



Field Intelligence Model

Detailed Product Description

Using Volatile Data to Enhance Investigation with EnCase® Snapshot*

- The ability to immediately capture volatile data helps investigators quickly identify the state of a machine. Investigators can use this information in a number of important investigative activities:
 - Quickly assess detailed information about applications running at the time of seizure.
 - Determine what the machine was doing and what it was communicating with.
 - Assess the current state of the machine by allowing the quick isolation, identification and assessment of breaches when the issue relates to hacking activity.
 - Counter "trojans" by identifying running processes, open ports and other volatile data.

Volatile Data Capture with Snapshot:

Volatile data exists in the memory (RAM) of a server or workstation. If power is lost, or if a system fault occurs, the data is lost. By contrast, static data is stored on hard drives, USB devices and CDs, for example, and is typically not lost when a machine is powered down. Computers track numerous items that are critical during computer intrusion/incident response activities, including users on a system, TCP and UDP port information, open files, running processes and applications, and system resources. Snapshot captures this volatile data and provides easy to use information on what was occurring on a system at a given point in time.

Volatile Data Harvested by Snapshot:

Open Ports

Open ports are those currently in use or waiting for use by an application or operating system. Open port information helps the investigator understand who or what is communicating with a system at a particular point in time.

Active Processes, including driver and service enumeration

Active processes are those currently running on a system at a point in time. This information is critical when trying to identify if rogue, hidden, unknown, or unauthorized processes, services or drivers are active and running on a system.

Open Files

Open files are those currently in use on a system. Understanding which files are open shows an examiner what information a perpetrator or application is accessing.

Live Windows® Registry

Live registry are registry hives that are only active while the Windows machine is running. EnCase can quickly harvest valuable information from the live registry, so examiners can extract and assess data from the Windows live registry of multiple systems.

Network Users

Network users shows all the users who have logged onto a machine, including the user name, security ID, and last date and time of login.

Network Interfaces

These are the network cards and supporting IP information that could be relevant during an incident response or audit. Harvested information includes interface card manufacturer, the assigned IP address, MAC address and subnet mask.

dll Injection/Hidden Process/Rootkit Detection

These days, savvy hackers increasingly rely on advanced technology to compromise corporate networks. These tools let intruders operate — and return anytime they like — completely unseen, and they essentially "own" your network. EnCase® Enterprise offers the only available commercial-grade solution to find and remediate those threats. It peers deeply into your operating systems to identify and destroy injected dlls, hidden processes and hooks used by rootkits — even when hackers go to great lengths to remain invisible.

*The EnCase Snapshot capability is sold separately.

Operating System and File System Support

Two major attributes that make EnCase® software unique are the breadth of operating systems and file systems supported. For each operating system that exists there are a number of different file systems which the host operating system could utilize. The operating system and file system are separate but do have a deep relationship on how information is stored and how the host operating system operates with the file system. The ability to deeply analyze a broad range of operating system and file system artifacts is a critical component of enterprise investigations. EnCase software has the ability to interpret all of the file systems, over the network, for which a Servlet has been developed (currently Windows, Linux, Solaris, AIX and OSX operating systems; support for additional file systems is on the way). In addition, EnCase software can also interpret a number of file systems for which there is currently no Servlet developed.

- Operating systems on which the EnCase Servlet runs: Windows 95/98/NT/2000/XP/2003 Server, Linux Kernel 2.4 and above, Solaris 8/9 both 32 & 64 bit, AIX, OSX.
- File systems supported by EnCase software: FAT12/16/32, NTFS, EXT2/3 (Linux), Reiser (Linux), UFS (Sun Solaris), AIX Journaling File System (JFS and jfs) LVM8, FFS (OpenBSD, NetBSD and FreeBSD), Palm, HFS, HFS+ (Macintosh), CDFS, ISO 9660, UDF, DVD, and TiVo® 1 and TiVo 2 file systems.
- EnCase software uniquely supports the imaging and analysis of RAID arrays, including hardware and software RAIDs. Forensic analysis of RAID sets is nearly impossible outside of the EnCase environment.
- Dynamic Disk Support for Windows 2000/XP/2003 Server.
- Ability to preview and acquire select Palm devices.
- Ability to interpret and analyze VMware, Microsoft Virtual PC, DD and SafeBack v2 image formats.

Previewing: Nodes Searching Before Acquisition

One of the most powerful capabilities of the EnCase® Field Intelligence Model is the ability to "preview" a running computer over a LAN, WAN or crossover network connection. A preview is the process of securely reaching across the network connection to a running system that has the Servlet loaded into memory and remotely viewing all data on a target machine in a forensically sound fashion. Conducting a remote preview does not alert the user nor does it make changes to the machine being investigated. This critical capability enables investigators to quickly determine whether relevant evidence or suspect artifacts exist on a computer before having to acquire it.

