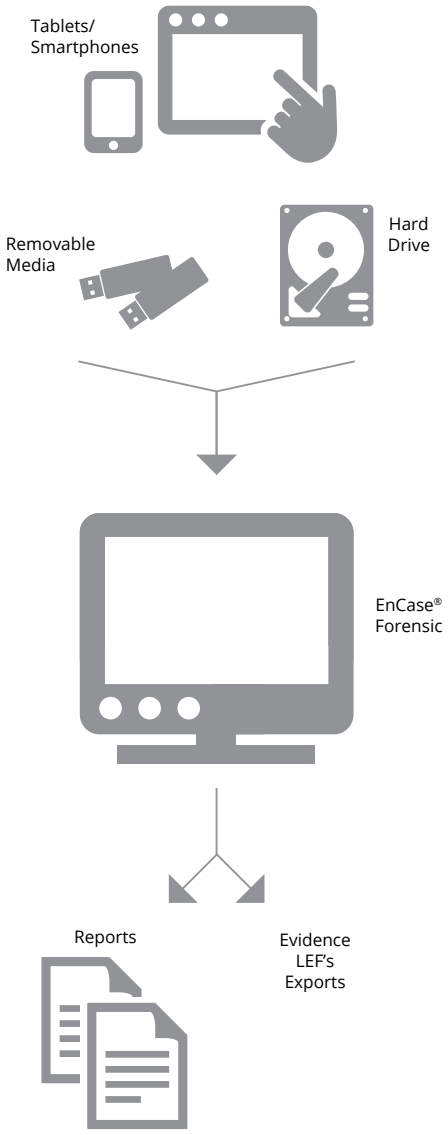
GUIDANCE SOFTWARE

EnCase® Forensic
TRANSFORM YOUR INVESTIGATIONS

Features and Functionality

EnCase Forensic v7 introduces features and capabilities designed with one clear objective: increase the examiners efficiency and effectiveness. To achieve this objective a new workflow-driven approach to forensics has been incorporated into EnCase Forensic v7. With this new workflow, examiners can automate common tasks, complete comprehensive searches, identify relevant items, and create compelling reports faster than ever before. This approach can be easily adapted to conform to any organization's need. This is a revolutionary change that will transform how forensic investigations are completed.



EnCase Forensic v7's New Approach to Digital Forensics:

Acquire Evidence: The key to acquiring forensically sound evidence is the method used to capture it. With EnCase Forensic, examiners can be confident the integrity of the evidence will not be compromised. All evidence captured with EnCase Forensic is stored in the court accepted EnCase evidence file formats. These formats (EO1 and L01) are widely held as the de facto standard forensically sound evidence containers. In version 7, the new evidence files (Ex01 and Lx01) can now be encrypted directly within EnCase Forensic, adding another level of security to the most trusted evidence file format in the industry.

Process Evidence: As the amount of evidence in each case increases, examiners need speedy, reliable processing capabilities in order to complete their investigations efficiently. In v7, the EnCase Evidence Processor gives examiners the ability to automate common tasks required to prepare the collected evidence for the investigation. This highly configurable processing engine can be tailored to meet any examiners needs. By adding custom EnScripts to the processor, examiners can eliminate the need to review EnScript results separately. Now, the result of those invaluable EnScripts can be indexed allowing for unified search and review of all evidence from one, easy to use interface.

Perform Deep Forensic Analysis: EnCase Forensic is known for its ability to uncover evidence that may go unnoticed if analyzed with other solutions. With version 7, this deep forensic analysis ability has been improved yet again. EnCase now supports analysis of EXT4 and HFSX file systems, Office 2010 files, Checkpoint/Pointsec encrypted drives, and iOS physical images. In addition to this expanded support, email investigations take a significant step forward with v7. The new email investigation platform makes performing email investigations as easy as reviewing emails in an inbox. With a streamlined interface and features enabling email conversation and related message analysis, examiners can perform succinct email investigations faster than ever before.

