



# EnCase<sup>®</sup> Enterprise Detailed Product Description

---

By Guidance Software

## Background

Organizations must have a procedural and technical infrastructure in place to respond immediately to computer-related security breaches and investigate malicious activity and employee malfeasance. Regardless of precautionary measures, computer-related incidents will occur and organizations must be prepared. Hacker attacks have become more prolific and more destructive. At the same time, an organization's biggest threat may arise from within, in the form of intellectual property theft, asset abuse, employee integrity issues, or fraud. Information security legislation, such as Sarbanes-Oxley, holds executives directly responsible for corporate controls, self-regulation and financial authenticity. An organization without an enterprise investigation and incident response capability not only has an incomplete security solution, but is also exposed to high levels of risk, potential liability and economic loss.

## EnCase Enterprise

EnCase Enterprise is a powerful, network-enabled, multi-platform enterprise investigation platform. It enables immediate response to any computer-related incidents and enables thorough forensic analysis. It also preserves volatile and static data on servers, workstations, and laptops on and off the corporate network without disrupting operations. Without EnCase Enterprise, organizations must resort to cumbersome and inefficient manual processes using stand-alone utilities that extend the response and investigation process by days or weeks, and require target systems to be taken out of service.

EnCase Enterprise brings industry standard, law-enforcement grade computer forensic technology to the enterprise for unprecedented incident response, eDiscovery, and investigative capability. Information security professionals, investigators, auditors and incident response teams can now reach any computer within the enterprise in seconds to perform any type of digital investigation. An immediate response is critical to maintaining network and application uptime and reducing the impact of incidents or attacks occurring internally or externally. This translates to anytime, anywhere response and investigative capabilities for information security professionals, computer incident response teams and forensic examiners.

This paper provides a detailed description of EnCase Enterprise functions, including an overview of key benefits, product components, capabilities and details on key features. The objective of this paper is to provide security professionals, investigators, incident response teams and management with a detailed understanding of EnCase Enterprise and its vast capabilities.

## Benefits of EnCase Enterprise

EnCase Enterprise is revolutionizing the practice of enterprise and computer investigations by providing immediate response and thorough analysis of servers, workstations and laptops anywhere on or off the corporate network. This enterprise investigation infrastructure provides a scalable integrated platform to immediately respond to and thoroughly investigate any type of computer-related event whether is responding to an eDiscovery request, computer related incident, or insider threat. EnCase Enterprise lets you:

- Respond immediately to incidents with without system downtime
- Limit damage by responding more quickly
- Capture and analyze volatile data, including active network sessions, open files and running processes
- Automatically respond and investigate event from IDS,SIM, and Data leakage technologies
- Use a single tool to investigate and analyze computers running on Windows, Linux and Solaris
- Securely investigate/analyze machines over the LAN/WAN from a central location
- Investigate and analyze multiple machines simultaneously at a disk level
- Find information despite efforts to hide, cloak or delete
- Carry out investigations without disrupting business or alerting targets
- Acquire and preserve data in a forensically sound, court-accepted fashion
- Share evidence files with law enforcement and legal representatives
- Conduct eDiscovery efficiently and effectively with automated analysis, collections and preservation
  - Audit individual or multiple machines for sensitive information, unauthorized processes and network connections
- Audit machines for compromise by zero-day attacks
- Identify and remediate Windows-based kernel rootkits
- Remediate or stop security events as they are identified

## EnCase Enterprise Components

The EnCase Enterprise investigative infrastructure includes five core components, with support for connecting via the IPv6 protocol:

### The SAFE (Secure Authentication For EnCase)

A server used to authenticate users, administer access rights, retain EnCase audit logs, carries out Snapshot analysis, distribute licenses, enable servlet call back, broker communications and secure data transmission. The SAFE communicates with Examiners and target nodes using 128-bit AES encryption to protect communication between components.

### The Enterprise Examiner

Software installed on an authorized investigator's computer to perform incident response, investigations and audit target systems. This software leverages the robust functionality of the world's leading investigative standard EnCase Forensic product – with network-enhanced capabilities, robust security and lightning fast speed – to carry out enterprise investigations. The examiner is available in both 32bit and 64bit versions.

### Servlet

A nonintrusive, auto-updating passive piece of software installed on workstations and servers to analyze suspect computers. Connectivity is established between the SAFE, the Servlet and the Examiner to analyze and acquire devices that have the EnCase servlet installed. The servlet has special stealth capabilities, including process hiding and the ability to define communication ports, for even the most challenging environments. Servlets run on the following operating systems: All Windows operating systems, Linux kernel 2.2 and above with Process File System (procs), Solaris 8/9, 32- and 64-bit, Solaris – 8 & 9 (32 and 64-bit), AIX – 4.3, 5.1, 5.2 & 5.3 (32 and 64-bit), OS/X – 10.2+, NetWare – 5.1 SP8, 6.0 SP4 and 6.5

## Check-in servlet

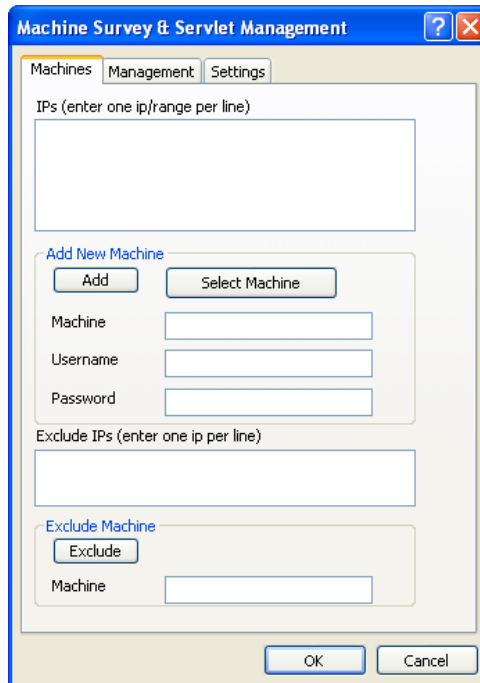
Gives organizations the ability to perform secure incident response and forensics operations on machines that are not connected to the corporate LAN or WAN. . With the new check-in feature the EnCase Enterprise servlet can initiate a connection to the SAFE from anywhere on internet enabling examiners to investigate machines where ever they are dramatically reducing the challenge of processing nodes that are outside of the corporate network. When this features is enabled Servlets will periodically attempt to connect to the SAFE and check to see if they need to be processed. Check-in has a rich set of configuration options giving organizations the maximum flexibility and control over how this feature works.

## Servlet throttling

Servlet priority allows network administrators to throttle a servlet's resource usage (low, medium, high) on target machines. When conducting a Preview, Acquisition, or Sweep Enterprise operation examiners have the ability to throttle the Servlet's resource usage on the target machine as needed. This feature is very useful when investigating machines when the examination is very sensitive or production servers that constantly run CPU intensive processes.

## Servlet deployment

EnCase has the option to deploy Servlets on your machine from within the Examiner interface, and also via push methods using Active Directory/Windows Domain Push. The Enterprise Machine Survey and Servlet Management interface allows users to enter in IP addresses or machine names, and with a username and password of appropriate permissions, automatically copy the servlet to the machine in question. The servlet deployment manager also allows for a range of machines to be set, with specific exceptions within the range allowed.



The screenshot shows a Windows-style dialog box titled "Machine Survey & Servlet Management". It has three tabs: "Machines", "Management", and "Settings", with "Machines" selected. The dialog contains several input fields and buttons:

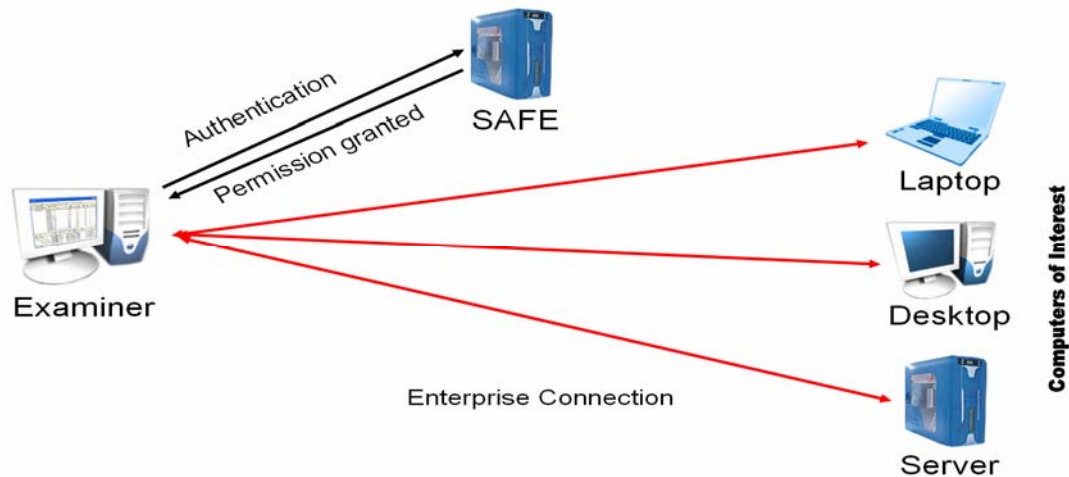
- A large text area for "IPs (enter one ip/range per line)".
- An "Add New Machine" section with an "Add" button and a "Select Machine" button.
- Three input fields for "Machine", "Username", and "Password".
- Another large text area for "Exclude IPs (enter one ip per line)".
- An "Exclude Machine" section with an "Exclude" button and a "Machine" input field.
- "OK" and "Cancel" buttons at the bottom right.

© 2007 Guidance Software. All Rights Reserved.

## Enterprise Connection

A secure virtual connection established between the Examiner and target machines. The number of concurrent connections controls the number of machines that can be analyzed simultaneously.

