways Forensics standardmäßig aktiv. Stellt sicher, dass nur auf bestimmten Laufwerksbuchstaben das Speichern und Editieren von Dateien erlaubt ist, nämlich Laufwerksbuchstaben, von denen

X-Ways Forensics auch beim Untersuchen eines Live-Systems annehmen kann, dass Sie zu Datenträgern des Ermittlers gehören. Dies sind 1. der Laufwerksbuchstabe, auf dem ein etwaiger aktiver Fall liegt, 2. der Laufwerksbuchstabe mit dem Verzeichnis für temporäre Dateien, 3. das Laufwerk, von dem aus X-Ways Forensics gestartet wurde und 4. der Laufwerksbuchstabe mit dem Verzeichnis für Image-Dateien.

- Den für Verschlüsselung und Entschlüsselung erforderliche **Schlüssel** können Sie entweder in ein normales Editierfeld **eingeben** oder **blind** (es erscheinen nur Sternchen). In letzterem Fall müssen Sie den Schlüssel bestätigen, um Eingabefehler zu vermeiden.

- Standardmäßig wird der **Schlüssel** verschlüsselt **im** Arbeits**speicher** ge**halten**, solange WinHex läuft, damit Sie ihn nicht mehrmals eingeben müssen, wenn Sie es mehrmals verwenden möchten. Möglicherweise ziehen Sie es vor, dass WinHex sich den Schlüssel **nicht** merkt.

- Entscheiden Sie, ob Sie WinHex **vor dem Ausführen von Scripten fragen** soll, oder auch nur vor dem Ausführen von Scripten per Befehlszeile.

- Optionally, checksums with multi-byte accumulators (16-bit, 32-bit, and 64-bit checksums) are computed byte-wise instead of adding units that are equivalent in size to the accumulator itself, e.g. 4 bytes for 32-bit checksums. Both variants exist in real life applications.

- The CRCs in .e01 chunks can be automatically checked on the fly when chunks are read, and any discrepancies will be reported in the Messages window. This costs a little computing power.

- Whether a password verification hash for .e01 evidence files created with 256-bit AES encryption is included in the .e01 evidence file or not is up to you to decide. The hash allows X-Ways Forensics to check whether the password that you enter when opening such an image is correct.

- If an .e01 evidence file that found to have very inefficient layouts (less than 32 chunks per table section or compressed chunks with a compression ration of less than 0.1%), that is brought to the users attention so that they can avoid whatever software or hardware created that image.

- Es gibt die Möglichkeit, große .e01-Evidence-Files nach dem ersten Mal schneller zu öffnen, indem einige interne Image-Metadaten zur Navigation in separaten Dateien (mit Dateinamenserweiterung .xmet) gespeichert werden. Das kann einen großen Unterschied machen, wenn das Image auf einem Datenträger mit langsamem Zugriff gespeichert ist, insbes. auf einem Netzlaufwerk. Wenn die Option voll gewählt ist, wird die separate Datei im selben Verzeichnis wie das Image selbst gespeichert, so dass auch andere Fälle / andere Benutzer sofort in den Genuss des schnelleren Öffnens kommen, wenn die separate Datei bereits zuvor erzeugt wurde. Wenn nur halb gewählt, wird die separate Datei im internen Metadaten-Verzeichnis des Asservats im aktuellen Fall gespeichert und ist folglich nur in dem Fall wirksam. Paranoiden Benutzern, die nicht nur die Originaldatenträger von Beschuldigten über einen Hardware-Schreib-Blocker anschließen, sondern sogar ihre eigenen Datenträger,

wenn diese die Sicherungen (Images) enthalten, wird aus offensichtlichen Gründen empfohlen, diese Option halb zu wählen, wenn sie von dem Geschwindigkeitsvorteil profitieren möchten.

A general password collection can be maintained by clicking a button in the security options dialog window. It is stored in the file "Passwords.txt". The password collection of a newly created case is initialized with that general password collection. The password collection of a case is used with encrypted archives as well as encrypted documents whenever the case is loaded.

One of the buttons in this dialog box allows to exhaust system memory, for example in order to get comparable results with performance tests that could get distorted if for example Windows still has parts of an image file in its file buffer.

Ein weiterer Schalter bietet die Möglichkeit, den verwendeten Rechner planmäßig nach einer bestimmten Anzahl von Minuten herunterzufahren oder (sofern unterstützt) in den Ruhezustand zu versetzen, unter Optionen | Sicherheit. Das funktioniert nur dann garantiert, wenn den Rechner nichts davon abhält, heruntergefahren zu werden, z. B. andere Anwendungen mit noch nicht gespeicherten Daten o. ä. Wenn Sie die Option zum „brutalem" Herunterfahren halb wählen, sollte das Herunterfahren des Rechners auch dann gelingen, wenn eine Anwendung hängengeblieben ist. Wenn ganz gewählt, dann sollte nicht länger als ein paar Sekunden auf Anwendungen gewartet werden, die den Anwender fragen, wie mit ungesicherter Arbeit verfahren werden soll. Wenn Sie die Instanz von WinHex/X-Ways Forensics, in der Sie das Herunterfahren avisiert haben, beenden, wird das Herunterfahren nicht eingeleitet. Es ist möglich, ein bereits geplantes Herunterfahren ohne Neustart des Programms abzubrechen.

9.8 Suchoptionen

Groß-/Kleinschreibung beachten: Suchvorgänge können optional zwischen Groß- und Kleinschreibung unterscheiden und suchen den Text dann immer in genau der Schreibweise, in der Sie ihn vorgeben. Z. B. wird „Beispiel" mit einem großen B nicht bei der Vorgabe „beispielsweise" gefunden. Wenn Sie das Häkchen in diesem Kontrollkästchen entfernen, suchen Sie nach allen Groß- und Kleinschreibungsvarianten der Suchbegriffe, und die Suche wird selbst bei „bEIsPiEl" fündig. Dies funktioniert beim Befehl „Text suchen" nur mit Buchstaben von a-z und deutschen Umlauten (äöü), bei der parallelen Suche auch mit sonstigen sprachspezifischen Buchstaben (z. B. çåê oder Kyrillisch). In der parallelen Suche können Sie bei halb gewählter Option zeitgleich manche Suchbegriffe unter Beachtung von Groß- und Kleinschreibung suchen, indem Sie diesen Suchbegriffen die Zeichen „case:" voranstellen, und die anderen in allen Groß- und Kleinschreibungsvarianten.

Unicode: Der Text wird im Unicode-Zeichensatz gesucht (UTF-16 Little Endian). Dieser Zeichensatz reserviert im Normalfall 16 Bit je Zeichen. Die parallele Suche erlaubt es, denselben Text gleichzeitig in Unicode und in anderen Codepages zu suchen.

Sie können ein frei wählbares **Jokerzeichen** (ein Zeichen bzw. ein zweistelliger Hex-Wert) verwenden, das genau ein Byte abdecken kann. Z. B. kann man mit der Such-Zeichenfolge »Sp?ck« sowohl »Speck« als auch »Spock« finden.

Nur ganze Wörter suchen: Die zu suchende Zeichenfolge wird nur erkannt, wenn sie als einzelnes Wort vorkommt, also von anderen Buchstaben (a...z, A...Z, äöüß, ...) durch Nichtbuchstaben, also z. B. durch Leer-, Satz- oder Steuerzeichen oder Ziffern, getrennt ist. Bei einer Parallelen Suche werden entweder alle Suchbegriffe als ganze Wörter gesucht oder nur solche, die eingerückt (vorne mit einem Tabulatorzeichen versehen) sind oder keine, in Abhängigkeit vom Status des zugehörigen Kontrollkästchens. Wenn die Einrückung für die Suche als ganzes Wort mit dem Präfix für Beachtung von Groß- und Kleinschreibung kombiniert werden soll, muss erst „case:“ kommen und dann das Tabulatorzeichen für die Einrückung.

Bei der Parallelen Suche ist "Nur ganze Wörter" eine dreistufige Option. Der mittlere Zustand sucht nach Wortanfängen, d. h. erfordert eine Wortgrenze am Anfang eines Suchtreffers. Das bedeutet, mit "echt" finden Sie auch "echte" und "echten", aber nicht "recht" oder "rechts". Das ist ansonsten nur mit regulären Ausdrücken zu erreichen, und falls Sie manchen Suchbegriffe als ganze Wörter und andere als Wortanfänge suchen möchten, setzen Sie bitte dafür weiterhin reguläre Ausdrücke ein.

Sie können die Wortgrenzenerkennung für Sprachen, die die Codepage Latin 1 verwenden, individuell anpassen, d. h. entweder strenger machen (für weniger Suchtreffer) oder weicher (für mehr Suchtreffer), indem Sie das Alphabet von Zeichen definieren, die als Buchstaben betrachtet werden (d. h. Zeichen, die zu Wörtern gehören), im Gegensatz zu Nicht-Wort-Zeichen. Ein Wort-Zeichen gefolgt von einem Nicht-Wort-Zeichen (oder andersherum) wird als Wortgrenze angesehen. Es gibt drei leicht zu verwendete vordefinierte Einstellungen. Die Einstellung für das gründlichste Suchergebnis ist als Standard vorgesehen. Benutzer, die von unsinnigen Suchtreffern für kurze Suchbegriffe in Nicht-Text-Daten wie Base64 oder binären Mülldaten überschwemmt werden, können die beiden anderen Optionen probieren. Diese zwei Optionen können dazu führen, in bestimmten Konstellationen gültige Suchtreffer zu verpassen (hängt vom Dateiformat ab), aber sind immer noch zu rechtfertigen als große Zeitersparnis für Suchen in Textdokumenten, eher in der sog. Electronic Discovery, eher nicht in der Computerforensik.

For more explanation and an example of how the whole words option works, please read on: A word boundary is a boundary between two consecutive characters of which one character is a word character and the other character is not a word character. If two consecutive characters are both word characters (e.g. "ns"), then obviously the "s" does not start a new whole word, and the "n" cannot be the end of a whole word. It can be somewhere in the middle of a whole word (e.g. "mansion"), but in between these two characters "ns" there is definitely no word boundary. If both characters are non-word characters (e.g. "! ", exclamation mark followed by a space), then obviously the position between the two is not a word boundary either. The exclamation mark cannot be the end of a word (cannot occur anywhere within a word), and the space cannot be the start of a word (cannot occur anywhere within a word either, excluding compound words). If you are searching for "man" as a whole word within "our mansion", then XWF will provisionally/internally find "man", and then first check whether the character before the "m" is a word character. That character is a space. A space character is not a word character. Then it also checks whether "m" is a word character according to the alphabet. It is. That means there is a word boundary before the "m". Next XWF needs to check whether "n" and "s" are word characters. Both are. That means that after the "n" there is no word boundary. Hence the three letters "man" within "mansion" are not considered a whole word occurrence of "man".

The whole words only restriction of the Simultaneous Search is not applied to search hits that are not words according to the user's selected alphabet definition (checking only the first and the last character in the search hit). For example if you are searching for "LOL!!", then this cannot possibly be a whole word because the exclamation mark is not a letter and thus not contained in the defined alphabet (well, unless you have added the exclamation mark to it manually). However, the RegEx word boundary indicator \b is still applied in such a case, for example to be able to search for certain data in between words, data that is not considered a word itself.

In addition to the alphabet of characters for the Latin 1 code page (for all Western European languages), an optional additional alphabet can be defined for letters of another language. If activated, it is used for searches in UTF-16, UTF-8 and regional ANSI/OEM/IBM/ISO/Mac code pages with only 1 byte character such as for Cyrillic, Greek, Turkish, Arabic, Hebrew, Vietnamese, and various Central/Eastern/South Eastern European languages. The Cyrillic alphabet is predefined.

Suchrichtung: Bestimmen Sie, ob von vorne bis hinten oder von der aktuellen Position an ab- oder aufwärts gesucht werden soll.

Bedingung: Offset modulo x = y: Der Suchalgorithmus erfasst nur Vorkommnisse an Offsets, die die genannte Bedingung erfüllen. Wenn Sie bspw. Daten suchen, von denen Sie wissen, dass sie an Position 10 eines Festplatten-Sektors stehen, geben Sie x=512 und y=10 an. Wenn Sie DWORD-ausgerichtete Daten suchen, verwenden Sie x=4, y=0, um irrelevante Treffer auszuschließen.

Nur im Block suchen: Es wird nur derjenige Teil der Datei/des Datenträgers/des virtuellen Speichers durchsucht, der innerhalb des Blockes liegt.

In allen geöffneten Fenstern suchen: Die Suche wird der Reihe nach in allen in WinHex offenen Editierfenstern durchgeführt. Wird WinHex in einem Fenster fündig, kann die Suche danach im selben Fenster normal fortgesetzt werden (durch F3); zum nächsten Fenster geht WinHex mit der Funktion „Globale Suche fortsetzen“ (F4) über. Wenn „Nur im Block suchen“ aktiviert ist, wird in jedem Fenster nur der dort festgelegte Block durchsucht.

Fundstellen zählen (und speichern): Die Anzahl der Vorkommnisse des gesuchten Texts/der gesuchten Hex-Werte in der Datei/auf dem Datenträger/im virtuellen Speicher wird ermittelt. Die Positionen der Vorkommnisse werden ggf. im Positions-Manager gespeichert, so dass sie zu einem späteren Zeitpunkt wiedergefunden und bearbeitet werden können.

Suche nach „Nicht-Treffern“: Unter „Hex-Werte suchen“ können Sie einen einzelnen Hex-Wert mit einem Ausrufungszeichen als Präfix angeben (z. B. !00), um WinHex das erste Byte mit einem davon *abweichenden* Wert finden zu lassen.

Reguläre Ausdrücke: Nur verfügbar bei der Parallelen Suche. Reguläre Ausdrücke sind ein mächtiges Suchwerkzeug. Ein einziger regulärer Ausdruck kann viele verschiedene Wörter abdecken. Entweder werden alle Suchbegriffe als reguläre Ausdrücke interpretiert oder nur solche, denen Sie "grep:" voranstellen oder keine, abhängig vom Status des zugehörigen Kontrollkästchens. Es ist auch möglich, denselben Suchbegriffen gleichzeitig sowohl "case:" (s.

o.) als auch "grep:" voranzustellen, in dieser Reihenfolge. Die folgenden Zeichen haben in regulären Ausdrücken eine besondere Bedeutung, wie unten erklärt: ( ) [ ] { } | \ . # + ?. An Stellen, an denen diese besonderen Zeichen wörtlich zu verstehen sind, muss ihnen ein umgekehrter Schrägstrich (\) vorangestellt werden.

Der Oder-Operator (|) wird verwendet, um Alternativen zu formulieren. So kann man mit *Auto(s|reifen)* nach Autos oder Autoreifen suchen, Autoseifen wird hingegen nicht gefunden. Es wird also immer nach einer kompletten Zeichenkette gesucht, die vor, hinter, oder zwischen |-Zeichen steht. Die Wirkung von | wird nur durch runde Klammern begrenzt.

. und # sind Platzhalter (Joker-Zeichen): . passt auf alle Zeichen, # passt auf alle Ziffern. Weitere Zeichenmengen lassen sich innerhalb von eckigen Klammern angeben: [xyz] passt auf die Zeichen x, y, und z. [^xyz] passt auf alle Zeichen außer x, y, z. Auch Intervalle können angegeben werden: [a-z] passt auf alle Kleinbuchstaben. [^a-z] passt auf alle Zeichen außer Kleinbuchstaben. Die Auflistung darf mehrere einzelne Zeichen und Listen zugleich enthalten. Daher passt [aceg-loq] auf die Zeichen a, c, e, g, h, i, j, k, l, o, und q. Alle Zeichen außer [,], -, \ werden zwischen eckigen Klammern wörtlich interpretiert, auch die Platzhalter . und #.

\b steht für den Anfang oder das Ende eines Wortes, d. h. die Grenze zwischen einem Wort-Zeichen und einem Nicht-Wort-Zeichen. Welche Zeichen/Buchstaben als Wort-Zeichen gelten, ist in der parallelen Suche vom Benutzer frei definierbar. Der Anfang und das Ende einer Datei gelten auch als Wortgrenzen. \b wird nur am Anfang und/oder Ende eines Suchbegriffs unterstützt, und nicht zusammen mit |. Die Anker (\b, ^, $) funktionieren nur, wenn in Asservaten von Fällen gesucht wird, und nicht in Index-Suchen.

Byte-Werte, die ASCII-Zeichen entsprechen, die nicht bequem über die Tastatur erzeugbar sind, können in dezimaler oder hexadezimaler Schreibweise angegeben werden. Zum Beispiel sind \032 und \x20 äquivalent zum Leerzeichen im ASCII-Zeichensatz. Diese Art der Notation wird auch innerhalb von eckigen Klammern unterstützt. Z. B. deckt [\000-\x1f] alle nichtdruckbaren ASCII-Zeichen ab.

Multiplikatoren (*, + und ?) bestimmen, dass das/die vorangehende Zeichen mehr als einmal vorkommen können oder müssen (s. u.). Komplexes Beispiel: a(b|cd|e[f-h]i)*j passt auf aj, abj, acdj, aefij, aegij, aehij, abcdj und abefij.

Innerhalb von eckigen Klammern werden die Zeichen .*+?{}()| nicht als besondere Zeichen, sondern wörtlich behandelt.

<u>Kurzübersicht der unterstützten Syntax</u> (alles andere wird wörtlich interpretiert)

.	Ein Punkt steht für ein einzelnes beliebiges Zeichen.
#	Eine Raute steht für ein einzelnes numerisches Zeichen [0-9].
\nnn	Ein Byte-Wert angegeben durch drei dezimale Ziffern (\000..\255).
\xnn	Byte-Wert angegeben durch zwei hexadezimale Ziffern (\x00...\xFF). z. B. \x0D\x0A = Zeilenende
\unnnn	Ein Unicode-Wert angegeben durch vier hexadezimale Ziffern. Entspricht je nach Codepage unterschiedlichen und unterschiedlich vielen Byte-Werten.
?	Deckt 1 oder 0 Vorkommnisse des/r vorangehenden Zeichen(s) ab.

* Deckt eine beliebige Anzahl von Vorkommnissen des vorangehenden Zeichens ab, auch 0.
+ Deckt eine beliebige Anzahl von Vorkommnissen des vorangehenden Zeichens außer 0 ab.
[XYZ] Zeichen in eckigen Klammern decken ein beliebiges der darin angegebenen Zeichen ab.
[^XYZ] Ein Zirkumflex am Anfang des geklammerten Ausdrucks bedeutet NICHT.
[A-Z] Ein Bindestrich innerhalb von eckigen Klammern zeigt ein Intervall von Zeichen an.
\ Bewirkt, dass das folgende besondere Zeichen wörtlich zu behandeln ist.
{X,Y} Wiederholt das/die vorangehenden Zeichen X bis Y mal.
(ab) Verhält sich wie eine Klammerung in einem mathem. Ausdruck.
Gruppiert a und b für +, ?, *, | und {}.
a|b Verhält sich wie ein logisches ODER (a oder b).
\b Steht für eine Wortgrenze.
^ Steht für den Anfang einer Datei.
$ Steht für das logische oder physische Ende einer Datei, je nach Suchoptionen.

RegEx-Beispiele

E-Mail-Adressen
[a-zA-Z0-9_\-\+\.]{1,20}@[a-zA-Z0-9\-\.]{2,20}\.[a-zA-Z]{2,7}
(Das + vor dem @ wird in Gmail-Adressen unterstützt.)

Internet-Adressen mit http://, https://, ftp://
[a-zA-Z]+://[a-zA-Z0-9/_\?$&=\-\.]+

Visa- und Mastercard-Kreditkartennummern
[^#a-z][45]################[^#a-z]
[45]###-####-####-####
[45]### #### #### ####
(am besten über eine X-Tension mit dem Luhn-Algorithmus prüfen und ohne [^#a-z] suchen)

Überlappende Treffer erlauben: Wenn Sie mit regulären Ausdrücken nach Suchtreffern variabler Länger suchen, können mehrere gültige Treffer an derselben Stelle entstehen. Wenn Sie z. B. nach E-Mail-Adressen suchen, und der Suchalgorithmus wird mit der Zeichenfolge "mail@x-ways.com" gefüttert, dann stellt er fest, dass die Zeichen ab dem "m" von "mail" auf den regulären Ausdruck passen und vermerkt einen Treffer. Anschließend macht er beim "a" in "mail" weiter und stellt fest, dass ail@x-ways.com auch auf den regulären Ausdruck passt. Und il@x-ways.com passt auch, ebenso wie l@x-ways.com. All dies könnten gültige E-Mail-Adressen sein. Damit liegt der Suchalgorithmus also richtig, aber i. d. R. möchte man solche zusätzlichen Treffer als Benutzer nicht sehen. Wenn Sie daher überlappende Treffer nicht erlauben, werden neue Treffer erst wieder nach dem "m" von ".com" gewertet. Überlappenden Treffer nicht zu erlauben, bedeutet, dass alle von einem Treffer abgedeckten Zeichen allein diesem Treffer zuordnet und keinem anderen Treffer mehr "gegönnt" werden

Suchfenster, Umgebungssuche

Die Größe des Suchfensters bei der RegEx Suche beträgt standardmäßig 128 Bytes. Das bedeutet, es ist nicht garantiert, dass Sie mit einem regulären Ausdruck variabler Länge, d. h.

unter Verwendung der Syntax-Features {}*+, Daten finden können, die sich über mehr als 128 Bytes erstrecken. Sie können das Suchfenster verbreitern, wenn Sie mehr als das abdecken möchten.

Das Suchfenster ist z. B. für Umgebungssuchen (Kontextsuchen) relevant. Wenn Sie Dokumente suchen, in denen zwei Suchbegriff zugleich vorkommen, und zwar relativ nah beieinander, können Sie nach diesen Begriffen mit zwei regulären Ausdrücken suchen und die maximale Entfernung, die zwischen ihnen erlaubt sein soll, als zweiten Parameter in den geschweiften Klammern angeben:
keyword1.{0,*maxdistance*}*keyword2*
keyword2.{0,*maxdistance*}*keyword1*
Die benötigte Suchfensterbreite in Bytes (Annahme: Suche in einem 8-Bit-Zeichensatz) ist die Summe von *maxdistance*, Länge(*keyword1*) und Länge(*keyword2*).

Bitte beachten Sie, dass die bevorzugte Methode zum Auffinden von zwei Suchbegriffen nahe beieinander die NEAR-Kombination in der Suchbegriffsliste ist, die zur Verfügung steht, wenn zwei Suchbegriffe bereits mit einem logisch UND verknüpft sind, nachdem Sie separat voneinander gesucht wurden.

9.9 Ersetzen-Optionen

Auf Bestätigung warten: An jeder Fundstelle entscheiden Sie, ob dort ersetzt und ob der Vorgang evtl. abgebrochen werden soll.

Alles ersetzen: Alle Vorkommnisse werden automatisch ersetzt.

