X-Ways Software Technology AG

WinHex

Computer Forensics, Data Recovery, and IT Security Tool.

Hexadecimal Editor for Files, Disks & RAM.

Powerful System Utility.

White Paper

http://www.winhex.com/winhex/WinHex_White_Paper.pdf

Contents

1 Feature Overview

1.1 In a Nutshell

WinHex is an advanced tool for everyday and emergency use: Inspect or repair all kinds of files, recover deleted files or lost data from corrupt hard drives or digital camera cards. This hex editor grants access to data other programs hide from you. Features include:

- Disk editor for hard disks, floppy disks, CD-ROM & DVD, ZIP, Smart Media, Compact Flash memory cards, and more.
- Powerful directory browser for FAT12, FAT16, FAT32, and NTFS.
- RAM editor, providing access to other processes' virtual memory
- Data interpreter, knowing 20 data types
- Editing data structures (e.g. partition tables, boot sectors) using templates
- Concatenating and splitting files, unifying and dividing odd and even bytes/words
- Analyzing and comparing files
- Particularly flexible search and replace functions
- Drive cloning (tolerates physically damaged source sectors)
- Drive images (optionally compressed or split into e.g. 650 MB archives)
- Scripting. Application programming interface. *Professional and Specialist license only.*
- Sophisticated undo and backup mechanism.
- Various data recovery mechanisms.
- 128-bit encryption. Hashing: checksums, CRC16, CRC32, MD5, SHA-1, SHA-256, PSCHF.
- Erase (wipe, shred) confidential files or entire hard drives securely.
- Import of all clipboard formats, incl. ASCII hex values.
- Conversion formats: Binary, Hex ASCII, Intel Hex, and Motorola S.
- Character sets: ANSI ASCII, IBM ASCII, EBCDIC, (Unicode).
- Instant window switching.
- Printing.
- Random-number generator.
- Supports files and disks of virtually any size (> 2 GB).
- Very fast. Easy to use. Extensive online help.

Having all the bits and bytes in a computer at your fingertips has become a reality. WinHex is a universal hexadecimal editor, and at the same time possibly the most powerful system utility ever. Available in English, German, French, Spanish, Portuguese, and Italian!

1.2 Details

- **Analyzing files**

e.g. to determine the type of data recovered as lost cluster chains by ScanDisk or chkdsk. Examples. Tools | Analyze File

- **Wiping confidential files or disks**

...so no one (not even computer forensics specialists) will be able to retrieve them. To securely erase a file, use File Manager | Delete Irreversibly. For disk wiping, open the disk with the disk editor and use Edit | Fill Disk Sectors. E.g. fill with zero bytes (hexadecimal value 00) or random bytes.

- **Wiping unused space and slack space**

...either to close security leaks, to securely destroy previously existing classified files that have been deleted in the traditional way only, or to minimize the size of your disk backups (like WinHex backups or Norton Ghost backups), since initialized space can be compressed 99%. On NTFS drives, WinHex will even offer to wipe all currently unused $Mft (Master File Table) file records, as they may still contain names and fragments of files previously stored in them. File slack can be found in the unused end of the last cluster allocated to a file, which usually contains traces of previously existing files. Slack space - like everything else - is processed by WinHex very fast.

- **Trusted download** *Specialist license only.*

Solves a IT security problem. When transferring unclassified material from a classified hard disk drive to unclassified media, you need to be certain that a copied file will have no extraneous information in any cluster or sector "overhang" spuriously copied along with the actual file, since this slack space may still contain classified data from a time when it was allocated to a different file. The command Tools | Specialist Tools | Trusted Download exactly copies files in their current size, no entire sectors or clusters. Not one byte beyond the end of the file will be copied to the destination disk. Minimize your IT risks. Multiple files in the same folder can be copied at the same time.

