X-Ways Software Technology AG

X-Ways Forensics

Integrated Computer Forensics Environment
Advanced Data Recovery and IT Security Software
in English, German, French, Spanish, Italian, and Portuguese

- **Complete case management**

X-Ways Forensics manages your cases separately and will allow you to identify all sources and pieces of evidence related to your case. It creates a tree-like structure for each of your cases where you can freely add drives, images and any other file. For every item, notes and pieces of evidence found will be recorded separately.

- **Automated activity logging (audit logs)**

Logging of all activity is enabled by default. This can be helpful when backtracking your steps if you have to interrupt your work and take it up again some time later. Since every action will be recorded, use this to show the integrity of your evidence collection methods.

- **Automated reports in HTML format**

The automated activity logging will also allow you to generate a report from your audit using the descriptions you have entered and the steps you have taken. All your actions will be listed sorted by sources of evidence and including the results generated. This reporting feature saves you from the hassle of having to write your reports from your notes taken during the process. Refine the report by importing the HTML output into any application that supports HTML imports, like Microsoft Word or OpenOffice.org.

- **Protection against accidental changes to the evidence objects**

X-Ways Forensics does not allow any changes to evidence objects at all. Only files created in the current case's output or temp directories can be modified using X-Ways Forensics, thus enforcing common forensic procedure. WinHex, using a forensic licence, will be able to switch to edit modes, but will first ask the user to explicitly confirm this change to ensure no accidental change occurred.

- **View of all existing and deleted files on media by file type category**

X-Ways Forensics supports the approach of looking for specific file types beyond looking for one file extension at a time. Many times, forensic examiners are specifically looking for office documents, but not specifically Word files, or for image files regardless of the actual type. X-Ways Forensics can create a drive contents table that disregards the actual directory structure of the file system and instead uses predefined categories like "images", "office" or "Internet". These categories are fully customizable by the user.

- **Gallery view for pictures**

X-Ways Forensics offers a gallery view on image files contained in directories or the "images" category of the drive contents table. Viewing thumbnails of the images notably speeds up the search process for relevant images. Supported file types for the gallery view are JPEG, JPEG 2000, GIF, TIFF, Bitmap, PNG, TGA, PCX, WMF, EMF, MNG and JBG.

- **File Viewing**

Select multiple files in the directory browser for viewing. For display in the integrated viewer, a file does not even need to be extracted internally from a hard disk partition or image file first. If the integrated viewer cannot open the file, it will invoke an external viewer. Up to 3 different external programs can be defined and invoked directly. The internal view supports various image file formats as well as Windows Registry files.

- **Skin color detection**

In cases related to child pornography, it is clear from the start that relevant images most likely contain a notable amount of skin colors. To accelerate the examiner's search for images with potentially relevant content, X-Ways Forensics features an option to sort images by skin color percentage.

- **Detection of filename/file type mismatches**

X-Ways Forensics is aware of attempts to hide relevant files by renaming them to innocuous looking files using a different extension. For example, a JPEG image file might be located in the Windows directory named sys782.dll, making it virtually impossible for the human examiner to notice the illegitimate content of this file. In order to draw attention to such obvious cases of information hiding, X-Ways Forensics allows the creation of drive contents tables that specifically mark any file whose header does not match its extension.

- **File system examination**

Native support for FAT12, FAT16, FAT32, and NTFS, shortly also for Ext2, Ext3, ReiserFS, and CDFS.

- **Ability to read EnCase images**

Forensic experts might have used EnCase to create an image for their forensic examination. X-Ways Forensics can add such EnCase images to a case and examine them like any other source of evidence.

- **Detection of host-protected areas (HPA), a.k.a. ATA-protected areas**

One of the most sophisticated methods of hiding information on a hard drive is to change the size the hard drive reports to the operating system. This way, a 100 GB disk changed to 80 GB contains 20 GB of hidden storage space. These so-called host-protected or ATA-protected areas are discovered by X-Ways Forensics and brought to the examiner's attention.