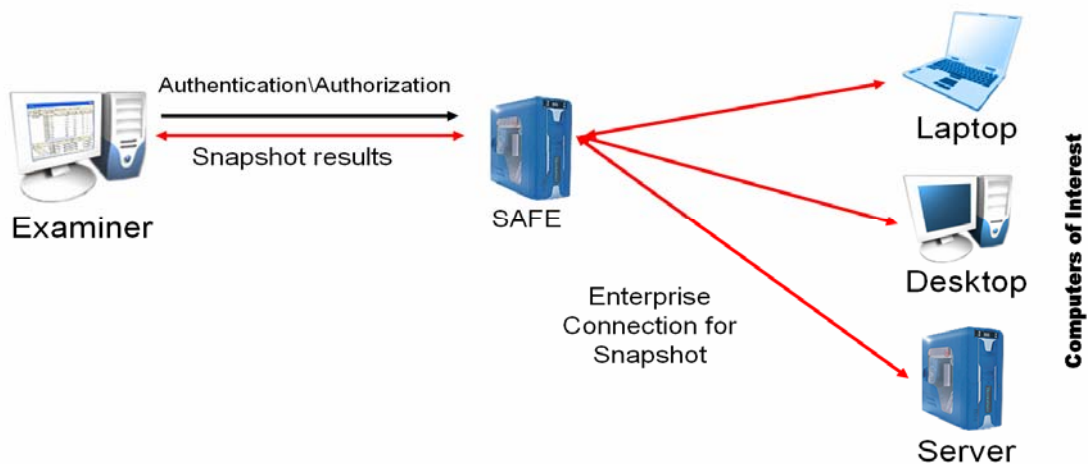
EnCase Enterprise components and **Enterprise** Concurrent connection logical representation:



## Incident Response Analysis (Snapshot)

Snapshot quickly captures volatile data to reveal details about open files, running processes and other crucial information at any given moment.

EnCase Enterprise components and **Incident Response (Snapshot™)** connection logical representation:



# Incident Response and Remediation

## Respond Immediately to Computer-Related Incidents with EnCase Enterprise

### Immediate Response and Capture of Volatile Data

The ability to immediately capture volatile data helps investigators and Computer incident response teams quickly identify the scope, magnitude and status of suspected incidents. This capability, along with the ability to quickly preview and validate static files on system media, gives investigators the power to quickly isolate, identify, assess and remediate both internal and external security breaches.

### Automated Volatile Data Capture with Snapshot

Volatile data exists in the RAM memory of a server or workstation. If power is lost, or a system fault occurs, the data is lost. By contrast, static data is stored on hard drives, USB devices, CDs, for example, and is typically maintained when a machine is powered down. Computers track numerous items that are critical during incident response including: Users on a system, TCP and UDP port information, open files, running processes and applications, and system resources. Snapshot captures this volatile data at lightning fast speed and provides detailed reports on what occurred on those systems at any given point in time. Snapshot data can be viewed in real time via a web browser if the web interface option is selected. Volatile data harvested by Snapshot consists of:

#### Open ports

Open ports are those currently in use or waiting for use by an application or operating system. Open port information assists the investigator in understanding who or what is communicating with a system at a particular point in time. Often, when a machine has been compromised or is being compromised, the breach occurs over open ports. Port information captured by Snapshot is organized by the process that triggered it. Information on local and remote IP addresses, current states, process identification and protocols is also collected.

#### Active processes including driver and service enumeration

Active processes are those processes currently running on a system at a point in time. This information is critical when trying to identify if rogue, unknown or unauthorized processes, services or drivers are active and running on a system. The process information captured during Snapshot is organized by processes, services and drivers. For each process that is running, specific information is captured such as whether the process is hidden, process ID, command line used to execute process, executable path, start time, MD5 hash value and more. In addition to the active process, services and drivers are enumerated and hashed for deep analysis of the state of the system.

#### Windows DLLs

Windows DLL, or dynamic link library files are the Microsoft implementation of the shared library concept. The original concept for DLL files was to ease hard drive and memory space requirements for Windows programs by allowing code that was frequently reused to be called by programs, rather than copying the same routine over and over into individual programs. DLLs allow for a great degree of modularity and an ease of “plugging in” to different interfaces. DLLs also, however, provide malicious code an easy path to being inserted into the operating system, as some common DLLs are called by even trusted programs. DLL files are also enumerated and hashed for inclusion in machine profiles.

### **Open files**

Open files are those files currently in use. Knowing which files are open reveals which information an application or suspect is accessing. In some cases, malicious applications hide information about running processes and network connections, but cannot conceal open files. The open file information captured by Snapshot is organized by the process that opened each individual file. For each open file, Snapshot captures name, process ID and file path and other specific information.

### **Live Windows Registry**

Live registry is registry hives that are only active while the Windows machine is running. EnCase Enterprise extracts and assesses valuable information from the Windows live Registry – quickly and automatically, and based on industry best practices for incident response. Information collected includes details on auto-run keys, devices, installed software, build information, networking details, user information and hardware.

### **Network users**

Provides details on all users who have logged onto a machine, including their user name, security ID and last date and time of login.

### **Network interfaces**

Reveals details on network cards and supporting IP information that could be relevant during an incident response or audit, including card manufacturer, assigned IP address, MAC address and subnet mask.

## **System Profiling and Auditing Rogue Processes**

### **System Profiling**

Quickly identifying which processes running on a computer are trusted – or not – remains a key challenge for incident response and related audits. To mitigate that challenge, the ability to build application descriptors and machine profiles has been added to EnCase Enterprise. Tying these two features together lets examiners focus only on information that is relevant during the incident response or auditing process. A number of default application descriptors and machine profiles are provided for all supported operating systems.

### **Application Descriptors**

Application descriptors provide categorization of single executables via hash values, which enables the examiner to positively identify running executables on a system via a hash value match. On a live system there are typically many processes running. Those processes can take just about any name. One of the only ways to identify a rogue or trojan process running on computers is to use the hash value of the binary and compare it to a predefined application descriptor. Application descriptors enable identification down to the single process level.

### **DLL Descriptors**

DLL descriptors provide categorization of Microsoft shared library files via hash values. DLL files are called by many applications, and malicious code can replace or be inserted into DLL files, allowing for rogue or Trojan processes to be run on a computer. With the addition of DLL descriptors, changes to DLL files can be instantly identified.

## **Machine Profiles**

Lets examiners create a custom profile of processes, drivers, and services authorized to run on a machine. Each profile contains a number of application and dll descriptors (see above), that reveal a detailed picture of processes authorized for a specific system.

## **Snapshot profile**

Snapshot profile provides examiners and auditors with specific information about each system it scans. Information gathered includes: Machine name, IP address, operating system, processor, system version, running processes, number of open ports, network interfaces and network users.

## **Incident impact analysis**

In addition to the incident response analysis information available across an enterprise in near real-time, the task of identifying exactly what happened to a machine remains challenging. EnCase Enterprise has the unique ability to analyze a system snapshot of data across time. This feature gives you a detailed analysis of the exact impact of a computer attack against a machine or set of machines across time.

# **System Auditing and Assurance**

## **Identify Rogue or Unauthorized Processes**

To successfully defend their networks, organizations must be proactive to identify unauthorized or malicious processes that may be running on their enterprise networks. These processes can range from a trojan, such as Optix Pro renamed as spool32, to Kazaa renamed as cmd.exe, to data wiping tools such as Eraser, or an unauthorized corporate application. EnCase Enterprise has the unique ability to quickly and thoroughly understand the processes running in any given environment. Using the high-speed capability of Snapshot, the solution uses MD5 hash analysis to identify those processes with a high level of certainty. The ability to scan for running processes by individual machine across multiple operating systems and networks is a critical capability in understanding the environment and identifying unauthorized or malicious activity.

To take full advantage of this capability, an organization must take steps to understand normal activity. EnCase Enterprise provides facilities and easy-to-use Application Descriptors and Machine Profiles to help define an acceptable baseline and related normal activity. When applications and dlls that vary from the baseline have been identified, EnCase Enterprise helps categorize them in a number of different ways: from malicious to authorized to trusted. The result of these periodic Snapshot scans can be quickly filtered and sorted to identify unauthorized activities. An examiner is able to identify processes that were spawned by other processes and capture the command-line keystrokes used to execute applications. By analyzing command line information, the examiner can identify whether applications were initiated, including unauthorized applications, such as Netcat. Those identified processes can be quickly reported upon for escalation to other teams, such as CIRT or other management authority. Through the use of proactive auditing of rogue or unauthorized processes, an organization can significantly mitigate the potential threats that continually affect them as a result of not knowing what types of applications are running in their environment.

## **Zero-Day Auditing and Compromise Assessment**

The ability to tie together the analysis of volatile and static data, EnCase Enterprise provides a revolutionary capability to identify and mitigate the effects of zero-day events such as MyDoom or other malicious code within a networked environment. EnCase helps you identify key attributes of malicious code as it hooks into various areas of the operating system. EnCase Enterprise captures artifacts of malicious activity that then can be used to sweep the network and identify infected machines meeting specific criteria. It identifies which processes communicate on specific ports, identifies the name and MD5 hash value of any rogue processes, searches the Windows Registry for specific keys, and reveals open files. The solution then parses the file system to see if the file is actually there. Once the analysis completes, EnCase Enterprise reveals which machines are infected and which are not infected with almost 100% certainty. This proven method identifies malicious code before virus definitions have been released by antivirus software vendors.

## **Hidden Process/Rootkit detection**

These days, savvy hackers increasingly rely on kernel level rootkits to compromise corporate networks. These tools lets intruders operate – and return anytime they like – completely unseen, to essentially “own” your network. Rootkits have grown more robust and widespread over time, becoming a tool of choice among attackers who plunder private customer data, then often extort money from the companies they hack. Windows-based kernel level rootkits were completely undetectable until recently. EnCase Enterprise offers the only available commercial-grade solution to find and remediate those threats. It peers deeply into the Windows operating systems to identify and destroy hidden processes and hooks used by rootkits – even when hackers go to great lengths to remain invisible.

## **Remediation**

EnCase enterprise not only provides the information necessary to identify if a malicious event has taken place it can also make it go away. In nearly all instances when dealing with incident response, you can see the issue but doing something means shutting down at least a portion of the network, not doing anything or using third-party tools to remediate. With EnCase you can document the incident in detail, then reach out to all affected systems and kill any rogue processes, delete suspicious files or modify the Registry information on compromised machines – all through the EnCase Examiner. For example, if a worm infiltrated an enterprise network, the security administrator could quickly learn which machines were infected, then target the exact process that is running and kill it – beginning with the machine that introduced the malicious code into the environment.

## **Forensic Investigation**

### **Operating System and File System Support**

Two major attributes that make EnCase 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 that the host system can use. The operating system and file systems are separate, but have a deep relationship based on how information is stored and how the host operating system interacts 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 Enterprise can interpret entire file systems over a network for which an EnCase Enterprise servlet has been developed. Currently supported operating systems include Windows, Linux and Solaris, with

support for other platforms under development. EnCase Enterprise can also interpret a number of file systems for which no Servlets have been developed.