Groß-/Kleinschreibung beachten: Bei der Suche nach der zu ersetzenden Zeichenfolge kann nach Groß- und Kleinschreibung unterschieden werden (s. a. Suchoptionen). WinHex verwendet die Ersatz-Zeichenfolge natürlich in jedem Fall in der von Ihnen gewählten Schreibweise.

Unicode-Zeichensatz verwenden: Der Text wird im 16-Bit-Unicode-Zeichensatz gesucht. Dieser Zeichensatz reserviert 16 Bit je Zeichen, wobei die ersten 256 Unicode-Zeichen den ANSI-ASCII-Zeichen entsprechen. Das höherwertige Byte ist dabei Null. In 32-Bit-Programmdateien beispielsweise sind Texte teilweise im Unicode-Zeichensatz gespeichert.

Sie können ein beliebiges Zeichen bzw. einen beliebigen zweistelligen Hex-Wert als **Jokerzeichen** verwenden. Z. B. kann man mit der Such-Zeichenfolge „Sp?ck“ sowohl „Speck“ als auch „Spock“ finden.

In der Ersatz-Zeichenfolge kann das Jokerzeichen verwendet werden, um an den betreffenden Stellen das bestehende Zeichen nicht zu ändern. Auf diese Weise kann man bspw. „Huhn“ und „Hahn“ in einem Schritt durch „Hund“ und „Hand“ ersetzen (entsprechende Eingabe: „H?hn“ ersetzen durch „H?nd“).
Ein Jokerzeichen, das im überstehenden Teil einer Ersatz-Zeichenfolge steht, die länger als die zugehörige Such-Zeichenfolge ist, wird selbst als Ersatz in die Datei geschrieben, da es kein bereits bestehendes Zeichen in der Datei gibt, das sich dem Jokerzeichen zuordnen lässt.

Ganze Wörter: Die zu suchende Zeichenfolge wird nur erkannt, wenn sie als einzelnes Wort vorkommt, also von anderen Buchstaben (z. B. durch Leer- oder Steuerzeichen) getrennt ist. Wenn diese Option gewählt ist, wird z. B. „Tomate“ nicht in „Automaten“ gefunden.

Suchrichtung: Bestimmen Sie, ob von vorne bis hinten oder von der aktuellen Position an ab- oder aufwärts ersetzt werden soll.

Nur im Block suchen: Es wird nur derjenige Teil der Datei/des virtuellen Speichers durchsucht, der innerhalb des Blockes liegt.

In allen geöffneten Dateien ersetzen: Der Vorgang wird der Reihe nach in allen von WinHex geöffneten Dateien durchgeführt (sofern sie nicht im Nur-Lesen-Modus geöffnet wurden). Wenn „Nur im Block suchen“ aktiviert ist, wird in jeder Datei nur im dort festgelegten Block ersetzt.

Hinweis:

WinHex ist in der Lage, eine Zeichenfolge durch eine andere Zeichenfolge unterschiedlicher Länge zu ersetzen. (Solche Vorgänge benötigen allerdings mehr Zeit und im Ersetzen-Modus mit Bestätigung werden die Änderungen nicht sofort angezeigt.) Immer, wenn Sie diese Möglichkeit nutzen möchten, können Sie bestimmen, auf welche Art dies geschehen soll:

1. Die Dateiinhalte hinter einem Vorkommnis der Suchzeichenfolge werden entsprechend der Längendifferenz von Such- und Ersatzzeichenfolge nach vorne oder hinten verschoben. Die Größe der Datei ändert sich. Viele Arten von Dateien (darunter ausführbare Dateien) werden dadurch unbrauchbar. Es ist sogar möglich, nichts als Ersatz-Zeichenfolge anzugeben. Jedes Vorkommen der Such-Zeichenfolge wird dann aus der Datei entfernt!

2. Die Ersatzzeichenfolge wird ungeachtet ihrer Länge dort in die Datei geschrieben, wo die Suchzeichenfolge gefunden wurde. Wenn die Ersatzzeichenfolge kürzer als Suchzeichenfolge ist, bleibt der hintere Teil des Vorkommnisses der Suchzeichenfolge in der Datei unverändert. Ist die Ersatzzeichenfolge länger, werden auch noch Daten hinter dem Vorkommnis mit dem überstehenden Teil der Ersatzzeichenfolge überschrieben (sofern das Dateiende nicht erreicht ist). Die Größe der Datei bleibt unverändert.

10 Verschiedenes

10.1 Block

Als „Block“ wird ein markierter Bereich innerhalb einer Datei oder eines Datenträgers bezeichnet, der in jedem in WinHex geöffneten Datenfenster festgelegt werden kann. Dieser Bereich ist Gegenstand vieler Funktionen im Bearbeiten-Menü, genau wie die Auswahl in anderen Windows-Programmen. Wenn kein Block definiert ist, beziehen sich diese Funktionen gewöhnlich auf den gesamten Datei- bzw. Datenträgerinhalt.

Die aktuelle Lage und Größe des Blocks werden in der Statusleiste angezeigt. Mit der ESCAPE-Taste oder mit einem Doppelklick der rechten Maustaste hebt man die Blockmarkierung auf.

10.2 Modifizieren von Daten

Mit dieser Funktion können Sie die Daten im aktuellen Block bzw. in der gesamten Datei (falls kein Block definiert ist) verändern. In dieser Version stehen vier verschiedene Operationen zur Verfügung. Entweder Sie *addieren* zu jedem Element der Daten eine Zahl, Sie *invertieren* die Bits, Sie führen eine bitweise *XOR*-Operation mit einer Konstanten aus (eine einfache Art der Verschlüsselung), eine *OR*- oder eine *AND*-Operation, Sie shiften Bits logisch, rotieren Bits nach links in einem zirkulierendem Muster (1. Byte um 1 Bit, 2. Byte um 2 Bits usw.) oder Sie *vertauschen* Bytes paarweise. Durch das Shiften (Verschieben) von Bits können Sie das Einfügen oder Entfernen eines einzelnen Bits am Anfang des Blockes simulieren. Daten lassen sich auch um ganze *Bytes* verschieben (derzeit nur nach links, durch Eingabe einer negative Anzahl von Bytes). Dies ist nützlich, wenn Sie im In-Place-Modus Bytes aus einer sehr großen Datei ausschneiden möchten, was sonst die Erstellung einer ebensogroßen temporären Datei erfordern würde.

Addition

Geben Sie einen positiven oder negativen, dezimalen oder hexadezimalen Summanden an, der jedem Datenelement des Blockes hinzuaddiert werden soll. Der numerische Datentyp bestimmt Größe (1, 2 oder 4 Bytes) und Art (vorzeichenbehaftet oder vorzeichenlos) eines Elements.

Es werden zwei Möglichkeiten angeboten, wie WinHex verfahren soll, wenn durch die Addition der Wertebereich des Formats über- oder unterschritten würde. Entweder der Wertebereich wird nicht verlassen, d. h. das Maximum bzw. Minimum des Wertebereichs wird als neuer Wert angenommen (I), oder die Addition wird dennoch durchgeführt und der entstehende Übertrag ignoriert (II).

Beispiel: 8 Bit, vorzeichenlos
I. FF + 1 → FF (255 + 1 → 255)
II. FF + 1 → 00 (255 + 1 → 0)

Beispiel: 8 Bit, vorzeichenbehaftet
I. 80 - 1 → 80 (-128 - 1 → -128)
II. 80 - 1 → 7F (-128 - 1 → +127)

- Bei Verwendung der ersten Methode erhalten Sie nach Abschluss der Operation eine Meldung, wie oft die Addition nicht durchgeführt werden konnte.
- Wenn Sie die zweite Methode verwenden, ist der Vorgang umkehrbar. Geben Sie einfach die Gegenzahl des zuvor benutzten Summanden bei gleichem Zahlenformat ein. Sie erhalten dann exakt die ursprünglichen Daten.
- Bei Wahl der zweiten Methode ist es egal, ob Sie ein vorzeichenbehaftetes oder vorzeichenloses Format angeben.

Byte-Reihenfolge umkehren

Vertauscht benachbarte Bytes paarweise (16-Bit-Vertauschung) oder in 4er-Gruppen (32-Bit-Vertauschung) innerhalb des aktuellen Blocks bzw. innerhalb der gesamten Datei, wenn kein Block definiert ist. Der Bereich muss dazu ein Vielfaches von 2 (16-Bit-Vertauschung) bzw. 4 (32-Bit-Vertauschung) Bytes enthalten. Mit dieser Funktion können Sie „Big Endian"-Daten in „Little Endian"-Daten verwandeln.

10.3 Konvertierungen

WinHex und X-Ways Forensics erlauben es, mit dem Befehl »Konvertieren« im Bearbeiten-Menü je nach Lizenztyp Daten in andere Formate umzuwandeln, zu verschlüsseln und zu entschlüsseln, zu komprimieren und zu dekomprimieren. Die Konvertierung kann optional in allen in WinHex geöffneten Dateien statt nur im aktiven Datenfenster durchgeführt werden. Die mit einem Stern (*) gekennzeichneten Formate können auch blockweise umgewandelt werden, d. h. es müssen nicht zwangsweise die gesamten Daten im aktuellen Datenfenster konvertiert werden. Die folgenden Formate/Konvertierungsmethoden werden unterstützt:

• ANSI-ASCII, IBM-ASCII (zwei sich teilweise unterscheidende ASCII-Zeichensätze)*
• EBCDIC (ein IBM-Mainframe-Zeichensatz)*
• Groß-/Kleinbuchstaben (ANSI-ASCII)*
• Binär (Rohdaten)
• Hex-ASCII (Hexadezimal-Darstellung von Rohdaten als ASCII-Text)
• Intel-Hex (=Extended Intellec; Hex-ASCII-Daten in einem speziellen Format, incl. Prüfsummen etc.)
• Motorola-S (=Extended Exorcisor; dto.)
• Base64
• UUCode
• Percentage URL Encode
• Quoted Printable
• 7-Bit-ASCII-Code in lesbaren 8-Bit-ASCII-Text verwandeln, was z. B. für SMS in konventionellen Mobiltelefonen nützlich ist.
• Conversion of so-called Nandroid backup files of the NAND flash memory of Android devices to regular raw images.
• ZLIB-Kompression/Dekompression
• LZFSE-Kompression/Dekompression
• ZSTD-Kompression/Dekompression
• LZVN-Dekompression

Bitte beachten Sie:
• Beim Konvertieren von Intel-Hex oder Motorola-S in ein anderes Format werden die in den Daten enthaltenen Prüfsummen nicht auf Korrektheit überprüft.
• In Abhängigkeit von der Dateigröße wird der kleinstmögliche Subtyp in der Ausgabe verwendet: Intel-Hex: 20-Bit oder 32-Bit. Motorola-S: S1, S2 oder S3.
• Beim Konvertieren von Binär nach Intel-Hex oder Motorola-S werden nur Speicherbereiche

übersetzt, die nicht mit hexadezimalen FFs gefüllt sind, um die Ergebnisdatei kompakt zu halten.

Der Befehl »Konvertieren« kann auch Rohdaten einer beliebigen Anzahl kompletter 16-Cluster-Einheiten dekomprimieren, die vom NTFS-Dateisystem komprimiert wurden, sowie (mit forensischer Lizenz) herauskopierte ganze hiberfil.sys-Dateien bestimmter Windows-Versionen sowie einzelne xpress-Blöcke daraus.

Verschlüsselung/Entschlüsselung*

Als Schlüssel geben Sie eine Zeichenfolge aus 1-16 Zeichen ein. Je mehr Zeichen Sie eingeben, umso sicherer ist die Verschlüsselung. Der Schlüssel wird nicht direkt für Ver- und Entschlüsselung benutzt, sondern ist nur Datenmaterial für einen Digest. Er wird nicht auf der Festplatte gespeichert. Fall die entsprechende Sicherheitsoption gewählt ist, wird er in verschlüsselter Form im Arbeitsspeicher gehalten, solange WinHex läuft.

Es wird empfohlen, einen Schlüssel zu verwenden, der aus mind. 8 Zeichen besteht. Der Schlüssel ist abhängig von Groß- und Kleinschreibung. Widerstehen Sie der Versuchung, ein Wort aus einer belieben Sprache zu wählen. Am besten ist eine zufällige Kombination von Buchstaben, Satzzeichen und Ziffern. Beachten Sie, dass Groß- und Kleinbuchstaben unterschieden werden. Es ist unmöglich, ohne den richtigen Schlüssel die verschlüsselten Daten wiederherstellen zu können. Der zur Entschlüsselung eingegebene Schlüssel wird nicht auf Korrektheit überprüft.

Verschlüsselungsalgorithmus: 256-Bit-AES/Rijndael, im Counter-Modus (CTR). Dieser Algorithmus benutzt einen 256-Bit-Schlüssel, der mit SHA-256 gehasht wird aus der 512-Bit-Konkatenation des SHA-256 des von Ihnen angegebenen Schlüssels und 256 Bits kryptographisch einwandfreien Zufallszahlen („Salz“). Die Datei wird um 48 Bytes vergrößert, um das Salz (32 Bytes) und einen 16 Byte großen zufällig gewählten Initialzählstand unterzubringen.
WinHex erlaubt es nicht nur, eine gesamte Datei, sondern alternativ auch nur einen Block von Daten zu verschlüsseln. In diesem Fall werden Sie jedoch gewarnt, dass weder „Salz“ noch ein zufälliger Initialzählstand verwendet werden. Sie dürfen dann keinesfalls denselben Schlüssel mit derselben Methode wiederverwenden, um andere Daten zu verschlüsseln. Die Größe des Blocks bleibt unverändert.

10.4 Überlagerung von Sektoren

Mit dieser Funktion können Sie Sektoren von als schreibgeschützt geöffneten Datenträgern oder interpretierten Images mit anderen Daten überlagern. Das kann nützlich sein, wenn Sie kleinere, vorübergehend erforderliche, virtuelle Änderungen an den Daten in den Sektoren innerhalb des Programms vornehmen müssen, um die Daten intern richtig interpretiert zu bekommen, wenn Sie aber die Daten auf dem Datenträger oder im Image selbst nicht ändern möchten oder dürfen (oder nicht können, weil es sich nicht um ein Roh-Image, sondern ein .e01-Evidence-File handelt) und auch nicht eine weitere komplette Arbeitskopie eines Images von z. B. 2 TB Größe erzeugen möchten, wenn nur 1 Byte geändert werden muss. Solche Anpassungen können vonnöten sein z. B. in Fällen, in denen eine Partitionstabelle oder Dateisystem-Metadaten leicht falsche Werte

enthalten, in denen lediglich das Fehler einer bestimmten Signatur WinHex davon abhält, das Dateisystem zu erkennen, oder in denen ein einziges umgekipptes Bit verhindert, dass WinHex $MFT in NTFS findet oder lediglich ein falsches Nibble das Erkennen einer Partition als eine LVM2-Container-Partition vereitelt usw. usf. In solchen Situationen können Sie die korrigierten Daten manuell bereitstellen und über die gelesenen Daten legen und dann hoffentlich ohne weitere Probleme mit dem Datenträger bzw. dem Image arbeiten und alle Partitionen und Dateien aufgelistet bekommen, als ob alles in Ordnung wäre. Diese Funktionalität ist gedacht für fortgeschrittene Benutzer, die nicht so leicht aufgeben, wenn sie zunächst "nichts" sehen, und ein gewisses Maß an Verständnis für Datenstrukturen auf niedriger Ebene mitbringen und Wissen darüber, wie diese zu reparieren sind.

Sie können die Überlagerung ein- und ausschalten für den Datenträger oder die Partition im aktiven Datenfenster durch Aufruf des Menübefehls Bearbeiten | Sektoren überlagern. Dieser Befehl erlaubt es Ihnen, eine Datei auszuwählen mit dem Roh-Inhalt von Sektoren. Z. B. können Sie eine solche Datei erzeugen, indem Sie ein oder mehrere Sektoren als Block auswählen, den Block in eine neue Datei kopieren, die notwendigen Änderungen darin vornehmen (sogar in X-Ways Forensics möglich, weil normale Dateien anders als Datenträger und interpretierte Images editiert werden können) und die Datei dann speichern. Wenn die Datei dann angewandt wird, wird ihr Inhalt über die gelesenen Originalsektoren geschichtet, beginnend mit dem Sektor, indem sich der Cursor befindet, oder falls die Datei einen Namen der Art "*n*.sector" hat, wobei *n* eine Zahl ist, wird sie auf die Sektoren beginnend bei Sektor *n* angewandt, und alle anderen Dateien im selben Verzeichnis, deren Namen auf die gleiche Maske passen, werden ebenfalls auf die entsprechenden Sektoren wie im jeweiligen Dateinamen angegeben angewandt. Sie sehen nun die überlagernden Daten sofort, wenn Sie zu den betroffenen Sektoren navigieren, und können auch weitere Änderungen an der Datei vornehmen, wenn Sie sie in einem separaten Datenfenstern offenhalten. Sobald Sie die Änderungen in dem Fenster gespeichert haben, werden sie auch wirksam in dem Datenfenster, das den Datenträger bzw. die Partition repräsentiert, deren Daten Sie korrigieren möchten, wenn Sie die Ansicht aktualisieren, einen neuen Datei-Überblick erstellen, den Anfang einer Partition definieren, erneut versuchen, eine Datei mit einem defekten FILE-Record zu öffnen usw. usf.

Bitte beachten Sie, dass nur vollständige Sektoren, keine Teile davon, überlagert werden können. Die Überlagerung kann nur für einen offenen Datenträger oder eine Partition gleichzeitig aktiv sein. Wenn sie für einen physischen, partitionierten Datenträger aktiv ist oder ein Image davon und Sie eine Partition von innerhalb dieses Datenträgers öffnen, sehen Sie die überlagerten Daten auch in der Darstellung dieser Partition. Bei Bedarf können Sie eine vollständige Kopie (Image oder geklonter Datenträger) des virtuell reparierten Datenträgers bzw. Images mit den üblichen Befehlen erzeugen, während die Überlagerung aktiv ist, so dass in der Kopie die künstlich aufgetragenen Daten direkt eingebettet sind. Ein Asservat in einem Fall merkt sich eine aktive Sektorüberlagerung stellt sie automatisch wieder her, wenn es das nächste Mal geöffnet wird, und erinnert Sie daran.

10.5 Löschen und Initialisieren

Zum sicheren Löschen (Schreddern) von Daten in Datenträgersektoren, unbenutzten Datenträger-bereichen (Menü Disk-Tools) oder von mit der Funktion „Sicheres Löschen“ ausgewählten

Dateien, aber auch zum einfachen Füllen von Dateien mit bestimmten Byte-Werten, bietet WinHex folgende Optionen an:

Mit konstanten Byte-Werten in Hexadezimalnotation: Geben Sie bis zu 16 jeweils zweistellige Hex-Werte an, die aneinandergehängt in den aktuellen Block bzw. in die Datei kopiert werden. Sehr schnell.

Mit konventionellen Pseudozufallszahlen: Geben Sie ein Intervall innerhalb von 0-255 (dezimal) an, aus dem zufällig jedem einzelnen Byte des aktuellen Blocks bzw. des gesamten Dateiinhalts ein Wert zugeordnet wird. Jeder Wert aus dem Intervall wird mit gleicher Wahrscheinlichkeit ausgewählt. Schnell.

Mit Pseudozufallszahlen, die Verschlüsselung simulieren: Zufallsdaten, deren Ziel es ist, nicht von verschlüsselten Daten unterscheidbar zu sein. Recht schnell.

Mit kryptographisch sicheren Pseudozufallszahlen: Erzeug von einem kryptographisch sicheren Pseudozufallszahlengenerator (CSPRNG) names ISAAC, *sehr* langsam.

Auf Wunsch kann diese Funktion in allen geöffneten Dateien ausgeführt werden. Dazu muss in allen Dateien entweder ein Block definiert oder in allen Dateien kein Block definiert sein.

Um die Sicherheit zu maximieren, wenn Sie Schlupfspeicher, freien Speicher, unbenutzte NTFS-Records oder ganze Datenträger permanent löschen möchten, können Sie mehr als einen Durchlauf (bis zu drei) zum Überschreiben einstellen.

Gemäß der sogenannten Clearing and Sanitization Matrix, dem im Betriebshandbuch 5220.22-M des U.S.-Verteidigungsministeriums (Department of Defense, DoD) beschriebenen Standard, Methode „c“, kann eine Festplatte oder eine Diskette gelöscht werden, indem alle adressierbaren Bytes mit einem einzelnen Zeichen (einmal) überschrieben werden. Üblicherweise ist dies der Hexadezimalwert 0x00, kann aber auch jeder andere Wert sein. Um Festplatten so sicher zu löschen, dass sie bedenkenlos an andere Personen/Abteilungen/Organizationen weitergegeben werden können ("sanitizing"), müssen gemäß Methode „d“ alle adressierbaren Bytes mit einem Zeichen, dann seinem Komplement und schließlich einem Zufallswert überschrieben und muss anschließend überprüft werden. (Diese Methode ist vom DoD nicht für das Sanitizing von Datenträgern mit *Top*-Secret-Informationen freigegeben worden.)

Der „DoD“-Schalter konfiguriert WinHex für das Sanitizing, so dass erst mit 0x55 (binär 01010101), dann mit dem Komplement (0xAA = 10101010) und schließlich mit einem zufälligen Byte-Wert überschrieben wird.

Der „0x00“-Schalter konfiguriert WinHex für eine einfache Initialisierung, also einmaliges Schreiben von Nullbytes.

10.6 Klonen von Datenträgern

Tools | Disk-Tools | Datenträger klonen lässt Sie eine bestimmte Anzahl von Sektoren kopieren, **von** einem Quell*datenträger* (Schalter mit Datenträger-Icon anklicken) oder einer Quell*datei* (Schalter mit Datei-Icon anklicken) **auf** einen Ziel*datenträger* oder in eine Ziel*datei*.

Dazu müssen im Fall, dass sowohl Quelle als auch Ziel Datenträger sind, beide Datenträger dieselbe Sektorgröße aufweisen. Mit dieser Funktion können Sie exakte Duplikate ganzer Festplatten herstellen, indem Sie einfach *alle* Sektoren kopieren. Aktivieren Sie die entsprechende Option, damit die richtigen Zahlen automatisch für Sie eingetragen werden. Der Zieldatenträger darf nicht kleiner als der Quelldatenträger sein. Als *Datenträger* können Sie auch ein als Datenträger interpretiertes Image wählen oder eine vom physischen Datenträger aus im Hintergrund geöffnete Partition. Als Ziel kommt jedoch kein interpretiertes .e01-Evidence-Files in Frage, da es nicht beschrieben werden kann, höchstens ein Roh-Image. Als *Dateien* kommen nur unsegmentierte Roh-Images in Frage, z. B. .dd, .001, .img usw, keine anderen Image-Typen wie .e01, .vhd oder .vmdk.