- **RAM editor**

e.g. for debugging purposes (programming), for examining/manipulating any running program and in particular computer games (cheating). Tools | RAM Editor

- **ASCII - EBCDIC conversion**

Allows to exchange text between mainframe computers and the PC in both directions. You may even tailor the character translation table in WinHex (ebcdic.dat) for your own needs. Edit | Convert

- **Binary, Hex ASCII, Intel Hex, and Motorola S conversion, Unifying and dividing odd and even bytes/words**

e. g. for (E)PROM programmers. Edit | Convert. File Manager | Unify/Dissect

- **Conveniently editing data structure**

using custom templates. Download a tutorial. View | Template Manager

- **Splitting files that do not fit on a disk**

File Manager | Split/Concatenate

- **WinHex as a reconnaissance and learning tool**

Are you sure Microsoft Word really discards previous states of your document? You may be

surprised to find text deleted long ago in your .doc files. Maybe text that you really do not wish to be seen by the person you are going to pass the .doc file to? Discover what various software programs save in their files. Study unknown file formats and learn how they work. Investigate e.g. how executable files are structured and how they are loaded in RAM. The possibilities are practically unlimited. Here is another important one:

- **Manipulating text**

...that one is not supposed to edit, e.g. in binary files. It is not convenient, but possible to translate practically any software into another language by editing text in the executable files, e.g. if the source code is not available (e.g. lost). Or you would like to edit text in files of a certain binary type that the native application does not let you modify.

- **Viewing and manipulating files that usually cannot be edited**

because they are protected by Windows (e.g. the swap file, temporary files of the Internet Explorer), using the disk editor. Tools | Disk Editor

- **Viewing, editing, and repairing system areas**

such as the Master Boot Record with its partition table and boot sectors. Tools | Disk Editor | Access button

- **Hiding data or discovering hidden data**

...e.g. behind the supposed end of .jpg files (steganography), or in unused parts of logical drives or physical disks. WinHex specifically supports access to surplus sectors that are not in use by the operating system because they do not add to an entire cluster or cylinder.

- **Copy & Paste**

Use copy & paste or copy & write (=overwrite) with files, disks, and RAM. You may freely copy from a disk and write the clipboard contents to a disk, without regard to sector boundaries!

- **Undo**

When editing manually or using any command, be able to reverse your steps. Edit | Undo

- **Jump back and forward**

WinHex keeps a history of your offset jumps, and lets you go back and forward in the chain, like an Internet browser does. Position | Back/Forward

- **Scripting** *Professional and Specialist license only.*

Automated file editing using scripts, to accelerate recurring routine tasks or to carry out certain tasks on unattended remote computers. The ability to execute scripts other than the supplied sample scripts is limited to owners of a professional license. Scripts can be run from the Start Center or the command line. While a script is executed, you may press Esc to abort. With its wider range of application, scripting supersedes the Routine feature known from previous WinHex versions. Find out more about scripts in the program help.

- **API (Application Programming Interface)** *Professional and Specialist license only.*

Professional users may also make good use of WinHex' advanced capabilities in their own programs written in Delphi, C/C++, or Visual Basic. The WinHex API provides a convenient

interface for random access to files and disks (at the sector level). The provided functions are similar to the scripting commands. Details

- **Data recovery**

for erroneously deleted files or generally after an experienced loss of data. Can be done manually (see undeleting files) or automatically. There are automatic recovery modes for FAT12, FAT16, FAT32, and NTFS drives. On FAT drives, WinHex can re-create entire nested directory structures in a few seconds (details here). One recovery mode requires just filename patterns to be entered, another one recovers all files of a certain type at a time ("file recovery by type", supported file types: jpg, png, gif, tif, bmp, dwg, psd, rtf, xml, html, eml, dbx, xls/doc, mdb, wpd, eps/ps, pdf, qdf, pwl, zip, rar, wav, avi, ram, rm, mpg, mpg, mov, asf, mid). In particular owners of digital cameras quite often encounter problems with their media. WinHex is likely to help with this automated function that profits from the existence of file *headers* (characteristic signatures at the beginning of a file) on a disk. Tools | Disk Tools | File Recovery

- **128-bit encryption**

to make files unreadable by others. Edit | Convert

- **Checksum/digest calculation**

to make sure a file is not corrupt and was not manipulated, or to identify common known files. Tools | Calculate Hash.

- **Generating pseudo-random data**

for various (e.g. scientific simulation) purposes. Edit | Fill File

1.3 Technical Information

Maximum number of edit windows:	1000 (WinNT/2000/XP) / 500 (Win9x/Me)
Maximum file and disk size supported:	≈2,000 GB
Maximum number of simultaneous program instances:	99
Maximum number of reversible keyboard inputs:	65535
Encryption depth:	128 bit
Character sets supported:	ANSI ASCII, IBM ASCII, EBCDIC, Unicode (limited)

2 WinHex as a Computer Forensics Tool

This chapter particularly targets computer investigative specialists in private enterprise and law enforcement.