- Operating systems that EnCase Enterprise Servlets runs on: Windows 95/98/NT/2000/XP/2003 Server, Linux kernel 2.2 and above with Process File System (procs), Solaris 8/9, 32- and 64-bit, Solaris – 8 & 9 (32 and 64-bit), AIX – 4.3, 5.1, 5.2 & 5.3 (32 and 64-bit), OS/X – 10.2+, NetWare – 5.1 SP8, 6.0 SP4 and 6.5.
- File systems supported by EnCase Enterprise: FAT12, FAT16, FAT32, 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, Novell NWFS and NSS, FreeBSD UFS2 (FFS2).
- EnCase uniquely supports the imaging and analysis of RAID arrays, including hardware and software RAID. EnCase Enterprise also includes support for Hardware RAID 5 disk sets with 1 missing disk by using Null devices. Forensic analysis of RAID sets is nearly impossible outside of the EnCase Enterprise process.
- Dynamic disk support for Windows 2000/XP/2003 Server.
- New NTFS features to support Windows Vista
- Ability to preview and acquire select Palm devices.
- Ability to interpret and analyze VMware, MS Virtual PC, dd, SafeBack v2 image formats, and Mac DMG disk images, as well as CD/DVD Inspector files.

## Forensic Analysis and Data Preservation

### Extremely large data set support

EnCase Enterprise examiners come in two different versions (32bit & 64bit giving organizations the comfort in knowing they can tackle the largest investigations now and in the future Common investigations are now involving massive datasets with hundreds of gigabytes to tens of terabytes of static data requiring analysis. The size of these datasets can easily exceed the memory limitations of 32-bit applications.. With the 64bit version of EnCase users will note a performance increase, because a 64-bit CPU can handle more memory and larger files. One of the most critical features of 64-bit processors is the amount of memory the system can support. 64-bit architecture will allow systems to address up to 1 terabyte (1000GB) of memory. The new 64-bit version of EnCase Examiner v6 delivers improved multi-threading and a more efficient use of all available memory.

### Previewing Nodes and Multi-Machine Analysis

One of the most powerful and unique capabilities of EnCase Enterprise is the ability to “preview” computers over the network. A preview is the process of securely reaching across the network to a running system or systems that have the servlet installed and remotely viewing all static data in a forensically sound manner. This includes unallocated, deleted, allocated, file slack, volume slack, and file system attributes on hard drives; RAID arrays; CD ROMs; FireWire devices; mounted PGP volumes; and, thumb drives of target machines. Conducting a preview does not alert the user or make changes to the machine being investigated. This critical capability lets investigators quickly determine whether relevant evidence or suspect artifacts exist on a computer without first acquiring them.

Preview is the only means possible to effectively determine which computers contain relevant evidence when the examiner is faced with investigating numerous drives or other media from different operating systems, or has severe time constraints. All EnCase investigation features and

© 2007 Guidance Software. All Rights Reserved.

capabilities can be used during the preview process, including key-word searches, Snapshot, filtering, scripts, conditions, hashing and file signature analysis. The preview process can be performed across a single machine or multiple machines that have different file systems and operating systems. For example, users can analyze a running Windows 2000 server, Solaris server and Linux server simultaneously from a single EnCase Examiner. The ability to preview across multiple machines and operating systems simultaneously makes EnCase Enterprise a true enterprise investigative and analysis tool.

### **Data Acquisition and EnCase Evidence Files**

EnCase Enterprise incorporates all of the robust acquisition capabilities of the stand-alone EnCase Forensic software -- the standard computer investigation tool used by law enforcement and major government agencies.

## **Acquisition**

The EnCase acquisition process begins with the creation of a complete physical bit-stream image of a subject drive or drives in a completely non-invasive manner. The acquisition can occur across multiple systems simultaneously while continuing to investigate the systems being acquired or other systems. During the process, which makes a bitstream copy, the data is continuously transferred securely to the examiner machine to create an EnCase evidence file. The evidence file is an exact duplicate of the data as it existed at the time of acquisition. Throughout the acquisition process the bit-stream image is continually verified by Cyclical Redundancy Checksum (CRC) blocks, which are calculated concurrent to the acquisition. When the acquisition is completed, a second validation check is performed over the entire data set acquired. The second check is called an MD5 (Message Digest 5) hash, which is automatically calculated and embedded as part of the evidence file for validation of the acquired media. EnCase also supports Device Configuration Overlays (DCO), as well as Host Protected Areas (HPA), allowing for areas hidden via these methods to be detected.

### **Acquisition Read Ahead**

One of the biggest challenges dealing with network data acquisitions is overcoming data transfer due to latency on WAN links and in communication between components. The Acquisition Read Ahead feature is a unique capability that allows EnCase to cache blocks of data ahead of time so they are available for commands in process on the remote node. This decreases acquisition time considerably when doing network acquisitions.

### **Acquisition Granularity**

Each enterprise environment has different requirements and processes for dealing with various types of investigations, such as those connected with Human Resources or legal departments. Thus, EnCase gives the examiner the ability to truly control the way hard drive data is acquired. Historically, when a read error is found on a hard disk during an acquisition, the entire block of data containing the read error is zeroed out by EnCase. Through the use of granularity, the investigator has the flexibility to specify the number of sectors within a block of data that contains the read error to be zeroed. In addition, users can now define the amount of data that is being acquired during an acquisition operation. That ensures that EnCase examiners collect every bit of data available and acquire it at the fastest rates possible.

## **Acquisition Restart**

One of the biggest challenges customers face when dealing with forensic network acquisitions is a dropped network connection. In the past, an examiner could spend hours acquiring media via a wireless LAN or WAN and then experience a network disconnect – dropping the acquisition and requiring the reacquisition of the entire media. The Acquisition Restart feature allows the user to automatically continue a Windows-based acquisition from where it was terminated or stopped rather than from the beginning, saving valuable time and enabling the acquisition of mobile users that come and off the network.

## **Auto Acquisition**

It's often impossible to track down mobile users coming on and off the corporate network. The Auto Acquisition feature lets you specify a machine or number of machines by host name or MAC address. When those machines come on line, EnCase Enterprise can automatically acquire related media. Auto Acquisition is configurable to check a target list of machines on a scheduled basis. In addition to automatically acquiring specified machines, it uses the acquisition restart capability to pick up the device acquisition where it left off. It's the most advanced and robust solution for acquiring Windows-based computers coming on and off the network -- without having to wait for the right moment.

## **Alternate storage destination**

As the size of storage devices continues to grow the challenge of acquiring the entire data set of the source media is challenging and many times requires storing data to multiple data repositories. Examiners have the option to define alternate evidence storage destinations when faced with extremely large collections.

## **Check-in Servlet**

Check-in Servlet gives organizations the ability to perform secure incident response and forensics operations on machines that are not connected to the corporate LAN or WAN. With the new check-in feature the EnCase Enterprise servlet can initiate a connection to the SAFE from anywhere on internet enabling examiners to investigate machines where ever they are dramatically reducing the challenge of processing nodes that are outside of the corporate network. When this features is enabled Servlets will periodically attempt to connect to the SAFE and check to see if they need to be processed. Check-in has a rich set of configuration options giving organizations the maximum flexibility and control over how this feature works.

## **Logical Evidence Files**

A revolutionary feature of EnCase is the ability to create logical evidence files. In today's environment, the average size of hard drives exceeds 40 GB, with 120 GB often standard. The traditional practice of acquiring the entire hard drive, including unnecessary data, is no longer feasible or required. With EnCase logical evidence files, you can choose specific files or folders across multiple machines for forensic preservation. Unlike copying files from a device and altering critical metadata, logical evidence preserves the original files as they existed on the media at time of acquisition, plus they include a wealth of additional information. Some of the attributes included

for each file in a logical evidence file are file name, file extension, last accessed, file created, last written, entry modified, logical size, physical size, MD5 hash value, permissions, starting extent and the original path of the file. Users also have the option of selecting whether hash values and folder or file contents are stored when creating logical evidence files.

Since logical file acquisition uses the EnCase Acquisition engine and preserves the evidence in the EnCase evidence file format with relevant metadata, you can feel confident of the validity of logical evidence files. Logical evidence files can be created from previewed media or existing evidence files. They offer another way to preserve data such as e-mail archives and individual files without having to acquire the entire drive or partition. Logical evidence files can be treated separately or a collection of independent logical evidence files can be put into a logical evidence container.

Logical evidence files are automatically verified when opened ensuring evidence gathered by EnCase is self authenticating like standard EnCase evidence files.

## **EnCase Linen Utility**

The Linen utility is a Linux version of the industry standard DOS-based EnCase acquisition tool, only with much more power. It provides an alternate method of acquiring a device using a FastBloc in Windows. This method allows you to acquire hard drives, USB and FireWire drives with a Linux-based tool. Linen supports the ability to switch into ATA mode, allowing for acquisition of older hard drives. It helps users overcome limitations when working with non-Windows-based operating systems, and handles extremely large hard drives and acquires data much faster. Linen includes an enhanced EnCase acquisition option that allows you to refine the number of sectors EnCase acquires at one time. With Linen, users are able to acquire Linux machines via a crossover cable from the Windows EnCase examiner client. Linen is included with many popular security distributions of Linux, including Auditor, Helix, and Fire. The version of Linen shipped with EnCase also allows for injection of Linen into an iso file, allowing any distribution of Linux to be Linen enabled.

## **EnCase Evidence File (Preservation)**

The EnCase Evidence File is a proprietary file created by Guidance Software to compress and preserve bit-stream images of acquired media. The EnCase Evidence File is widely known throughout the law enforcement and computer security industries and has been court accepted to the federal appellate level. For court decisions related to EnCase please visit the Legal section of the Guidance Software Web site: [www.guidancesoftware.com](http://www.guidancesoftware.com).

EnCase Evidence Files are used to preserve evidence and continue the examination without having to restore the image to separate media. The resulting bit-stream image, called an EnCase evidence file, can be mounted as a read-only file or virtual drive from which EnCase Enterprise reconstructs the file structure using the logical data in the bit-stream image. This allows the investigator to search and examine the contents of the acquired drive within the EnCase Enterprise Examiner environment. The EnCase Evidence File contains an exact copy of the data from the original media, including time stamps, deleted files, unallocated space and file system attributes. The EnCase Evidence File can be easily transferred to different types of media and archived for future reference. If necessary, the Evidence File can also be used to restore the exact image to another hard drive if necessary.