Examiners are often faced with numerous pieces of media from different operating systems, file systems, servers, and/or severe time constraints. Because of this, preview is the only means possible to effectively determine if a computer contains relevant evidence. All of the investigative features of EnCase can be used during the preview process, including keyword searches, Snapshot, filtering, automated scripts, hashing and file signature analysis. The preview function can be used to perform complete investigations with ease across a number of different file systems, operating systems and hardware configurations. Its capability to preview, analyze and acquire when necessary makes the Field Intelligence Model a true mobile investigative solution.

Preview the following data:

- unallocated space
- allocated space
- deleted files
- file slack
- file system attributes
- RAID arrays
- CD ROMs/DVDs
- mounted FireWire and USB devices
- mounted encrypted volumes

Acquisition

The EnCase® acquisition process begins with the creation of a complete, physical bitstream image of a subject drive or drives in a completely noninvasive manner. The EnCase evidence file is an exact duplicate of the data as it existed during the time of acquisition. Throughout the acquisition process, the bitstream image is continually verified by Cyclical Redundancy Checksum (CRC) blocks, which are calculated concurrent to the acquisition. At the completion of the acquisition process, a second validation check, called a Message Digest 5 (MD5) hash, is performed over the entire data set acquired, and it is embedded as part of the evidence file for validation of the acquired media.

- **Acquisition Read Ahead:** (For EnCase Field Intelligence Model and EnCase Enterprise) This unique capability caches blocks of data ahead of time during the acquisition process so that data is available on the remote node when needed, thereby decreasing acquisition times considerably.

- **Acquisition Granularity:** Examiners have more control over the way hard drive data is acquired.
 - Errors: Historically, when a read error is found on a hard disk, the entire block of data containing the read error is zeroed out. With EnCase Enterprise, you have the flexibility to specify the number of sectors that get zeroed when an error is found.
 - Acquisition Blocks: Examiners can define the amount of data to acquire during an acquisition operation, ensuring the fastest acquisition rates possible.
- **Acquisition Restart:** Examiners can continue a Windows-based acquisition from its point of interruption, and not have to reacquire the entire device from the beginning.
- **Auto Acquisition:** (For EnCase Field Intelligence Model and EnCase Enterprise) This lets examiners specify a machine by hostname or IP address to automatically acquire once it is present on the corporate network. Auto acquisition can be configured to check for its target list of machines on a scheduled basis.
- **Logical Evidence Files:** These let you selectively choose exactly which files or folders you want to preserve, instead of acquiring the entire drive. Unlike copying files from a device and altering critical metadata, logical evidence preserves the original files as they existed on the media and include a wealth of additional information such as file name, file extension, last accessed, file created, last written, entry modified, logical size, physical size, MD5 hash value, permissions, starting extent and original path of the file.

EnCase LinEn Utility: The LinEn utility is a Linux version of the industry-standard DOS-based EnCase acquisition tool. While it performs the same basic function as the DOS version, it overcomes a number of Linux limitations, such as non-Windows operating systems, extremely large hard drives and acquisition speed.

EnCase Evidence File (Preservation)

The EnCase® Evidence File is a proprietary file created by EnCase to compress and preserve bitstream images of acquired media. The EnCase Evidence File is widely known throughout the law enforcement and computer security industries. It has been accepted by courts to the federal appellate level and around the world. For court decisions related to EnCase software, please visit the Legal Resources page.

Powerful Analytical Functionality

The ability to analyze and search large amounts of data quickly and easily is a critical capability of any incident response, computer investigation or analysis tool. EnCase software offers the most advanced, comprehensive and easy-to-use tool to carry out these complicated and time-consuming tasks, across multiple file systems and languages.

Automated Analysis: SweepCase lets examiners automatically choose the types of analysis they want to perform on a set of media instead of having to initiate each tool separately.

Multiple Sorting Fields: Examiners can sort files according to 30 different fields, including all four time stamps (File Created, Last Accessed, Last Written and Entry Modified), file names, file signatures and extensions, hash value, full path, permissions.

Filters and Filter Conditions: Filters let the examiner reduce the amount of information displayed, based on user-specified criteria. More than 150 filters are provided with EnCase software, ranging from deleted files to password-protected Word documents.

Queries: Examiners can combine filters to create complex queries using simple "OR" or "AND" logic.

View "Deleted" Files and Other Unallocated Data in Context: EnCase offers a Windows-Explorer-type view of deleted and unallocated data. This includes file slack, swap files, print spooler data and all other unallocated data files.