Die Funktion „Datenträger klonen“ bietet verschiedene Möglichkeiten zu verfahren, wenn defekte Sektoren auf dem Quelldatenträger angetroffen werden:

- Standardmäßig werden Sie benachrichtigt und gefragt, ob der Vorgang abgebrochen oder dennoch fortgesetzt werden soll. Bei eingeschalteter Option „Protokolldatei schreiben“ werden Informationen über die gesamte Operation in eine Logdatei in den Ordner für temporäre Dateien geschrieben (Dateiname „Cloning log.txt“). Darin sind auch die Nummern etwaiger unlesbarer Sektoren enthalten, die nicht kopiert werden können. Diese Option verhindert, dass WinHex jeden defekten Sektor während des Vorgangs einzeln meldet.
- WinHex kann die Zielsektoren, die mit dem Inhalt unlesbarer Quellsektoren beschrieben werden müssten, entweder unverändert lassen oder mit einem ASCII-Muster Ihrer Wahl füllen (z. B. Ihre Initialen oder so etwas wie „BAD “). Lassen Sie das Editierfeld für das Muster leer, um solche Sektoren mit *Nullbytes* zu füllen. Übrigens wird das gewählte Muster auch verwendet, um den Inhalt eines nicht lesbaren Sektors im Disk-Editor anzuzeigen.
- Defekte Sektoren treten häufig in zusammenhängenden Gruppen auf, und jeder Versuch, einen defekten Sektor zu lesen, dauert gewöhnlich sehr lange. WinHex kann solche beschädigten Bereiche versuchen zu meiden: Wenn ein defekter Sektor erkannt wird, kann WinHex eine von Ihnen anzugebende Anzahl folgender Sektoren überspringen. Dies ist nützlich, um den Klonvorgang zu beschleunigen, wenn Sie in Kauf nehmen, dass auch einige unbeschädigte Sektoren nicht mit kopiert werden.

Das konventionelle Klonen ist bei austauschbaren Datenträgern (wie Disketten) nicht möglich, wenn nur *ein* entsprechendes Laufwerk installiert ist. Eine geeignete Vorgehensweise für diesen Fall ist *Disk Imaging*, also eine Art „verzögertes“ Klonen. Ein Disk-Image kann auf einen anderen Datenträger zurückgespielt werden. Das Ergebnis ist dann dasselbe wie beim Klonen.

Wenn Sie eine Datei namens „dev-null“ als Ziel angeben, werden die Daten nur gelesen und nirgendwohin kopiert (und Sie werden diesbezüglich gewarnt). Dies ist nützlich, wenn Sie nur an dem Bericht über defekte Sektoren interessiert sind und den Datenträger nicht wirklich klonen oder in einer Datei sichern möchten.

Sie können „simultane E/A“ probieren, wenn das Ziel nicht auf dem gleichen physischen Datenträger liegt wie die Quelle. Das bietet die Möglichkeit, den Klonvorgang um bis zu 30% zu beschleunigen.

Nur mit Specialist-Lizenz oder höher: Zusammen mit der simultanen E/A können Sie WinHex Sektoren auch in *umgekehrter* Reihenfolge kopieren lassen, also von hinten (vom Ende des Datenträgers beginnend) *rückwärts*. Das ist nützlich, wenn die Quellfestplatte schwerwiegende physische Defekte aufweist, die z. B. ein Sicherungsprogramm oder gleich den ganzen Computer zum Einfrieren oder Absturz bringen, wenn ein bestimmter Sektor erreicht wird. In einem solchen Fall können Sie zusätzlich ein Image in umgekehrter Reihenfolge erzeugen, wobei die Sektoren von der Platte einzeln rückwärts gelesen werden, oder noch besser, es ist sogar möglich, ein bereits auf konventionelle Weise (vorwärts) erzeugtes, aber (aufgrund eines Absturzes) unvollständiges unsegmentiertes Roh-Image zusätzlich noch von hinten so zu *ergänzen*, dass es so vollständig wie möglich wird, da von beiden Seiten befüllt, und nur irgendwo in der Mitte einen idealerweise kleinen mit binären Nullen gefüllten blinden Fleck aufweist, der den nicht lesbaren beschädigten Bereich des Quelldatenträgers repräsentiert. Dazu wählen Sie einfach ein unvollständiges Roh-Image, das Sie schon haben, als Zieldatei aus, und Sie werden dann gefragt, ob Sie es ergänzen statt überschreiben möchten. WinHex besorgt alles weitere, also allokiert die fehlenden Sektoren in der Image-Datei (mit Nullen gefüllt), so dass es die vollständige Größe des Quelldatenträgers hat, und befüllt die Datei dann soweit wie möglich von hinten. Stellen Sie sicher, dass Sie rückwärts zu befüllende Images immer auf NTFS-Partitionen erzeugen, nicht FAT32. Der Startsektor der Quelle, der beim umgekehrten Kopieren von Sektoren anzugeben ist, ist derselbe wie für normales Vorwärtskopieren, also normalerweise 0, wenn man einen Datenträger vollständig kopieren möchte.

Für Datenträgersicherungen wird grundsätzlich stattdessen die Verwendung des Befehls Datei | Datenträger-Sicherung empfohlen, aus diversen Gründen (mit einer forensischen Lizenz: Unterstützung von .e01-Evidence-Dateien, Kompression, Hashing, Verschlüsselung, Metadaten, technischer Detailbericht, bequemer). Nur in Sonderfällen, wenn Sie sich z. B. mit schwerwiegenden physischen Plattendefekten herumärgern müssen oder wenn Sie lediglich gezielt bestimmte Sektorbereiche kopieren möchten, können fortgeschrittene Benutzer den Befehl Extras | Disk-Tools | Datenträger klonen verwenden, um eine noch größere Kontrolle darüber zu bekommen, welche Sektoren von wo nach wo und in welcher Reihenfolge kopiert werden sollen.

10.7 Images und Sicherungen

Der Befehl „Datenträger-Sicherung“ bzw. „Sicherung anlegen“ im Dateimenü erlaubt es, eine Sicherung/ein Image des geöffneten Datenträgers bzw. der geöffneten Datei anzufertigen. Drei verschiedene Ausgabeformate mit jeweils besonderen Vorteilen stehen zur Auswahl.

Dateiformat:	WinHex-Backup	**Evidence-File**	**Roh-Image**
Dateiendung:	.whx	.e01	z. B. .dd
Interpretierbar:	nein	ja	ja
In Segmente aufteilbar:	ja	ja	ja
Komprimierbar:	ja	ja	nein
Verschlüsselbar:	no	ja	nein

Optionaler Hash:	integriert	integriert	separat
Optionale Beschreibung:	integriert	integriert	separat
Nur bestimmte Sektoren:	ja	(ja)	(ja)
Auf Dateien anwendbar:	ja	nein	nein
Automat. Verwaltung:	Sicherungs-Mngr.	nein	nein
Kompatibilität:	nein	(ja)	ja
Benötigte Lizenzart:	keine	forensisch	privat

Der große Vorteil von Evidence-Files und Roh-Images ist es, dass sie von WinHex wie die Original-Datenträger interpretiert werden können (mit dem entsprechenden Befehl im Specialist-Menü). Daher sind sie auch geeignet für den Gebrauch als Asservate in Ihren Fällen. Evidence-Files sind im besonderen Maße prädestiniert dafür, da sie auch eine optionale Beschreibung einen integrierten Hash für spätere Verifizierung enthalten können. Roh-Images sind sehr universell und können leicht zwischen noch mehr forensischen Tools ausgetauscht werden als Evidence-Files. Alle Ausgabe-Formate erlauben das Splitten in Segmente einer benutzerdefinierten Größe. Eine Segmentgröße von 650 oder 700 MB z. B. ist geeignet zum Archivieren auf CD-Rs. Evidence-Files müssen bei maximal 2047 MB gesplittet werden, damit sie mit X-Ways Forensics vor Version 14.9 und mit EnCase vor Version 6 und mit bestimmten anderen Tools kompatibel sind. Mit einer forensischen Lizenz können Roh-Image-Dateien und Evidence-Files automatisch sofort nach Erstellung überprüft werden, indem der ursprünglich für den Originaldatenträger berechnete Hash über das Image neu berechnet und verglichen wird.

Zum Komprimieren von Evidence-Files und WinHex-Backups wird der weit verbreitete Deflate-Algorithmus der *zlib*-Bibliothek verwendet. Er basiert auf LZ77-Kompression und Huffman-Codierung. Mit der „normalen“ Kompressionsstufe können Sie bei durchschnittlichen Daten eine Kompressionsrate von 40-50% erreichen. Die Speicherplatzersparnis bezahlen Sie allerdings mit einer deutlich verringerten Sicherungsgeschwindigkeit. „Schnelle/adaptive“ Komprimierung ist ein *sehr guter* und *intelligenter* Kompromiss zwischen Geschwindigkeit und guter Kompression, nicht einfach wie die gewöhnliche Option „schnell“ in anderen Programmen. Bei „starker“ Komprimierung gewinnen Sie nur weniger weitere Prozentpunkte an Kompression, bei unverhältnismäßig hohen Geschwindigkeitseinbußen. Für WinHex-Backups ist „adaptiv“ das gleiche wie „normal“.

Roh-Image-Dateien können auf NTFS-Dateisystemebene komprimiert werden, wenn sie auf NTFS-Partitionen erzeugt werden. Entweder können Sie normale NTFS-Kompression verwenden, oder die Image-Datei als „Sparse“-Datei anlegen, so dass größere Mengen von Nullbytes keinen Speicherplatz benötigen.

Bereinigte Sicherung: With a forensic license, there is an acquisition option for those users who need to or want to exclude certain files from forensic images, called "Omit excluded files". The data stored in clusters that are associated with files that you *exclude* before starting the imaging process will automatically be zeroed out in the image. That won't have any effect on files whose contents are not stored in their own clusters. Before you start the imaging process for a partitioned disk, open the partitions in which the files are located that you would like to exclude. Wait till the volume snapshot has been taken if it was not taken before. Then exclude the files. You do not need to open and take volume snapshots of partitions whose data you would like to include completely. All other data is copied to the image normally. There is an option to "watermark" wiped sectors in the image with an ASCII or Unicode text string, so that when working with the image you are reminded of the omission when you look at the affected areas. Cleansed images

are useful for anyone who needs to redact certain files in the file system, but otherwise wants to create an ordinary forensically sound sector-wise image, compatible with other tools. A must in countries whose legislation specially protects the most private personal data of individuals and certain data acquired from custodians of professional secrets (e.g. lawyers and physicians, whose profession swears them to secrecy/confidentiality). Limitation: Not available for disks partitioned as Windows dynamic disks or with Linux LVM*. Only files in supported file systems can be omitted. Note that you can also retroactively cleanse (redact) already created conventional raw images, in WinHex, by securely wiping files selected files via the directory browser context menu. The granularity of this operation is not limited to entire clusters that way. For example, that means it can also wipe files in NTFS file systems with so-called resident/inline storage and it does not erase file slack along. For a comparison of evidence file containers, skeleton images and cleansed images please see our web site. All of those are images that only transport a subset of the original data.

Eine andere Art bereinigter Sicherung ist ein Image, in dem all die Cluster, die vom Dateisystem als frei definiert sind, mit Null-Bytes gefüllt werden (nur mit Specialist- oder forensischer Lizenz). Das ist nützlich, wenn Sie ein Image als Backup und nicht für forensische Zwecke erzeugen, oder wenn Sie für forensische Zwecke keine Daten im freien Laufwerksspeicher benötigen oder solche Daten gar nicht sichern sollen (wenn die Untersuchung auf existierende Dateien beschränkt werden soll). Bei eingeschalteter Kompression hat diese Option das Potential, eine Menge Plattenplatz zu sparen, abhängig davon wieviel freien Speicher es gibt, und die Sicherung dramatisch zu beschleunigen, wenn es große zusammenhängende freie Bereiche gibt. Beachten Sie, dass im Fall von Dateisysteminkonsistenzen Cluster zu Unrecht als frei betrachtet werden könnten. Wenn Sie sowohl bestimmte (ausgeblendete) Dateien auslassen möchten als auch freie Cluster, dann blenden Sie bitte zusätzlich die virtuelle Datei "Freier Speicher" und schalten die Bereinigung des freien Speichers in den Optionen des Datei-Überblicks aus.

Das Erzeugen von bereinigten Sicherungen muss gesondert bestätigt werden, um die unbeabsichtigte Erzeugung von Images zu verhindern, die im konventionellen Sinn nicht forensisch einwandfrei sind. In einem moderneren Sinn des Wortes können sie aber durchaus als forensisch zu bezeichnen sein, abhängig von der Rechtslage und Rechtsprechung und der Gesamtsituation, in der Sie arbeiten. Eine übermäßige Datenerhebung ist in Deutschland gemäß Bundesverfassungsgericht zu vermeiden, Verhältnismäßigkeitsgrundsätze müssen beachtet werden. Bereinigte Sicherungen bieten die wohl beste Lösung zum Schutz des Kernbereichs privater Lebensgestaltung und zur Wahrung von Zeugnisverweigerungsrechten von Berufsgeheimnisträgern wie Ärzten und Rechtsanwälten.

X-Ways Forensics prüft auf und warnt vor überlappenden Partitionen, wenn Sie eine bereinigte Sicherung eines partitionierten physischen Datenträgers erzeugen. Clusters in von der Überlappung betroffenen Bereichen werden nicht ausgelassen. In einer solchen Situation wird empfohlen, die relevanten Partitionen für sich zu sichern.

Mit forensischer Lizenz: Beim Erzeugen eines Images wird der technische Detailbericht aufgerufen und in eine Textdatei geschrieben, die die Image-Datei begleitet. Für .e01 Evidence-Files wird es außerdem direkt in die .e01-Datei als Beschreibung integriert. Die SMART-Informationen werden nach Abschluss des Vorgangs erneut abgefragt und in die Textdatei geschrieben, so dass Sie erstens sehen, ob sich der Zustand einer bereits defekten Platte weiter verschlechtert hat und zweitens feststellen können, wie sich die „power on time“ geändert hat,

was nützlich ist, um auf die Maßeinheit schließen zu können (normalerweise Stunden, aber das kann je nach Festplattenmodell anders sein). Die Textdatei gibt auch die für die Sicherung benötigte Zeit an, die erzielte Kompressionsrate, das Ergebnis der sofortigen Überprüfung der Image-Datei mittels Hash-Wert (falls gewählt) sowie etwaige Sektorlesefehler.

Mit forensischer Lizenz: Möglichkeit, bei Bedarf eine zweite Kopie eines Images schon bei der Datenträger-Sicherung zu erzeugen, was viel schneller ist als das nachträgliche Kopieren der Image-Datei und Sinn hat, wenn die zweite Kopie auf einem anderen Datenträger erzeugt wird. Das Aufteilen in mehrere Segmente geschieht synchron für beide Kopien, auch wenn der freie Speicherplatz nur auf einem der beiden Ziellaufwerke erschöpft ist.

Mit forensischer Lizenz: You may specify an overflow location in advance where further image file segments will be stored should space on the primary output drive be exhausted. If you leave that field blank or if even the overflow location has no more space left, you will be prompted for a new path as before when needed. If an overflow location is specified in advance and at the same time you chose to create two copies of the image, then please note that the overflow location is used only for the first image copy that runs out of space, if any. For the other image copy you would be prompted if space is scarce.

Mit forensischer Lizenz: Es besteht die Möglichkeit, zwei Hash-Werte gleichzeitig zu berechnen. Wenn Sie davon Gebrauch machen, werden beide Hash-Werte in der begleitenden Textdatei gespeichert. Der erste Hash-Wert ist derjenige, der auf Wunsch am Ende des Sicherungsvorgangs automatisch überprüft wird. Sie könnten hierfür gezielt den schnelleren Algorithmus wählen, denn der Hauptzweck ist hierbei wohl lediglich das Erkennen von Lese-, Schreib- und Dateifehlern. Der zweite Hash-Wert wird in die Asservateigenschaften übernommen, wenn Sie das Image einem Fall hinzufügen.

Eine besondere Option erlaubt es, den Arbeitsspeicher kurz vor der Hash-Überprüfung so auszulasten, dass die von Windows verwendeten Dateipuffer automatisch aufgelöst werden und ein Lesen der Image-Daten direkt von der Platte erzwungen wird (so dass die Daten nicht aus dem Speicherpuffer entnommen werden). This option exists for small images and for somewhat paranoid or uber-diligent users. It is not required for images that are much larger than the physical amount of RAM that is installed in your machine because by the time when the final parts of the image have been written, the initial parts are no longer in the buffer, and once the final parts are about to be verified they are no longer in the buffer because at that time the initial parts are in the buffer as they have been verified just before. Your system may behave a little bit sluggish for a while when using this option, and verification may be slightly slower than normally.

Mit forensischer Lizenz: Optional können Sie weitere Datenträgersicherungen in zusätzlichen Programminstanzen im Voraus anzusetzen, die zunächst abwarten, bis bereits laufende Sicherungsoperationen in früheren Instanzen beendet sind, um die ineffiziente, simultane Erzeugung mehrerer Image-Dateien auf demselben Zieldatenträger zu vermeiden (was unnötig langsam ist und hochgradig fragmentierte Sicherungsdateien erzeugt). Die weiteren Instanzen warten nur auf solche vorherigen Instanzen, in denen das Kontrollkästchen ebenfalls angekreuzt war.

Mit forensischer Lizenz: Wenn Sie eine Datenträger-Sicherung mittendrin abbrechen, schließt X-Ways Forensics das .e01-Evidence-Dateiformat (im aktuellen Segment) noch schnell ab, damit

man ein konsistentes Image erhält, auch wenn es nicht vollständig ist. Nützlich z. B. in einer Notfallsituation, wenn Sie eine Sicherung vor Ort vornehmen, weil ein ohne Fehlermeldungen nutzbares unvollständiges Image besser ist als ein nicht nutzbares defektes Image. Wenn eine Hash-Berechnung stattfand, kann der Hash-Wert dadurch später verifiziert werden.

Mit forensischer Lizenz: Die beschreibende Text-Datei, die während der Sicherung erzeugt wird, gibt für alle Segmente von Roh-Images deren exakte Größe in Bytes und für alle Segmente von .e01-Evidence-Dateien deren genaue Block-Anzahl an. Sollte, aus welchen Gründen auch immer, eines oder mehrere Segmente verloren gehen oder beschädigt werden, ermöglicht dies die Erzeugung künstlicher Ersatz-Segmente in der passenden Kapazität, um die Lücken zu füllen, womit die Daten in folgenden Segmenten die korrekte logische Distanz zu den Daten in vorangegangen Segmenten haben, um die Gültigkeit interner Verweise in den Daten zu erhalten (die Startsektoren von Partitionen in der Partitionstabelle, Cluster-Nummern in den Dateisystem-Strukturen) sofern diejenigen Original-Image-Segmente vorhanden sind, die Quelle und Ziel des Verweises enthalten.

Mit forensischer Lizenz: Sie haben die Wahl zwischen dem althergebrachten, standardisierten Kompressionsalgorithmus für Images im .e01-Format, der kompatibel mit anderen Tools ist, und einem deutlich moderneren Kompressionsalgorithmus, der ein viel besseres Verhältnis bietet zwischen erzieltem Kompressionsgrad und Kompressionsgeschwindigkeit plus Dekompressions-geschwindigkeit. Ganz grob gesagt, abhängig von den jeweiligen Daten, komprimiert die "moderne" Normaleinstellung fast so stark wie das kompatible Normal (vielleicht ein paar Prozentpunkte weniger stark), braucht aber vielleicht nur ein Viertel der Zeit für die Kompression und ein Drittel der Zeit für die Dekompression. (Wir beziehen uns hier rein auf die Rechenzeit der CPU, mit einem einzigen Thread, unter Ausschluss von Datenübertragung). Wenn der moderne Algorithmus auf "stärker+" eingestellt ist, erreicht er vielleicht den Kompressionsgrad wie das alte "normal" (oder etwas besser), aber benötigt nur etwa die Hälfte der Zeit für die Kompression und 40% der Zeit für die Dekompression (oder weniger). "Stärker++" braucht deutlich mehr Zeit und ist normalerweise nicht empfehlenswert, weil die zusätzlich erzielte Speicherplatzersparnis oft sehr gering ist, aber auch diese Einstellung kann immer noch schneller sein als der alte Algorithmus, besonders bei der *De*kompression (die wohlgemerkt im Gegensatz zur Kompression normalerweise mehr als einmal erfolgt, z. B. bei der Image-Überprüfung sofort nach der Erstellung, bei einer etwaigen nochmaligen Überprüfung zu einem späteren Zeitpunkt, bei einer Datei-Header-Signatur-Suche, bei einer oder mehrere Stichwortsuchen, bei diversen Analysen, beim Herauskopieren von Dateien usw.). Allgemein empfehlen wir die moderne Normal-Einstellung. Bitte beachten Sie noch, dass Sie mit dem modernen Kompressionsalgorithmus ein Image erzeugen, das sich nur für den Gebrauch in X-Ways Forensics und X-Ways Investigator 20.9 und neuer eignet. Die "sparse"-Einstellung der modernen Kompressionsmethode, die extrem effizient ist beim Sichern von Datenträgern, die nur minimal verwendet wurden, und zwar 11 Mal (!) so speicherplatzsparend für "genullte" Daten wie die Sparse-Einstellung der kompatiblen Kompressionsmethode, wird bereits seit v18.9 verstanden.

Mit forensischer Lizenz: Es besteht die Möglichkeit, die Kompressionsstufe/-stärke (aber nicht die Kompressionsmethode) jederzeit während der Erzeugung eines .e01-Evidence-Files zu ändern. Nützlich, wenn Ihre Prioritäten (höhere Kompressionsrate oder höhere Geschwindigkeit) sich ändern, z. B. wenn Sie sehen, dass der verbleibende Plattenplatz plötzlich weniger groß aussieht oder wenn Sie den Vorgang schneller als zuvor gedacht beenden müssen. Auch nützlich

zum Experimentieren, wenn Sie nicht sicher sind, welche Kompressionsstufe für eine bestimmte Systemkonfiguration am geeignetsten ist, etwa wenn Sie vor Ort ein laufendes System sichern und das Image über eine langsame USB-Schnittstelle auf eine externe Festplatte schreiben müssen, was mit extrem erfolgreicher Kompression schneller sein könnte als ohne.

Mit forensischer Lizenz: For the .e01 evidence file format, you may choose the internal chunk size. Might be regarded as useful by some to achieve a marginally better compression ratio for ordinary data, at the expense of more time needed when creating the image and when later randomly accessing data in the image, but improves compression noticeably for extremely compressible data (e.g. a wiped or unused areas of a hard disk). A 512 KB chunk size reduces the image size with ideal data (e.g. only 0x00 bytes) ceteris paribus by an additional 40% compared to a 32 KB chunk size. Special optimizations are applied internally for chunk sizes of 32, 128, and 512 KB.

