X-Ways Software Technology AG • Agrippastr. 37-39 • D-50676 Köln
Web: http://www.x-ways.com • E-Mail: mail@x-ways.com • Tel.: +49-221-420 486 5 • Fax: +49-721-151 322 561

X-Ways Capture

Executive Summary

Specialized computer forensics tool for the evidence collection phase of a forensic investigation that captures Windows and Linux live systems. X-Ways Capture employs various methods to search the the running computer for indications of resident encryption software and detects an active ATA password protection. X-Ways Capture dumps the physical RAM and images all connected media to a user-defined output path, e.g. an external USB hard disk. This enables you to examine even encrypted or otherwise protected data during the analysis phase that was unlocked at the point of time when the system was acquired. X-Ways Capture saves you from unnecessarily returning empty-handed after pulling the plug and imaging hard disks the conventional way when you discover that the relevant files are encrypted! Plus you may be able to find passwords in the memory dump. All steps and settings are fully user-configurable in advance and will be thoroughly logged.

How It Works

X-Ways Capture consists of two modules, one for Windows 2000/XP, one for Linux (Intel x86 architecture each, no matter whether workstation or server). Accidentally executing the wrong module is usually impossible, but would be caught by the software itself otherwise.

The user needs to be aware of the fact that attaching another medium to a running computer and executing X-Ways Capture will slightly alter the system, at least a small amount of main memory. To keep X-Ways Capture as small as possible, it was designed without a graphical user interface. Like this, it alters as little memory upon loading as possible and the probability that it triggers the operating system to swap main memory to the hard disk before the hard disk is imaged is low. *In order to safeguard protected data in a decrypted state, in many cases you have no other choice than to put up with such a minor alteration.* If that is not acceptable in the judiciary system you work in and you have to trust on being able to retrieve passwords somehow after pulling the plug, then X-Ways Capture may not be for you, unfortunately.

Also please note that from the point of view of the operating system a hard disk may not be in an consistent state during a live acquisition (e.g. because temporary files were being in use).

The program executes the following steps unless you specify a different procedure in the configuration file:

- Dumps of the physical RAM and (under Windows only) the virtual memory of all running processes.
- Detects the ATA password protection status and any present host-protected area (HPA).
- Checks for active encryption software.
- Images attached media physically.
- Copies files logically.

The main memory is dumped first to catch it in a state as original as possible. After that, the computer is checked for settings and programs that would prevent access to the data after pulling

the plug: ATA password protection and encryption software. In the next step, locally attached media may be imaged physically depending on the findings in the previous steps. By default, this is done before the logical copying process to get as original images as possible. Only then all files from all drives may be copied logically.

In case X-Ways Captures runs out of space on the output drive while imaging or copying, it prompts for another medium. To log file, too, will be continued on the new medium. The log segments are named with an incrementing number that allows you to correctly concatenate them later.

All files in the output path are named with a prefix that designates the date and time when the program was started. The log file for instance has the name <*prefix*>-log-<*incrementing number*>.txt.

The configuration file contains a section [steps] that controls the exact sequence of steps. Each step that is to be executed is listed in this section. The steps in more detail:

0. Program start, operating system detection

a) The Windows module detects the exact Windows version and prevents an execution under Linux+Wine. The Linux module detects the exact Linux version and is not executable under Windows.

b) The command line parameters are parsed. The output path can be specified with the command line. With -i <*filename*> you may specify a configuration file other than the standard “capture.ini”.

c) X-Ways Capture asks the user for the output path, where images, the log, and all other files are written, if no such path was passed as a command line parameter. The path needs to be an absolute one.

d) The current date and time are retrieved from the system and always used as a prefix in the notation YYYY-MM-DD, HH-MM-SS. The advantage of this notation is that all file browsers list files with such a prefix in chronological order. Optionally, the steps GetUserDate, GetUserTime ask the user for the time, to be able to verify later whether the system clock was off.

e) The configuration file used is added to the log so that there is no doubt later about how X-Ways Capture was configured. [steps] name: AppendIni

f) Optionally, additional information can be logged through the Ask command
Ask "Enter text"
will prompt “Enter text” and wait for the user to enter information. Alternatively,
Ask "Enter IP address" ???.???.???.???
will prompt for an IP address, and validate the input, where ? equals any character.