## **Hard Drive serial number**

The burden of associating forensic hard drive acquisitions with original media has been challenging examiners since the beginning of time. EnCase now has the ability to automatically enumerate and document a hard drives true serial number providing a solid undeniable link from forensic image copy to physical source device.

## **Powerful Analytical Functionality**

The ability to analyze and search large amounts of data quickly and easily is critical for any incident response, investigation or analysis tool. EnCase Enterprise provides the most advanced, comprehensive and easy-to-use tools to carry out such complicated and time-consuming tasks across multiple operating and file systems and languages across the enterprise network.

### **Advanced User Interface**

The EnCase user interface is continually enhanced to better organize functionality and allow quick and easy access to the most advanced set of investigative capabilities within a single software package. The user interface provides examiners with broad access and dedicated views of specific types of information, such as e-mail or Internet artifacts analysis, and all file analysis. It allows for analysis and reporting on multiple machines within a single interface and allows for multi-case analysis and reporting so examiners can maximize their time. In addition, it provides raw access to hard drive data living on each sector and reveals how the physical maps to the logical world of forensic analysis. The user interface also has usability enhancing features such as the ability to undock and re-dock panes in areas the examiner chooses.

### **Records**

The records tab replaces the email, internet history, and webCache tabs in previous versions of the EnCase Examiner. Moving all internet related search information to the records tab allows examiners to quickly view one of the most important parts of any investigation, internet activity. Email files like PST, DBX, and EDB files, that are parsed on the entries tab will populate on the records tab. Searches run through the search dialog for email and internet history will also populate the records tab. Users can search and bookmark items on the records tab, just as in any other type of search hit. In addition, the user can modify which properties that are displayed in columns, with the most common internet properties displayed by default.

### **Automated Analysis**

Sweep case enables the examiner to automatically choose the types of analysis to perform on cases. Without EnCase, an examiner initiates one analysis tool at a time, such as file finder, HTML carver, machine profiler, file reporter, event-log analyzer or e-mail address finder, and waits for the individual results. Now an examiner can use can use case processor and automatically bring together a rich set of deep-dive analysis tools into one function, with maximum flexibility that reduces analysis time by automating multiple time-consuming tasks.

### **Multiple Sorting Fields**

EnCase allows the examiner to 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, hash category, full path, permissions, and many more.

## **Filters and Conditions**

Filters and conditions enable the examiner to reduce the amount of information displayed based on the user's specified criteria. In a typical investigation, the amount of data investigators must search and review is immense and can be overwhelming. Filters and conditions allow an examiner to quickly reduce the amount of information presented and focus on any number of particular file types or attributes. Over 400 conditions were created from real-world experience and are provided with EnCase Enterprise bringing years of investigative knowledge into every examiners hands. Conditions range from deleted files to password-protected Word documents to all office documents. Filters and conditions can be easily modified to meet the evolving needs of examiners, auditors and security administrators.

## **Queries**

Queries are similar to filters but they allow the examiner to combine filters with simple logic to create complex queries using OR logic or AND logic. The examiner can combine any number of filters to focus on information relevant to the particular investigation. More than 75 queries are provided with EnCase Enterprise, ranging from all MS Office documents of a certain date to all multimedia files.

## **View "Deleted" Files and Other Unallocated Data in Context**

EnCase provides a Windows Explorer-like view of deleted and unallocated data, which includes file slack, swap files, print spooler data and all other unallocated data files. In addition to allowing you to view the information, EnCase automatically interprets deleted and unallocated data, which allows the examiner to carry out a complete investigation without rebuilding all the data manually. EnCase can automatically rebuild data from unallocated space, including Microsoft Outlook PST e-mail files, Microsoft Office documents, HTML pages, NTFS Info2 records, partition information, Zip files, link files and various graphics.

## **Single Files Option**

Single file capability allows the quick creation and analysis of logical files containing a number of external files. Many times when doing analysis, not all the data is contained on the hard drive. Sometimes relevant files exist on shared servers, loose files from a thumb drive, files on a CD or on a PST from the mail server. EnCase allows the user to drag and drop files from other sources directly into the EnCase Examiner without having to acquire the host media prior. This allows for the quick analysis of file fragments that are typical for many types of cases. Once added into the Examiner, single files can be analyzed and acquired into logical evidence files and added to the case for future reference and preservation.

## **VMware Analysis**

EnCase has native ability to analyze VMware .vmdx data files and VMware snapshot files. VMware is powerful virtual machine software that allows organizations and users to host multiple operating systems on a single piece of hardware. Since VMware is a virtual operating system, it includes volatile and static data artifacts that should be addressed during the course of an examination. EnCase can interpret the data files that compose the physical and logical structure of the virtual hard drive, including unallocated space, and allow for quick and thorough analysis of VMware. EnCase Enterprise can also do live system analysis of running VMware instances with machines that have the servlet installed. Having the ability to quickly analyze VMware technology is critical in almost every environment. Before the ability to interpret VMware files, examiners did not really have a meaningful way to analyze VMware data from a forensic perspective. Current VMware version 5 support is included in EnCase.

© 2007 Guidance Software. All Rights Reserved.

### **Windows Virtual PC support**

EnCase also has the ability to analyze Virtual PC files. Virtual PC files are the Microsoft equivalent to VMWare appliances, with the ability to run most x86 operating systems. Virtual PC 2004 runs on both Windows and Macintosh host operating systems. Since Virtual PC is the equivalent to a computer within a computer, Virtual PC files contain volatile and static data which can be parsed by EnCase. Virtual PC disks can be examined in the same manner as normal examinations, including viewing unallocated space.

### **International Language Support**

EnCase supports Unicode data decoding. The Unicode standard provides a unique encoding number for every character, regardless of platform, computer program or language. EnCase can search and display any language that Unicode supports, and code pages that Unicode supports. This allows examiner the ability to search and view data in its native format such as German, Arabic or Kanji. There is also an option allowing examiners to set a global code page when mounting a device, greatly simplifying the use of several different languages across acquired media.

### **NTFS and UNIX File Permissions and Ownership filters**

Every file and folder on an NTFS and UNIX file system has an owner, a group and a set of permissions. While this information is stored differently in various file systems, EnCase automatically extracts the security data and displays a wealth of information for each file and folder. For example, EnCase will list the owner, the group and permissions organized by owner or group. With security information exposed, it is possible to filter on a particular security identifier to see if a person or entity had rights to access or modify a particular file or set of files across a range of machines.

### **Encrypted Volumes and Hard Drive decryption**

A challenge faced by many examiners is dealing with encrypted data. In some cases, subjects will use encryption technology for legitimate and/or illegitimate purposes. Regardless, investigating encrypted data is typically difficult and a sometimes impossible problem to overcome. With EnCase Enterprise it's now possible to overcome many of the challenges presented by encrypted volumes and hard drive wrapper technologies. Many encryption technologies make it easy to store and retrieve data from encrypted volumes of various sizes by mounting them as logical volumes on the host machine. EnCase Enterprise can analyze and acquire mounted encrypted volumes such as PGP and DriveCrypt when they are mounted as logical volumes. Many enterprises have begun the deployment of hard drive encryption wrappers like Safeboot to protect mobile users while the data is at rest and active. EnCase Enterprise provides examiners with full access to hard drives wrapped with encryption while machines are running. EnCase Enterprise also includes support for decrypting Volumes and Hard Drives encrypted with PC Guardian and Utimaco encryption software provided a user or administrator password is supplied.

### **File Extraction**

There are times when it is necessary to automatically extract files from a target machine or machines to aid in an investigation. The file extraction processes can extract data of a specific type from target machines or media. Once given the appropriate parameters, such as file type and keywords, the software will automatically go through a machine or set of machines and extract the files meeting specified criteria. It will then copy the files to the examiner machine or alternate location. This makes it very easy for an investigator to extract a copy of all Word documents that, for example, contain a specific keyword such as "fraud" or a particular product name, for further analysis.

## **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. Link files are important because each user's Windows desktop, recent, start menu and send to folders can yield evidence in the form of shortcut files. The shortcut files refer to target files, such as applications, directories and data files, or to non-file system objects such as printers or external drives. Icons exist on the desktop for each shortcut file. Someone using shortcuts can open a file or directory, or start an application program, by double-clicking on the appropriate desktop icon. The ability to quickly discover and interpret link files can provide the examiner with valuable information, such as a suspect that was transferring company data onto a thumb drive or other external media, or reveal which files, applications and shares a suspect commonly used. Linux symlinks (ln -s) are also examined, providing valuable information on Linux link files.

## **Active Directory Information Extractor**

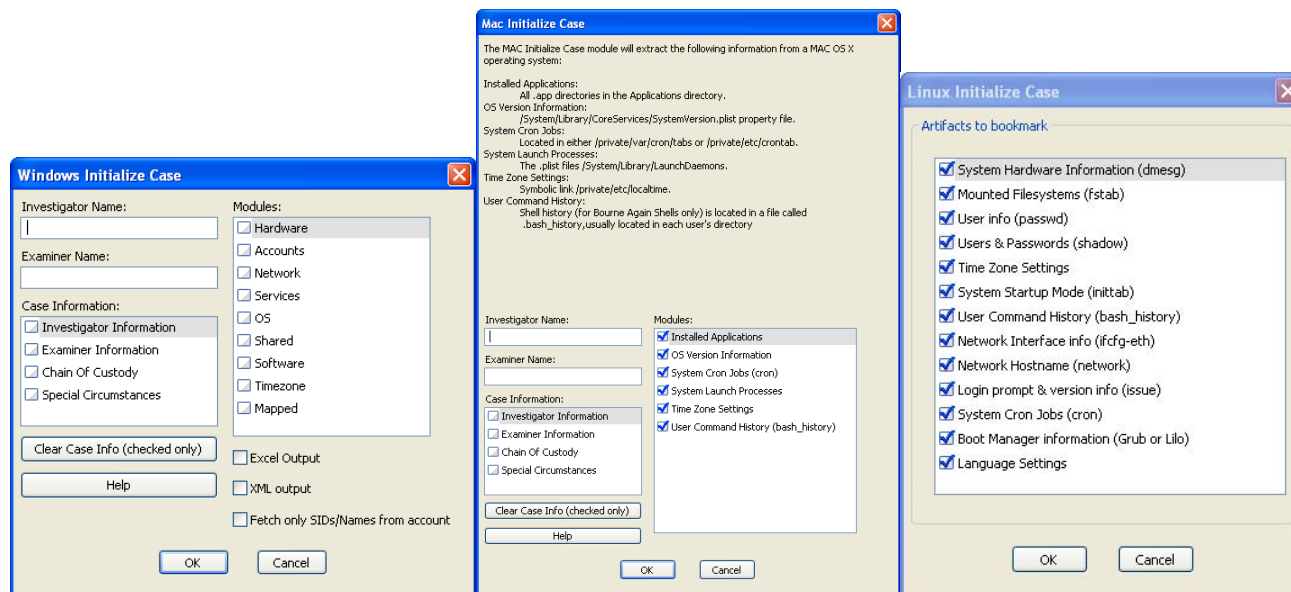
In the Microsoft Active Directory environment, each domain controller contains a wealth of information about its users and resources it can grant access to. The Active Directory Information Extractor will forensically analyze the Active Directory database (NTDS.DIT) and extract the username, SID, home directory, e-mail address, last login, last failed login and next password change. This valuable information can then be imported into the Security ID option of EnCase to create relationships between SID information and user-friendly names. Once the relationship has been established, EnCase will then use the Security ID list to resolve SID numbers to names while doing an analysis, making it easier to understand who accessed what particular files.