Mit forensischer Lizenz: Beim Sichern mit aktiver Kompression im .e01-Format gibt X-Ways Forensics Ihnen in Echtzeit eine grafische Rückmeldung über die auf dem Datenträger vorgefundene Datendichte. Das ist möglich, weil Plattenbereiche, die niemals beschrieben wurden, sowie Datenträgerbereiche, die mit binären Nullen überschrieben wurden, extrem hohe Kompressionsraten erzielen, und Daten, die bereits komprimiert oder verschlüsselt gespeichert sind, überhaupt keine Kompression mehr erlauben, und weil normale Daten halbwegs komprimierbar sind. Die Datendichte wird während der Sicherung durch vertikale Balken in einem separaten Fenster abgebildet. Hohe rote Balken stehen für eine hohe Datendichte = mehr Speicherplatzbedarf für das Image = geringen Kompressionserfolg = mehr zu analysierende Daten = (wenn die Balken bis zur oberen Begrenzung reichen) potentiell Verschlüsselung. Mit einem Mausklick irgendwo in dem Fenster können Sie umschalten zwischen Datendichte und dem Gegenstück, der Kompressionsrate. Hohe blaue balken zeigen höhere Kompression an = niedrigere Datendichte = keine Verschlüsselung = weniger Speicherplatzbedarf für das entstehende Image = weniger zu analysierende Daten = weniger Arbeit. Bitte beachten Sie, dass die exakte Höhe der Balken auch von der verwendeten Kompressionsmethode und -stärke abhängt. Die Statistik wird in .e01-Evidence-Dateien gespeichert, so dass dasselbe Diagramm auch zu einem beliebigen späteren Zeitpunkt noch aufgerufen werden kann, und zwar im Asservateigenschaftsfenster durch Klick auf den Schalter, der "Datendichte" oder "Kompression" heißt, wenn das Image offen ist.

Mit forensischer Lizenz: Ability to specify how many extra threads to use for compression when creating .e01 evidence files. By default X-Ways Forensics will use no more than 4 or 8, and it depends on how many processor cores your system has, but you could try to increase the number on very powerful systems with even more cores usually without problems, for a chance to further increase the speed, or you can reduce it you run into stability problems.

Mit forensischer Lizenz: You have the option to change the nature of an image (disk or volume) and its sector size when creating the image. This is possible not only for .e01 evidence files, where both is explicitly defined in the internal metadata (compatible with other tools), but also for raw images (via external metadata, compatible only with X-Ways Forensics/Image v18.4 and later, lost if the image leaves the realm of NTFS file systems). Useful whenever the source of the data is not an ideal interpretation. For example, if a reconstructed RAID actually represents a volume, not a physical disk, then you can already adjust the nature of the image accordingly when you create it. Or if the sector size of the reconstructed RAID or a disk in an enclosure does

not match the sector size of the file system in a partition, you can adjust the sector size of the image accordingly. All of this will allow for smoother and more successful usage of the image later, in particular by users who do not pay much attention to details such as image type and sector size. With the additional metadata present for a raw image, X-Ways Forensics does not need to prompt users for the nature of the image and its sector size even if under normal circumstances it would (for example because the image does not start with an easily identifiable partitioning method or volume boot sector).

Technically minded users may want to set the desired attributes of newly created image files, such as "read-only" or "encrypted", as well as buffering flags for performance tweaking in unusual environments such as "write through". Attributes are defined most thoroughly at https://docs.microsoft.com/en-us/windows/win32/fileio/file-attribute-constants, flags at https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-createfilea. The flag for "no buffering" should not be used. Attributes and flags are combined by oring (or adding) them and have to be specified in hexadecimal notation.

Am Ende des Datenträgersicherungsprozesses kann der Computer optional heruntergefahren oder (wenn von Ihrem System unterstützt) in den Ruhezustand versetzt werden, um Strom zu sparen. Wenn Sie den Ruhezustand gewählt haben, aber Windows signalisiert, dass dieser nicht erreicht werden kann, versucht X-Ways Forensics stattdessen, den Computer herunterzufahren.

Es gibt eine Option, neu erzeugte Images sofort dem Fall hinzuzufügen und ihre(n) Datei-Überblick(e) automatisch ohne weitere Benutzerinteraktion zu erweitern, sofern der Quelldatenträger dem aktiven Fall hinzugefügt wurde und überhaupt ein Fall aktiv ist zu dem Zeitpunkt, wenn Sie die Sicherung starten.

Die Verwendung dieses Befehls ist die empfohlene Methode zum Erzeugen von Images. Um eine beliebige Auswahl von Sektoren zu imagen, können Sie einen Block definieren und dann in eine Datei kopieren mittels Bearbeiten | Block kopieren | In neue Datei, oder Sie rufen den Befehl Extras | Disk-Tools | Datenträger klonen auf. Letzterer Befehl ist besonders dann nützlich, um Festplatten mit schweren physischen Defekten (nicht bloß normalen nicht lesbaren Sektoren) ausschnittsweise zu sichern, und er kann Sektoren sogar rückwärts kopieren.

Eine Automatisierung ist über die Befehlszeile möglich, s. dort.

Der Verschlüsselungsalgorithmus, der in Evidence-Files optional zum Einsatz kommt, ist entweder 128-Bit oder 256-Bit AES/Rijndael, im Counter- (CTR-) Modus. Er erlaubt wahlfreien Zugriff in ein Evidence-File. Die 128-Bit-Implementierung ist neuer und schneller und wird nur von X-Ways Forensics 16.4 und neuer verstanden. Verschlüsselung macht ein .e01-Evidence-File inkompatibel zu anderen Tools. Der Verschlüsselungsalgorithmus benutzt einen 256-Bit-Schlüssel, der mit SHA-256 gehasht wird aus der 512-Bit-Konkatenation des SHA-256 des von Ihnen angegebenen Schlüssels und 256 Bit kryptographisch sicheren Zufallszahlen („Salz“), die im Header des Evidence-File gespeichert werden. Für 128-Bit-AES wird der 256-Bit-Schlüssel zu einem 128-Bit-Schlüssel reduziert durch ver-xor-en von 1. und 2. Hälfte. Der 128-Bit große Counter wird zufällig initialisiert und pro Verschlüsselungsblock inkrementiert, als Little-Endian-Integer in 256-Bit-AES, als Big-Endian-Integer in 128-Bit-AES. Die Größe eines Verschlüsselungsblocks in AES beträgt 128 Bit. Ein zusätzlicher SHA-256 wird im Header gespeichert (für 256-Bit-AES optional, s. Sicherheitsoptionen) und später verwendet, um zu

überprüfen, ob ein vom Benutzer für die Entschlüsselung angegebenes Passwort korrekt ist oder nicht. Der SHA-256-Algorithmus wird angewandt auf eine Konkatenation des Salzes, einem Hash *X* und einem Hash *Y*, um diesen Passwort-Prüfungs-Hash zu berechnen. Dabei ist der Hash *X* der SHA-256 des vom Benutzer angegebenen Schlüssels und Hash *Y* ist der SHA-256 der Konkatenation des vom Benutzer angegebenen Schlüssels und Hash *X*. Für 128-Bit-AES wird *Y* erneut als *X* verwendet und erneut konkateniert und gehasht, immer und immer wieder, 100.000 Mal, um Angriffe mit Rainbow-Tables praktisch unmöglich zu machen. Please note that when you use compression and encryption at the same time, each chunk in an .e01 evidence file is first compressed, then encrypted. So an educated guess about the nature of the data in a given chunk might be possible, merely judging from the compressed size of the chunk (i.e. its compression ratio), even if the compressed data is encrypted.

Wenn Sie den Namen eines WinHex-Backups automatisch vergeben lassen (Format „???.whx“), wird sie im Verzeichnis für Sicherungsdateien erstellt (s. Allgemeine Optionen), mit dem nächsten freien Namen, der der Konvention des Sicherungsmanagers entspricht (xxx.whx). Bei Bedarf kann das Original dann mit dem Sicherungsmanager wiederhergestellt werden. Wenn Sie selbst Dateinamen und Pfad angeben, kann die WHX-Datei immer noch mit dem Menübefehl „Sicherung laden“ wiederhergestellt werden, und im Fall von aufgeteilten Sicherungen hängt WinHex automatisch die Teilsicherungsnummerm an die Dateinamen an.

10.8 Platzhalter-Segmente

X-Ways Forensics hat die Fähigkeit, bequem Ersatz/Platzhalter-Segmente für .e01-Evidence-Dateien zu erzeugen, die fehlende/verlorene/defekte Original-Segmente ersetzen können, mit dem Befehl Datei | Neu. Der Benutzer muss die benötigte Block-Größe und die Anzahl der Blöcke angeben, und den Dateinamen für das gewünschte Segment (die Dateierweiterung muss korrekt sein, also die benötigte Segment-Nummer identifizieren, nicht Nummer 1). Die in die Blöcke geschriebenen Daten können ein wiederkehrendes Text-Muster / Wasserzeichen sein ("FEHLENDES IMAGE-SEGMENT" wenn man X-Ways Forensics mit der deutschsprachigen Benutzeroberfläche betreibt), damit Sie wissen, wenn Sie auf eine Lücke zwischen den verfügbaren Daten schauen, wenn Sie später auf das interpretierte, kombinierte Image schauen. Das ist allerdings optional, aus Gründen der Geschwindigkeit. Ausgenullte Blöcke sind deutlich schneller zu erzeugen.

Die Idee hinter solch einem künstlichen Platzhalter-Segment ist natürlich, dass bei korrekter Größe die Daten in den folgenden Segmenten den korrekten logischen Abstand von den Daten in vorangegangenen Segmenten haben. Der Hash der gesamten Sicherung kann natürlich nicht mehr erfolgreich verifiziert werden, wenn die Original-Daten fehlen, und natürlich sollte diese Funktionalität nur als letzter Ausweg verwendet werden, falls es kein Backup des fehlenden Segmentes gibt oder die Wiederherstellung der Daten fehlschlägt, etc. Die Erzeugung und Verwendung eines solchen Platzhalter-Segments sollte ordentlich dokumentiert werden.

Bei der Interpretation einer .e01-Evidence-Datei, die Platzhalter-Segmente beinhaltet, werden Sie darüber informiert, und die Gesamtzahl der Platzhalter-Blöcke wird in den Eigenschaften des Asservates beim Hinzufügen zum Fall festgehalten.

Falls Sie einen Platzhalter für ein einzelnes fehlendes Segment benötigen, dessen Blockgröße und Blockanzahl Sie nicht kennen, weil die Sicherung ohne eine beschreibende Textdatei mit dieser Information erzeugt wurde, können Sie diese auf mind. zwei Arten ermitteln:

1) Ändern Sie die Dateierweiterung des vorletzten Segmentes zu der des fehlenden Segments, um die Lücke zu schließen. Benennen Sie das letzte Segment in das jetzt fehlende vorletzte um. (Sollte es sich bei dem fehlenden Segment um das vorletzte gehandelt haben, brauchen Sie nur den letzten Schritt; sollte das letzte Segment das fehlende sein, muss gar nichts umbenannt werden.) Fügen Sie dann das Image (das erste Segment) ganz normal zu einem Fall in X-Ways Forensics hinzu. X-Ways Forensics wird Sie auf das falsch benannte Segment im Nachrichtenfenster hinweisen, was ignoriert werden kann. Schauen Sie in den Eigenschaften des Asservates nach der Blockgröße und die erwartete und die tatsächlich referenzierte Block-Anzahl. Subtrahieren Sie die tatsächlich referenzierte von der erwarteten Block-Anzahl. Das Resultat ist die Zahl der fehlenden Blöcke. Benennen Sie die Segmente wieder korrekt um und erzeugen Sie dann das fehlende Platzhalter-Segment mit der korrekten Block-Größe und -Anzahl und der korrekten Erweiterung.

Mit einer Abweichung funktioniert dieser Ansatz auch, wenn mehrere zusammenhängende Segmente fehlen, indem Sie weitere verfügbare Segmente so umbenennen, dass die Lücke im ersten Schritt geschlossen wird, und Sie erzeugen soviele Platzhalter-Segmente, wie benötigt werden, um die Lücke zu schließen. Welches Platzhalter-Segment genau wieviele Blöcke enthält, ist nicht entscheidend, hauptsache, die Gesamtzahl der Ersatzblöcke entspricht genau der Gesamtzahl der fehlenden Blöcke.

oder (einfacher)

2) Sie notieren sich die gemeldet Blockgröße schon beim Hinzufügen des Images mit dem fehlenden Segment zum Fall. Dann erzeugen Sie schnell ein sehr kleines provisorisches Platzhalter-Segment basierend auf dieser Blockgröße und eine beliebigen kleinen Anzahl von Blöcken, z. B. 1000. Dann fügen Sie das Image erneut dem Fall hinzu. Sie werden von der Anwendung darüber informiert, wie viele Blöcke fehlen (diese Zahl nennen wir *x*). Dann erzeugen Sie das endgültige Platzhalter-Segment mit 1000+*x* Blöcken.

Falls mehrere nicht zusammenhängende Segmente fehlen, funktioniert keine dieser Methoden; entsprechende Platzhalter-Segmente können nur erzeugt werden mit den Details aus der beschreibenden Textdatei, wie sie von X-Ways Forensics und X-Ways Imager erzeugt wird..

10.9 Hinweise zum Datenträger-Klonen und -Imaging

Von WinHex/X-Ways Forensics erstellte Datenträger-Klone und -Sicherungen (= Image-Dateien) sind exakte, sektorweise erstellte, forensisch einwandfreie Kopien, mit allem freien Speicherplatz und Schlupfspeicher. Ein Image ist normalerweise einem Klon vorzuziehen, weil darin alle Daten (und Metadaten wie Zeitstempel) vor Veränderung durch das Betriebssystem geschützt sind.

Wenn Sie einen Datenträger zu Backup-Zwecken klonen/sichern, vermeiden Sie, dass auf ihn

währenddessen schreibend zugegriffen wird, durch Windows oder andere Programme, z. B. in dem Sie als Laufwerksbuchstaben geladene Partitionen vorher entladen. Solche Schreiboperationen sind natürlich unvermeidbar, wenn man die Platte klont/sichert, die die aktive Windows-Installation enthält, von der aus Sie WinHex/X-Ways Forensics ausführen. Wenn auf den Quelldatenträger während der Operation geschrieben wird, hat der Klon/die Image-Datei aus Sicht des Betriebssystems evtl. einen inkonsistenten Zustand (was sich z. B. darin äußern kann, dass sich von einer geklonten Platte Windows nicht mehr booten lässt). Aus computerforensischer Sicht jedoch, beim Klonen/Sichern eines lebendigen Systems, ist dies jedoch ein weniger großes Problem, auch wenn das Vermeiden von weiteren Schreibvorgängen natürlich wünschenswert ist, weil Sie in jedem Fall immer noch eine korrekte Momentaufnahme jedes einzelnen Sektors erhalten.

Wenn das Ziel eines Klonvorgangs oder der Wiederherstellung einer Image-Datei (Zurückspielen einer Sicherung) eine Partition ist, die als Laufwerksbuchstabe geladen ist, versucht WinHex, alle von Windows vorgehaltenen internen Puffer von der Zielpartition freizugeben. Wenn Sie dennoch mit dem Windows Explorer nicht den neuen Inhalt auf der Zielpartition sehen, kann ein einfaches Neubooten helfen.

WinHex ändert Partitionsgrößen nicht dynamisch und passt sie nicht an Zieldatenträger an, die eine andere Größe haben als die Quelldatenträger.

10.10 Minimalsicherungen

Nur mit forensischer Lizenz. Ein typisches Feature von X-Ways, das die Spitzenstellung von X-Ways Forensics als das Tool zementiert, das dem Benutzer die größtmögliche Kontrolle überlässt beim Auswählen, Erfassen und Filtern von Daten auf jeder vorstellbaren Ebene: Die Fähigkeit, von Datenträgern forensische Minimalsicherungen zu erzeugen, die nur solche Sektoren enthalten, die für die gewünschten Zwecke erforderlich sind, unter Beibehaltung der Kompatibilität mit anderen Tools. Diese Sektoren können diejenigen sein, die Partitionstabellen enthalten, Dateisystem-Datenstrukturen, deren benachbarte Sektoren, oder Sektoren mit Datei-Inhalten sowie beliebige Sektoren im unpartitionierten Niemandsland einer Festplatte. Eine Minimalsicherung ist üblicherweise nur spärlich mit Daten besetzt, so dass es sinnvoll ist, die Sparse-Datei-Technologie von NTFS dafür einzusetzen. Unbeschriebene Bereiche in einer Minimalsicherung mit Sparse-Eigenschaft verhalten sich beim späteren Lesen so, als ob sie binäre Nullen enthalten. Ohne Sparse-Eigenschaft enthalten Sie auch tatsächlich lauter binäre Nullen.

Sie beginnen eine Minimalsicherung, indem Sie den Menübefehl Datei | Minimalsicherung erstellen aufrufen. Welche Sektoren fortan in das Image aufgenommen werden, wird nun indirekt bestimmt, indem man X-Ways Forensics solche Sektoren vom Quelldatenträger *lesen* lässt, die für bestimmte Zwecke erforderlich sind. Wenn das Ziel-Image im Hintergrund geöffnet ist, öffnen Sie normalerweise als nächstes den physischen Datenträger oder die Partition oder öffnen und interpretieren das Image, das Sie teilweise sichern möchten. Es wird dabei automatisch als Datenquelle für die Sicherung eingestellt. Dadurch werden auch bereits Leseoperationen während der wichtigen Phase des Öffnens oder Interpretierens ausgelöst, wenn Partitionstabellen und Bootsektoren ausgewertet werden müssen, so dass die essentiellen Datenstrukturen, die

Partitionen definieren und Dateisysteme identifizieren, auf jeden Fall schon mal in die Minimalsicherung aufgenommen werden!

Nach dem Öffnen eines partitionierten physischen Datenträgers haben Sie also eine grundlegende Struktur in Ihrer Sicherungsdatei: Partitionstabellen, die auf Partitions-Bootsektoren oder verschachtelte weitere Partitionstabellen zeigen, deren Aufgabe es ist, all die anderen Daten dazwischen (Dateisystemdaten und Benutzerdaten) zu beherbergen. Wenn es Ihr Ziel ist, dass man auch von der Minimalsicherung aus einen Datei-Überblick von einer bestimmten Partition erzeugen kann, d. h. eine Liste aller Dateien und Verzeichnisse erhält, die von dem Dateisystem in der Partition referenziert werden, dann öffnen Sie die betreffende Partition vom Quelldatenträger aus, so dass ein Datei-Überblick erzeugt wird. Erneut werden alle diejenigen Sektoren, die während dieses Vorgangs vom Quelldatenträger gelesen werden, gleichzeitig in die Sicherungsdatei kopiert, und diese enthalten die Dateisystem-Datenstrukturen, z. B. $MFT in NTFS, alle Verzeichnis-Cluster in FAT und die Katalogdatei in HFS+. Das fügt Ihrer Minimalsicherung also schon deutlich mehr und filigranere Verwaltungs- und auch Metadaten hinzu, aber immer noch keine (oder kaum) Benutzerinhalte. Nicht mit dem Dateisystem zusammenhängende/von ihm genutzte Sektoren werden nämlich nicht gelesen und damit auch nicht kopiert. Das bedeutet auch, dass die Möglichkeiten, in der Minimalsicherung ehemals existierenden Dateien zu finden, eingeschränkt sind.

Wenn Sie ein beliebiges Intervall von Sektoren sichern möchten, brauchen Sie nur einen Weg zu finden, um X-Ways Forensics zum Lesen dieser Sektoren zu bewegen. Z. B., um die Sektoren von Nummer 1.000.000 bis 1.000.999 zu kopieren, definieren Sie diese 1.000 Sektoren als ein Block und hashen diesen Block (im Disk-Modus) mit den Menübefehl Extras | Hash berechnen, oder Sie führen eine physische Suche nur in diesem Block aus. Oder, um eine ungewöhnlich große Partitionslücke zwischen Partition 1 und 2 zu sichern, können Sie die virtuelle Datei, diesen Bereich repräsentiert, hashen. Sie können auch manuell zu jedem potenziell relevanten Sektor navigieren, um ihn in die Sicherung aufzunehmen (z. B. Navigation | Sektor aufsuchen) oder einen der Befehle im Navigationsmenü zum Navigieren im Dateisystem verwenden. All das funktioniert, weil das Lesen von Sektoren deren Aufnahme in die Sicherung anstößt.

Wenn Sie allerdings gezielt bestimmte *Dateien* sichern möchten, ist das einfacher, und dafür ist es eine gute Idee, die ständige indirekte Sicherung aller für welchen Zweck auf immer gelesenen Sektoren auszuschalten, so dass z. B. eine Datei, die Sie in der Vorschau betrachten, allein aufgrund der Vorschau-Operation noch nicht gesichert wird, denn bei der Vorschau stellt sich ja evtl. heraus, dass die Datei irrelevant ist. Dazu ändern Sie den Status der im Hintergrund offenen Sicherungsdatei auf "wartend", über den Status-Befehl im Dateimenü. Im Zustand “wartend” erlaubt nur der Befehl "Hinzufügen zu [Name der Sicherungsdatei]" im Kontextmenü des Verzeichnis-Browsers das Sichern ausgewählter Dateien (durch vorübergehendes Aktivieren des Images und Anstoßen von Leseoperationen).

Wenn Sie einige Betriebssystemdateien in die Sicherung aufnehmen möchten, wie etwa Windows-Registry-Hives, erkunden Sie die betreffende Partition vom Stammverzeichnis aus rekursiv, setzen einen Filter auf solche Dateien und rufen den Befehl „Hinzufügen zu“ im Kontextmenü des Verzeichnis-Browsers auf. (Nur verfügbar, wenn nicht zeitgleich auch ein Datei-Container im Hintergrund zum Befüllen geöffnet ist.) Der Ermittler, der nur die resultierende Minimalsicherung hat, wird dann konsequenterweise in der Lage sein, die kopierten Hive-Dateien einzusehen und einen Registry-Bericht über sie anzufertigen, vorausgesetzt, Sie

hatten auch bereits die Dateisystem-Datenstrukturen kopieren lassen, weil diese erforderlich sind um herauszufinden, in *welchen* Sektoren die Inhalte der Dateien gespeichert sind.

Das Dialogfenster zum Ändern des Status der Sicherungsdatei erlaubt es Ihnen auch, diese zu schließen, d. h. das Sichern vorübergehend oder endgültig zu beenden. Dieselbe Sicherungsdatei lässt sich zu einem beliebigen späteren Zeitpunkt weiter vervollständigen, indem man sie mit dem Befehl „Minimalsicherung erstellen“ erneut auswählt, aber dann nicht überschreiben lässt, sondern sie aktualisiert.