International Language Support: EnCase supports Unicode data decoding and can search and display any language that Unicode supports. This allows examiners to search and view data in its native format such as German, Arabic or Kanji.

Encrypted Volumes and Hard Drive Encryption: EnCase can analyze and acquire mounted encrypted volumes, such as PGP and DriveCrypt, and give examiners full access to data on hard drives that are wrapped with encryption technology, such as SafeBoot.

Link File Examination: This automated process reads all forms of link (.lnk) files — both allocated and unallocated — and decodes the results for quick and easy analysis. Being able to quickly discover and interpret link files gives the examiner valuable information, such as learning that a suspect is transporting company data onto a thumb drive or external media, or what files, applications and shares the suspect commonly used.

Active Directory Information Extractor: The Active Directory Information Extractor forensically analyzes the Active Directory database (NTDS.DIT) and extracts the username, SID, home directory, email address, last login, last failed login and next password change.

Hardware Analysis: Automatically culls through the registry and configuration files to quickly identify the types of hardware installed on a target machine, including NIC cards, FireWire devices, thumb drives, IDE devices and other hardware information.

Recover Folders: Automatically rebuilds the structure of formatted NTFS and FAT volumes.

Log and Event File Analysis: EnCase provides a single means by which to analyze, search and document log and event file data.

Symbolic Link Analysis: EnCase gives access to and analysis of symbolic link information to simplify analysis of UNIX-based file systems.

Compound Document and File Analysis: Many files — such as Microsoft Office documents, Outlook PSTs, TAR, GZ, thumbs.db and ZIP files — store internal files and metadata that contain valuable information once exposed. EnCase automatically displays these internal files, file structures, data and metadata. Once these files have been virtually mounted within EnCase, they can be searched, documented and extracted in a number of different ways.

File Signature Analysis: EnCase can automatically verify the signature of every file it searches and identify those modified extensions.

Hash Analysis: EnCase can automatically create hash values for all of the files in a case.

Built-in Registry Viewer: The integrated registry viewer organizes the registry data file into folders, giving examiners an expedient and efficient way to view the Windows registry and determine values.

External File Viewers: Occasionally, an examiner will find file types that EnCase does not have the built-in capabilities to view (such as an MP3 or AVI file), or examiners might want to view a file type that EnCase does support with a third-party tool or program. In either situation, EnCase can be enhanced quickly to use external file viewers, easing the analysis of foreign file types and allowing the use of native applications from the source machine.

VMware Analysis: EnCase can analyze VMware (.vmdk) data files. It interprets the data files that compose the physical and logical structure of the virtual hard drive, including unallocated space, which enables quick and thorough analysis of VMware.

Single File: You can quickly analyze individual logical files that contain a number of external files. Sometimes relevant files exist on shared servers, loose files from a thumb drive, files on a CD or a PST from the mail server. Once added into the Examiner, these single files can be analyzed and acquired into Logical Evidence Files, then added to the case for future reference and preservation.

File Finder: This feature automatically searches through the page file, unallocated clusters, selected files or an entire case, looking for predefined or custom file types. This feature differs from the standard search, because it looks through the defined areas for the file header information and sometimes the footer.

Search Technologies

The powerful EnCase® search engine can locate information anywhere on physical or logical media.

Proximity Search: This feature searches through all files in a case for a specific keyword and returns the responsive documents with the keyword and a specified number of bytes surrounding it. This is a critical function when trying to add context around the information you are searching for.

Internet and Email Search: This feature will find, parse, analyze and display various types of Internet and email artifacts across machines. The Internet and email search finds mail formats (such as Hotmail, Outlook, Lotus Notes, Yahoo, AOL, Netscape, mbox and Outlook Express) and Internet artifacts from Internet Explorer, Mozilla, Opera and Safari.

Search Options: In addition to the standard search feature, EnCase software offers a number of options that can be used to search through data:

- **Case Sensitive:** The keyword will be searched for, but only in the exact case specified in the text box.

- **GREP:** The keyword is a regular expression to search, using the Global Regular Expressions Post (GREP) advanced searching syntax.
- **RTL Reading:** This will search for the keyword in a right-to-left sequence for international language support.
- **Active Code Page:** This lets you enter keywords in many different languages.
- **Big Endian/Little Endian Unicode/UTF-8/UTF-7:** EnCase software allows examiners to search using multiple Unicode standards as opposed to ASCII. This enables investigators to search for keywords with international language characters.

Logical File Recognition: Files often span noncontiguous clusters and EnCase software can search all such allocated files. Without EnCase software, if you search Windows text files using a forensic utility that cannot logically search across data clusters, you'll often miss search hits or receive inaccurate search results.