1. Memory dump

a) The physical RAM is dumped to the output path as a raw image file, as far as access is not prevented by missing administrator or root rights or so-called Linux Security Enhancements.

[steps]-Name: DumpPhysicalMemory. It is normal that Windows prevents several rather small regions in memory from being accessed. A warning will be issued if so.

b) Under Windows only: The virtual memory of each process will be dumped to a file. The filename is composed of the common prefix and the name and the number of the process. [steps]-Name: DumpProcessMemory

c) The list of running processed is logged. [steps]-Name: DumpProcessList

d) The list of driver names is written to a file (Windows: DumpDriverList, Linux: AppendToLog /proc/modules)

2. ATA hard disk check

a) Generally under Windows, under Linux with root rights only: The model designation of ATA hard disks and their security settings (password protection) are detected. [steps]-Name: ATACheck

- Support for security mode feature set y/n
- Security mode aktive y/n
- Hard disk locked y/n
- Security freeze lock y/n
- Security level high/ maximum

Functionality cannot be guaranteed for *S*-ATA disks. Results for non-ATA disks (in particular hardware RAIDs), if output, are undefined.

b) Under Windows only, unless access is prevented by missing administrator rights: Check for active HPA (host-protected area) and notification of the result. ([steps]-Name: HPACheck)

c) List drives and partitions
This step logs information about the mapping between partitions and hard disks. For each partition, its associated disk and start offset on that disk are given. For hard disks, Capture tries to detect the model designation, the hardware serial number (only under Windows), the size, the bus type and whether it is partitioned as a so-called dynamic disk (only for Windows). The [steps] name under Windows is ListMountedVolumes, under Linux the default capture.ini has been configured to achieve the same behaviour through two calls to AppendToLog.

3. Check for active encryption software

This step is comprised of several stages, which depend on the operating system.

Under Windows, the following methods are employed to check for indications of active encryption, where the first positive result causes any following method to be omitted, unless flagged as mandatory in the configuration file:

a) EncryptionCheckProcessList:
The names of active processes are matched against a list with the names of known Windows-based encryption software programs, specified in the section

[SearchProcessesFor Encryption]. For example, the name of the resident service/process of PGP Desktop 9.02 is “PGPserv.exe”.

b) CheckDriverListForEncryption
Searches the driver list creating by DumpDriverList for driver names taken from the section [SearchDriverListForEncryption]. If the driver list has not been created yet, it is produced for this step.

c) EncryptionCheckProcessMemory:
The loaded .exe files of all running processes are searched for keywords that appear in the [SearchProcessMemory] section of the configuration file, both in the ASCII and the Unicode character set. With this approach, X-Ways Capture can identify a known encryption software product even if its .exe file has been renamed such that the running process has an unexpected name. Suitable keywords are e. g. internal program names or copyright notices as they appear the version information within .exe files. E. g. “PGPsdkService” is the internal name of the service “PGPserv.exe”.

d) EncryptionCheckDiskSectors
Unless access is prevented by missing administrator rights: Certain sectors on each hard disk are read with two different methods. The results are compared. Different results indicate that the hard disk is encrypted by a resident software such as “SecureDoc” or “CompuSec”.

e) EncryptionCheckAllFiles
All files on NTFS drives are checked for EFS encryption. This stage is usually the most time-consuming one in this section, depending on the number of files on NTFS drives. This test excludes the drive that X-Ways Capture was started from as well as the output drive. This step is useful only if Logicalbackup is skipped, since LogicalBackup will always copy and report EFS files under Windows. The parameter network controls whether this step affects network drives. +network enables encryption search on network drives, -network disables this. –network is the default.

f) CheckForBitLockerVolumes
Unless access is prevented by missing administrator rights: All mounted volumes are checked for a BitLocker signature.