Wie Sie sehen, haben Sie die volle Kontrolle darüber, welche Daten es in die Sicherung schaffen. Die Herangehensweise setzt nur voraus, dass Sie ein gewisses Verständnis davon mitbringen, was für Daten Sie wollen/brauchen und wo diese zu physisch zu finden sind, sofern diese Daten nicht einfach nur gewöhnliche auswählbare Dateien sind. Die Sektoren können in jeder beliebigen Reihenfolge adressiert werden. Mehrfaches Lesen derselben Sektoren ändert nichts in der Sicherungsdatei und hat keine negative Auswirkung, außer dass es unnötige doppelte Zeilen in der optionalen Protokolldatei zur Folge haben kann, die X-Ways Forensics erzeugen kann. Solch eine .log-Datei wird im selben Verzeichnis wie die Sicherungsdatei erzeugt. Sie listet alle kopierten Sektorintervalle auf, optional jeweils mit einem dazugehörigen Hash-Wert, was es ermöglicht, die Daten in bestimmten Bereichen manuell zu verifizieren, sollten diesbezüglich Zweifel entstehen. Wenn Sie den "Hinzufügen zu"-Befehl zum Sichern von Dateien in eine Minimalsicherung verwenden, wird auch der Name einer solchen Datei in das Protokoll aufgenommen, gefolgt von den Sektorintervallen, die der Datei zugeordnet sind (mehr als eins, wenn die Datei fragmentiert ist oder X-Ways Forensics die Sektoren einfach in mehreren Stücken kopiert).

Es bietet sich u. U. an, die Minimalsicherung vom Roh-Format in ein komprimiertes und/oder verschlüsseltes .e01-Evidence-File zu konvertieren oder sie zu hashen, oder sie mit WinRAR oder 7-Zip etc. vor der Weitergabe an andere Benutzer zu komprimieren. Die Kompressionsdate wird ungewöhnlich hoch sein, wenn die Minimalsicherung nur spärlich mit Daten besetzt ist, und die Lesegeschwindigkeit extrem hoch, weil undefinierte/nicht allozierte Bereiche gar nicht von der Platte gelesen werden müssen. Für Ihren eigenen Bedarf können Sie die Sicherungsdatei einfach so lassen wie sie ist, weil sie in ihrem Grundzustand nicht so viel Plattenplatz benötigt wie die nominelle Dateigröße befürchten lässt, dank der Sparse-Speicherung von NTFS. Wenn Sie eine Minimalsicherung im Roh-Format kopieren möchten, kopieren Sie sie auf jeden Fall als Sparse-Datei (kann in X-Ways Forensics mit dem Befehl Extras | Datei-Tools | Sparse kopieren erledigt werden), so dass die Kopie auch eine Sparse-Datei wird und nur so viel Plattenplatz wie die Originaldatei verbraucht. Ein konventioneller Kopierbefehl würde auch die riesigen unbenutzten und nicht allozierten Bereiche innerhalb der Sparse-Datei als binäre Nullen kopieren.

Zum Überprüfen der Unverändertheit der in die Minimalsicherung übertragenen Daten kann für diese als Ganzes ein Hash-Wert berechnet werden, wie bei einem normalen Image. Alternativ und viel schneller ist die Verwendung des Befehls "Minimalsicherung überprüfen", die die laut .log-Datei übertragenen Sektorbereiche erneut hasht (aus dem Image lesend) und mit den Hash-Werten in der .log-Datei vergleicht. Dann überprüft die Funktion, ob die .log-Datei ihrerseits unverändert ist, hasht diese dazu und vergleicht den sich daraus ergebenden, mächtigen, allumfassenden Master-Hash-Wert mit dem in der .log.log-Datei genannten Hash-Wert, sofern diese optionale Datei erzeugt wurde. Es könnte auch wünschenswert sein zu verifizieren, dass

alle ungenutzten Bereiche in einer Minimalsicherung weiterhin nicht alloziert oder zumindest mit Nullen gefüllt sind. Dies erledigt die Funktion nicht.

Optionen:

- A skeleton image should be created as an NTFS sparse file unless you intend to copy more than half of the sectors perhaps (just a very rough rule of thumb).
- If you don't have X-Ways Forensics set the nominal (logical) image file size to the full size of the source disk, then when interpreting the skeleton image and reading from it, a smaller "capacity" will be reported and you may get sector read errors. Still worth thinking about it for example if you wish to capture merely the first 1 MB of a 1 TB hard disk. Saves a lot of time if you wish to convert the skeleton image to an .e01 evidence file or want to hash it in its entirety.
- Skipping already zeroed out source sectors (sectors of the source disk that only contain binary zeroes) will treat such sectors exactly like sectors that were not acquired. This makes the resulting skeleton image smaller ("more sparse"), but it prevent you from showing with just the skeleton image that these sectors only contained zeroes on the source disk. They are indistinguishable from sectors that were not acquired.
- "Include directory data structures of the file system" has an effect when you apply the "Add to" command of the directory browser context menu to selected directories. If this option is active, you will also copy the data structures of the file system for these directories, if there are any, e.g. INDX buffers in NTFS, subdirectory clusters in FAT, etc. (nothing in HFS+), otherwise only the contents of the files *in* these directories.
- "Vermerke" erzeugt im Datei-Überblick der Quelle einen Vermerk für jede Datei, die Sie gezielt der Minimalsicherung hinzugefügt haben, so dass Sie leicht sehen können, welche Dateien bereits kopiert wurden, sollte es diesbezüglich Zweifel geben.
- If "Create log file" is at least half checked, a .log file will be created that references all copied sector ranges. X-Ways Forensics makes an effort to prevent acquiring duplicate sectors, e.g. when copying the exact same sector range a second time or when copying overlapping sector ranges, so that can explain why you may not get more lines in the .log file when copying the same sectors again. If the checkbox is fully checked, a .log.log file about the .log file will be created with a hash of the .log file.
- All copied sector ranges can be optionally hashed, and the hash values can be written to the .log file and can be verified after closing the skeleton image.

Vorteile von Minimalsicherungen:

- Teilweises Image, spart Plattenplatz.
- Schnell zu erzeugen, insbes. im Fall einer über eine langsame Verbindung mit F-Response gesicherte Festplatte eines Rechners im Netz.
- Transportiert/enthüllt nur speziell adressierte Daten, schließt Daten ohne Bezug aus, wie u. U. erfordert von Gesetzen, gesundem Menschenverstand, Zeitdruck oder Kundenwunsch.
- Ideal geeignet für technische Datenstrukturen (Partitionstabellen und Dateisysteme) und Dateien im Dateisystem gleichermaßen.
- Möglichkeit, alle entscheidenden Dateisystem-Daten ohne Wissen über Dateisysteme zu sichern und insbes. ohne zu wissen, in welchen Sektoren die Dateisystem-Datenstrukturen gespeichert sind.
- Das Ergebnis lässt sich genau wie ein konventionelles Roh-Image einer Platte einlesen,

für alle beabsichtigten Zwecke, sofern adäquat vorbereitet, mit Original-Offsets und beibehaltenen relativen Entfernungen zwischen Datenstrukturen (anders als in einem Datei-Container).
- Das Datei-Format ist universell, und alle forensischen Tools, die Roh-Images unterstützen, haben die Chance, die Daten zu verstehen, es sei denn, sie brauchen mehr als die eingebundenen Daten oder verstehen schon die Partitionierungsmethode oder das Dateisystem auf dem Originaldatenträger nicht.

Vorbehalte:
- Eine auf dem Bildschirm dargestellte Suchtrefferliste mit Kontextvorschau um die Suchtreffer herum verursacht unzählige Leseoperationen, so dass Sie den Status einer im Hintergrund geöffneten Sicherungsdatei in bestimmten Situationen besser auf „wartend“ ändern
- Um zu vermeiden, dass die Startsektoren von Dateien und Verzeichnissen, die Sie im Verzeichnis-Browser im Modus Partition/Volume lediglich anklicken, in die Sicherungsdatei aufgenommen werden (weil ein solcher Klick automatisch zum jeweiligen ersten Sektor springt), navigieren Sie im Verzeichnis-Browser im Modus Legende oder ändern den Status der Sicherungsdatei auf „wartend“.
- Das Lesen von Daten aus den meisten *extrahierten* Dateien wie E-Mails, Datei-Anhänge von E-Mails, Dateien in Zip-Archiven, Standbilder von Videos, in MS-Excel-Tabellen eingebettete Bilder usw. stößt keine Leseoperationen auf der Datenträger-Ebene an, so dass sie nicht gesicht werden können. Minimalsicherungen eignen sich nur für Dateien auf der Dateisystemebene, nicht auf anderen Ebenen, die man im Datei-Überblick sieht. Verwenden Sie Datei-Container für solche Zwecke.
- Beachten Sie, dass einem arglosen Ermittler eine Minimalsicherung wie ein herkömmliches vollständiges Image erscheinen kann. Solche Ermittler müssen auf die unvollständige, nur dünn mit Daten besetzte Natur der Sicherung aufmerksam gemacht werden. Im Gegensatz zu Datei-Containern werden Dateien, deren Inhalt nicht im Image enthalten ist, im Datei-Überblick einer Minimalsicherung nicht besonders gekennzeichnet. X-Ways Forensics v17.1 und neuer informieren den Benutzer aber über die Natur der Sicherung, wenn sie einem Fall hinzugefügt wird, wenn sie als Minimalsicherung erkannt wird.

Ein Vergleich von Datei-Containern und Minimalsicherungen findet sich auf der Web-Site.

Punktuelle Sicherung

Eine Variante der Minimalsicherung wird punktuelle Sicherung genannt. Klicken Sie auf den gleichnamigen Schalter im Dateiauswahldialog des Menübefehls „Datei | Minimalsicherung erstellen“, um eine punktuelle Sicherung anzustoßen. Alle Sektoren, die von X-Ways Forensics gelesen werden, egal von welchem Datenträger oder welchen Image, während die punktuelle Sicherung aktiv ist, werden in separate Dateien geschrieben, die nach der Sektornummer benannt sind und die Erweiterung .sector erhalten, in einem Unterverzeichnis des Standardverzeichnisses für Sicherungsdateien, das nach dem jeweiligen Datenträger bzw. Image benannt wird. Zusammenhängend gelesene Sektoren landen in einer einzigen Datei.

Die punktuelle Sicherung kann beendet werden über den Menübefehl Datei | Punktuelle Sicherung. Punktuelle Sicherungen sind nur in speziellen Situationen nützlich, z. B. zu Debug-Zwecken, wenn man nur wenige Sektoren gezielt sichern möchte, die am besten von der Software automatisch ermittelt werden (z. B. Datenstrukturen, die beim Öffnen einer bestimmten Datei benötigt werden). Im Vergleich zu einer Minimalsicherung kann eine punktuelle Sicherung vorteilhaft sein, weil keine Image-Datei von derseben Größe wie der Quelldatenträger erzeugt wird. (Auch wenn die Größe nur eine nominelle Größe und die Image-Datei sparse ist, hilft doch die Sparse-Eigenschaft nicht, wenn die Datei über das Internet verschickt oder in ein Dateisystem kopiert werden soll, das die Sparse-Eigenschaft der Datei nicht beibehält.)

Dank kompatibler Namen, können punktuelle Sicherungen (die .sector-Dateien) bei Bedarf direkt für die Sektor-Überlagerung eingesetzt werden. Sie können auch bequem und aufgrund ihrer typischerweise geringen Größe sehr, sehr schnell auf andere Datenträger zurückkopiert werden, alle solche Dateien im selben Verzeichnis auf einmal, natürlich unter Berücksichtigung der Startsektornummern in den Dateinamen, durch Klick auf den Schalter "Punktuelle Sicherung" im Dialogfenster zu Datei | Sicherung wiederherstellen.

10.11 Sicherungs-Manager

In der wahlweise nach dem Erstellungszeitpunkt, dem Dateinamen oder dem Pfad geordneten Liste können Sie WinHex-Backups auswählen, die Sie wiederherstellen möchten. Ein neues Editierfenster zeigt daraufhin den Datei- bzw. Sektorinhalt vom Zeitpunkt der Sicherung an.

Sie können die Sicherung wiederstellen
- in eine Temporärdatei, so dass sie erst noch gespeichert werden muss,
- sofort direkt auf den Datenträger oder
- in eine neue Datei.

Im Fall von Datenträgersektoren können Sie auch das Ziel der Wiederherstellung (Datenträger und Sektornummer) ändern. Sie können außerdem optional nur einen Teil der Sektoren aus der Sicherung extrahieren (Sektoren am Anfang einer *komprimierten* Sicherung können allerdings nicht übersprungen werden). Wenn die Sicherung mit einer Prüfsumme und/oder einem Digest versehen war, werden die Daten erst auf Authentizität überprüft, bevor sie direkt auf den Datenträger geschrieben werden.

Mit Hilfe des Sicherungs-Managers können Sie außerdem Sicherungen löschen, die Sie nicht mehr benötigen. Die automatisch erzeugten Sicherungsdateien für die „Rückgängig“-Funktion werden von WinHex standardmäßig selbständig gelöscht (s. Rückgängig-Optionen).

Die Sicherungsdateien, die vom Sicherungs-Manager verwaltet werden, heißen „???.whx“ und befinden sich in dem unter Allgemeine Optionen gewählten Ordner. An die Stelle von ??? tritt eine aus drei Ziffern bestehende eindeutige Identifikationsnummer, die im Sicherungs-Manager in der letzten Spalte angegeben ist.

10.12 Wiederherstellen/Kopieren-Befehl

Ermöglicht es, die ausgewählten Dateien von ihrer aktuellen Position, z. B. aus einer interpretierten Image-Datei oder einer lokalen Platte heraus, an einen beliebigen Ort zu kopieren, der für einen Standard-Windows-Dateidialog erreichbar ist. Dies kann sowohl auf existierende als auch auf gelöschte Dateien angewandt werden. Ungültige Zeichen in Dateinamen werden herausgefiltert.

If necessary, you can manually enter the output path by clicking the "..." button in the same line where the path is displayed. Useful if you wish to specify a network location that Windows does not list by default in the dialog window for the path selection. If you enter a non-existing output path, you will be notified and may proceed anyway, in which case that path will be created automatically if possible. The unlabeled check box next to the "..." button can be used to indicate that you would like to get a Windows Explorer window opened for the output path once copying has completed to check out the result.

Mit einer forensischen Lizenz stehen vielfältige Zusatzfunktionen zur Verfügung:

- Optional können Dateien im Ausgabe-Ordner mit ihrem vollständigen Originalpfad erstellt werden, oder auch einem Teilpfad, wenn die Option halb gewählt wird. Der Asservatname wird ebenfalls als Pfad wiederhergestellt, wenn entweder aus dem Asservatüberblick heraus kopiert wird oder wenn Sie sich generell nicht den jeweiligen Asservat-Ordner unterhalb des Falls als Standardausgabeverzeichnis vorschlagen lassen (s. Falleigenschaften). Ein Teilpfad ist nur der Teil des Pfades, der unterhalb des aktuell erkundeten Verzeichnisses liegt bzw. beim Kopieren aus einem rekursiv erkundeten Asservat-Überblicksfenster nur der Name des Asservats, nicht der Pfad innerhalb des Asservats.
- Überlange Pfade werden unterstützt (mehr als 260, bis zu 510 Zeichen, für den Ausgabepfad + optional den Originalpfad + den Originaldateinamen). Sie können Pfadlängen immer noch freiwillig auf die herkömmliche Länge von 260 Zeichen oder weniger begrenzen, wenn Sie solche Datei ohnehin nicht weiter verarbeiten können (z. B. einsehen, kopieren, löschen), denn herkömmliche Programm wie der Windows Explorer von Windows 7 erlauben das nicht. Wenn der Ausgabepfad einer ausgewählten Datei das Limit übersteigt, wird der Name der Datei gekürzt, bis das Limit eingehalten wird. Ist es auf diese Weise nicht möglich, das Limit einzuhalten, wird die Datei nicht kopiert, sondern mit einem Vermerk versehen, so dass Sie später bequem alle ausgelassenen Dateien erneut auswählen und separate ohne Pfad kopieren können, wenn Sie möchten.
- It is possible to create a 2nd copy of all selected files in a separate directory. Useful if you need to provide two parties with copies of relevant files and wish to save time. The logging option is for the 1st copy only, though.
- Eine Option steht zur Verfügung, um Dateien nach dem Inhalt einer beliebigen Spalte des Verzeichnis-Browser zu benennen, wie etwa eindeutige ID, Hashwert, ID, Kommentar, Offset im Dateisystem usw. usf. Solche Metadaten können auch an den ursprünglichen Namen angehängt oder ihm vorangestellt werden, was z. B. nützlich sein kann bei alternativem Namen, Existenzstatus, Vermerke, Zeitstempel, Autor, Absender, Beschreibung, Attribute, Analyseergebnis, Hash-Set, ... Wenn der Zellinhalt aus mehreren Zeilen besteht (z. B. bei den Spalten Kommentar oder Metadaten), wird nur die erste Zeile verwendet. Umgekehrte Schrägstriche in den Pfad-Spalten werden automatisch durch Unterstriche

ersetzt. Das erlaubt es, eine Datei namen ihrem ursprünglichen vollständigen Pfad zu benennen.

- Dateien, die nicht kopiert werden konnten (wenn z. B. der Pfad zu lang ist), werden mit einem Vermerk versehen.
- Die Original-Zeitstempel der Dateien (Erstellung, Änderung, letzter Zugriff, sofern verfügbar) werden wiederhergestellt.
- Der vermutete korrekte Dateityp von Dateien, deren Typ neu erkannt wurde, kann optional an den Ausgabe-Dateinamen angehängt werden, wenn er von der Dateiendung laut Dateiname abweicht oder die Datei gar keine Dateinamenserweiterung aufweist. Gleichzeitig hat diese Einstellung auch Auswirkungen auf das Herauskopieren zum Einsehen mit dem verknüpften Programm.
- Sofern Sie gleichnamige Dateien, die im Ausgabeverzeichnis existieren, nicht explizit überschreiben oder überspringen lassen, werden doppelt vorkommende Dateinamen durch Einfügen einer laufenden Nummer vor der Dateinamenserweiterung eindeutig gemacht. Wenn Sie also alle Dateien in dasselbe Verzeichnis kopieren, auch Dateien von verschiedenen Asservaten, erhalten alle herauskopierten Dateien eindeutige Namen (und die copylog-Datei erlaubt es später herauszufinden, welche Datei ursprünglich wie hieß und woher stammte und welche Metadaten hatte).
- Die Dateisystem-Zeitstempel einer kopierten Originaldatei (Erstellung, Änderung, letzter Zugriff, sofern verfügbar) werden auf die erzeugte Kopie übertragen, wenn das Kontrollkästchen dafür zumindest halb gewählt ist. Außerdem fungiert der interne Zeitstempel "Erzeugung des Inhalts", sofern verfügbar, bei Bedarf als Ersatz für einen fehlenden Erstellungszeitstempel aus dem Dateisystem. Wenn das Kästchen ganz gewählt ist, unternimmt X-Ways Forensics besondere Anstrengungen, um Erstellung, Änderung und letzten Zugriff auf einige Original-Zeitstempel zu setzen, um zu vermeiden, dass diese drei Standard-Zeitstempel auf den Zeitpunkt verweisen, an dem der Wiederherstellen/Kopieren-Befehl angewandt wurde. Z. B. haben extrahierte E-Mails oder Datei-Anhänge oder Dateien in Archiven oder aus Sektoren ausgegliederte Dateien u. U. nicht alle diese Zeitstempel oder gar keine davon. X-Ways Forensics kann dann behelfsweise Zeitstempel von Datensatz-Änderungen, alternative Erzeugungszeitstempel, Erzeugung des Inhalts und Änderungszeitstempel als Ersatz für Erzeugung, Änderung und letzten Zugriff heranziehen. Eine weiteres Kontrollkästchen lässt wiederhergestellte/kopierte Dateien notfalls Zeitstempel von Elterndateien oder übergeordneten Verzeichnissen erben. Das Kästchen hat ebenfalls drei Zustände. Wenn es halb gewählt wird, werden nur Zeitstempel von Elterndateien geerbt (offensichtlich sinnvoll bei E-Mails, die mit Datei-Anhängen daherkommen, oder Bilddateien, die Miniaturansichten enthalten). Wenn es ganz gewählt ist, werden Zeitstempel auch von übergeordneten Verzeichnissen geerbt, sowie deren Oberverzeichnisse usw. usf. Ein extremes Beispiel ist eine aus Sektoren ausgegliederte Dateien ohne jegliche Zeitstempel. Die übergeordneten Verzeichnisse dieser Dateien sind virtuelle Verzeichnisse und haben daher auch keine Original-Zeitstempel. In dem Fall würde der Erzeugungszeitstempel des Stammverzeichnisses geerbt, sofern verfügbar (nicht bei FAT-Dateisystemen). Der Erzeugungszeitstempel eines übergeordneten Verzeichnisses könnte als hilfreich erachtet werden, weil er ein unteres chronologisches Limit für den unbekannten Erzeugungszeitpunkt der Datei darstellt. Der Erzeugungszeitstempel einer Elterndatei kann als oberes Limit für den den unbekannten Erzeugungszeitpunkt einer enthaltenen Datei angesehen werden, wenn die Elterndatei ein Datei-Archiv oder eine E-Mail ist. Wenn die enthaltene Datei eine Miniaturansicht in einem JPEG- oder HEIC-Bild ist, sollte der Erzeugungszeitstempel der

Elterndatei genau richtig für das Unterobjekt sein.

