EnCase® Forensic Features and Functionality

Every Investigation Matters

Digital investigators need a solution that easily captures relevant data to support an investigation or compliance requirement and features sophisticated technical analysis capabilities for finding buried and/or hidden data. EnCase® Forensic is a powerful investigation platform that collects digital data, performs analysis, reports on findings and preserves them in a court validated, forensically sound format.

How EnCase® Forensic Works:

1) Obtain Forensically Sound Acquisitions

EnCase® Forensic produces an exact binary duplicate of the original drive or media, then verifies it by generating MD5 hash values for related image files and assigning CRC values to the data. These checks and balances reveal when evidence has been tampered with or altered, helping to keep all digital evidence forensically sound for use in court proceedings.

2) Save Valuable Time with Advanced Productivity Features

Examiners can preview data while drives or other media are being acquired. Once the image files are created, examiners can search and analyze multiple drives or other media simultaneously. EnCase Forensic also features a case indexer. This powerful tool builds a complete index in multiple languages, allowing for fast and easy queries. Indices can also be chained together to find keywords common to other investigations. This Unicode-supported index contains personal documents, deleted files, file system artifacts, file slack, swap files, unallocated space, emails and web pages. In addition, EnCase has extensive file system support, giving organizations the ability to analyze all types of data.

3) Customize EnCase® Forensic with EnScript® Programming

EnCase forensic features EnScript® programming capabilities. EnScript, an object-oriented programming language similar to Java or C++, allows users create to custom programs to help them automate time-consuming investigative tasks, such as searching and analyzing specific document types or other labor-intensive processes and procedures. This power can be harnessed by any level of investigator by using one of Forensics tools, such as the “Case Developer” or one of the numerous built-in filters and conditions.

4) Provide Actionable Data, Report on it, and Move on to the Next Case

Once investigators have bookmarked relevant data, they can create a report suitable for presentation in court, to management or to another legal authority. Data can also be exported in multiple file formats for review.

Guidance® SOFTWARE
The World Leader in Digital Investigations™

EnCase Forensic Features and Functionality Checklist

Acquisition

- ☐ Acquisition Granularity:
  - o Errors: Specify the number of sectors that get zeroed when an error is found.
  - o Acquisition Blocks: Define the block size.
- ☐ Acquisition Restart: continue a windows-based acquisition from its point of interruption.
- ☐ Logical Evidence Files: an evidence container with only the files or folders you need.
- ☐ CRC: image verified by cyclical redundancy checksum (CRC) and MD5
- ☐ LinEn utility - acquire evidence via boot disk
- ☐ WinEn utility – acquire RAM evidence

Automation Tools - Speeds the investigation process.

- ☐ EnScript: write scripts or use the pre-built scripts
- ☐ Filters and Conditions: more than 150 available
- ☐ Combine filters to create complex queries using simple “OR” or “AND” logic
- ☐ Active Directory Information Extractor
- ☐ Hardware Analysis: automatically culls through the registry and configuration files
- ☐ Recover partitions: automatically rebuilds the structure of formatted NTFS and FAT volumes.
- ☐ Recover deleted files/folders

Analysis Features

- ☐ Windows event log parser
- ☐ Link file parser – find in unallocated space
- ☐ Compound (e.g., zipped) document and file
- ☐ File Signature analysis
- ☐ Hash analysis
- ☐ File finder – find files in unallocated space

Viewers

- ☐ Native viewing for ~400 file formats
- ☐ Built-in Registry Viewer
- ☐ External File Viewers
- ☐ Integrated Picture Viewer with Gallery View
- ☐ Timeline/Calendar viewer

Searching

- ☐ Unicode index search - search extracted text of docs
- ☐ Binary search – search raw binary data
- ☐ Proximity Search
- ☐ Internet and email search
- ☐ Case Sensitive • GREP • Right to Left Reading
- ☐ Active Code Page: keywords in many languages.
- ☐ Big Endian/Little Endian, UTF-8/UTF-7
- ☐ Search file slack and unallocated space

Reporting - Automatic Reports

- ☐ Listing of all files and folders in a case
- ☐ Detailed listing of all URLs and corresponding dates and times of web sites visited
- ☐ Document incident response report
- ☐ Log Records
- ☐ Registry
- ☐ Detailed hard drive information about physical and logical partitions
- ☐ View data about the acquisition, drive geometry, folder structures and bookmarked files and images.
- ☐ Export reports in RTF or HTML formats.

Bookmark Features

- ☐ Highlighted Data
- ☐ Notes
- ☐ Folder Information
- ☐ Notable Files
- ☐ File Groups

Internet and Email Investigation

Browser History Analysis

- ☐ Internet artifacts
- ☐ WEB History & cache analysis
- ☐ HTML carver
- ☐ HTML page reconstruction
- ☐ Kazaa toolkit
- ☐ Instant Messenger toolkit - Microsoft® Internet Explorer, Mozilla Firefox, Opera and Apple Safari

Email Support Includes

- ☐ 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
- ☐ Yahoo
- ☐ Hotmail
- ☐ Netscape Mail
- ☐ MBOX archives

System Support

- ☐ Hardware and software RAIDs.
- ☐ Dynamic disk support for Windows 2000/XP/2003 Server
- ☐ Interpret and analyze VMware, Microsoft Virtual PC, DD and SafeBack v2 image formats.
- ☐ File systems: Windows FAT12/16/32, NTFS; Macintosh HFS, HFS+; Sun Solaris UFS, ZFS; Linux EXT2/3; Reiser; BSD FFS, FreeBSD’s Fast File System 2 (FFS2) and FreeBSD’s UFS2; Novell’s NSS & NWFS; IBM’s AIX jfs, JFS and JFS with LVm8; TiVo Series One and Two; CDFS; Joliet; DVD; UDF; ISO 9660; and Palm

About Guidance Software (GUID)

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® platform provides the foundation for government, corporate and law enforcement organizations to conduct thorough, network-enabled, and court-validated computer investigations of any kind, such as responding to eDiscovery requests, conducting internal investigations, responding to regulatory inquiries or performing data and compliance auditing - all while maintaining the integrity of the data. There are more than 27,000 licensed users of the EnCase technology worldwide, and thousands attend Guidance Software’s renowned training programs annually. Validated by numerous courts, corporate legal departments, government agencies and law enforcement organizations worldwide, EnCase has been honored with industry awards and recognition from eWEEK, SC Magazine, Network Computing, and the Socha-Gelbmann survey. For more information about Guidance Software, visit www.guidancesoftware.com.