2.1 In a Nutshell

WinHex is a powerful hexadecimal file, disk, and RAM editor, but in fact it is even more than that. WinHex is also designed to serve as a low-level cloning, imaging, and disk analysis tool. WinHex is able to clone/image most drive formats, and supports drives and files of virtually unlimited size (terabytes on NTFS volumes!). It integrates various checksum and digests algorithms, including the common 128-bit MD5 message digest and even 256-bit strong one-way hashes to ensure absolute data authenticity and an uncompromised evidentiary procedure.

WinHex performs safe recoveries on hard disks, floppy disks, ZIP, JAZ, PC Card ATA flash disks, and more. WinHex is able to create true mirrors (including all slack space) of most media types. It incorporates sophisticated, flexible and lightning-fast search functions that you may use to scan entire media (or image files), including slack, for deleted files, hidden data and more. Via physical access, this can be accomplished even if a volume is undetectable by the operating system e.g. due to an unknown or corrupt file system.

2.2 Details

- **Disk Editor, File Editor, RAM Editor**

WinHex is an advanced binary editor that provides access to all files, clusters, sectors, bytes, nibbles, and bits inside your computer. It supports virtually unlimited file and disk sizes up to the terabyte region (thousands of gigabyte)! Memory usage is minimal. Speed of access is top-notch.

- **Directory Browser for FAT & NTFS**

Similar to and as easy to use as the Windows Explorer's right-hand list. This browser lists existing as well as deleted files and directories, with all details. Allows to list cluster chains, to navigate to files and directories in the disk editor, and to copy files off the drive. Works on image files and partitions even if not mounted in Windows.

- **Disk Cloning/Disk Imaging under DOS and Windows**

WinHex produces exact sector-wise copies of most media types, either to other disks (clones, mirrors) or to image files, using physical or logical disk access. Very important for forensic examiners because it allows to work on a forensically sound duplicate. Image files can optionally be compressed or split into independant archives. WinHex can silently generate log files that will note any damaged sector it encounters during cloning. All readable data will make it into the mirror. WinHex lets you check the integrity and authenticity of image files before restoring them.

Besides, a simple DOS-based hard disk cloning tool is included. Most Windows environments tend to access a newly attached drive without asking, thereby e.g. altering the last access dates of some files. This is avoided under DOS. X-Ways Replica *Specialist license only.*

- **Hard Drive Cleansing/Disk Wiping**

WinHex can quickly fill every sector of a disk with zero bytes (or in fact any byte pattern you like, even *random* bytes), as often as you like (to maximize security). This effectively removes any traces of files, directories, viruses, proprietary and diagnostic partitions, etc. WinHex can also securely erase specific files or *unused* space on a drive only. Besides, you can fill sectors with a byte pattern that stands for an ASCII string such as "Bad Sector" on the destination disk before *cloning*: This will make those parts of the destination disk easily recognizable that have not been overwritten during cloning because of unreadable (physically damaged) source sectors or because of a smaller source drive. (Alternatively, unreadable source sectors can be written as zero-filled sectors on the destination disk.)

- **File Slack Capturing** *Specialist license only.*

Slack space occurs whenever a file's size is not evenly divisible by the cluster size (which is practically always the case). The unused end of the last cluster allocated to a file still contains traces of other, previously existing files, and often reveals leads and evidence. WinHex gathers slack space in a file, so you can examine it conveniently and coherently. Tools | Specialist Tools | Gather Slack Space

- **Unused Space Capturing** *Specialist license only.*

Unused clusters, currently not allocated to any file or directory, also may still contain traces of other, previously existing files. WinHex can gathers free space in a file, too, for later examination. Tools | Specialist Tools | Gather Free Space

- **Inter-Partition Space Capturing** *Specialist license only.*

Gathers all space on a hard disk that does not belong to any partition in a file, for quick inspection to find out if something is hidden there or left from a prior partitioning. Tools | Specialist Tools | Gather Inter-Partition Space

- **Text Capturing** *Specialist license only.*

Recognizes and gathers text from a file, a disk, or a memory range in a file. This kind of filter is useful to considerably reduce the amount of data to handle e.g. if you are looking for leads in the form of text, such as e-mail messages, documents, etc. The target file can easily be split at a user-defined size.