- Wenn die spezielle Protokollierung dieses Befehls aktiv ist (konfigurierbar in den Falleigenschaften), wird der Kopier-/Wiederherstellungsvorgang in der Datei „copylog.html“ oder „copylog.txt“ dokumentiert. Praktisch alle Metadaten der kopierten Dateien und die Ausgabedateinamen (optional incl. Zielpfad) können festgehalten werden. Die Datei kann entweder im Unterverzeichnis _log des Falls erzeugt werden oder im ausgewählten Zielverzeichnis des Wiederherstellen/Kopieren-Vorgangs. S. a. Falleigenschaften.
- Schlupfspeicher kann optional ebenfalls mit ausgegeben werden, entweder als Teil der Datei oder separat, oder es kann sogar *nur* der Schlupf kopiert werden.
- Sie können entscheiden, ob Unterobjekte gewählter Dateien mit kopiert werden sollen oder nicht.
- Sie können entscheiden, ob herausgefilterte Dateien kopiert werden sollen
- Wenn Sie X-Ways Forensics den Originalpfad für kopierte Dateien reproduzieren lassen, muss auch die Position von solchen Dateien in der Hierarchie korrekt wiedergespiegelt werden, die Unterobjekte anderer Dateien sind. Und dies muss mit Hilfe eines Verzeichnisses geschehen, da normale Dateisysteme das Konzept, dass Dateien weitere Dateien enthalten können, wie es in einem Datei-Überblick in X-Ways Forensics gang und gäbe ist, nicht unterstützen. Allerdings gibt es dann u. U. einen Namenskonflikt wenn ein künstliches Verzeichnis erzeugt würde mit dem gleichen Namen wie die Elterndatei, weil diese Elterndatei auch zum Kopieren ausgewählt sein kann und natürlich im selben Verzeichnis erstellt würde wie das vorgenannte künstliche Verzeichnis, das für die korrekte hierarchische Einordnung des Unterobjekts benötigt wird. Daher muss das künstliche Verzeichnis etwas anders benannt werden. Der Name kann nach einer benutzerdefinierten Anzahl von Zeichen abgeschnitten werden, und das ist besonders für E-Mails nützlich, die nach ihrer Betreffzeile benannt werden und natürlich Datei-Anhänge als Unterobjekte enthalten können, um überlange Pfade zu vermeiden. Auch kann entweder ein benutzerdefiniertes Suffix von 1 Zeichen Länge angehängt werden (und standardmäßig ist das ein spezielles Unicode-Zeichen, das in vollständigen Unicode-Schriftarten unsichtbar ist, so dass das Verzeichnis den gleichen Namen wie die entsprechende Elterndatei zu haben scheint) oder eine Beschreibung wie " Unterobjekte" (aber das verlängert leider die Gesamtpfadlänge, die ja allzuoft normale Grenzen überschreitet). Wenn das Eingabefeld für das Suffix-Zeichen leer zu sein scheint, dann liegt das wahrscheinlich daran, dass es das bereits erwähnte unsichtbare Unicode-Zeichen enthält. Dieses Zeichen hat eine Breite von 0. Um es durch ein anderes Zeichen zu ersetzen, entfernen Sie es zunächst, durch Klicken in das Eingabefeld und Drücken der Rücksetz-Taste auf der Tastatur.
- Dateien können in separaten Ausgabeverzeichnissen gruppiert/klassifiziert werden, basierend auf bis zu zwei ausgewählten Verzeichnis-Browser-Spalten, darunter Existenzzustand (um leicht zwischen ursprüngliche existierenden und gelöschten Dateien unterscheiden zu können), Beschreibung, Asservat, Dateityp, Dateityp-Beschreibung, Dateityp-Kategorie, Absender, Besitzer, Hash-Set, Hash-Kategorie, Vermerke, Suchbegriffe. Es ist auch möglich, den Namen des Gruppierungsverzeichnisses auf eine bestimmte Anzahl von Zeichen zu beschränken. Das kann sehr nützlich sein, wenn Sie Dateien z. B. nach Jahr gruppieren möchten (= die ersten vier Zeichen in Erzeugungs- oder Änderungszeitstempeln, geeignete Notationseinstellungen vorausgesetzt) oder einfach um eine riesig große Zahl von auszugebenden Dateien in einigermaßen gleich große Unterverzeichnisse aufzuteilen (mit den ersten 1-2 Zeichen des Hash-Werts, um 16 oder 256 solche Unterverzeichnisse zu erzeugen), basierend auf dem Gesetz der großen Zahlen, oder einfach um das Risiko von überlangen

Gesamtpfaden zu reduzieren.

- Files of certain supported types can be converted to PDF format, to share with computer users who otherwise would not have suitable applications to view the files. You can define the file types that do not need to be converted, e.g. those that can easily be displayed by a web browser or with Windows tools. If no conversion is possible, the original file is copied unconverted. There is also an pption to turn all selected files into a single PDF document. This includes even file types that would usually not be converted to PDF individually.
- Reiner Text kann aus Dateien bestimmter unterstützter Typen extrahiert und in Form von Textdateien ausgegeben werden. Das ist dieselbe Textdarstellung, die Sie bekommen, wenn Sie vom normalen Vorschaumodus in den Text-Vorschaumodus wechseln, und derselbe Text, den eine logische Suche zusätzlich durchsuchen würde bei einer Datei, die Sie "decodieren" lassen. Dateien, die nicht für eine Textextraktion geeignet sind (z. B. Bilddateien) oder aus denen aus welchen sonstigen Gründen auch immer kein Text extrahiert werden kann, werden entweder normal kopiert (mit dem Originalinhalt), wenn das zugehörige Kontrollkästchen halb gewählt ist, oder ausgelassen, wenn es voll gewählt ist (so dass die tatsächliche Ausgabe 100%ig aus Text besteht).
- Wenn sowohl ein Dateianhang als auch die zugehörige E-Mail (sein Elter) zum Kopieren ausgewählt sind und nicht von Filtern ausgeschlossen werden, kann der Anhang optional in die resultierende .eml-Datei in Form von Base64-Code eingebettet statt separat kopiert werden. Das macht es bequemer, die E-Mail incl. Anhänge einzusehen. .eml-Dateien können eingesehen werden z. B. in Outlook Express, Windows Mail, Windows Live Mail oder Thunderbird (alle kostenlos). Wenn bestimmte Dateianhänge nicht eingebettet werden können, erhalten Sie darüber eine Meldung im Nachrichtenfenster, und in einem solchen Fall werden sie separat kopiert, als ob die Option zum Einbetten nicht aktiv wäre.
- Alternative Datenströme (ADS) von NTFS können optional als ADS ausgegeben werden. Standardmäßig werden sie in Form gewöhnlicher Dateien wiederhergestellt, damit sich leichter zugreifbar sind.
- X-Ways Forensics can try to encode zeroed out areas in a file as sparse when writing the data. This will have an effect only if the zeroed areas are somewhat aligned and sufficiently large, and of course only when writing to an NTFS or ReFS volume, not FAT. Works no matter whether the source file is defined as sparse or not. This option will reduce the data transfer rate and is only recommendable if you know that the data that you are copying is probably suitable.
- You may use the alternative names of files, if available, for the output. The alternative name, if one exists, can be seen in the directory browser in square brackets. For example, when parsing iPhone backups, X-Ways Forensics automatically changes artificial generic filenames back to what they were originally. Or, when parsing $I files from the Windows recycle bin, the corresponding $R files are given their original names. If for some reason you prefer the untranslated filenames when copying such files off the image to your own hard disk, for example because you wish to process these files with some external tool that expects the artificial filenames, then you can now use this option.

Wenn der Wiederherstellen/Kopieren-Befehl in einer Suchtrefferliste eingesetzt wird, werden Verzeichnisse, die Suchtreffer enthalten, im Ausgabeordner als Dateien wiederhergestellt, da es wahrscheinlich ist, dass der Benutzer die Originaldaten kopieren möchte, die den eigentlichen Suchtreffer enthalten Unterobjekte werden beim Kopieren aus Suchtrefferliste nie mit ihren Elternobjekten mit kopiert.

10.13 Duplikaterkennung

Wenn Sie doppelte Dateien nur einmal begutachten möchten und Metadaten des Dateisystems wie Zeitstempel und Löschzustand zunächst von sekundärer Bedeutung sind, können Sie den Befehl "Duplikate in Liste finden" im Kontextmenü des Verzeichnis-Browsers verwenden, um Duplikate unter den aktuell aufgelisteten (aufgelisteten, nicht ausgewählten!) Dateien zu erkennen, basierend auf Hash-Werten (sofern berechnet) oder anderen Kriterien. Auf Wunsch können können Duplikate im Datei-Überblick sogleich ausgeblendet werden. Dabei wird nur jeweils eine Datei in jeder Gruppe von identischen Dateien wird nicht ausgeblendet. Jede Gruppe von identischen Dateien kann optional mit einem eindeutigen Vermerk versehen werden, um diese Gruppe per Filter leicht auf einmal betrachten zu können, selbst dann, wenn sie sich über mehrere Asservate verteilen.

Im Zweifelsfall behält diese Funktion beim Ausblenden existierende (nicht gelöschte) Dateien bei, und gibt unter gelöschten Dateien denjenigen den Vorzug, die über Dateisystem-Datenstrukturen gefunden wurden und nicht per Signatursuche. Und im Zweifelsfall wird diejenige Kopie einer Datei beibehalten, deren Besitzer bekannt ist. Optionale Sonderregeln: Identische E-Mails mit unterschiedlichen Dateianhängen (Unterobjekten) werden als Duplikate gekennzeichnet, aber nicht ausgeblendet. Identische Anhänge (Unterobjekte) werden als Duplikate gekennzeichnet, aber nur dann indirekt ausgeblendet, wenn sie Teil von identischen E-Mails sind und diese auch ausgeblendet werden. Dies erleichtert die Untersuchung und vermeidet die Situation, dass das übergeordnete Objekt (die E-Mail) einer E-Mail+Anhang-Familie und das Kind (der Dateianhang) einer anderen Familie ausgeblendet wird.

Wenn Sie später relevante Dateien finden, für die es Duplikate gab, und Sie sich nun auch für diese Duplikate interessieren (z. B. deren Dateinamen, Pfade oder Zeitstempel), können Sie ein Hash-Set der gefundenen relevanten Datei erzeugen, um alle Duplikate bequem und automatisch zu identifizieren, indem Sie die Hash-Werte aller Dateien gegen dieses spezielle Hash-Set abgleichen und dann den Hash-Set-Filter verwenden. Oder Sie verwenden den Filter der Hash-Spalte direkt.

Pairs of duplicates in the same volume snapshot can be optionally linked as so-called related items, so that it's easy to navigate from one such file to at least one duplicate. However, that does not work across evidence object boundaries. Marking the files as duplicates in the Description column is optional.

The most common and reliable criterion to identify files as duplicate is a regular hash value. Allerdings kann die Berechnung von Hash-Werten in großen Datensätzen sehr zeitraubend sein, so dass jede vernünftige Deduplizierungsoption, die ohne Hash-Werte auskommt, hoffentlich von einigen Benutzern geschätzt wird. Alternative criteria are available. You could compare files simply based on identical names. This is a case-insensitive comparison and of course should be used only if you know what you are doing, as it does not compare the file contents at all. Could be useful for example if you wish to get rid of multiple copies of the same files found in backups if you do not need to keep different versions of these files. If prior to the comparison for example you sort by last modification date in descending order, this will ensure that the newest version of the file will be kept and all older versions will be excluded. Files with identical names are not marked as duplicates in the Attr. column. The number of characters to compare in filenames is

user-definable.

Another useful criterion is the modification timestamp. The timestamps are compared as strings, and the more characters are checked, the more precise you require timestamps to be identical. With your notation settings in mind, you could choose to compare only the date, or date + times with precision of minutes, or seconds, milliseconds or anything in between, by defining the number of characters.Das Dialogfenster illustriert die aktuellen Notationseinstellungen für Zeitstempel und die von Ihnen angegebene Anzahl an zu vergleichenden Zeichen anhand eines Beispiels, so dass Sie direkt sehen, mit welcher Genauigkeit Sie ggf. fast gleiche Zeitstempel als gleichwertig ansehen möchten. Sowohl mit der Anzahl der zu vergleichenden Zeichen als auch mit der Anzahl der Nachkommastellen in den Notationseinstellungen beeinflussen Sie die Duplikatserkennung, sei es bewusst oder unwissentlich. Eine Beschränkung der Genauigkeit kann wünschenswert sein, z. B. um Kopien von Dateien in NTFS und FAT auch dann als identisch zu werten, wenn sich die Änderungszeitstempel um 1 Sekunde unterscheiden, weil das aufgrund der Rundung von Zeitstempeln in FAT zu erwarten ist. Auf die Notationseinstellungen können Sie nun direkt vom Dialogfenster für die Deduplikation aus zugreifen.

Sie haben nun die Möglichkeit, ein oder zwei zusätzliche Kriterien für die Identifikation von Duplikaten heranzuziehen: Änderungszeitstempel (in voller verfügbarer Genauigkeit) und Größe. Diese beiden kombiniert mit dem Dateinamen als Hauptkriterium sind ziemlich verlässlich für nicht 100%ig exakten forensischen Gebrauch. Eine weitere Möglichkeit ist die Verwendung des Strukturtyps für die Deduplikation, für unterstützte Dateitypen. Diese identifiziert eigentlich Gruppen von ähnlichen oder verwandten Dateien. Kombiniert mit Änderungszeitstempel und Größe ist der Strukturtyp ziemlich verlässlich für die Ermittlung von Dubletten.

If you have access to PhotoDNA in X-Ways Forensics, you may also identify and exclude duplicate pictures using PhotoDNA. All duplicates can be marked as "duplicates found" in the Description column, and all except one will be excluded. When in doubt, deleted files or pictures with a poor resolution will be excluded and existing files and pictures with a higher resolution will be kept. Please note that the hash value comparison is a potentially time-consuming operation if many pictures are listed in the directory browser, much more so than for conventional hash values. However, you can abort the comparison at any time. This operation requires that PhotoDNA hash values have been computed beforehand, using Specialist | Refine Volume Snapshot | Picture processing | Compute PhotoDNA hash values. It is useful for example for law enforcement agencies that wish create PhotoDNA hash sets of unique pictures only and for that purpose maintain a lawful collection of incriminating pictures without duplicates. The strictness of the picture comparison is the same as set in the Specialist | Refine Volume Snapshot | Picture processing dialog window for matching against the PhotoDNA hash database.

10.14 Ersatzmuster

Wenn das Programm Probleme hat, Daten zu lesen zur Darstellung im Modus Disk/Partition/Volume oder im Modus Datei/Vorschau oder für Suchen, fürs Hashen, zum Sichern usw. usf., stellt sich die Frage, welche Daten stattdessen dem Anfrager präsentiert werden. Für Lesefehler auf unterschiedlichen Ebenen gibt es unterschiedliche Ersatztextfragmente für den Notfall, von denen viele übrigens sprachabhängig sind. Diese

Textfragmented werden wiederholt in den Lesepuffer kopiert, bis dieser voll ist, so dass ein wiederkehrendes Muster entsteht, das bei Anzeige auf dem Bildschirm gleich ins Auge springt und den Benutzer auf das Problem aufmerksam macht.

1) "DATEI NICHT LESBAR!" for example means that at least certain portions/segments/extents of a file cannot read because the file system does not define where to find them or because it does but that definition is invalid or because it does but X-Ways Forensics does not understand it.

Example: The file system defines that a file consists of 6 clusters starting at cluster 1000 in the volume and 4 clusters starting at cluster 55,555 in the volume.

One possible reason for "DATEI NICHT LESBAR!" in this example would be that the volume consists of 40,000 clusters only. The first 6 clusters of the file can be read, but the last 4 clusters of the file cannot be read, simply because there is no cluster 55,555 that could be read. If this concerns an existing file, it is some kind of file system corruption or volume inconsistency. Could happen if something went wrong when a volume was shrunk, or if it's a spanned volume covering multiple disks of which only the first segment is available treated as if it was the entire volume. Another possible reason for "DATEI NICHT LESBAR!" would be that X-Ways Forensics was able to reconstruct a previously existing file partially only. The size may be known from $LogFile or a volume shadow copy, and the first few clusters of the file may be known from the source, but the whereabouts of the remaining clusters may be unknown. Another possible reason for "DATEI NICHT LESBAR!" if it's a compressed file in a file archive would be that the file archive is corrupt so that the contained compressed file cannot be read completely any more

If it's a file system problem, then you can find more more precisely what is going on by looking at the file system data structures that define the volume. Users can usually easily locate them in 2 seconds via a right click on the file, Navigation | Seek [name of the data structure].

2) "DEFEKTES EVIDENCE-FILE!" refers to a problem in an image in .e01 evidence file format. A possible reason to see that pattern would be that the requested sector is contained in the 2nd half of a compressed chunk (also called block) in which a few bits flipped so that only roughly the first half could be successfully decompressed.

3) "SEKTOR NICHT LESBAR!" ist ein Muster, das in Optionen | Allgemein definiert ist. Es kommt immer dann zum Einsatz, wenn die eigentlich in Datenträger-Sektoren gespeicherten Daten aufgrund von Lesefehlern nicht ermittelt werden können, zur Anzeige auf dem Bildschirm, beim Sichern von Datenträgern in eine Image-Datei, beim Klonen, beim Hashen, beim Suchen usw. usf. Wenn Sie Hash-Werte von Datenträgern mit defekten Sektoren bilden und die Ergebnisse mit einem anderen Tool vergleichen/reproduzieren möchten, dann können Sie hier das gleiche Muster angeben wie von dem anderen Tool verwendet. Beachten Sie jedoch, dass es schwierig ist, solche Hash-Werte zu reproduzieren, weil defekte Festplatten-Sektoren sich im Laufe von mehreren Versuchen vermehren können. Wenn beim Versuch des Lesens von nicht lesbaren Sektoren Null-Bytes zurückgeliefert werden sollen, löschen Sie das Muster ganz heraus (stellen Sie sicher, dass das Editierfeld vollkommen leer ist). If you keep the pattern, it will make it much easier to tell which sectors could be read and which sectors could not be, on the original hard disk directly, and that is also the case when you look at the same sectors in an image of that hard disk, provided that the pattern was active at the moment when the image was created with X-Ways Forensics. A bad sector on a hard disk is for example one whose internal CRC does not

match the payload data in that sector any more.

4) Other surrogate patterns are "FEHLENDES IMAGE-SEGMENT", "HINTER DEM ENDE DES IMAGES !!", and "SEITE UNLESBAR!", all of which should be basically self-explanatory. ("Seite" bezieht sich auf eine Seite im Arbeitsspeicher.)

10.15 RAID-Systeme zusammensetzen

WinHex und X-Ways Forensics können RAID-Systeme der Level 0, 5, 5EE and 6 sowie JBOD intern zusammenführen, die aus bis zu 16 Komponenten bestehen (physische Festplatten oder Sicherungen). Auf diese Weise ist es nicht erforderlich, RAID-Systeme mit Hilfe eines Scripts zusammenzuführen und in eine Image-Datei zu exportieren, was Zeit und Plattenplatz spart. Stellen Sie sicher, dass Komponenten, die in Form von Sicherungsdateien (Images) vorliegen, bereits geöffnet und interpretiert sind, wenn Sie diese Funktion aufrufen. Komponenten, die Partitionen sind, müssen erst geöffnet werden, bevor das RAID zusammengesetzt werden kann.

Sie müssen die Komponenten in der richtigen Reihenfolge angeben. WinHex lässt Sie die Blockgröße in Sektoren (oftmals 128 oder eine andere Potenz von 2 wie 32, 64, 256) angeben sowie individuelle RAID-Header-Größen pro Komponente (normalerweise einfach 0). Die Blockgröße (Strip Size) multipliziert mit der Anzahl der RAID-Komponenten ergibt die sog. Stripe-Size, d. h. eine ganze Zeile.

Der Header ist ein reservierter Bereich am Anfang einer Komponente, den einige RAID-Controller für eigene Daten freilassen und der daher von der Rekonstruktion ausgenommen werden muss. Wenn es einige reservierte Sektoren am Ende einer Komponentenplatte gibt, dann können Sie *vor* dem Zusammensetzen die Anzahl der tatsächlich genutzten Sektoren plus Header-Größe für jede Komponente über den Menübefehl Extras | Disk-Tools | "Plattenparameter eingeben" als Gesamtzahl der Sektoren angeben. Oder aber Sie geben eine Footer-Größe in Sektoren beim Zusammensetzen des RAIDs an, um eine definierte Anzahl an Sektoren am Ende davon auszuschließen. Das könnte besonders für JBODs nützlich sein, wenn der mittendrin eingestreute unbenutzte Speicher den logischen Zusammenhang der Daten stört.

Dass entweder Komponentenreihenfolge, Blockgröße, Verteilungsmuster oder RAID-Header-Größe nicht korrekt von Ihnen ausgewählt wurden, erkennen Sie normalerweise daran, dass keine Partitionen erkannt werden oder Partitionen mit unbekannten Dateisystemen oder mit Dateisystemen, die nicht richtig interpretiert werden.

Wenn Sie zusammengesetztes RAID-System einem Fall hinzufügen (und optional daraus geöffnete Partitionen), werden die gewählten RAID-Parameter zusammen mit dem Asservat gesichert, so dass Sie auf das RAID-System zu einem späteren Zeitpunkt ohne Zeitverlust erneut zugreifen können (nur forensische Lizenzen).

RAID Level 5 und 6 werden von verschiedenen RAID-Controller-Herstellern in unterschiedlicher Weise implementiert, d. h. sie verwenden unterschiedliche Stripe-/Parity-Muster. Die unterstützten Muster sind die folgenden:

```
Level 5: Backward Parity aka Left Asynchronous (Adaptec)
Component 1:  1  3  P
Component 2:  2  P  5
Component 3:  P  4  6

Level 5: Backward Dynamic Parity aka Left Synchronous (AMI and
Linux standard)
Component 1:  1  5  9  P
Component 2:  2  6  P  10
Component 3:  3  P  7  11
Component 4:  P  4  8  12

Level 5: Backward Delayed Parity (HP/Compaq)
Component 1:  1  3  5  7   9   11  13  15
Component 2:  2  4  6  8   P   P   P   P
Component 3:  P  P  P  P   10  12  14  16

Level 5: Forward Parity (aka Right Asynchronous)
Component 1:  P  3  5
Component 2:  1  P  6
Component 3:  2  4  P

Level 5: Forward Dynamic Parity (aka Right Synchronous)
Component 1:  P  6  8  10
Component 2:  1  P  9  11
Component 3:  2  4  P  12
Component 4:  3  5  7  P

Level 5: Forward Delayed Parity
Level 5: Forward Dynamic Delayed Parity (CRU/Dataport)

Level 5EE: Backward Parity (Adaptec)
Component 1:  1  3  S  P
Component 2:  2  S  P  7
Component 3:  S  P  5  8
Component 4:  P  4  6  S   (S = spare)

Level 5EE: Forward Parity
Component 1:  1  P  S  7
Component 2:  2  3  P  S
Component 3:  S  4  5  P
Component 4:  P  S  6  8

Level 6: Backward Parity (Adaptec/JetStor)
Component 1:  1  3  P  Q
Component 2:  2  P  Q  7
Component 3:  P  Q  5  8
Component 4:  Q  4  6  P

Level 6: Backward Dynamic Parity
Component 1:  1  4  P  Q
Component 2:  2  P  Q  7
```

```
Component 3:  P  Q  5  8
Component 4:  Q  3  6  P

Level 6: Forward Delayed Parity
Level 6: Forward Parity
```

Die Parity-Startkomponente kann für viele RAID-Varianten erforderlichenfalls anders definiert werden. Um beim gewählten Standardmuster zu bleiben, belassen Sie diesen Wert auf 0. Um eine Nicht-Standard-Parity-Startkomponente festzulegen, geben Sie die Nummer der Komponente an, auf der sich das Parity zuerst befindet (von 1 an gezählt).

Der Verzug (Delay), mit dem das Parity sich bei HP/Compaq-Controllern rückwärts bewegt, beträgt meistens 4 oder 16, ist aber frei konfigurierbar.

Wenn eine der RAID-Komponentenplatten nicht verfügbar ist, können Sie ein RAID-5-System dennoch zusammensetzen, weil eine Komponente redundant ist. Wählen Sie einfach behelfsweise einen Ersatz (eine der *anderen, verfügbaren* Komponenten desselben RAID-Systems) als *fehlende* Komponente aus und kennzeichnen Sie sie als fehlend. Auch für RAID 5EE und RAID 6 darf eine Komponente fehlen.

