



THE STANDARD IN COMPUTER FORENSICS

Law enforcement, government, military and corporate investigators depend on the **EnCase Forensic** software to conduct thorough and conclusive computer examinations.

Protecting a company's intellectual property, reputation and shareholder information remains crucial in today's high-stakes business environment.

EnCase Forensic provides a comprehensive set of tools to investigate IP theft and fraud, as well as other employee integrity issues, within a single software interface – while reducing the time examiners spend on individual cases by up to 75 percent.

As the industry-leading tool in computer forensics, EnCase Forensic remains the solution of choice for law enforcement, government, consultants and small businesses around the world. It supports the broadest range of file systems that challenge investigators daily.

EnCase Forensic software has withstood numerous challenges in court on reliability and accuracy. In 2003, the National Institute of Standards and Technology (NIST) certified the EnCase Forensic imaging

engine. In addition, EnCase Forensic provides licensed support for the computer forensic image formats certified by NIST.

EnCase Forensic software has been awarded the prestigious *eWEEK* Excellence Award and *SC Magazine's* Five-Star Rating. No other computer forensic solution has this track record of credibility established by its users, independent organizations and courts.

Advanced productivity features save you valuable time. . .

EnCase Forensic software offers advanced time-saving features to let your investigators be more productive. Examiners can preview data while drives or other media are being acquired. Once image files are created, examiners can search and analyze multiple drives or other media simultaneously, using keyword searches, hash analysis, file signature analysis, file-specific filters and multiple filters.

Forensically sound acquisitions. . .

EnCase Forensic provides the industry's most validated media acquisitions. The solution produces an exact binary duplicate of the original drive or media, then verifies it by generating MD5 hash values for related image files. In addition, it assigns CRC values to the data to reveal when evidence has been tampered with or otherwise altered. The approach has been validated by NIST and has withstood multiple court challenges.

Added flexibility to meet your investigative needs. . .

EnCase products include Enscript[®] programming, a macro-programming language that lets users create custom scripts to automate time-consuming investigative tasks, such as searching and analyzing specific document types. Enscript[®] programming is based on JAVA and C++.

New x64-bit version

Provides improved performance, enhanced multi-threading and the ability to more efficiently use all of your available memory.

EnCase[®] Forensic

allows investigators to easily manage large volumes of computer evidence, by viewing all relevant files, including "deleted" files, file slack and unallocated space.

FEATURES

■ Case Indexer

Builds a complete index of English and foreign language words with a new patent-pending technology that permits fast and easy query for keywords by non-computer forensic investigators. The indices can be chained together to find possible keywords common in other investigations. The Unicode-supported index is built from the contents of personal documents, deleted files, file system artifacts, file slack, swap files, unallocated space, emails and web pages.

■ Native viewing for almost 400 file formats

Native document viewing allows you to see files within EnCase, as if they were in their native applications. You no longer have to export to third-party tools. You can print, bookmark and copy/paste for almost 400 different file formats. This significantly reduces the number of false positives during searches.

■ Broader file system support

Supports the widest range of file systems, including Windows FAT12 (Floppy), FAT16, FAT32, NTFS; Macintosh HFS, HFS+; Sun Solaris UFS; Linux EXT2/3; Reiser; BSD FFS, FreeBSD's Fast File System 2 (FFS2) and FreeBSD's UFS2; Novell's NSS and NWFS; IBM's AIX jfs, JFS and JFS with LVM8; TiVo Series One and Two; CDFS; Joliet; DVD; UDF; ISO 9660; and Palm. Coming soon: HP-UX (vxfs).

■ Expanded email support

Interprets the largest number of email formats, including Outlook PSTs /OSTs ('97-'03), Outlook Express DBXs; Microsoft Exchange EDB Parser; Lotus Notes v6.0.3, v6.5.4 and v7; AOL 6.0, 7.0, 8.0 and 9.0 PFCs; web-based email formats including Yahoo, Hotmail, Netscape Mail and MBOX archives (the de facto standard used by almost every popular email reader on UNIX, Windows and Mac).

The newly enhanced email support now includes the ability to display deleted emails, notes, contacts and calendar entries for PSTs and OSTs. In addition, you can now copy/insert email messages to the popular msg format for external review.

■ Internet browser support

The solution also decodes the user's Web-browsing history and reveals cached HTML pages and associated images. It supports Microsoft Internet Explorer, Mozilla Firefox, Opera and Apple Safari (Mac OS X default).

■ Flexible acquisition options

Provides the ability to image media using multiple operating systems, allowing flexibility and time savings when dealing with difficult acquisitions. The solution supports imaging in Windows, DOS and Linux, and has several options for compression, speed and error handling.

■ Expanded timeline views

Provides a "Calendar View" of all file activity, showing when files were created, last written or accessed. The calendar scales across months and years to help examiners see patterns of file activity.

■ Detailed reports

Generates detailed information on specific files, folders, volumes, physical disks and cases. View data about the acquisition, drive geometry, folder structures and bookmarked files and images. Export reports in RTF or HTML formats.

CHOOSE THE CORPORATE DELUXE PACKAGE FOR EXPANDED FUNCTIONALITY

As part of your EnCase Forensic Corporate Deluxe package, you receive the powerful functionality of our Guidance Software modules, which can dramatically improve your productivity:

FastBloc® SE (Software Edition) Module

FastBloc SE is a new write-blocking software solution for Windows acquisitions of USB, FireWire, IDE and SCSI media. The module lets examiners "write-block" suspect drives and other media to preserve evidence without adding time-consuming hardware solutions. In addition, this solution provides the ability to reach Host Protected Areas (HPAs) and Device Configuration Overlays (DCOs) on IDE and SATA hard drives.

EnCase Decryption Suite (EDS) Module

Saves time and improves productivity when dealing with decryption and password recovery tasks. Examiners can access encrypted files and folders by the NTFS Encrypting File System (EFS) and retrieve protected password information from the Windows Registry.

EnCase Physical Disk Emulator (PDE) Module

Eliminates the hours-long chore of restoring evidence from one hard drive to another. The solution lets examiners mount computer evidence as local disks for further examination using VMware and other third-party tools.

EnCase Virtual File System (VFS) Module

Lets examiners mount computer evidence as a read-only, off-line network drive for further examination using Windows Explorer and other third-party tools, e.g., password crackers and virus, malware and steganography detectors.

CD/DVD Module

Eliminates the time-consuming task of producing evidentiary findings and media archives. Examiners can acquire, analyze or create logical evidence files while verifying the data and archiving the media to CD or DVD. EnCase reports, bookmarks and notes can also be archived directly to CD or DVD.

NOTE:

The EDS, PDE, and VFS modules are also available in the EnCase Forensic Professional Suite and are provided as part of the Premium License Support Program.

ABOUT GUIDANCE SOFTWARE

Founded in 1997, Guidance Software is recognized worldwide as the industry leader in digital investigation solutions. Its EnCase® solutions provide the foundation for both law enforcement and corporate enterprise investigations that enable corporate, government and law enforcement agencies to conduct effective computer investigations of all types, respond promptly to eDiscovery requests, and conduct rapid and thorough internal investigations involving digital evidence, all while maintaining the forensic integrity of the data. More than 20,000 investigators depend on EnCase software, and nearly 4,000 investigators attend Guidance Software's forensic methodology training annually. Validated by numerous courts worldwide, EnCase is also frequently honored with top security awards from *eWEEK*, *SC Magazine*, *Network Computing* and others.

For product and service information please visit:
<http://www.guidancesoftware.com/products/index.asp>