Compile Findings: A completed case is only as good as its final report. In v7 the reporting capabilities take a quantum leap forward. Using customizable templates, examiners can create compelling, easy to read, professional reports for every case. With easily configurable reporting capabilities, examiners can craft templates for any type of case, audience, and purpose. Once configured, these templates can be used for any case, ensuring the quality of reports can be consistent across an examiners entire caseload.

Archive Case: To ensure examiners have everything they need when a case needs to be reviewed in the future, EnCase Forensic v7 has a built in archiving capability. When a case is completed, the examiner can, with just a few clicks, archive the evidence, findings, and reports associated with the case, ensuring everything remains intact.

EnCase Forensic v7 Features at a Glance

Version 7 of EnCase Forensic represents a step change in the art and science of digital forensics. Here are just a few of the major improvements and new capabilities examiners will see in EnCase Forensic v7.

Acquisition

Smartphone and Tablet support: Acquire data from devices running the following operating systems

- Apple's iOS
- Google's Android™ OS
- Rim's Blackberry™ OS
- HP's Palm™ OS
- Nokia Symbian
- Microsoft's Windows Mobile OS

Native Encryption support: Encrypt evidence files directly in EnCase Forensic v7, using AES-256 strength encryption

Improved Evidence File Format: The new and improved Ex01 and Lx01 file formats, built on the trusted E01 and L01 formats, bring increased performance and optimized data management

Processing

EnCase Evidence Processor: Automate common tasks associated with preparing evidence for investigation, includes:

- Recover Folders
- File Signature Analysis
- Protected File Analysis
- Hash Analysis (MD5 and SHA-1)
- Expand compound files
- Find Email (PST, NSF, DBX, EDB, AOL, MBOX)
- Find Internet Artifacts (IE, Firefox, Safari)
- Search for Keywords
- Index

EnScript Module Processing: v7 incorporates the following modules by default in the processor

- System Info Parser
- IM Parser (AOL, MSN, Yahoo)
- File Carver
- Personal Information (CC, Phone Numbers, Email, SSN)
- Windows Event Log Parser
- Windows Artifact Parser
- Unix Login
- Linux Syslog Parser

Custom EnScript Module Processing: Add custom EnScripts into the EnCase Evidence Processor

New Indexing Engine: Optimized for the forensic examiners needs with robust query language.

Deep Forensic Analysis

New Supported Files: The following new file systems and file types are supported

- EXT4
- HSFX
- Microsoft Office 2010
- iOS Physical Images (iPad, iPhone, iPod)

New Encryption Support: Now supporting Checkpoint/Pointsec Full Disk Encryption. Existing encryption product support updated.

New E-Mail Investigation Platform: Email investigations are now as easy as reading email in an inbox. Added capabilities to review e-mail conversations and related messaged to uncover context and identify all individuals related to the case.

Tagging: Create custom tags and apply to any file, including hash records, to enable easy export of files for review by others.

Unified Search: Now search across the entire case from one easy to use, flexible, and powerful search interface. Incorporate the index, keyword search results, and tags into a single search.

Reporting

Customizable Templates: Create custom report templates for consistent reporting for every case.

Formatting: Choose formatting for each section of the report, tailoring the representation of finding to meet the audiences needs.

Easy Export Options: Save reports in any of the following formats:

- Text
- RTF (opens in Microsoft Office)
- HTML
- XML
- PDF

Built-In Smartphone Report: Predefined Smartphone report, displaying detailed information about the evidence acquired from a Smartdevice. Report includes ability to export KML data.

About Guidance Software

At Guidance, we exist to turn chaos and the unknown into order and the known—so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. Makers of EnCase®, the gold standard in digital investigations and endpoint data security, Guidance provides a mission-critical foundation of applications that have been deployed on an estimated 25 million endpoints and work in concert with other leading enterprise technologies from companies such as Cisco, Intel, Box, Dropbox, Blue Coat Systems, and LogRhythm. Our field-tested and court-proven solutions are used with confidence by more than 70 of the Fortune 100 and hundreds of agencies worldwide. Get to know us at guidancesoftware.com.