Unterstützung von Software-RAIDs

Linux MD-RAID-Container-Partitionen werden automatisch als solche erkannt. Diese Partitionen werden als zwei separate Objekte dargestellt: Als statischer Vorspann, der Metadaten über das RAID enthält (normalerweise beim relativen Offset 4096) und als erkundbare Partition, die als die RAID-Komponente fungiert. Im Fall von RAID-Level 1 enthält diese erkundbare Partition ein in sich vollständiges Volume, dessen Dateisystem normal eingelesen werden kann, sofern unterstützt, ohne die besondere Anstrengung einer RAID-Rekonstruktion unternehmen zu müssen. Bei anderen RAID-Leveln muss die Zusammensetzung wie üblich über den Befehl "RAID-System zusammensetzen" im Specialist-Menü erfolgen, und einige Hinweise die richtigen Rekonstruktionsparameter betreffend werden als Kommentare angezeigt, die an den jeweiligen statischen Vorspann angeheftet sind. Bitte beachten Sie, dass Sie alle relevanten Partitionen zuerst öffnen müssen, damit Sie Ihnen zur Auswahl als RAID-Komponenten angeboten werden. Das Ergebnis der RAID-Zusammensetzung ist ein einziges Volume, das von einem virtuellen physischen Datenträger umfasst wird. Die RAID-Komponenten müssen aus internen Gründen im Fall als Asservate verbleiben, um das spätere erneute Öffnen des zusammengesetzten RAIDs mit einem einzigen Mausklick zu ermöglichen.

Windows storage pool container partitions are also automatically recognized as such, and it is possible to properly open partitions whose sectors size is a multiple of the sector size of the underlying physical disk. This is important for example for Windows storage space partitions in Windows storage space pool disks. These partitions and disks have a simulated sector size of 4 KB even if they reside on physical disks with a sector size of 512 bytes. The search for lost partitions can find NTFS storage space partitions within storage space container partitions despite sector size discrepancies, which is a useful work-around for simple single-disk storage spaces.

Windows drive letters are accepted as components to internally reconstruct RAIDs. That doesn't make much sense, but allows you to reinterpret a drive letter as a physical storage device in X-

Ways Forensics if necessary, by selecting it as the sole component of a JBOD. This could be useful if for some reason you need to apply menu commands to it that only make sense to apply to physical storage devices and are only available for physical storage devices, such as Scan For Lost Partitions. For example a RAID that is reconstructed/mounted outside of X-Ways Forensics may somehow present itself as a drive letter (although it does not have a volume boot sector / file system starting at sector 0 and thus cannot be put to any good use in Windows itself).

10.16 NSRL RDSv3-Format

NSRL RDSv3 files cannot be imported directly into an X-Ways Forensics hash database. First, a universal hash set text file must be generated from the NSRL RDSv3 database, and then the generated text file imported.

Either download the current full NSRL RDSv3 (SQLite) database that you need, or else update your local full copy from a downloaded delta, following the instructions on the NSRL web site.

To generate a hash set suitable for import by X-Ways Forensics:

Install sqlite3 if not already installed, and then from the command line:

```
cd "NSRL DB folder"
```

replacing "NSRL DB folder" with the location that contains your current copy of the NSRL RDSv3 database. Then type:

```
sqlite3 RDS_2022.01.3_curated.db
.mode tabs
.header on
.once md5.txt
select md5 from metadata;
.once sha1.txt
select sha1 as 'sha-1' from metadata;
.q
```

The date and version stamp "2022.01.3" above may be different for your copy of the database. Amend as necessary.

The above commands will generate a file of MD5 hashes into the file md5.txt in the same folder as the NSRL RDSv3 database, and a file of SHA-1 hashes into the file sha1.txt. You can omit the two lines containing md5 or sha1 in the instructions above if you don't need a hash set for that hash type.

You can now import the generated text files into your X-Ways Forensics hash library following the import procedure described in the chapter about the hash database. There will be duplicate hash values, and the import will discard them; this is normal.

Anhang A: Schablonen-Definition

1 Schablonen-Kopf

Der Kopf einer Schablonen-Definition hat das folgende Format. Die Ausdrücke in Klammern sind optional. Die Reihenfolge der Ausdrücke ist nicht von Bedeutung.

```
template "Titel"
[description "Beschreibung"]
[applies_to (file/disk/RAM)]
[fixed_start offset]
[sector-aligned]
[requires Offset "Hex-Werte"]
[big-endian]
[hexadecimal/octal]
[read-only]
[multiple [fixe Gesamtgröße]]
// Hier ist Platz für allgemeine Kommentare.
begin
      Variablen-Deklarationen
end
```

Ausdrücke müssen nur in Hochkommata eingeschlossen werden, wenn sie Leerzeichen enthalten. Kommentare dürfen überall in einer Schablonen-Definition auftauchen; Zeichen, die einem doppelten Schrägstrich folgen, werden vom Parser ignoriert.

Dem Schlüsselwort `applies_to` muss genau eins der Wörter `file`, `disk` oder `RAM` folgen. WinHex gibt eine Warnmeldung aus, wenn Sie eine auf diese Weise gekennzeichnete Schablone auf Daten von einer anderen Quelle anwenden.

Während standardmäßig die Schablone beim Starten die Daten an der aktuellen Cursor-Position interpretiert, sorgt die optionale Anweisung `fixed_start` dafür, dass dies am angegebenen absoluten Offset der Datei bzw. des Datenträgers geschieht.

Wendet man eine Schablone auf einen Datenträger an, so stellt das Schlüsselwort `sector-aligned` sicher, dass sie ungeachtet der exakten Cursor-Position auf den Anfang des aktuellen Sektors bezogen wird.

Ähnlich wie ein `applies_to`-Ausdruck ermöglicht es die `requires`-Anweisung WinHex, eine unabsichtliche Anwendung einer Schablonen-Definition auf nicht auf sie passende Daten zu verhindern. Geben Sie hinter `requires` einen Offset und eine Hex-Wert-Kette beliebiger Länge an. Dies soll die Daten, für die die Schablone konzipiert wurde, identifizieren. Zum Beispiel lässt sich ein gültig Master-Boot-Record an den Hex-Werten 55 AA an Offset 0x1FE erkennen, eine ausführbare Datei an den Hex-Werten 4D 5A (“MZ”) an Offset 0x0. Es dürfen mehrere `requires`-Anweisungen im Definitionskopf vorkommen, die alle berücksichtigt werden.

Das Schlüsselwort `big-endian` sorgt dafür, dass alle aus mehreren Bytes bestehende Integer-

und Boolean-Variablen in Big-Endian-Reihenfolge gelesen und geschrieben werden (höchstwertiges Byte vorn).

Das Schlüsselwort `hexadecimal` bewirkt, dass Integer-Variablen innerhalb der Schablonen-Definition in hexadezimaler Schreibweise angezeigt werden.

Das Schlüsselwort `read-only` stellt sicher, dass die Schablone nur benutzt werden kann, um Datenstrukturen einzusehen, nicht um sie zu manipulieren. Die Editierfelder der Schablone erscheinen dann grau.

Wenn das Schlüsselwort `multiple` im Definitionskopf angegeben wird, erlaubt WinHex das Wechseln zu benachbarten Datensätzen derselben Struktur. Das erfordert, dass WinHex die Größe eines Datensatzes kennt. Sofern diese nicht fest als Parameter der `multiple`-Anweisung angegeben wurde, nimmt WinHex an, dass die Gesamtgröße sich berechnet als die aktuelle Position nach der Anwendung der Schablonen-Definition minus Startposition. Die Datenmenge kann als variabel eingestuft werden, wenn die Länge von Variablen in der Schablonen variabel ist, in welchem Fall kein Wechsel nach links (zum vorherigen Datensatz) möglich ist. Das Schlüsselwort `multiple` darf alternativ auch im Rumpf verwendet werden. Wenn es dort eingesetzt wird, muss ein Parameter folgen, der die von der Schablone abgedeckte Datenmenge in Bytes angibt. Der Parameter darf eine Formel sein und dabei (anders als bei der Verwendung im Kopf) Konstanten und Variablen verwenden. Dies erlaubt es dem Benutzer, zu benachbarten Datensätzen links und rechts zu navigieren.

2 Schablonen-Rumpf: Variablen-Deklarationen

Der Rumpf eine Schablonen-Definition besteht im wesentlichen aus Variablen-Deklarationen, ähnlich wie die in Programmiersprachen. Eine Deklaration hat folgende Gestalt:

```
type "Bezeichnung"
```

wobei `type` einer der folgenden Datentypen sein kann:

- `int8, uint8 = byte, int16, uint16, int24, uint24, int32, uint32, uint48, int64,`
- `uint_flex,`
- `binary,`
- `float = single, real, double, longdouble = extended,`
- `char, char16, string, string16,`
- `zstring, zstring16,`
- `boole8 = boolean, boole16, boole32,`
- `hex,`
- `DOSDateTime, FileTime, OLEDateTime, SQLDateTime, UNIXDateTime = time_t, JavaDateTime,`
- `GUID`

Die Bezeichnung der Variablen muss nur dann in Hochkommata gesetzt werden, wenn sie

Leerzeichen enthält. Sie darf nicht nur aus Ziffern bestehen. WinHex unterscheidet nicht zwischen Groß- und Kleinschreibung. Maximal werden zur Identifikation einer Variablen 41 Zeichen verwendet.

`type` kann jeweils maximal ein Modifikator der folgenden Modifikatorengruppen vorangestellt werden:

```
big-endian      little-endian
hexadecimal     decimal         octal
read-only       read-write
local
```

Diese Modifikatoren wirken sich nur auf die unmittelbar folgende Variable aus. Sie sind redundant, wenn sie bereits im Definition-Kopf angegeben werden. "local" übersetzt Zeitstempel außer DOSDateTime von UTC in die in den Allgemeinen Optionen angegebene Zeitzone.

Die Nummern am Ende der Typnamen bezeichnet die Größe einer Variablen dieses Typs (Strings: eines Zeichens) in Bits. Mit den Typen `char16` und `string16` unterstützt WinHex Unicode-Zeichen und -Strings. Höhere Unicode-Zeichen als die ersten 256 ANSI-äquivalenten werden allerdings nicht unterstützt. Es können außerdem maximal Strings einer Größe von 8192 Bytes editiert werden.

Die Typen `string`, `string16` und `hex` erfordern einen zusätzlichen Parameter, der die Anzahl der Elemente angibt. Dieser Parameter kann eine Konstante oder eine zuvor deklarierte Variable sein. Wenn es sich um eine Konstante handelt, kann sie entweder dezimal oder hexadezimal geschrieben werden, im zweiten Fall muss ihr `0x` vorangestellt werden.

Sie können Arrays (Felder) deklarieren, indem Sie in eckigen Klammern die gewünschte Größe angeben, entweder hinter der Typangabe oder hinter der Variablenbezeichnung. Geben Sie "unlimited" als Array-Größe an, hört die Schablone mit dem Auslesen der Daten erst auf, wenn das Dateiende erreicht wird. Bspw. deklarieren die folgenden zwei Zeilen einen ASCII-String, dessen Länge dynamisch von der vorherigen Variable bestimmt wird:

```
uint8        "Länge"
char[Länge]  "Ein String"
```

Dasselbe Ergebnis könnte mit folgenden zwei Deklarationen erzielt werden:

```
byte         "Länge"
string Länge "Ein String"
```

Eine Tilde (“~”) kann als Platzhalter eingesetzt werden, um zur Laufzeit mit der tatsächlichen Array-Elementnummer ersetzt werden (s. u.). Dies trifft nicht auf Arrays des Typs `char` zu, da diese von WinHex automatisch in einen String übersetzt werden.

Numerische Parameter für string-, string16- und hex-Variablen ebenso wie die Größenangaben von Arrays dürfen in mathematischer Notation angegeben werden. Sie werden vom integrierten Formel-Parser verarbeitet. Solche Ausdrücke müssen in Klammern angegeben werden. Sie dürfen keine Leerzeichen enthalten. Sie dürfen zuvor deklarierte Integer-Variablen verwenden,

deren Namen selbst ebenfalls keine Leerzeichen enthalten. Unterstützte Operationen sind die Addition (+), Subtraktion (-), Multiplikation (*), Integer-Division (/), Modulo-Division (%), bitweises AND (&), bitweises OR (|) und bitweises XOR (^). Gültige mathematische Ausdrücke sind zum Beispiel (5*2+1) oder (len1/(len2+4)). Das Resultat ist immer ein Integer und muss ein positiver Wert sein.

`zstring` und `zstring16` sind Null-terminierte Strings, deren Größe dynamisch zur Laufzeit bestimmt wird.

Konstanten

Sie können auch Konstanten in Schablonen zu definieren, die einen Namen haben, einen beliebigen Integer-Typ und einen Wert Ihrer Wahl. Konstanten können in Berechnungen eingesetzt werden. Wenn ein Konstantenname ein Leerzeichen enthält, muss er in Anführungszeichen geschrieben werden. Der Wert kann selbst eine Formel sein und von anderen Konstanten oder Variablen abhängen, die zum Zeitpunkt der Definition der Konstante bereits bekannt sind. Konstanten werden in einem Schablonenfenster zusammen mit Variablen aufgelistet. Beispiel:

```
const int16 100 "Meine Konstante"
const int16 ("Meine Konstante"*10) "Meine andere Konstante"
goto ("Meine andere Konstante"*5)
```

Diese Anweisung ändert die aktuelle Position der Schablonen-Interpretation auf Offset 5000.

Möglichkeit, intern vordefinierte Konstanten namens Bytes_per_sector und Bytes_per_cluster in Formeln einzusetzen, in Schablonen, die auf Datenträger oder interpretierte Images oder Partitionen/Volumes angewandt werden.

Eine weitere neue vordefinierte Konstante ist Bytes_per_record. Ihr Wert hängt ab von der Datensatzgröße, die unter Ansicht | Datensatz-Darstellung eingestellt ist, sofern aktiv. Wenn diese Anzeigeoption nicht aktiv ist, hat die Konstante in Partitionen/Volumes mit einem Dateisystem vom Typ Ext2/Ext3/Ext4, XFS oder UFS die jeweilige Inode-Größe als Wert bzw. in NTFS-Dateisystemen die FILE-Record-Größe.

Eine weitere neue vordefinierte Konstante ist Base_offset. Das ist der Offset im aktiven Datenfenster, auf den die Schablone vom Benutzer angewandt wurde und der sich ändern kann, wenn der Benutzer zu benachbarten Datensätzen wechselt.

3 Schablonen-Rumpf: Fortgeschrittene Befehle

Variablendeklarationen können in geschweiften Klammern eingeschlossen werden, so dass sie einen Block bilden, der als ganzes wiederholt eingesetzt werden kann. Beachten Sie aber, dass Blöcke in der aktuellen Implementation nicht verschachtelt werden dürfen. Eine Tilde (“~”) kann als Platzhalter für eine spätere Ersetzung mit dem aktuellen Stand des Wiederholungszählers in Variablennamen verwendet werden. Die optionale `numbering`-Anweisung legt dabei fest, mit

welcher Nummer die Zählung begonnen werden soll (standardmäßig mit Null).

```
numbering  1
{
byte  "Länge"
string Länge "String Nr. ~"
}[10]
```

In diesem Beispiel werden die tatsächlichen Variablennamen in der Schablone „String Nr. 1“, „String Nr. 2“, ..., „String No. 10“ lauten. Anstelle einer fix vorgegebenen Zahl von Wiederholungen (im Beispiel 10) können Sie auch „unlimited“ angeben. In diesem Fall wiederholt WinHex den Block bis zum Ende der Datei. „ExitLoop“ kann dazu verwendet werden, vorzeitig eine Wiederholungsschleife zu verlassen. „Exit“ beendet die Abarbeitung einer Schablone ganz.

Mit dem Befehl „IfEqual“ können zwei Ausdrücke miteinander verglichen werden. Die Vergleichsoperanden können zum einen beide numerisch sein, also jeweils entweder ein konstanter Wert (in dezimaler Schreibweise), eine Integer-Variable oder mathematische Ausdrücke. Zum anderen werden Ausdrücke, die entweder als Text oder als hexadezimale Zeichenfolge angegeben werden, byteweise miteinander verglichen. Ausdrücke in Anführungszeichen werden als Zeichenketten interpretiert, Hexadezimalwerte werden durch ein vorangestelltes „0x“ identifiziert. Mathematische Ausdrücke müssen von runden Klammern umschlossen sein.

```
{
byte       Wert
IfEqual    Wert 1
     ExitLoop
EndIf
} [10]
```

Jedes „IfEqual“ muss mit einem „EndIf“ abgeschlossen werden. Wenn die Ausdrücke gleich sind, wird der nachfolgende Teil der Schablone abgearbeitet. Ist ein „Else“ angegeben, dann wird bei Ungleichheit der Teil nach diesem Schlüsselwort abgearbeitet. „IfEqual“-Anweisungen dürfen nicht verschachtelt sein. Für den Befehl „IfGreater“ gelten dieselben Regeln wie für IfEqual, nur dass die Vergleichsbedingung erfüllt ist, wenn der erste Ausdruck größer ist als der zweite. Strings und Hex-Werte werden lexikographisch verglichen.

Um die Übersichtlichkeit einer Schablone zu verbessern, lassen sich Gruppen von Variablen auch visuell bilden, so dass die zugehörigen Editierfelder durch freien Raum im Dialogfenster voneinander getrennt erscheinen.:

```
section "...Bezeichnung des Bereichs..."
...
endsection
```

Die Anweisungen `section`, `endsection` und `numbering` haben keinen Einfluss auf die aktuelle Position der Datenauswertung durch die Schablone.

Es gibt noch zwei weitere Befehle, die auch keine Variablen deklarieren, aber explizit benutzt werden, um die aktuelle Position zu manipulieren. Dies kann z. B. geschehen, um irrelevante

Daten zu überspringen (Vorwärtsbewegung) oder um bestimmte Variablen mehrfach in Form von unterschiedlichen Datentypen erfassen zu können (Rückwärtsbewegung). Benutzen Sie die „`move n`“-Anweisung, um `n` Bytes von der aktuellen Position aus zu überspringen, wobei `n` auch negativ sein darf. `goto n` setzt die aktuelle Position auf `n`, einen absoluten (positiven) Offset basierend auf der Basisposition, auf die die Schablone angewandt wird. `gotoex n` springt zu einem absoluten Offset gemessen vom Anfang des Datenfensters an (z. B. vom Anfang einer Datei oder eines Datenträgers).

Das folgende Beispiel demonstriert den Zugriff auf 4 Bytes an Daten als 32-Bit-Integer und als eine Kette von 4 Hex-Werten:

```
int32      "Seriennummer des Datenträgers (dezimal)"
move -4
hex 4      "Seriennummer des Datenträgers (hexadezimal)"
```

4 Schablonen-Rumpf: Flexible Integer-Variablen

Ein besonderer Variablentyp, der von Schablonen unterstützt wird, ist uint_flex. Dieser Typ ermöglicht es, einen vorzeichenlosen Integer-Wert aus verschiedenen individuellen Bits innerhalb eines 32-Bit- (=4-Byte-) Bereichs in beliebiger Reihenfolge zusammenzusetzen, und ist sogar flexibler als das sogenannte Bit-Feld der Programmiersprache C.

uint_flex erfordert als zusätzlichen Parameter eine Zeichenkette in Anführungszeichen, die genau festlegt, welche Bits in welcher Reihenfolge verwendet werden, getrennt von Kommas. Das zuerst genannte Bit wird das signifikanteste (höchstwertige) Bit in der resultierenden Zahl und es wird nicht als Vorzeichen interpretiert. Das zuletzt genannte Bit wird das insignifikanteste Bit der resultierenden Zahl.

Die Bits werden gezählt beginnend mit 0. Bit 0 ist das am wenigsten signifikante Bit des ersten Bytes. Bit 31 ist das signifikanteste Bit des vierten Bytes. Die Definition basiert also auf der Little-Endian Philosophie.

Zum Beispiel ist
uint_flex "15,14,13,12,11,10,9,8,7,6,5,4,3,2,1,0" "Standard 16-Bit-Integer"
genau das gleiche wie uint16, die gewöhnliche vorzeichenlose 16-Bit-Integer Variable.

uint_flex
"31,30,29,28,27,26,25,24,23,22,21,20,19,18,17,16,15,14,13,12,11,10,9,8,7,6,5,4,3,2,1,0"
"Standard 32-Bit-Integer"
ist genau das gleiche wie uint32, die gewöhnliche vorzeichenlose 32-Bit-Integer Variable.

Der Vorteil von uint_flex ist aber der, dass die Anzahl, die Position und die Interpretationsreihenfolge aller Bits völlig frei gewählt werden kann. Zum Beispiel erzeugt
uint_flex "7,15,23,31" "Ein ungewöhnlicher 4-Bit-Integer"
einen 4-Bit-Integer aus den jeweils signifikantesten Bits von jedem der vier beteiligten Bytes. Wenn diese vier Bytes beispielsweise den Wert

F0 A0 0F 0A = 11110000 10100000 00001111 00001010
besitzen, dann gilt: Bit 7 ist 1, Bit 15 ist 1, Bit 23 ist 0 und Bit 31 ist 0. Der resultierende uint_flex ist also 1100 = 1*8 + 1*4 + 0*2 + 0*1 = 12.

Anhang B: Verzeichnis der Scriptbefehle

Groß- und Kleinschreibung spielt bei den Scriptbefehlen keine Rolle. Kommentare dürfen überall in einem Script eingefügt werden. Zu ihrer Kenntlichmachung müssen ihnen zwei aufeinanderfolgende Schrägstriche vorangestellt werden. Parameter dürften max. 255 Zeichen lang sein. Sollten Sie im Zweifel sein, weil sowohl Hex-Werte als auch Zeichenketten (oder auch Zahlen) als Parameter akzeptiert werden, können Sie Anführungszeichen benutzen, um die Interpretation eines Parameters als Text zu erzwingen. Anführungszeichen sind zwingend erforderlich, wenn eine Zeichenkette oder ein Variablenname eines oder mehrere Leerzeichen enthält, damit alle Zeichen innerhalb der Anführungszeichen als ein Parameter erkannt werden. Wenn der Text innerhalb von Anführungszeichen ein definierter Variablenname ist, wird die Variable als Parameter verwendet.

Wo immer numerische Parameter erwartet werden, ermöglicht der integrierte Formel-Parser die Verwendung mathematischer Notation. Solche Ausdrücke müssen in Klammern angegeben werden. Sie dürfen keine Leerzeichen enthalten. Sie dürfen zuvor deklarierte Variablen verwenden, die als Integer-Werte interpretiert werden können. Unterstützte Operationen sind die Addition (+), Subtraktion (-), Multiplikation (*), Integer-Division (/), Modulo-Division (%), bitweises AND (&), bitweises OR (|) und bitweises XOR (^). Gültige mathematische Ausdrücke sind zum Beispiel (5*2+1), (MyVar1/(MyVar2+4)), oder (-MyVar).