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

WinHex, the technical core of X-Ways Forensics, 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**

X-Ways Forensics 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. X-Ways Forensics can silently generate log files that will note any damaged sector it encounters during cloning. All readable data will make it into the mirror. X-Ways Forensics 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

- **Hard Drive Cleansing/Disk Wiping**

X-Ways Forensics 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. X-Ways Forensics 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 using a pattern of your choice on the destination disk.)

- **File Slack Capturing**

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. X-Ways Forensics gathers slack space in a file, so you can examine it conveniently and coherently. Specialist | Gather Slack Space

- **Unused Space Capturing**

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

- **Inter-Partition Space Capturing**

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. Specialist | Gather Inter-Partition Space

- **Text Capturing**

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**

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.
The drive contents table can also be generated against a hash database of either know good files or malware to include or exclude files, respectively. Supported hash database formats are NSRL RDS 2.x, ILook, and HashKeeper. During drive contents table generation, a database can also be created in NSRL RDS 2.x format.

- **CD Raw Mode**

Raw mode for reading Audio CDs and for access to the full 2352-byte sectors on data CDs (CD-ROM and Video CDs), including error correction codes.

- **NTFS Compression Support**

Access, open, recover, and examine files that are compressed at the NTFS file system level. They are decompressed transparently to the user "on the fly" when needed.

- **Media Details Report**

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**

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, X-Ways Forensics can access and open the partitions contained in the image individually as known from “real” physical hard disks.
X-Ways Forensics is even able to interpret *spanned* image files, that is, image files that consist of separate segments of any size. For X-Ways Forensics 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**

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, and more. (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. X-Ways Forensics 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. X-Ways Forensics can also ignore read errors during searches, which proves useful on physically damaged media.

- **Simultaneous Search**

Specialist | 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. X-Ways Forensics 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 image files in a single pass for words like street synonyms for drugs, alternative spellings, names of known dealers, at the same time! This will help to narrow down the examination to a list of files upon which to focus.

- **Scripting**

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.). They are also automatically included in the case report.

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

X-Ways Forensics can calculate several kinds of checksums 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, X-Ways Forensics not only provides for manual file recovery. X-Ways Forensics 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 X-Ways Forensics do the rest. Works on FAT12, FAT16, FAT32, and NTFS. It can also simply list found files in the directory browser for inspection, without actually recovering them yet.
2. File recovery by *type*: X-Ways Forensics can recover all files that can be recognized by a certain file *header*. Support 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. This works on all file systems, even on raw physical disks with no healthy file system at all. The recovery can be limited to a certain range of sectors simply by selecting a block prior to using it. (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**

X-Ways Forensics lets you edit FAT12, FAT16, FAT32, and NTFS boot sectors as well as partition tables using tailored templates.

Pricing:
Base license: EUR 249.90 / USD 305
Each additional license: EUR 159.90 / USD 195
(subject to change)

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/forensics/
Ordering: http://www.x-ways.net/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. WinHex was first released in 1995. X-Ways Forensics 11.7 was released in September 2004. X-Ways Forensics runs on Windows 95, 98, Me; Windows NT 4.0, Windows 2000, and Windows XP. Further reading: WinHex manual (http://www.x-ways.net/winhex/winhex.pdf)

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), particularly in the USA, military units in various NATO countries, national institutes (e.g. the Oak Ridge National Laboratory in Tennessee), the Technical University of Vienna, the Technical University of Munich (Institute of Computer Science), the German Aerospace Center, the German federal bureau of aviation accident investigation, Microsoft Corp., Hewlett Packard, Toshiba Europe, Siemens AG, Siemens Business Services, Siemens VDO AG, Infineon Technologies Flash GmbH & Co. KG, Ontrack Data International Inc., KPMG Forensic, Ernst & Young, Ericsson, National Semiconductor, Lockheed Martin, BAE Systems, TDK Corporation, Seoul Mobile Telecom, Visa International, and many other companies.

Related products:

WinHex – The core of X-Ways Forensics
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