## **Hardware Analysis**

Automatically culls through the registry and related configuration files to quickly identify the types of hardware installed or previously installed on a target machine. Company information is often copied to an external device that is then carried off the premises. The hardware analysis will show what type and brand of device (IDE, USB, FireWire, etc) installed. It can also be used to identify if and where unauthorized hardware devices were used on a system.

## **Auto System Profiling**

One of the most difficult tasks when dealing with any type of system analysis is to deeply understand operating systems attributes in which users or applications operate. Using fragmented, stand-alone methods, investigators can spend weeks finding all the relevant operating system information on multiple systems. EnCase Enterprise can automatically gather this information for you. In the Windows environment, the solution can quickly harvest the operating system version information, time zone, networking information, user information, last shutdown time, hardware information, installed software, services, mapped drives and shared folders. In the Linux environment, EnCase Enterprise retrieves details on mounted hardware, mounted file systems, user information, passwords, time zone settings, startup information, command history, network information, system cron, language settings and boot manager information. This automatic system profiling capability presents a wealth of information that provides valuable background on the machine being analyzed. EnCase Enterprise retrieves information from Linux and Macintosh systems, allowing investigators to view applications that are installed, cron jobs (jobs scheduled automatically on a system), version information, applications that are launched on system startup, time zone information, and a history of all commands typed into shell prompts.



## Registry Parser

EnCase Enterprise can automatically scan the Windows registry for a variety of different keys. This provides investigators to obtain a list of applications, uninstalled programs, and internet artifacts from the registry. The registry parser also allows for the detection of various hardware devices in the registry, allowing the investigator to obtain information on the CPU type and various system busses, as well as pulling out information about what devices may be attached to the PCI/IDE/Firewire/USB busses. The registry parser also pulls information on recently used files for various applications, including the windows recently used file list and Windows media player recently played file list. The registry parser also allows the examiner to search for stream MRUs, giving a picture of recently run commands, desktop backgrounds, and other vital clues into a user's recent computer access.

## Recover Folders

Automatically rebuilds the structure of formatted NTFS and FAT volumes. When a person or application formats an NTFS volume – either maliciously or unintentionally – it becomes very difficult to recover the formatted volume. Formatting deletes the tree structure that indicates where the folders and files are on the disk. Without EnCase, it often takes days to meticulously pick through the unallocated space looking for fragments of the Master File Table (MFT) and rebuild the partition manually. With the NTFS and FAT Recover Folder feature, EnCase automatically searches the drive and finds artifacts from the previous partition. The partition information, directory structure and folder structure are then automatically rebuilt. The NTFS Volume structure is then ready for analysis. This ability is of critical importance in cases where a machine has been repurposed to another employee in the organization. If a repurposed machine was previously used by an individual who is the subject of an investigation, it would be necessary to recover the files from the previous NTFS Volume.

## USB Thumb Drives

Another challenge faced by analysts is dealing with the growing array of external media such as USB thumb drives and FireWire IDE drives. These technologies offer a great convenience, but also create a gigantic risk for corporations when not managed properly. Now that external storage is

readily available and easy to use, corporations find their intellectual property walking out of the office on a regular basis – taken mostly by employees using USB thumb drives. With EnCase Enterprise you can identify, analyze, search, and collect these external devices covertly across multiple machines.

### **Log and Event File Analysis**

Many times analysts may wish to analyze system, security and application log files during the course of an investigation or security event. EnCase provides a single means to analyze, search, preserve, and document log and event file data. Traditionally, this type of activity required different tools and modification of data on the target system. With EnCase's log and event file analysis capabilities it is possible from a single tool to parse Windows, Solaris and Linux logs looking for specific information and document or export the findings.

### **File Extent Analysis**

File Extents are the number of extents (data runs) of a file that is fragmented on the drive. EnCase provides quick and easy access to file extent information such as (start byte, bytes, start sector, sectors, start cluster and clusters). File Extent Analysis is an advanced feature that lays out the physical location and fragmentation of the file on the disk.

### **Symbolic Link Analysis**

In UNIX-based file systems (including AIX), symbolic, or soft links are files, similar to Windows .LNK shortcut files, that point to other files. Symbolic links do not contain the data found in the target file, but can provide links to directories, or files on remote devices. EnCase provides access to and analysis of the symbolic link information to simplify analysis of UNIX-based file systems.

### **Secure Storage**

EnCase provides the ability to view users, groups, and SAM keys, as well as protected files. EnCase finds all information in the Windows registry about SAM keys and users. With these artifacts all aggregated in one place, it provides a simple way to attempt decryption of files by utilizing dictionary attacks. EnCase also allows for dictionary attacks against Windows and \*nix user accounts, which are stored in the Secure Storage tab.

### **Compound Document and File Analysis**

Many files, including Microsoft Office documents, Outlook PST's, TAR, GZ, GZIP, MS Thumbs.db and ZIP files, store internal files and metadata that contain valuable information once exposed. Many of these compound files even have their own internal file allocation tables, unallocated data and complex structure. EnCase Enterprise automatically displays these internal files, file structures, data and metadata. EnCase uses hard disk caching to greatly speed the opening and analysis of large and complex compound files, such as Microsoft Exchange EDBs and Lotus Notes NSFs. Once the files have been virtually mounted within EnCase, they can be searched, documented and extracted in a number of ways. Without EnCase's advanced document and file analysis capability, users would need to expose the data using time-consuming manual processes or third-party applications. The number of document and file types EnCase can analyze is continually growing to meet the evolving needs of examiners in the Windows, Linux, and UNIX environments.

### **File Signature Analysis**

Most files contain a few bytes at the beginning of the sector that constitute a unique "signature" of the file. EnCase can automatically verify the signature of every file it searches and compare it against a list of known file signatures and associated extensions. If there is a mismatch, as when a

suspect has “hidden” a file or renamed the extension in an attempt to conceal its identity, EnCase automatically identifies those modified files and reports the correct file extension. When new or “custom” file signatures are needed, they are easily created in EnCase for future use.

### **Hash Analysis**

An MD5 file hash is a unique numeric value determined by the file’s contents. EnCase provides the ability to automatically create hash values for all of case files. The hash value can be considered a cryptographic fingerprint that gets associated in EnCase with the data of every file. That MD5 hash value is unique for every file unless the files are exactly the same. Once hashes have been calculated, they can be used in numerous ways to speed analysis. The Hash Creation feature within EnCase allows the investigator to build a library of hash sets. By building or importing a library of these hashes, investigators can use EnCase to identify any exact file matches from the examined evidence or target machine. An examiner may wish to create a hash set of known intellectual property, child pornography images, hacker tools or noncompliant software to identify any files regardless of whether they have been deleted or cloaked. EnCase automatically identifies the files and notifies the examiner. EnCase permits categorization of different hash sets with “Hash Category” allowing for enhanced sorting and filtering of known files. The examiner can create various categories, such as known, unknown and suspect.

### **Built-in Registry Viewer**

EnCase Enterprise’s Integrated Registry Viewer organizes registry data file into folders, providing the examiner with an expedient and efficient means to view the Windows Registry and determine values. This feature allows the investigator to browse, search and bookmark evidence contained in the registry files. It also allows EnScripts access to the all areas of the registry. The registry files of the Security, System and Software (SAM) contain information valuable when carrying out a variety of investigations.

### **Native file viewer**

EnCase includes Stellant® Outside In® file viewing technology to display over 400 file formats natively in the document tab. Data displayed via Outside In technology in printable, and text viewed via the technology can be bookmarked. Outside-In technology allows an investigator to see how documents would be rendered in their native applications, eliminating the need to export document to third party viewing tools or native applications. Another benefit to Outside In technology is the ability to extract text only information from file formats that would otherwise not allow text to be extracted (PDFs), drastically cutting down on false positives during searches.

### **External File Viewers**

Occasionally, an investigator will find file types that EnCase does not have the built-in capabilities to view, such as an MP3 or AVI. Investigators may also want to view a file type that EnCase does support with a third-party tool or program. In either situation, EnCase can be quickly enhanced to use external file viewers. That makes it easier to analyze foreign file types or use native applications from the source machine.

### **Intellitype and hotkeys**

Are a set of features the exposes a quick method to find relevant files by attribute of perform various EnCase analysis functions. With Intellitype, examiners can type in a specific word or file attribute and instantly jump to the relevant place. The hotkeys function is a quick and easy way to call many of EnCase’s analysis functions without having to click through the GUI.

© 2007 Guidance Software. All Rights Reserved.

# Search Technologies

The powerful EnCase search engine can locate information anywhere on the physical or logical media by using its deep analysis features discussed above. A key component of any search is the keywords and their rules. Keywords must often be quickly modified and input in a variety of simple and complex ways. EnCase can search for each term byte-by-byte, from the beginning to the end of every medium, both logically and physically. EnCase has a number of the most advanced search capabilities to find the information investigators need.