- **Drive Contents Table** *Specialist license only.*

Creates a table of existing and deleted files and directories, with user-configurable information such as attributes, all available date & time stamps, size, number of first cluster, hash codes, NTFS alternate data streams (which contain hidden data), etc. Extremely useful to systematically examine the contents of a disk. Allows to limit the search for files of a certain type using a filename mask (e.g. *.jpg). The resulting table can be imported and further processed by databases or MS Excel. Sorting by date & time stamps will result in a good overview of what a disk has been used for at a certain time. E.g. the NTFS attribute "encrypted" might quickly reveal what files may turn out to be the most important ones in a forensic analysis.

- **Media Details Report** *Specialist license only.*

Shows information about the currently active disk or file and lets you copy it e.g. into a report you writing. Most extensive on physical hard disks, where details for each partition and even unallocated gaps between existing partitions are pointed out.

- **Interpret Image File As Disk** *Specialist license only.*

Treats a currently open and active disk image file as either a logical drive or physical disk. This is useful if you wish to closely examine the file system structure of a disk image, extract files, etc. without copying it back to a disk. If interpreted as a physical disk, WinHex can access and open the partitions contained in the image individually as known from "real" physical hard disks.
WinHex is even able to interpret *spanned* image files, that is, image files that consist of separate segments of any size. For WinHex to detect a spanned image file, the first segment may have an abritrary name and a non-numeric extension or the extension ".000". The second segment must have the same base name, but the extension ".001", the third segment ".002", and so on. The DOS cloning tool X-Ways Replica is able to image disks and produce such file segments. This is useful because the maximum image file size supported by FAT16 and FAT32 is 2 GB or 4 GB, respectively.

- **Bates-Number Files** *Specialist license only.*

Bates-numbers all the files within a given folder and its subfolders for discovery or evidentiary use. A prefix (up to 13 characters long) and a unique serial number are inserted between the filename and the extension in a way attorneys traditionally label paper documents for later accurate identification and reference.

- **Data Interpreter**

Knows all integer types, floating-point types, date formats, assembler opcodes, and more, and converts in both directions. (Details)

- **Data Analysis**

Find out what kind of binary data you are dealing with. (Details)

- **Binary Search/Text Search**

Search for any data you can imagine, specified in hexadecimal, ASCII, or EBCDIC, in both directions, even generic text passages hidden within binary data. WinHex can either stop at each occurrence, or simply log the results, aborting only when prompted or if the end of disk is encountered. This is particularly useful for locating certain keywords for investigative purposes. WinHex can also ignore read errors during searches, which proves useful on physically damaged media.

- **Simultaneous Search** *Specialist license only.*

Tools | Specialist Tools | Simultaneous Search. A parallel search facility, that lets you specify a virtually unlimited list of search terms, one per line. The search terms are searched simultaneously, and their occurrences can be archived either in the Position Manager, or in a tab-delimited text file, similar to the disk catalog, which can be further processed in MS Excel or any database. WinHex will save the offset of each occurrence, the search term, the name of the file or disk searched, and in the case of a logical drive the cluster allocation as well! (i.e. the name and path of the file that is

stored at that particular offset, if any)
That means you are now able to systematically search multiple hard drives and disk images in a single pass for words like street synonyms for drugs, alternative spellings, names of known dealers, at the same time! This will narrow down the examination to a list of files upon which to focus.

- **Scripting** *Professional and Specialist license only.*

Using tailored scripts you are able to automate routine steps in your investigation. For example, you may want to concatenate searches for various keywords, or repeatedly save certain clusters into files on other drives, or execute any long-running or toilsome operations while you are absent.

- **Position Manager**

Save logged occurrences of search strings or otherwise important addresses within files or disks as bookmarks for later use. Archive bookmark collections as dedicated position files or export them as HTML tables (for use in MS Excel etc.).

- **Checksums, CRC16, CRC32, MD5, SHA-1, SHA-256, PSCHF**

WinHex can calculate several kinds of and hash values of any file, disk, partition, or any part of a disk, even 256-bit digests, for the most suspicious ones. In particular, the MD5 message digest algorithm (128-bit) is incorporated, which produces commonly used unique numeric identifiers (hash values). The hash value of a known file can be compared against the hash value of an unknown file on a seized computer system. Matching values indicate with statistical certainty that the unknown file on the seized system has been authenticated and therefore does not need to be further examined.

