

ENCASE FORENSIC V7 AT A GLANCE

EnCase® Forensic v7 represents a leap forward in terms of ease of use, customization, extensibility, and scalability. Investigators are increasingly facing larger data sets, diverse technologies, case backlogs, and tighter budgets. EnCase Forensic v7 is specifically engineered to handle these critical challenges by integrating more tools and technologies, supporting more operating systems and applications, and providing investigators the ability to easily modify and adapt EnCase Forensic v7 to their workflow and investigative process.

Version 7 is designed to handle the new challenges for investigators today and in the future. The EnCase Forensic platform seamlessly integrates with other forensic tools to make it faster and easier to analyze evidence from smartphones, tablets, internet chat, and other technologies in one interface. In addition, the processing and indexing engines now handle evidence more quickly and allow users to control how potential evidence is processed. Further, investigators can configure the vsoftware; from building hash libraries, to creating word searches, to customizing report templates, to adding EnScripts® and third-party apps from EnCase® App Central—each improvement investigators add makes Version 7 a more powerful and efficient investigative tool.

The Standard in
Digital Investigations



What's New in Encase Forensic Version 7

Remote Forensic Capability: Remote Forensic Capability provides investigators the ability to preview and collect from a remote computer quickly and easily. Lets you discreetly and directly access a suspect's hard drive or RAM. The investigator is able to triage and/or acquire an image of individual files, directories, partitions, or physical devices as well as physical memory and process memory.

Distributed Processing: Distribute the processing of evidence across one or multiple machines in a lab with EnCase Forensic v7. Exploding case loads and growing data sets have increasingly challenged investigators over the past several years. Now you can use idle machines in the lab to handle processing while leaving primary machines free for investigation and analysis.

Evidence Processor Manager: The Evidence Processor Manager allows investigators to handle the distribution and control of evidence processing for one or more EnCase Examiner machines or EnCase Processor nodes. Investigators can simplify, automate and increase the speed of evidence processing and acquisition by:

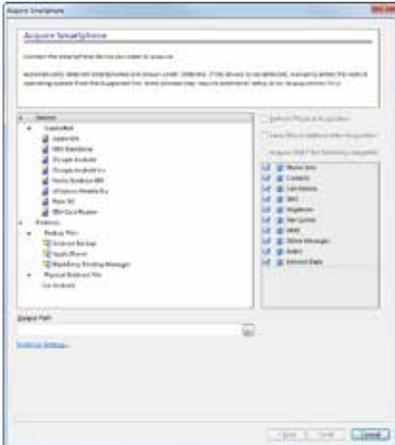
- Distributing the processing workload across multiple machines
- Queuing evidence in the jobs list to be processed
- Prioritizing the execution of evidence to be processed
- Monitoring the processing progress of evidence.

Not only does the Evidence Processor Manager give you full control of how your evidence is processed, it also optimizes system resources to process the data more efficiently, significantly increasing processing speeds.

Integrated Smartphone and Tablet Module: The Smartphone and Tablet module is integrated in Version 7 and is included with the software. The module provides support for physical and logical Android acquisitions including Kindle Fire as well as the latest versions of Android like Jelly Bean and Ice Cream Sandwich.

The module also supports logical acquisitions of iOS devices, including the latest iPhone and iPads, as well as other popular models of smartphones and tablets, including Blackberry, Samsung, and more. The Smartphone and Tablet Module has a reporting feature which lists the relevant data instantly including the number of text, SMS messages, email, pictures, call history, and more.

External Review Package: The External Review Package allows investigators to share the evidence that they tag and bookmark with non-EnCase Forensic users such as co-investigators, attorneys, field agents, or other interested parties. Outside parties can not only view the actual evidence in its native format, but also add descriptive tags that can be imported directly back into EnCase.



Improved Search and Index Features: Users can search across the entire case from one easy-to-use, faster, flexible, and more powerful search interface. Users have the ability to search across diverse types of information including email, system, and user-generated files, smart-phones, and any other data in one results view. Index searches scour the evidence for matching content and file metadata using robust syntax queries, with near instantaneous search times. Also, because the Evidence Processor is recursive, all files, emails, and module output are indexed.

Further, EnCase Forensic provides three principal methods of searching through the evidence: Index Searches, Tag Searches and Keyword Searches through Raw Data. This process incorporates the index, keyword, and tags search results into a single tab allowing easier review of each piece of evidence independently or in the aggregate. The searches results are comprehensive across the three search methods and each search can be saved as part of the case.

EnCase® App Central

EnCase App Central has the goal of providing functionality and efficiency to EnCase users by offering EnScripts®, templates, and third-party apps. This one-stop shop allows investigators to find EnScripts or apps that were previously scattered among thousands of websites and blogs.

Separate Processor License: The purchase of EnCase Forensic gives you access to a separate processor license. Thus, the processor license can now be dedicated solely to processing evidence on an alternative machine. With this added capability, organizations can simultaneously review and analyze evidence in one case and process evidence in another.

Case Analyzer: Case Analyzer lets you click on one button to quickly view dozens of automated reports. The reports instantly provide user-generated activity such as browser history, cookies, logon information, and more. The reports are driven by metadata and each piece of evidence can be bookmarked just as if it was identified in a traditional search in EnCase Forensic.

Iterative and Prioritized Processing: Two new enhancements have been made concerning how investigators choose to process an evidence file. First, you can select which tasks they would like to run from the evidence processor. Second, you can also choose to process different files at different times. In the same way users can choose how the files are processed, users can also select which files are processed, allowing critical files to be processed first.

Customizable Processing Templates: Investigators can set up and run key processing tasks needed to analyze a case, including Signature Analysis, Hash Analysis, Indexing, Email Parsing, Internet History, Event Log Parsing, System Information and more; while saving the selections into a template.

Enhanced Email Review Feature: Email review enhancements now feature an interface that is similar to that of the original email program. Investigators can easily show or remove duplicate emails to streamline conversations for straightforward review. Email threads can be tracked across devices in the case by the email header or subject line.

Customizable Report Templates: The new report templates in Version 7 are geared to be easily customized. Adding hyperlinks, photos, evidence metadata, and other fields is easy in the HTML report templates.

Includes Module Support for:

- EnCase Decryption Suite
- Physical Disk Emulator
- Virtual File System
- FastBlock SE

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.

Guidance Software®, EnCase®, EnScript®, EnCE™, EnCEP™, Linked Review™, EnPoint™ and Tableau™ are trademarks owned by Guidance Software and may not be used without prior written permission. All other trademarks and copyrights are the property of their respective owners.