Im Folgenden finden Sie Beschreibungen aller gegenwärtig unterstützten Scriptbefehle, incl. Beispiel-Parameter.

Create "D:\My File.txt" 1000
Erzeugt die angegebene Datei mit einer anfänglichen Dateigröße von 1000 Bytes. Wenn die Datei bereits existiert, wird sie überschrieben.

Open "D:\My File.txt"
Open "D:*.txt"
Öffnet die angegebene(n) Datei(en). Geben Sie "?" als Parameter an, um den Nutzer die zu öffnende Datei wählen zu lassen.

Open C:
Open D:
Öffnet das angegebene logische Laufwerk. Geben Sie "?" als Parameter an, um den Nutzer das zu öffnende logische Laufwerk oder den physischen Datenträger wählen zu lassen.

Open 80h
Open 81h
Open 9Eh

Öffnet den angegebenen physischen Datenträger. Die Nummerierung von Floppy-Laufwerken beginnt mit 00h, die fest eingebauter und Wechseldatenträger mit 80h und die für optische Laufwerke mit 9Eh.

Optional können Sie einen zweiten Parameter mit dem Open-Befehl angeben, der den Editier-Modus angibt, in dem die Datei oder der Datenträger zu öffnen ist ("in-place" oder "read-only").

CreateBackup
Erzeugt ein WHX-Backup der aktiven Datei in seinem aktuellen Zustand.

CreateBackupEx 0 100000 650 true "F:\My backup.whx"
Erzeugt ein WHX-Backup der aktiven Platte, beginnend mit Sektor 0 bis Sektor 1.000.000. Die Backup-Datei wird automatisch in Stücke von 650 MB segmentiert. Komprimierung ist aktiv ("true"). Die erzeugte Datei ist der letzte Parameter.

Wenn die Backup-Datei nicht segmentiert werden soll, geben Sie 0 als dritten Parameter an. Um Komprimierung abzuschalten, übergeben Sie "false". Um vom Backup-Manager automatisch einen Namen zuweisen zu lassen und die Datei im Verzeichnis für Backup-Dateien ablegen zu lassen, geben Sie "" als letzten Parameter an.

Goto 0x128
Goto MyVariable
Bewegt die aktuelle Cursor-Position zur hexadezimalen Adresse 0x128. Alternativ kann auch eine existierende Variable (bis zu 8 Bytes groß) als numerischer Wert interpretiert werden.

Move -100
Bewegt die aktuelle Cursor-Position um 100 Bytes (dezimal) zurück.

Write "Test"
Write 0x0D0A
Write MyVariable
Schreibt die vier ASCII-Zeichen "Test" oder die zwei Hexadezimal-Werte "0D0A" an die aktuelle Position (im Überschreiben-Modus). Kann auch den Inhalt einer als Parameter angegebenen Variablen schreiben. Bewegt die aktuelle Cursor-Position entsprechend der Anzahl geschriebener Bytes vorwärts. Um das sicherzustellen, wird, falls das Ende der Datei erreicht wird, ein Nullbyte hinten angehängt. Das ist nützlich, damit weitere Write-Aufrufe nicht das letzte vom vorherigen Write-Aufruf geschriebene Byte wieder überschreiben.

Write2
Identisch zu Write, aber hängt kein Nullbyte an, wenn das Ende der Datei erreicht wurde. Daher darf man sich nicht darauf verlassen, dass Write2 die aktuelle Position um die Anzahl der geschriebenen Bytes vorwärts bewegt.

Insert "Test"
Arbeitet genau wie der "Write"-Befehl, jedoch im Einfügen-Modus. Darf nur mit Dateien benutzt werden.

Read MyVariable 10
Liest 10 Bytes von der aktuellen Position aus in die Variable namens "MyVariable". Wenn diese Variable noch nicht existiert, wird sie erzeugt. Bis zu 48 verschiedene Variablen sind erlaubt. Eine andere Art, eine Variable zu erzeugen, ist der "Assign"-Befehl.

ReadLn MyVariable
Liest von der aktuellen Position in eine Variable namens "MyVariable" bis das nächste Zeilenende-Zeichen gefunden wird. Wenn die Variable bereits existiert, wird ihre Größe entsprechend angepasst.

Close
Schließt das aktive Fenster ohne es zu speichern.

CloseAll
Schließt alle Fenster ohne zu speichern.

Save
Speichert die Änderungen an der Datei oder dem Datenträger im aktiven Fenster.

SaveAs "C:\New Name.txt"
Speichert die Datei im aktiven Fenster unter dem angegebenen Namen und Pfad. Geben Sie "?" als Parameter an, um den Nutzer das Ziel selbst auswählen zu lassen.

SaveAll
Speichert alle Änderungen in allen Fenstern.

Terminate
Bricht die Ausführung des Skripts ab.

Exit
Bricht die Ausführung des Skripts ab und beendet WinHex.

ExitIfNoFilesOpen
Bricht die Ausführung des Skripts ab, wenn aktuell keine Dateien in WinHex geöffnet sind.

Block 100 200
Block "My Variable 1" "My Variable 2"
Legt den aktuellen Block im aktiven Fenster fest beginnend bei Adresse 100 und endend bei Adresse 200 (dezimal). Alternativ können auch existierende Variablen (jede bis zu 8 Bytes groß) als numerische Werte interpretiert werden.

Block1 0x100
Legt den Anfang des Blocks auf die hexadezimale Adresse 0x100. Eine Variable ist ebenfalls als Parameter möglich.

Block2 0x200
Legt das Ende des Blocks auf die hexadezimale Adresse 0x200. Eine Variable ist ebenfalls als

Parameter möglich.

Copy
Kopiert den aktuell definierten Block in die Zwischenablage. Wenn kein Block festgelegt ist, bewirkt der Befehl das gleiche wie der "normale" Kopieren-Befehl im Bearbeiten-Menü.

Cut
Schneidet den aktuell markierten Block aus der Datei aus und speichert ihn in der Zwischenablage.

Remove
Entfernt den aktuell markierten Block aus der Datei.

CopyIntoNewFile "D:\New File.dat"
CopyIntoNewFile "D:\File +MyVariable+.dat"
Kopiert den aktuell markierten Block in die angegebene Datei ohne die Zwischenablage zu benutzen. Wenn kein Block festgelegt ist, bewirkt der Befehl das gleiche wie der "normale" Kopieren-Befehl im Bearbeiten-Menü. Kann Datenträger-Sektoren genauso kopieren wie Dateien. Erlaubt eine unbegrenzte Anzahl von "+" Konkatenationen im Parameter. Eine Variable wird als Integer interpretiert wenn sie nicht größer als 2^24 (~16 Mio.) ist. Nützlich für Schleifen und Datenrettung.

Paste
Schreibt den aktuellen Inhalt der Zwischenablage an die aktuelle Position in einer Datei, ohne die aktuelle Position zu ändern.

WriteClipboard
Schreibt den aktuellen Inhalt der Zwischenablage an die aktuelle Position ein einer Datei oder auf einem Datenträger ohne die aktuelle Position zu verändern und indem es die Daten an der aktuellen Position überschreibt.

Convert Param1 Param2
Konvertiert die Daten der aktiven Datei von einem Format in ein anderes. Gültige Parameter sind ANSI, IBM, Binary, HexASCII, IntelHex, MotorolaS, Base64, UUCode, LowerCase, UpperCase und hiberfil, in den Kombinationen wie sie vom herkömmlichen Konvertieren-Menübefehl bekannt sind.

AESEncrypt "My Password"
Verschlüsselt die aktive Datei oder den Datenträger oder einen davon ausgewählten Block mit dem angegebenen Schlüssel (bis zu 32 Zeichen lang) mit AES.

AESDecrypt "My Password"
Entschlüsselt die aktive Datei oder den Datenträger.

Find "John" [MatchCase MatchWord Down Up BlockOnly SaveAllPos Unicode Wildcards]
Find 0x0D0A [Down Up BlockOnly SaveAllPos Wildcards]

Sucht im aktiven Fenster nach dem Namen John bzw. dem Hexadezimal-Wert 0x0D0A und hält beim ersten Treffer an. Die anderen Parameter sind optional. Standardmäßig durchsucht WinHex die komplette Datei bzw. Platte. Die optionalen Parameter funktionieren wie von den WinHex-Suchoptionen bekannt.

ReplaceAll "John" "Joan" [MatchCase MatchWord Down Up BlockOnly Unicode Wildcards]
ReplaceAll 0x0A 0x0D0A [Down Up BlockOnly Wildcards]
Ersetzt alle Suchtreffer einer Zeichenkette oder eines Hexadezimal-Wertes in der aktiven Datei durch etwas anderes. Kann auf Laufwerke nur im In-Place-Modus angewandt werden.

IfFound
Ein boolescher Wert, der davon abhängt, ob die letzte Suchen- oder Ersetzen-Anweisung erfolgreich war. Setzen Sie Anweisungen, die ausgeführt werden sollen, wenn etwas gefunden wird, hinter die IfFound-Anweisung.

IfEqual MyVariable "Hello World"
IfEqual 0x12345678 MyVariable
IfEqual MyVariable 1000
IfEqual MyVariable MyOtherVariable
IfEqual MyVariable (10*MyOtherVariable)
Vergleicht entweder zwei numerische Integer-Werte (von denen jede ein konstanter Wert, eine Integer-Variable oder ein mathematischer Ausdruck sein kann) oder zwei Variablen, ASCII-Zeichenketten oder Hexadezimal-Werte auf binärer Ebene. Der binäre Vergleich zweier Objekte mit unterschiedlichen Längen liefert immer das Ergebnis „falsch“. Wenn die beiden Objekte gleich sind, werden die folgenden Befehle ausgeführt. If-Bedingungen dürfen nicht verschachtelt werden.

IfGreater MyVariable "Hello World"
IfGreater 0x12345678 MyVariable
IfGreater MyVariable 1000
IfGreater MyVariable MyOtherVariable
IfGreater MyVariable (10*MyOtherVariable)
Akzeptiert die gleichen Parameter wie IfEqual. Wenn der erste größer ist als der zweite, werden die folgenden Anweisungen ausgeführt. If-Bedingungen dürfen nicht verschachtelt werden.

Else
Darf nach IfEqual und IfFound auftreten. Setzen Sie Anweisungen, die ausgeführt werden sollen, wenn nichts gefunden wurde oder wenn die verglichenen Objekte nicht gleich sind, hinter die Else-Anweisung.

EndIf
Beendet die bedingte Befehlsausführung (nach IfFound, IfEqual, IfGreater).

ExitLoop
Beendet eine Schleife. Eine Schleife wird von geschweiften Klammern definiert. Der schließenden Klammer kann direkt ein Integer-Wert in eckigen Klammern folgen, der die Anzahl

der Rundendurchläufe angibt. Dies kann auch eine Variable oder das Schlüsselwort "unlimited" (in diesem Fall kann die Schleife nur durch die Anweisung "ExitLoop" verlassen werden) sein. Schleifen dürfen nicht verschachtelt werden.

Beispiel für eine Schleife:
{ Write "Schleife" }[10] schreibt das Wort "Schleife" zehn Mal.

Label ContinueHere
Erzeugt ein Label mit dem Namen "ContinueHere"

JumpTo ContinueHere
Setzt die Ausführung des Skriptes mit der Anweisung, die dem Label folgt, fort.

NextObj
Springt zyklisch zum nächsten geöffneten Fenster und macht es zum "aktiven" Fenster. Wenn beispielsweise drei Fenster offen sind und das Fenster Nr. 3 aktiv ist, macht NextObj Fenster Nr. 1 zum neuen aktiven Fenster.

ForAllObjDo
Der folgende Block von Skriptbefehlen (bis EndDo auftritt) wird auf alle offenen Dateien und Laufwerke angewandt.

CopyFile C:\A.dat D:\B.dat
Kopiert den Inhalt von C:\A.dat in die Datei D:\B.dat.

MoveFile C:\A.dat D:\B.dat
Verschiebt die Datei C:\A.dat nach D:\B.dat.

DeleteFile C:\A.dat
Löscht überraschenderweise die Datei C:\A.dat.

InitFreeSpace
InitSlackSpace
Initialisiert den freien bzw. den Schlupfspeicher auf dem aktuellen logischen Laufwerk unter Verwendung der aktuellen Initialisierungs-Einstellungen. InitSlackSpace setzt das Laufwerk vorübergehend in den In-Place-Modus, womit alle noch anstehenden Änderungen gespeichert werden.

InitMFTRecords
Initialisiert alle unbenutzten MFT-FILE-Records auf dem aktuellen logischen Laufwerk, sofern es mit NTFS formatiert ist, unter Verwendung der aktuellen Initialisierungs-Einstellungen. Tut nichts auf anderen Dateisystemen. Die Änderungen werden unmittelbar auf die Platte geschrieben.

Assign MyVariable 12345
Assign MyVariable 0x0D0A
Assign MyVariable "I like WinHex"

Assign MyVariable MyOtherVariable
Speichert die angegebene Integer-Zahl, Binärdaten, ASCII-Text oder den Inhalt einer anderen Variable in eine Variable mit Namen "My Variable". Wenn diese Variable noch nicht existiert, wird sie erzeugt. Andere Methoden, eine Variable anzulegen, sind z. B. Read, GetUserInput, InttoStr. Bis zu 48 verschiedene Variablen sind erlaubt, d. h. können gleichzeitig existieren.

Release MyVariable
Specifically disposes an existing variable. Mandatory to invoke only when more than 48 variables with different names are to be used during the execution of a script, so that earlier variables that are not needed any more can be destroyed.

SetVarSize MyVariable 1
SetVarSize MyVariable 4
Setzt die zugewiesene Speichergröße einer Variablen ausdrücklich auf eine bestimmte Byte-Größe zu diesem Zeitpunkt. Dies kann hilfreich sein, z. B. um Variablen, die Integer-Werte enthalten und die aus einer Berechnung stammen, in eine binäre Datei mit einer fixen Struktur zu schreiben. Ohne Aufruf von SetVarSize dürfen keinerlei Annahmen über die Größe einer Variablen gemacht werden. Zum Beispiel könnte die Zahl 300 in einer beliebigen Zahl von Bytes größer als 1 gespeichert werden. Wenn die neue Größe mit SetVarSize kleiner ist als die bisherige, wird der zugewiesene Speicher abgeschnitten. Wenn die neue Größe größer ist, wird der zugewiesene Speicher ausgeweitet. In jedem Fall wird der Wert der verbleibenden Bytes beibehalten.

GetUserInput MyVariable "Bitte geben Sie Ihren Namen ein:"
Speichert den ASCII-Text oder die binären Daten (0x...), die der Nutzer zur Laufzeit des Skripts eingegeben hat (max. 128 Bytes), in einer Variablen mit Namen "MyVariable". Der Nutzer erhält ein Dialogfenster mit der Nachricht, die Sie als zweiten Parameter angeben. Wenn die Variable nicht existiert, wird sie erzeugt. Andere Möglichkeiten zur Erzeugung einer Variablen: Assign, Read.

GetUserInputI MyIntegerVariable "Bitte geben Sie Ihr Alter in Jahren ein:"
Funktioniert wie GetUserInput, akzeptiert und speichert aber nur Integer-Werte.

Inc MyVariable
Interpretiert eine Variable als Integer (sofern sie nicht größer als 8 Bytes ist) und inkrementiert sie um eins. Praktisch in Schleifen.

Dec MyVariable
Interpretiert eine Variable als Integer (sofern sie nicht größer als 8 Bytes ist) und dekrementiert sie um eins.

IntToStr MyStr MyInt
IntToStr MyStr 12345
Speichert die dezimale ASCII-Text-Repräsentation der Integer-Zahl, die als zweiter Parameter übergeben wird, in die Variable, die als erster Parameter angeben ist.

StrToInt MyInt MyStr

Speichert die Binärcodierung der Integer-Zahl, die als dezimaler ASCII-Text als zweiter Parameter übergeben wird, in die die Variable, die als erster Parameter angegeben ist.

StrCat MyString MyString2
StrCat MyString ".txt"
Hängt eine Zeichenkette an eine andere an. Der zweite Parameter kann eine Konstante oder eine Variable sein. Der erste Parameter muss eine Variable sein. Das Ergebnis wird in der Variablen gespeichert, die als erster Parameter übergeben wurde, und darf nicht länger als 255 Zeichen sein.

GetClusterAlloc MyStr
Kann auf ein logisches Laufwerk angewendet werden. Holt eine textuelle Beschreibung der Zuordnung der aktuellen Position, z. B. welche Datei im aktuellen Cluster gespeichert ist, und speichert diese Beschreibung in der angegebenen Variablen.

GetClusterAllocEx IntVar
May be applied to a logical volume. Retrieves an integer value that indicated whether the cluster at the current position is allocated (1) or not (0), and saves that description in the specified variable.

GetClusterSize IntVar
May be applied to a logical volume. Retrieves the cluster size and saves that value in the specified integer variable.

InterpretImageAsDisk
Behandelt ein Roh-Image oder ein Evidence-File wie eine echte physische Platte oder Partition. Erfordert eine Specialist- oder forensische Lizenz.

CalcHash HashType MyVariable
CalcHashEx HashType MyVariable
Berechnet einen Hashwert wie es aus dem Extras-Menü bekannt ist und speichert ihn in der angegebenen Variablen (die erzeugt wird, wenn sie nicht existiert). Der HashType-Parameter muss einer der folgenden sein: CS8, CS16, CS32, CS64, CRC16, CRC32, MD5, SHA-1, SHA-256, PSCHF. CalcHashEx zeigt den Hashwert zusätzlich in einem Dialogfenster an.

MessageBox "Caution"
Zeigt ein Dialogfenster mit dem Text "Caution" an und bietet einen OK und einen Cancel-Knopf. Durch Drücken von Cancel wird der Skriptdurchlauf abgebrochen.

ExecuteScript "ScriptName"
Führt ein anderes Skript aus einem laufenden Skript heraus aus am aktuellen Punkt der Skriptausführung, z. B. abhängig von einer Bedingung. Aufrufe an andere Skripte dürfen verschachtelt sein. Wenn der Aufruf des Skripts beendet ist, wird das ursprüngliche Skript mit dem nächsten Kommando weiter ausgeführt. Diese Funktion ermöglicht eine bessere Strukturierung Ihrer Skripte.

Turbo On
Turbo Off

Im Turbo-Modus werden die meisten Bildschirm-Elemente zur Laufzeit des Skripts nicht aktualisiert und es ist nicht möglich, das Skript abzubrechen (beispielsweise durch Drücken von Esc) oder zu pausieren. Dies kann das Skript beschleunigen, wenn sehr viele einfache Befehle wie Move oder NextObj in einer Schleife ausgeführt werden.

Debug
Alle folgenden Befehle müssen vom Nutzer einzeln bestätigt werden.

UseLogFile
Fehlermeldungen werden in die Log-Datei "Scripting.log" im Verzeichnis für temporäre Dateien geschrieben. Diese Meldungen werden nicht in einem Meldungsfenster angezeigt, das Benutzerinteraktion verlangt. Nützlich insbesondere um Skripte unbeaufsichtigt auf einem Rechner laufen zu lassen.

CurrentPos
GetSize
unlimited
sind Schlüsselworte, die als Platzhalter fungieren und die benutzt werden können, wo numerische Parameter erwartet werden. Zur Skriptlaufzeit steht CurrentPos für die aktuelle Adresse im aktiven Datei- oder Laufwerksfenster und GetSize für seine Größe in Bytes. unlimited steht tatsächlich für die Zahl 2.147.483.647.

Anhang C: Aufbau des Master-Boot-Record

Der mit dem Disk-Editor editierbare Master-Boot-Record befindet sich am physischen Anfang einer Festplatte. Er besteht aus einem 446 Bytes langen Master-Bootstrap-Loader-Code und vier aufeinanderfolgenden, identisch aufgebauten Partitions-Records. Abschließend folgt die Hexadezimal-Signatur 55AA, die einen gültigen Master-Boot-Record kennzeichnet.

Das Format eines Partitions-Record sieht wie folgt aus:

Offset	Größe	Beschreibung
0	8 Bit	Der Hexadezimal-Wert 80 kennzeichnet eine aktive Partition.
1	8 Bit	Startkopf der Partition
2	8 Bit	Startsektor der Partition (Bits 0-5)
3	8 Bit	Startspur der Partition (Bits 8, 9 in „Startsektor“ als Bits 6, 7)
4	8 Bit	Betriebssystem-Kennung*
5	8 Bit	Endkopf der Partition
6	8 Bit	Endsektor der Partition (Bits 0-5)
7	8 Bit	Endspur der Partition (Bits 8, 9 in „Endsektor“ als Bits 6, 7)
8	32 Bit	Anzahl der Sektoren vor der Partition
C	32 Bit	Anzahl der Sektoren der Partition

***Betriebssystem-Kennungen** (Auswahl):

00	Leerer Partitionstabellen-Eintrag
01	DOS FAT12
04	DOS FAT16 (max. 32 MB)
05	DOS 3.3+ erweiterte Partition
06	DOS 3.31+ FAT16 (> 32 MB)
07	Windows NT NTFS, OS/2 HPFS, Advanced Unix
08	OS/2 v1.0-1.3, AIX bootable partition, SplitDrive
09	AIX Datenpartition
0A	OS/2 Boot Manager
0B	Windows 95+ FAT32
0C	Windows 95+ FAT32 (LBA-Modus INT 13 Erweiterungen verwendend)
0E	DOS FAT16 (> 32 MB, INT 13 Erweiterungen verwendend)
0F	Erweiterte Partition (INT 13 Erweiterungen verwendend)
17	Versteckte NTFS-Partition
1B	Versteckte Windows 95 FAT32-Partition
1C	Versteckte Windows 95 FAT32-Partition (LBA-Modus INT 13 Erw. verwendend)
1E	Versteckte LBA VFAT-Partition
42	Dynamische Partition
50	OnTrack Disk Manager, schreibgeschützte Partition
51	OnTrack Disk Manager
81	Linux
82	Linux Swap-Partition, Solaris (Unix)
83	Linux natives Dateisystem (ext2fs/xiafs)
84	Hibernation
85	Linux EXT
86	FAT16 Volume/Stripe-Set (Windows NT)
87	HPFS fehlertolerante, gespiegelte Partition, NTFS Volume/Stripe-Set
A0	Laptop Hibernation
BE	Solaris Boot-Partition
C0	DR-DOS/Novell DOS gesicherte Partition
C6	FAT16 Volume/Stripe-Set (Windows NT), "corrupted"
C7	NTFS Volume/Stripe-Set, "corrupted"
DE	DELL OEM Partition
F2	DOS 3.3+ Sekundärpartition
FE	IBM OEM Partition