X-Ways Software Technology AG

Evidor

Electronic Evidence Acquisition for Computer Forensics and Civil Discovery.

Target group: lawyers, law firms, corporate law and IT security departments, licensed investigators, and law enforcement agencies.

What it does: Evidor retrieves the context of keyword occurrences on computer media, not only by examining *all files* (the entire allocated space, even Windows swap/paging and hibernate files), but also currently *unallocated space* and so-called *slack space*. That means it will even find data from files that have been *deleted*, if physically still existing.

Electronic discovery: Evidor is a particularly easy and convenient way for any investigator to find and gather digital evidence on computer media. Evidor also comes most handy in civil (pre-) litigation if one party wants to examine (inspect) the computers of the other party. Evidor can be used *on site* for electronic discovery, will not disclose irrelevant proprietary or confidential information and does not impose an undue burden on the responding party in terms of personnel, time and money. Evidor serves as an automated forensic examiner, saving you the cost of many hours of hard manual expert work. Evidor produces reliable, replicable, neutral, and simple results, just as needed before court. Powerful and fast.

IT security: Evidor is also an excellent tool for proving the presence or absence of confidential data on computer media, either to detect a security leak or confirm a lack thereof. With Evidor you often finds remnants (or even intact copies) of classified data that should have been encrypted, securely erased, or should not have existed on a media in the first place.

Additional Toolset: the following products are included in Evidor: a powerful, yet very easy to use data recovery tool (Davory), a tool that deciphers Internet Explorer's internal browsing log file (X-Ways Trace), and last not least a DOS-based hard disk cloning tool (X-Ways Replica). Reason: It is generally highly advisable to work on a copy, not on the original drive. 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.

How to use: simply select the disk to examine and provide a list of keywords (such as people's names, e-mail addresses, name of traded goods, etc.). Evidor will then retrieve the context of all occurrences of the keywords on the disk. When viewing the output file, you will likely find excerpts from documents that are closely related to the keywords, e.g. purchase orders, e-mail messages, address books, time tables, etc.

Evidor can either produce HTML documents (recommended) or plain text files. HTML

documents can be easily imported and further processed in MS Excel. In MS Excel you can sort the search term occurrences by search term and occurrence location, you can cut irrelevant results, etc. Plain text files can be viewed in any text editor, MS Word, etc.

X-Ways Trace: Browser log files deciphered... a computer forensics tool that allows to track and examine the web browsing activity that took place on a certain computer.

Deciphers Internet Explorer's ever-growing internal history/cache file index.dat. Displays complete URLs, date and time of the last visit, user names, file sizes, filename extensions, and more. Allows to sort by any criterion. Reads from a file you specify, or searches complete folders and subfolders, or even entire hard disks in all files, free space, and slack space, for traces of someone having surfed the Internet. Occassionally, accesses to local files are logged, too. You may search for specific domain, file, and user names. All the details compiled by X-Ways Trace can be exported to MS Excel. Part of the Evidor toolset, but also available separately. English, German, and French.

Davory: Easy-to-use data recovery tool. Davory undeletes files and recovers files from logically damaged or formatted drives. Incorporates data recovery technology introduced with WinHex and concentrates on ease of use. Offers two separate, fully automated data recovery mechanisms to maximize your chances of success. One mechanism works with files of any type, the other one recovers JPEG (JPG), PNG, GIF, BMP, MS Office (DOC, XLS), PostScript (EPS), Acrobat (PDF), Quicken (QDF), ZIP, RAR, RIFF (WAV, AVI), and MPEG (MPG). Specifically supports FAT12, FAT16, FAT32, and NTFS. Powerful, yet inexpensive.

As Davory works not only on hard drives, floppy disks, CDs, and DVDs, but also on CompactFlash cards, SmartMedia cards, memory sticks etc., it may save your day in particular if you are the owner of a digital camera. Davory can also be put to good use during computer forensic examinations, as you may extract files of certain types or files matching certain filename patterns (like Invoice*.doc) conveniently and quickly with only a few mouse clicks. Available in English, German, and French. Part of the Evidor toolset, but also available separately. English, German, and French.

Evidor Pricing: USD 495 / EUR 449 per license. Volume discount on request.

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.com
Product homepage: http://www.x-ways.net/evidor/
Ordering: http://www.x-ways.net/order.html
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. Evidor is based on WinHex. Idea for Evidor by Jerry Saperstein. Evidor runs on Windows 95, 98, Me; Windows NT 4.0, Windows 2000, and Windows XP.