Linux:

a) Certain files are searched depending on the EncryptionCheckFile command in the [steps] section. For each such command there is one [EncryptionCheckFile] section. Each such command needs to be followed by the path and name of the file to be searched. The same name and path needs to be the first line of the corresponding [EncryptionCheckFile] section. The remainder of the corresponding [EncryptionCheckFile] section contains the keywords to be searched. By default, the files /proc/mounts and /proc/modules are searched.

b) The names of active processes are matched against a list with the names of known Linux-based encryption software programs, specified in the section [Search ProcessesForEncryption].

4. Physical Imaging ([steps] name: PhysicalImaging)

In this step, X-Ways Capture creates images of physical disks if deemed necessary or forced. Physical imaging means that disks are copied sector-wise, not file-wise.

a) If hard disk encryption has been detected by the step EncryptionCheckDiskSectors or a currently unlocked ATA password protection has been detected by ATACheck, that particular disk is imaged.
b) If ATA password protection has been detected, yet Capture cannot clearly identify the affected hard disk, all hard disks are imaged.
c) If this step is forced, then all disks will be imaged.

Hard disks to exclude from physical imaging can be specified via model designations in the configuration file (see below). The physical medium from which X-Ways Capture is run and physical medium with the output path are automatically excluded. Under Windows 2000, the exclusion works with fixed media (hard disks) only, not with removable physical media such as USB sticks.

The imaging process involves sector-level access and requires that the user that is logged on has the necessary rights.

In the case of a software-encrypted, but currently readable hard disk, the data that is read from the hard disk is decrypted by the encryption software. The images can either be raw ("dd") images or evidence files (.e01 files). The size of the segments can be configured in the [settings] section. Evidence files can be optionally compressed. Under Linux, the list of attached media is taken from /proc/partitions. Floppy disks and net drives are omitted generally. Under Windows optical media are omitted, too. Optical media, net drives or specific file systems can be excluded from physical imaging through the configuration file.

During the imaging process, the hash value of the imaged media is computed and written to the evidence file or in the case of a raw image to a separate file. If during or after the process data is written to the media, the hash value is characteristic of the image only, not of the media any more.

5. **Volume Imaging** ([steps] name: LogicalImaging)

One way of detecting encryption of a volume (as created e.g. by Bitlocker or TrueCrypt) is to check whether the volume's first sector yields different data when reading the sector from the volume or when reading the same respective sector directly from the physical disk. Another criterion is a volume that cannot be matched to any partition on a disk (which means it is likely stored in a mounted container). This steps checks all volumes that are mounted as drive letter for whether these conditions are met, and if so, X-Ways Capture creates an image of such a volume, i.e. copies all its *sectors*. Unlike when merely copying *files* from that volume, the image will retain all free space, slack space, possibly deleted files, all metadata etc.. This step runs independently of previous analysis steps, does not affect further steps, and is available only for Windows.

6. **Logical Copying** ([steps] name: LogicalBackup)

If indications of encryption are found in step 3 (except EncryptionCheckDiskSectors) or if this step is flagged as mandatory in the configuration file, all files are additionally copied, one by one. This ensures that all files readable at the time of the acquisition are available in an unencrypted state at the time of the forensic analysis as well, even if the subject drive is encrypted or if files are located inside encrypted containers or if an ATA hard disk is password-protected (but unlocked at the time of the acquisition). The copying process retains

all filenames and paths in the output path. Under certain circumstances, however, the path and/or name needs to be modified such that the name and path is acceptable in all supported file systems. This is why paths and names are shortened to less than 255 characters if necessary. Shortened paths are collected in a separate subdirectory of the output path named "overlong". Illegal characters in filenames are replaced. If this leads to duplications of filenames, an incrementing number is inserted directly before the filename extension. The extension remains unchanged by this. All alterations are logged.