Documentation and Reporting

EnCase® Enterprise lets users define with detailed granularity what information is presented and how it is presented, depending on the purpose and target audience of the investigation. Almost all information revealed by EnCase software can be exported into various file formats for external reporting and analysis purposes.

Automatic Reports: Since the requirement to generate reports is so critical, EnCase has a number of automatically generated reports that can be created. These automated reports show a wealth of information depending on the type being generated. Here are some examples:

- Listing of all files and folders in a case
- Detailed listing of all URLs and corresponding dates and times that websites were visited
- Document incident report that helps create the required documentation relevant during the incident response process
- Detailed hard drive information about physical and logical partitions

Bookmarks: These are the individual components that drive the information contained in the EnCase report. During analysis, an examiner can use bookmarks in various ways to identify and document specific clues. There are seven different types of bookmarks:

- **Highlighted Data:** Created when highlighting specific text
- **Notes:** Allows the user to write additional comments into the report
- **Folder Information:** Used to bookmark the tree structure of a folder or device information of specific media
- **Notable File:** A file documented by itself
- **File Group:** Indicates that the bookmark was made as part of a group of selected files
- **Log Record:** Contains the results of log parsing activity
- **Registry:** Contains the results of Windows registry parsing activity

Instant Decoding of Nontext Data: Within the reporting section of EnCase, an examiner may "decode" nontext data, so it can be presented in a more recognizable format.

Integrated Picture Viewer with Gallery View: A fully integrated picture viewer automatically locates and displays many known graphical image types, including Microsoft thumbs.db files.

Timeline: This integrated viewer allows an examiner to see all relevant time attributes of all the files in the case (or selected group of files) in a powerful graphical environment.

Intellitype: A quick way for an examiner to jump to files of relevance, instead of having to sort by a particular file attribute and scroll through the data.

Time Zone Settings: Examiners can set the time zone for each piece of media in a case, enabling simple comparison of media from different time zones.

Built-in Help: Quick and easy access to relevant information in the user manual, with topics pertaining to almost every feature of the software. The user manual is a wealth of rich product-related information that can help even the most senior examiners.

Internet and Email investigation

Two of the most critical areas of any investigation typically involve the analysis of artifacts related to the Internet and email. EnCase® software has a number of powerful features that facilitate efficient examinations, including recognition of the various files typically associated with Internet and email artifacts.

Email

- **Analysis:** EnCase software has the ability to find, parse, analyze, display and document various types of email formats, including Outlook PSTs/OSTs ('97-'03), Outlook® Express DBXs, Lotus Notes NFS, webmail such as Hotmail, Netscape and Yahoo; UNIX mbox files like those used by Mac OS X; Netscape; Firefox; UNIX email applications; and AOL 6, 7, 8, 9. In some cases, EnCase can recover deleted files and depending on the email format, the status of the machine.
 - **Presentation:** Email analysis results are placed in a common EnCase format — which is easy to navigate to — where examiners can find information necessary to support the most complex investigations.

- **Browser History Analysis:** EnCase has powerful and selective search capabilities for Internet artifacts that can be done by device, browser type or user. EnCase can automatically parse, analyze and display various types of Internet and Windows history artifacts logged when websites or file directories are accessed through supported browsers, including Internet Explorer, Mozilla, Opera and Safari.
 - **Internet artifact search:** The Internet history keyword search searches out all Internet Explorer history information (in allocated space) and writes it out in HTML format, allowing the examiner to quickly and easily investigate the same sites that the subject visited.
 - **WEB cache analysis:** Most browsers automatically save a copy of each Web page that is viewed, including the pictures, text and multimedia elements. EnCase software can find, parse, analyze, display and document this information.
 - **HTML carver:** The HTML carver is a powerful search and export function that looks for HTML files independent of the browser or Internet-enabled application and allows the examiner to search those files by keyword or other criteria.
 - **HTML page reconstruction:** EnCase software can render HTML Web pages from within the Examiner for easy viewing and quick analysis.
 - **Kazaa toolkit:** Searches through a case looking for various Kazaa artifacts.
 - **Instant Messenger toolkit:** Searches through a case looking for various Instant Messenger artifacts.
 - **Presentation:** As with email, Internet history information is placed in a common interface — which is easy to navigate to — where examiners can quickly find information necessary to support the investigation.

EnScript® Searching Tools

Many of the powerful automated features and toolsets in EnCase are driven by the EnScript technology. The powerful EnScript programming language follows standards consistent with C++ and Java. It enables the automation of complex repetitive operations and enables communication with external systems, such as intrusion detection systems and Windows systems through WMI. EnScript programming allows an investigator to build custom-designed scripts for specific investigative needs and can save investigators days or weeks of analysis time by automating almost any investigative task. They can also be compiled and shared with other investigators in the larger community and with teammates.