## Concurrent Search

It can be very time-consuming to search for data across multiple machines simultaneously, especially if each machine is analyzed in a serial fashion. With EnCase Enterprise, when you initiate a search or analysis request, the application treats each computer node as individual resource to be analyzed. Each target machine conducts its own analysis and reports back to the Examiner, allowing for simultaneously analysis across multiple machines without having to deal with each machine individually.

## Indexing

EnCase® V6 introduces our new patent-pending, powerful indexing engine which indexes text extracted from evidence. You can now build a complete index of words from multiple languages based off your evidence file, and then create fast and easy queries using EnCase Conditions and Filters. These indices can be chained together to find possible keywords in common with 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.

## Identify code pages

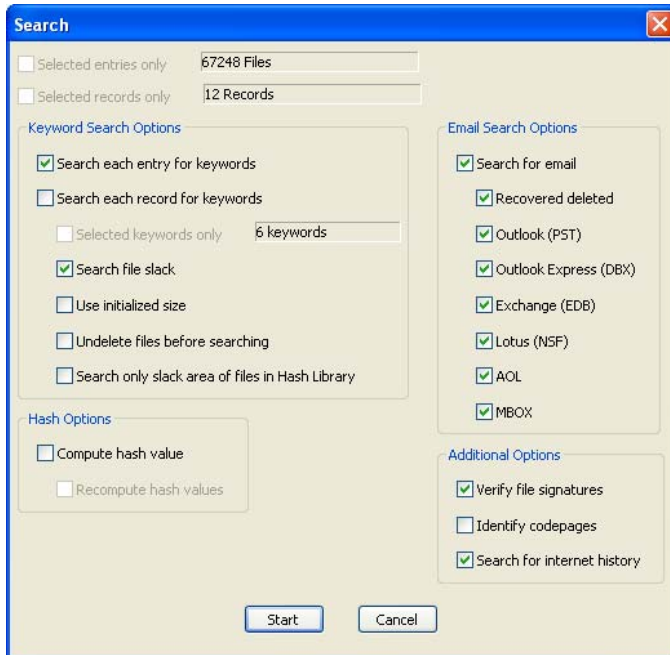
Many organization and government agencies are struggling with the challenges of searching and analyzing foreign languages. Unless you know what Unicode code page to use for searching, finding what you are looking for can be difficult. EnCase now has the ability to automatically identify the language of a given document has been written dramatically reducing the risk of missing critical information during general searches.

## Proximity Search

This feature searches through all files in a case for a specific keyword. It then documents the keyword and specific number of bytes surrounding it. The ability to do proximity search is a critical function when trying to add context around the information you a searching for. The result of the proximity search can easily be provided to an enterprise's legal or HR departments to help document and understand the context in which the term was used.

## IE-mail Search

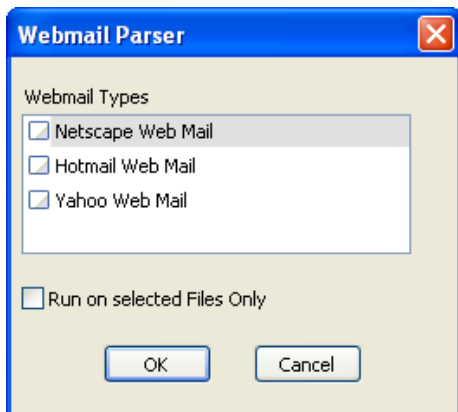
This feature automatically finds, parses, analyzes and displays various types of Internet and e-mail artifacts across machines. The internet and e-mail search runs in the background and searches across all selected media for a whole array of Internet and e-mail artifacts without having to identify the type of browser or e-mail client prior to the search. The E-mail Search feature finds mail formats such as Hotmail, Outlook, Yahoo, AOL, Netscape, mBox, Outlook Express.



It finds Internet artifacts from Internet Explorer, Mozilla, Opera and Safari. Upon completion of the search it will automatically mount and display Web and e-mail artifacts in an easily analyzed format.

### Webmail search

EnCase can automatically find, parse, and analyze webmail artifacts sent and received by Netscape, Hotmail, and Yahoo webmail. The webmail processor thread runs in the background, allowing the investigator to perform other tasks while it is running.



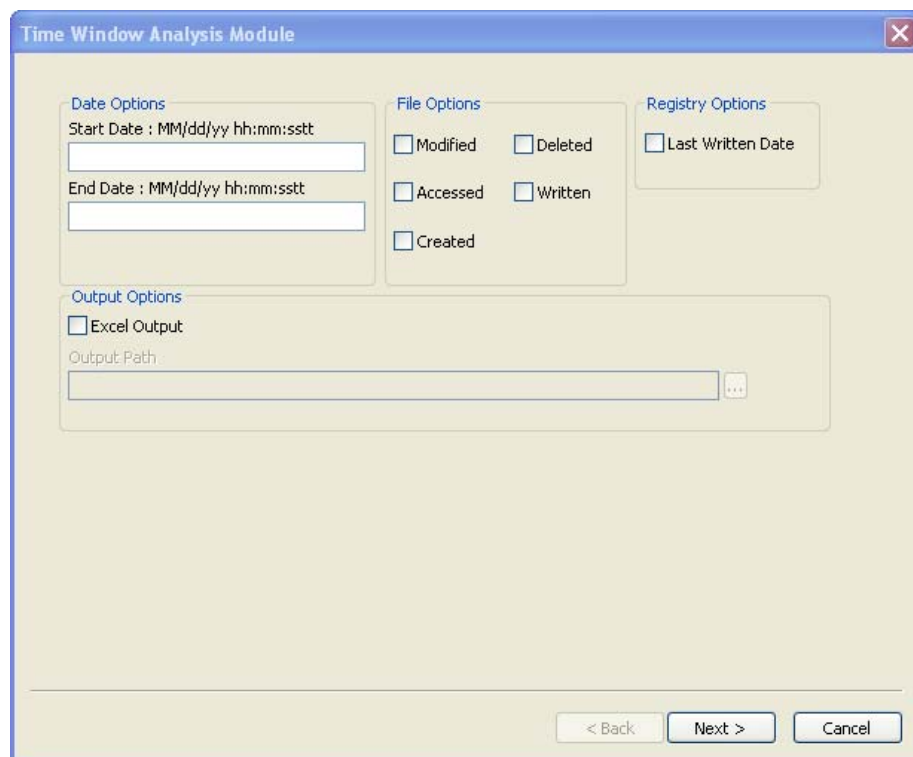
### Internet History Search

EnCase can automatically collect and analyze artifacts related to WWW browsing, allowing for a glimpse into a user's activities. Internet history can be searched for keywords, and files a user has deleted can be recovered. The Internet history search

### Time Window Analysis

Often times an investigator will have the need to search for files that were created, modified, accessed, or deleted within a certain time period. EnCase Enterprise offers the ability to search for all data with these criteria in a time window

of an investigator's choosing. EnCase can also be set to automatically generate reports based upon the analysis performed.



### **E-mail Address Search**

This feature automatically searches the case for specific e-mail addresses, which may reside in numerous places in addition to the primary e-mail application. The feature examines the entire drive, including unallocated space, mail applications, documents and HTML pages. Not only does it find the e-mail address, it uses intelligence to identify whether the e-mail address is structured properly, reducing the amount of misinformation retrieved during standard searches.

### **GREP Search**

In addition to standard text search capabilities, EnCase features a powerful GREP search utility that enables the examiner to search for information with a known general format, such as any telephone numbers, credit card numbers, network IDs, logon records or Internet Protocol addresses, even when the specific number is not known.

### **File Finder**

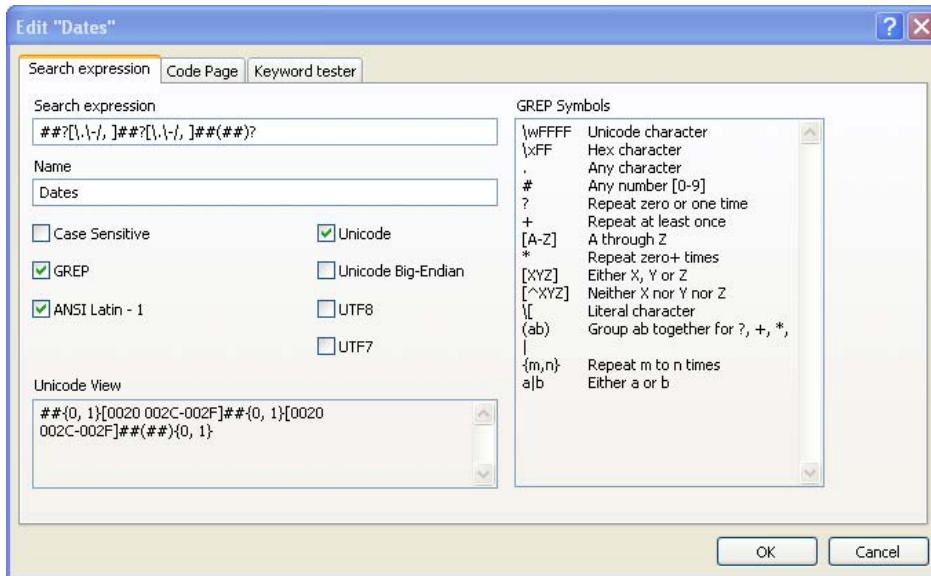
This feature automatically searches within the PageFile, unallocated clusters, selected files or an entire cases, looking for specific file types and structured data. This feature is different than the standard search, because it looks through the defined areas for the file header information and sometimes the footer information identifying the specific chunks of data. Numerous options are available with the File Finder feature such as the amount of data to extract, where to export files, bookmark search hits, or automatically rebuild HTML pages. Users can quickly define additional files types to search for by header and footer. The ability to search unallocated space automatically for files by header and footer is a powerful and time-saving feature.

© 2007 Guidance Software. All Rights Reserved.

