

Key Highlights

Analyze the most popular file systems

Search e-mail applications and Web browser artifacts simultaneously

Find key evidence from unallocated space

Automate time-consuming tasks

EnCase Forensic has long been the tool of choice by law enforcement, corporate, intelligence and military organizations around the world.

EnCase® Forensic Version 5

The Swiss Army knife of computer forensic solutions

EnCase Forensic has become the industry standard tool for uncovering, analyzing and presenting forensic data. Used by investigators in law enforcement, government, small businesses, consulting firms and corporations, EnCase Forensic provides a robust way to authenticate, search and recover computer evidence rapidly and thoroughly.

Computer evidence recovered with EnCase has been admitted into thousands of court proceedings in several countries and jurisdictions, and the EnCase software has been validated by the courts in several published decisions.

With the launch of Version 5, Guidance Software ensures that EnCase Forensic continues to meet the evolving needs of our customers. Using feedback from government, law enforcement and corporate investigators, we've enhanced nearly every component of EnCase Forensic. The result is an even more powerful tool that speeds up data acquisition and analysis to better support the rigors of criminal investigations and prosecutions.

Enhanced analytical features

A critical component of any investigation involves the analysis of e-mail communications, whether personal, corporate or Internet based. V5 offers enhanced e-mail support for:

- Outlook (PST) and Outlook Express (DBX)
- AOL 6.0, 7.0, 8.0, and 9.0 Personal File Cabinets (PFCs)
- Web-based e-mail formats including Yahoo, Hotmail, and Netscape Mail
- MBOX archives (the de-facto standard used by almost every popular mail reader, on UNIX, Windows and Mac)
- Outlook Newsgroups in DBX

In addition, V5 features Web browsing display support for cached HTML pages from the Internet, as well as detailed access to browsing history.

V5 also offers expanded support for the most popular Web browsers, including Mozilla Firefox, Opera and Apple Safari (Mac OS X default).

And there is expanded file system support for:

- IBM's Journaling File System (jfs and JFS) and AIX LVM8
- TiVo support, including TiVo Series One (Big Endian) and TiVo Series Two (Little Endian)

Acquisition enhancements

The first and most important step in the computer forensic process is the acquisition of the digital media and preserving its evidentiary value. The following improvements are new acquisition options for speed and error handling.

New "Linen" (Linux for EnCase) for bootable forensic CDs:

- Uses a familiar EnCase DOS GUI for drive-to-drive acquisitions, network crossover cable acquisitions and searches across seized media
- Offers the ability to run on a Linux workstation

An enhanced acquisition engine, which now offers:

- A user-designated granularity setting for acquiring hard drives with bad sector(s). Users can adjust variable block sizes up to 16MB in Windows, and set the level to one sector which forces slower acquisitions, but allows for a sector-by-sector read of hard drives with errors.
- Ability to record granularity and compression settings in the evidence file.
- Ability to change evidence file segment size with a quick reacquisition.

Enhanced digital evidence administration

Managing the vast amount of digital evidence in any investigation or inquiry can be cumbersome. The following features go a long way toward making the administrative tasks easier.

V5 can create "logical evidence files" to let examiners:

- Add or extract selected files from across seized media while maintaining the metadata/integrity of the original file, creating a new type of evidence file that contains only those selected files.
- Automatically generates MD5 hash values to authenticate the files of interest added to the logical evidence file.
- Create a logical evidence file container that lets you include multiple logical evidence file acquisitions.

In addition, users can make logical volume notations and edit the names of logical volumes, for easier recognition and improved clarification in the Case view.

About Guidance Software

Guidance Software is the leader in computer investigation and incident response solutions. Founded in 1997 and headquartered in Pasadena, Calif., Guidance Software has offices and training facilities in California, Virginia, New York and the United Kingdom. More than 15,000 corporate and government investigators depend on EnCase software, while more than 3,500 investigators attend Guidance Software's computer investigation methodology training annually. Accepted by numerous courts and honored with eWEEK's Excellence Award and SC Magazine's Annual Award for "Best Computer Forensic Solution." EnCase software is considered the standard computer forensic tool. For more information, visit Guidance Software's Web site at www.guidancesoftware.com

Interface changes and enhancements

The Encase V5 interface has been enhanced to enable better management and analysis of data. These enhancements give examiners and security practitioners quick and easy access to the powerful EnCase toolset. The Enhanced V5 interface, which is based on the V4 GUI, will allow users to:

- Undock selective windows within the interface and view them on separate computer monitors
- View new display tabs for e-mail contents, Web cache contents and Internet history.
- Save keywords locally by case file or globally in the keywords.ini file as sources for searching.

Finally, V5 offers online access to HTML help pages on Guidance Software's Web site, and offline access to local HTML help files via EnCase's Help menu.

These are just a few of the significant additions and enhancements for the initial release of EnCase Forensic V5.

Products

Guidance Software now offers three EnCase Forensic models to meet the needs of law enforcement and government, and corporate, which includes small businesses and consultants:

- Encase Forensic (Law Enforcement and Government)
- Encase Forensic (Corporate)
- EnCase Forensic Deluxe (Corporate)

For more information on how EnCase Forensic V5 can meet your investigative needs, please contact your Guidance Software Inside Sales Representative.