Before a file is copied, X-Ways Capture queries the date and time of the file's last read access. X-Ways Capture restores that original date and time after the file was copied because that timestamp is updated during copying. On Linux file systems and on NTFS, the original last inode or FILE record change timestamp, respectively, (not the timestamp of the last modification of the file itself) is irrevocably lost. This is noted in the log once. This is also why by default this step is executed only after physical imaging.

The output drive letter and the start drive letter of X-Ways Capture are excluded from this step if the computer is running Microsoft Windows. For Linux, all directories sharing the mount point with the start directory or output directory of X-Ways Capture are excluded. Since depending on the source and the destination file system not all metadata makes it to the copy, filenames, file sizes, timestamps, attributes, permissions (Linux), owners (Linux) and group name (where available) are logged in a separate file list. The file list has the name <*prefix*>-files-<*incrementing number*>.txt. If illegally long paths are encountered, warnings are output.

Under Windows, Capture will search all drives for EFS-encrypted files and will copy them, regardless of the results of previous encryption checks. If the previous check did not reveal an encryption module, directories and log entries will be created only for EFS-encrypted files, but paths to EFS-encrypted files are maintained. ADS are lost for EFS-encrypted files.

The parameter network controls whether this step affects network drives. +network enables this step on network drives, -network disables this. -network is the default.

Configuration File "capture.ini"

The configuration file "capture.ini" significantly influences various aspects of X-Ways Capture. This includes the sequence of the steps, media to exclude, paths, language, keywords to search, names of known encryption software, and much more. The file is a plain ASCII file and can be tailored to your needs using an appropriate text editor. The configuration file for Linux contains Linux-styled end-of-line characters, the configuration file for Windows contains Windows-styled end-of-line characters. The file comprises several sections, whose names are enclosed in square brackets, e.g. [steps]. The order in which these sections appear is arbitrary. Each line can be flagged as a remark and disabled by inserting a "#" as its first character. The following explains the meanings of the various sections.

The section [steps] determines the order of the individual steps. An example of such a section is:

AppendIni
DumpPhysicalMemory

DumpProcessMemory
DumpProcessList
ATACheck
HPACheck
EncryptionCheckProcessList
+EncryptionCheckProcessMemory
+EncryptionCheckDiskSectors
EncryptionCheckAllFiles
PhysicalImaging
LogicalImaging
+LogicalBackup

The meaning of each step is explained in the chapter “How It Works”. If a line is preceded by a minus sign (-), this suppresses the execution of this step. If a line is preceded by a plus sign (+), this flags a step as *mandatory*. “+” can be used in particular to force the logical copying process even when X-Ways Capture has found no indication of encryption or to force the execution of other checks for encryption even if one form of encryption has already been found.

The section [ListProcessesCommand] specifies the Linux command that is used to create a list of running processes. By default, this is “ps -A”.

The section [SearchFileForEncryption] is used for Linux only. The first line in such a section defines the file to be searched, all following lines define keywords that, if found in the specified file, indicate encryption. Since multiple [SearchFileForEncryption] sections are allowed, multiple files can be searched. By default, /proc/mounts is search for /dev/loop, and /proc/modules is searched for keywords such as “aes”, “blowfish”, “twofish” etc.

The section [SearchProcessListForEncryption] contains the process names of known encryption software, which are searched in the list of processes. If there is a match, this is considered an indication of an active encryption.

[SearchProcessMemoryForEncryption] contains keywords, which are searched in loaded .exe files under Windows.

[ExcludeDevicesFromPhysicalImaging] specifies the designation of physical media which should be omitted from the physical imaging step. Under Linux this is the /dev/ designation, which is to be specified without /dev/, e.g. hdb for /dev/hdb. Under Windows this is the manufacturer’s model designation of the media to be excluded, e.g. “SAMSUNG SP1614C”. The output hard disk is excluded automatically. The model designation to be specified under Windows can be seen e.g. in WinHex or X-Ways Forensics.