## Search Options

Besides the standard search feature, EnCase has a number of options to use when searching through data. Depending on the file system, operating system, CPU and language, data may need to be searched in very specific ways. EnCase provides the following search options:

- **Case sensitive** - Lets users search specific keywords by upper or lower case letters.
- **GREP** - Search using the Global Regular Expressions Post (GREP) advanced searching syntax
- **RTL Reading** – Search for the keyword in a right-to-left sequence when search text is written in foreign languages.
- **Active Code-Page** - Enter keywords in many different languages. The “Active Code-Page” option must be checked to enter keywords in certain languages. For English characters, use the “Latin I” code page. The Active-Code page also allows 32 bit Unicode and big-endian 32 bit Unicode (UTF-32).
- **Unicode** – The Unicode standard attempts to provide a unique encoding number for every character, regardless of platform, computer program or language. Unicode uses 16 bits to represent each character, as opposed to ASCII (which uses 7 bits). Unicode on Intel-based PCs is Little Endian.
- **Big Endian Unicode** – Non-Intel PC (UNIX and Macintosh) data formatting scheme in which the operating system addresses data by the most significant numbers first – the reverse of Little Endian.
- **UTF-8** - To meet the requirements of byte-oriented and ASCII-based systems, UTF-8 has been defined by the Unicode standard. Each character is represented in UTF-8 as a sequence of up to four bytes. The first byte indicates the number of bytes to follow in a multibyte sequence to allow efficient string parsing. UTF-8 is commonly used in transmission via Internet protocols and in Web content.
- **UTF-7** - Has the quality of encoding the full BMP repertoire using only octets with the high-order bit clear (7-bit US-ASCII values, [US-ASCII]), and is thus deemed a mail-safe encoding. UTF-7 is nearly obsolete and used primarily when searching for older Internet content.



### International Keywords

EnCase has the unique ability to search keywords with international language characters. This allows the investigator to search, for example, for Arabic keywords using Arabic characters, or Japanese keywords using Japanese characters. Search results can be displayed in the desired language, as well as the document in which the keyword was found.

### Logical File Recognition

Files often span noncontiguous clusters. EnCase is capable of searching these allocated files. On the other hand, searching Windows text files using a forensic utility that cannot logically search data clusters often results in missed search hits or inaccurate search results. While a keyword text search can be performed upon the evidentiary image disk using such utilities, the disk is only searched physically, meaning that logical searches of fragmented clusters are not performed. An examiner might, for example, enter the keyword “Manhattan Project.” With EnCase, a file containing that text and spread among several fragmented data clusters would be retrieved.

### Multiple Media Search

EnCase Enterprise allows the examiner to search and analyze multiple machines and media at one time. Many investigations involve multiple computers, floppies, zip disks, and other external media, each which might have a different file system and operating system. With EnCase, the examiner can search all media involved in a case in one pass. This saves a tremendous amount of time when searching computers across multiple machines in large investigations.

### Search Results or Search Sorting

When searching various media types across multiple machines, it is sometimes difficult to analyze the keyword search results. EnCase provides a number of ways to help the examiner slice and dice the data to focus on the most relevant information during analysis. All results from the search function are placed in a special search hits section of EnCase. Within that section, search results can be sorted by case, keyword, device or any combination thereof.

### Keyword Tester

Creating correct and relevant keywords is a challenge for the savviest EnCase users. The Keyword Tester tool can be used to compare a search string against a known file and test the results. This is

especially useful when searching with GREP expressions or across foreign languages.

## Documentation and Reporting

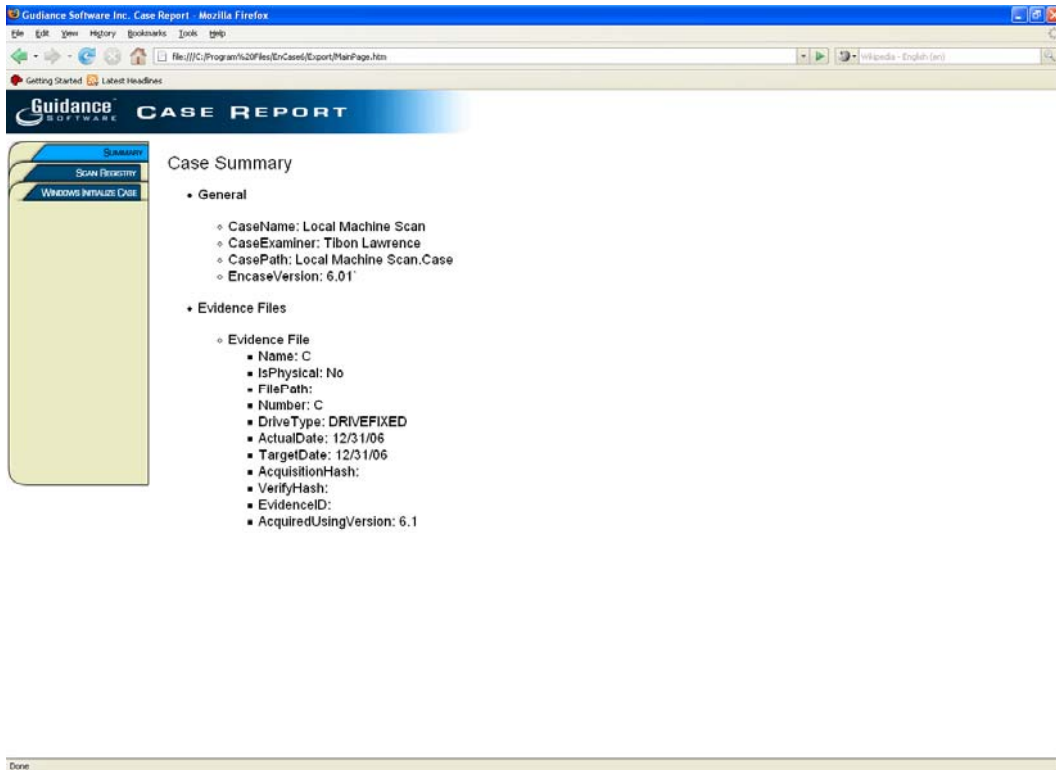
The importance of the reporting process during an investigation or computer analysis is often underestimated. Clues, analysis, notes and search results are sometimes mismanaged or forgotten when relying upon a separate application to document the examination. In many cases, the documentation is the end result of a detailed investigation or audit across a single piece of media or multiple machines. EnCase Enterprise has the ability to define in detail which information is presented, and how it is presented, depending on the purpose and target audience of the investigation. Almost all information exposed by EnCase can be exported into various file formats, depending on the data type, for external reporting and analysis purposes. Final EnCase reports, which include relevant evidence, investigator comments, bookmarks, search results, search criteria, pictures, data and time artifacts, can also be exported into a rich text format or HTML for quick and easy distribution to third parties, management and colleagues.

Since the requirement to generate reports is so critical, EnCase lets users create a number of automatically generated reports. These automated reports reveal a wealth of information, such as:

- A list of all files, folders and attributes in a case.
- A detailed list of all URLs and corresponding dates and times Web sites were visited.
- A Windows profile listing operating system version, time zone, networking information, user information, last shutdown time, hardware information, installed software, services, mapped drives and shared folders.
- A Linux profile of mounted hardware, mounted file systems, user information, passwords, time-zone settings, startup information, command history, network information, system cron, language settings and boot manager information.
- A document incident report that helps create the required documentation that is relevant during the incident response process.
- A list of running processes, open ports, open files and logged-on users running on a machine or set of machines.
- Hard drive information detailing physical and logical partitions.
- A list of all machines that are running unauthorized processes or taking part in unauthorized communication.

### Case reporter

Generating reports is critical but often time tedious part of any examination. The EnCase case Reporter module creates HTML reports based off of bookmarked artifacts that give examiners the ability to quickly and easily create a customizable easy to navigate report of evidentiary findings. The new reporting capabilities enable easy reviews by third parties from CDs and DVDs without requiring EnCase, training or the original evidence.



## Differential Snapshot

EnCase provides a comparison of multiple snapshots (taken at different times) of the same machine, noting any information that differs between the snapshots. A base snapshot is selected and every other snapshot is compared to this base snapshot; evaluating differences in vital areas such as open files, process information, user accounts, and hash information. Information differing from base is noted and exported to a medium of the investigator's choosing.

## Bookmarks

Bookmarks are the individual components that drive the information contained in the EnCase Report. An examiner can use bookmarks in various ways to identify and document particular clues during analysis. There are seven different types of bookmarks each one that provides a different mechanism of presenting information gathered during an analysis or audit.



**Highlighted Data Bookmark** – Created when highlighting specific text



**Notes Bookmark** – Allows the user to write additional comments into the report.



**Folder Information Bookmark** – Used to bookmark the tree structure of a folder, or device information of specific media.



**Notable File Bookmark** – Is a file documented by itself



**File Group Bookmark** – Indicates that the bookmark was made as part of a group of selected files

© 2007 Guidance Software. All Rights Reserved.



**Snapshot Bookmark** – Contains the results of a system snapshot of dynamic data for incident response and security auditing



**Log Record Bookmark** – Contains the results of log parsing activity



**Registry Bookmark** – Contains the results of Windows Registry parsing activity

In addition to the different types of bookmark information that can be captured, EnCase automatically tracks and keeps complete records of all conducted searches, including the time of the search, the scope of the media examined, keyword and GREP expressions used and related search results.

## Export and Import of Bookmarks

One of the challenges many groups face is the ability to quickly and easily share case information between examiners. Many times it's necessary to have multiple examiners look the same or different pieces of media. EnCase has introduced a new feature that gives the user the ability to import and export bookmarks. This allows the user to submit bookmarks to another investigator for review without the cumbersome task of including keywords, search hits and other details.

### Instant Decoding of Non-Text Data

Within the reporting section of EnCase, an examiner may “decode” non-text data, such as data found in unallocated clusters, by selecting the block of data that they wish to decode. Once the data has been identified, it can be decoded in a more meaningful way by presenting it in a recognizable format. Some of the options for decoding of non-text data include: Low ASCII, Hex, 8-bit Integer, 16-bit Integer, 32-bit Integer, various date/times for Windows and UNIX, partition entry, Base64-encoded pictures, DOS Directory Entry, and Win95 Info File Record, Reconstructed HTML, Win2K info file record, right to left, Base64, ROT 13 encoding, HTML, UUE-encoded pictures and more.

### Integrated Picture Viewer with Gallery View

EnCase features a fully integrated picture viewer that automatically locates and displays many common graphical image types. The integrated picture viewer also shows pictures contained within Microsoft thumbs DB files. The Gallery View displays known picture types, including deleted images, in a customizable thumbnail view. The examiner can then quickly scan a large number of images for relevant or suspect artifacts. Images rendered in the gallery view can be easily documented or extracted for external viewing.

### Timeline

EnCase features an integrated Timeline Viewer that allows an examiner to view all relevant time attributes of all the files in the case (or selected group of files) in a powerful graphical environment. File created, entry modified, written, access, and deleted times are placed in a clear and convenient graphical context. These various time stamp entries may be viewed all at once or in any combination selected by the user. This feature enables examiners to draw connections between various files and time stamp data. The capability is very useful for incident response, auditing, and employee integrity issues and many other types of computer investigations.