- **Data Recovery**

With its sophisticated disk editor, WinHex not only provides for manual file recovery. WinHex is also able to automatically recover files. There are three data recovery mechanisms integrated:

1. "File Recovery by Name": Simply specify one or more file masks (like *.gif, John*.doc, etc.) and let WinHex do the rest. Works on FAT12, FAT16, FAT32, and NTFS.
2. File recovery by *type*: WinHex can recover all files that can be recognized by a certain file *header* (e.g. JPEG files, MS Office documents). This works on all file systems, even on raw physical disks with no healthy file system at all. (Details)
3. There is a special automatic recovery mode for FAT drives, accessible via the Access button menu, which is able to re-create entire nested directory structures. (Details)

- **Partition Recovery/Boot Record Recovery**

WinHex lets you edit FAT12, FAT16, FAT32, and NTFS boot sectors as well as partition tables using tailored templates.

2.3 Disk Cloning and Imaging

The operation of creating exact duplicates of one media on another media of the same type is called *disk cloning*. The duplicate is also referred to as a mirror or a physical sector copy. *Disk imaging* is the term given to creating an exact copy of a disk in form of an image file. This image file can be stored on different media types for archiving and later restoration. Both cloning and

imaging are essential for data recovery and computer investigative purposes.

- **Risk-Free Work**

In a data recovery scenario, it is mandatory to know that working on damaged media directly can, and often does, result in the compounding of physical damage and/or corruption of the logic. Using WinHex to clone or image a disk enables you to work aggressively on a mirror without the possibility of making matters worse.

- **Investigative Analysis/Discovery**

In the realm of computer forensics, there is no alternative to disk cloning/imaging. An investigator *must* clone a disk before starting the analysis. Cloning/imaging ensures that the original media is unchanged, both by checksum and digest (MD5) confirmation, and the evidentiary procedure is uncorrupt.

- **Disk Spanning**

When imaging to a file, if the target media is smaller than the image file, you may prefer to pre-set a volume size. E.g. when using CD-Rs to store an image you can indicate a 650 MB volume size. This allows you to burn the individual volumes created by WinHex using your regular burning software.

- **Restoration**

You can recreate an entire image or any portion of that image. For instance, if you ever wish to restore only the boot sector of a drive, you can extract only this sector without having to wait for the entire image to restore.

3 About X-Ways

X-Ways Software Technology AG
Carl-Diem-Str. 32
32257 Bünde
Germany
Fax: +49 721-151 322 561

Web: http://www.x-ways.net
Product homepage: http://www.x-ways.net/winhex/
Ordering: http://www.x-ways.net/winhex/order.html
Support forum: http://www.winhex.net
E-mail address: mail@x-ways.com

X-Ways Software Technology AG is a stock corporation incorporated under the laws of the Federal Republic of Germany, originally founded in Munich. WinHex was first released in 1995. WinHex 11.25 was released in January 2004. WinHex runs on Windows 95, Windows 98, Windows Me; Windows NT 4.0, Windows 2000, and Windows XP. Further reading: WinHex manual (http://www.x-ways.net/winhex/winhex.pdf)

WinHex Pricing:

	Base License	Each Additional License
Professional	EUR 75.90 / USD 93	EUR 45.90 / USD 56
Specialist	EUR 124.90 / USD 153	EUR 72.90 / USD 89

(subject to change)

Excerpt from our customer list (referenced by name with permission): law enforcement and government agencies (e.g. the German national customs investigation service, the Australian Department of Defence), military units in various NATO countries, national institutes (e.g. the Oak Ridge National Laboratory in Tennessee, USA), the Technical University of Vienna, the Technical University of Munich (Institute of Computer Science), Microsoft Corp., Hewlett Packard, Toshiba Europe, Siemens AG, Siemens Business Services, Siemens VDO AG, Infineon Technologies Flash GmbH & Co. KG, Ontrack Data International Inc., National Semiconductor, Lockheed Martin, BAE Systems, Ericsson, Seoul Mobile Telecom, Visa International, German Aerospace Center, and many other companies and scientific institutes.

Related products:

Evidor – Electronic evidence acquisition
X-Ways Trace – Browser log files deciphered
Davory – Data recovery made easy
X-Ways Replica – Disk cloning under DOS
X-Ways Security – Reliable erasure