[ExcludeFromLogicalBackup] defines the directories, drive letters and media to omit during the logical copying process. These are absolute paths, that start with a drive letter under Windows and a / under Linux. All files and directories that match one of these paths will be excluded. For instance, c:\win even excludes c:\windows. The device directory /dev is excluded by default. Under Linux, the target device is automatically deduced from the output path and excluded from both logical copying and physical imaging.

[LinuxExcludeFS] defines the file systems that excluded from backup under Linux. The default configuration uses this section to exclude optical and net drives.

The [settings] section defines various settings and can e.g. look like this:

```
[settings]
language=English
#language=German
PromptForOutputPath
#UserShouldAcknowledge
DateFormat=mm/dd/yyyy
#DateFormat=dd.mm.yyyy
LogInfoMsgs
LogHints
LogWarnings
LogErrors
LogResults
PrintInfoMsgs
PrintHints
PrintWarnings
PrintErrors
PrintResults
ImageSegmentSize=2000
#PhysicalImageFormat=raw
#PhysicalImageFormat=e01-compressed
PhysicalImageFormat=e01-uncompressed
#PhysicalImageCalcHash=md5
#PhysicalImageCalcHash=sha-1
#PhysicalImageCalcHash=sha-256
#PhysicalImageCalcHash=none
```

“ImageSegmentSize“ denotes the desired segment size where to split physical images. Umcommenting this setting limits .e01 evidence files to about 2 GB, while the image size for raw images is limited only by the underlying file system. “PhysicalImageFormat” controls the format of such an image: “raw” creates a raw image file, “e01-compressed“ a compressed evidence file, “e01-uncompressed” an uncompressed one. The settings can easily be swapped with the remark indicator (#). “PhysicalImageCalcHash” defines the hash type to compute during the physical imaging process (md5, sha-1, sha-256 or none). Please note that with hashing the creation of images may take noticeably more time, esp. under Linux. “Language” switches between English and German. “FileSplitSize” is respected during the logical copying process (Linux only). Files that exceed this limit will be split.

The settings LogInfoMsgs, LogHints, LogWarnings, LogErrors, LogResults, PrintInfoMsgs, PrintHints, PrintWarnings, PrintErrors, PrintResults control, whether and how messages are output. All messages in X-Ways Capture belong to one of the categories Info, Hint, Warning, Error, and Result. The settings control which messages are sent to the log and/or to the console display (Print).

The “UserShouldAcknowledge” option forces the user to acknowledge important results by pressing the Enter key. Currently, the circumstances that trigger this behavior are if X-Ways Capture finds an ATA password-protected drive, an HPA, if a process has a name listed under [SearchProcessListFor Encryption], if a process contains a string listed under [SearchProcessMemory], if an encrypted

sector is found (Windows), if a file is encrypted on file system level (EFS/NTFS) or if a file is found that contains a string listed under [SearchFileForEncryption].

The option “PromptForOutputPath” can be used to prevent the prompt for an output path. When activated, X-Ways Capture will use the root directory of the partition from which it was started if run under Windows, or the mount point containing the executable under Linux. Without this option, the output path has to be typed in unless it is passed as command line parameter.

Tips

Under Linux you may use a FAT partition as the output path if the corresponding kernel module is loaded. Under Windows you may prefer NTFS to retain alternate data streams when copying a file logically.

In order to find out the output path that represents your target hard disk, the following may help. Under Linux, media are usually included automatically in the directory tree, usually under /mnt/ or /media/. With “mount” you may bring up a list of mounted file systems. The output of “df” may help as well. If the output hard disk was prepared with a file “owner.txt” that e.g. contains your name, you can be completely sure to correctly identify your own hard disk.

No more than one output medium at a time must be attached to a system on which X-Ways Capture is running. Since capture.ini is read only at program start, later changes in the file do not affect Capture.

The execution of the program can be aborted at any time by pressing Ctrl+C.

Important: X-Ways Capture must not be copied to or executed on one of the original media that belong to the live system that is to be captured. X-Ways Capture should be run from a CD or an external medium such as a USB stick or USB hard disk (e.g. the output medium).