© 2007 Guidance Software. All Rights Reserved.

## **Time Zone Settings**

Media in the same case often originates from different time zones, which makes comparing event times difficult. EnCase Enterprise allows the investigator to set the time zone for each piece of media in the case, independent of the system time zone other pieces of media in the case. If desired, the user can also view all dates relative to one consistent time zone. When a new time zone is assigned, dates and times in GMT-based file systems, such as NTFS, are adjusted accordingly.

## **Built-in Help**

Guidance Software provides users with quick and easy searchable access to the EnCase user manual. With the complexity of cases growing, and the tools within EnCase needed to analyze them continually changing, it is impossible for examiners to know all features within any technology. The user manual is a wealth of product-related information designed to help novice analysts and senior examiners. EnCase uses compiled help files, which provide an easily readable and searchable help file format.

## **Differential and Historical Snapshot reporting**

EnCase provides robust differential analysis reporting capability. Since all Snapshot data can be stored in a database and collected over time with subsequent Snapshots. Reports can be generated that show differences on a per machine basis on a per attribute basis between a specific time range and any combination of. This allows an examiner to really document and understand what is taking place on machine across their enterprise.

## **Incident Response reporting**

Snapshot provides a wealth of information to the examiner. When harvesting volatile data from over 40,000 nodes, the amount of information can be overwhelming. EnCase provides the ability to dump Snapshot data into a database for reporting and analysis purposes. There are a number of preconfigured reporting mechanisms that help the examiner create meaningful reports from the Snapshot data within the database. The examiner can create very specific reports of volatile data to show all machines that have been compromised during an attack, show the spread of a virus and where it originated, show machines running unauthorized process, or all machines that are running hidden processes. The Incident Response reporting capability is a robust tool that lets the largest organizations present information in a manner that is most meaningful – whether it's for another analyst or an executive.

## **Internet and E-mail investigation**

Two of the most critical areas of any investigation typically involve analysis of Internet and e-mail artifacts. EnCase offers powerful features to help the examiner efficiently carry out examinations dealing with those crucial artifacts, including those found in e-mail and browser applications, Web mail, P2P sharing applications and instant messaging applications.

## **Advanced E-mail analysis**

Every e-mail application stores information in a different format and location, making it difficult to analyze and search for relevant information across multiple data sources and operating system platforms. EnCase natively supports a number of different e-mail client types, making thorough

analysis of e-mail possible. EnCase has the ability to automatically find, parse, analyze, display and document these formats:

**Microsoft PST** files that are password protected and encrypted can be easily opened and expanded, representing the data in a fashion similar to Outlook but within EnCase. EnCase has the ability within the PST to search, extract and document any information represented such as e-mail header information, contacts, meetings, e-mail attachments, message body and tasks. Users can also search deleted e-mails within the PST's unallocated space. EnCase can also recover deleted content from Outlook 2000 and 2003. Also, EnCase has the ability to export all emails selected in the email tab to Outlook 2003 .msg messages.

**Microsoft EDB** files is the standard mail format for Microsoft Exchange servers. EnCase provides the ability to mount and search large compound EDB files from Exchange 2000 and Exchange 2003 servers to show every e-mail, including the attachments and folder structures to allow for analysis. Data from EDB files can be searched, documented, and extracted just like any other file.

**Lotus Notes NSF** files are the standard mail format for Lotus Notes. NSF files from Lotus Notes 5, 6, 6.5, and 7 can be mounted and read just like EDB, mBox, or other mail storage formats. EnCase can read and decipher IBM Domino server mailbox files.

**DBX files** are typically used by e-mail applications such as Outlook Express. EnCase can open the specific mailbox files and show each e-mail, including attachments and deleted e-mails, in a format for easy analysis. The data can be searched, documented and extracted as needed. EnCase Enterprise automatically decodes the files contained within the DBX by interpreting e-mail attachments that are encoded in Base64, UUE and MIME.

**Web mail** such as Hotmail, Netscape and Yahoo use HTML Web pages instead of a standard mail application. Although there is no single location from the remnants of Web mail usage, there are artifacts that can be analyzed to provide a clear picture of the time of the activity carried out through a Web mail service. EnCase provides automated search for these Web mail services and special filters to allow deep analysis and documentation of Web mail viewed on the target machine within a common interface.

**UNIX mBOX** is a standard mail type for **Mac OS X, Netscape, Firefox**, and UNIX e-mail applications. EnCase can find and open mBOX mail files and show each e-mail, including attachments and folder structure, for easy analysis. The data can be searched, documented and extracted as needed.

**AOL 6, 7, 8 and 9** support provides deep e-mail analysis of the personal file cabinet file structure. EnCase can open PFC files and show each e-mail, including attachments and folder structure, in a format for easy analysis. The data can be searched, documented and extracted as needed.

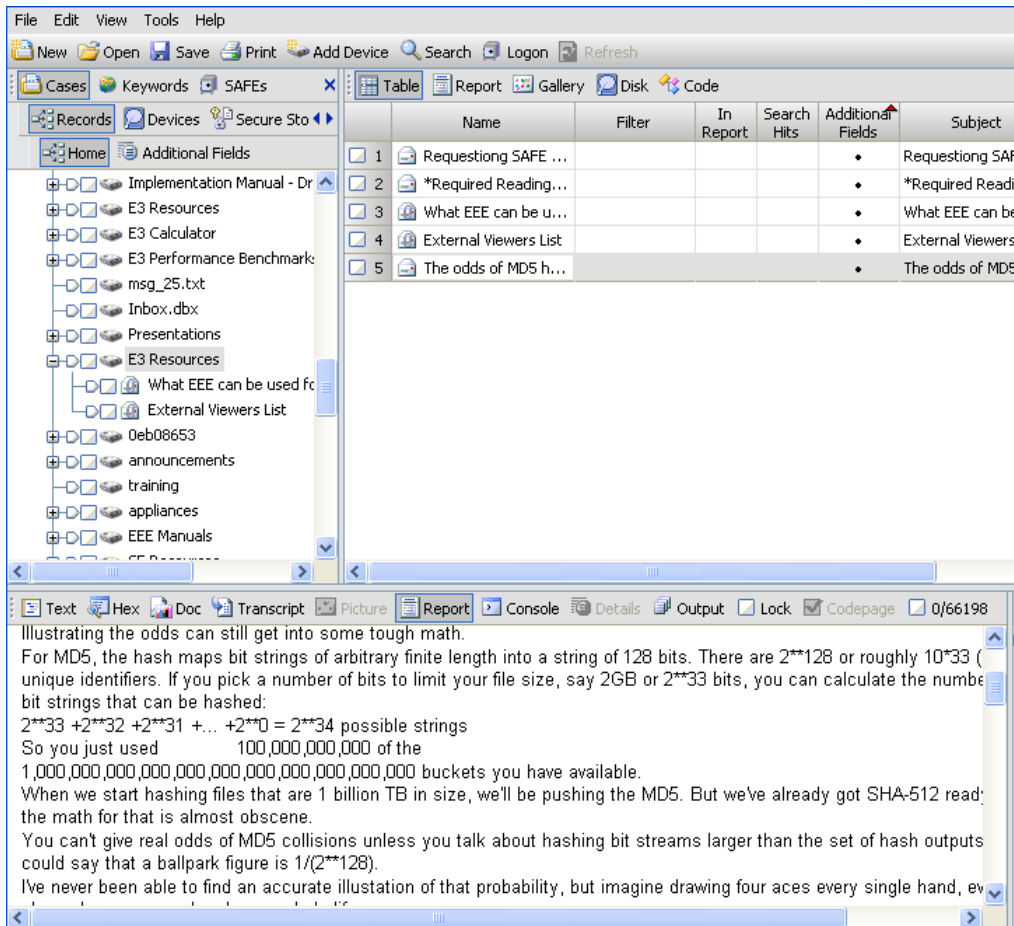
## Records

Email files like PST, DBX, and EDB files, that are parsed on the entries tab will populate in the records tab. Searches run through the search dialog for email and internet history will also populate the records tab. Users can search and bookmark items on the records tab. In addition, the user can modify which properties are displayed in the table using the show column feature in the Table panel. By default, the common email and internet properties are displayed in the table. For view file

structure operations that require a large amount of memory, the EnCase Examiner now uses a temporary disk cache to assist in displaying the records. This should improve the ability to parse large PST and EDB files. To locate additional field information, highlight the additional field column and the details panel in the view pane will activate and display a list of the entries properties and associated values.

E-mail analysis results are placed in a common EnCase format that is easily navigated to quickly find the information needed to support the most complex investigations. The e-mail analysis capability provides a wealth of information to the examiner that can be sorted, filtered and reviewed with several common columns, including:

- **Name** - Subject of the e-mail message
- **From** - Sender of the e-mail. Drafts may not have an entry in the “from” column
- **To** - Recipient of the e-mail message.
- **Subject** - Subject of the e-mail message
- **CC and BCC** – Carbon copy and blind carbon copy recipients
- **Created** - Date the e-mail message was created in Local Time format
- **Sent** - Date the e-mail message was sent in Local Time format
- **Received** - Date the E-mail message was received in Local Time format
- **Attachments** – Identification and access to any attachments within the message
- **Header** - Header information of the message. Internal e-mail messages may not have header information available
- **Folder** - The location of the entry from within the compound file.
- **Delivery Time** – Time that email was delivered.
- **User agent** – The mail agent software the user who sent the mail used.
- **Plus hundreds more.**



**EnCase E-mail Interface**

## DEDICATED INTERNET ARTIFACT ANALYSIS

Every browser or application stores information on machines in different formats and locations. Whether it's a browser, Instant Messaging application or peer-to-peer application, various artifacts persist well after the page was viewed, an IM conversation took place or data was swapped. EnCase provides a growing list of tools to find, analyze, document and interpret these data types and applications.

### Browser History Analysis

The forensic examination and analysis of user activity on the Internet or intranet can be the pivotal point of any case. EnCase exposes powerful selective searching capabilities for Internet artifacts by device, browser type or user. Users can now have EnCase automatically parse, analyze and display various types of Internet, Windows and Macintosh history artifacts logged when Web sites or file directories are accessed through supported browsers, including:

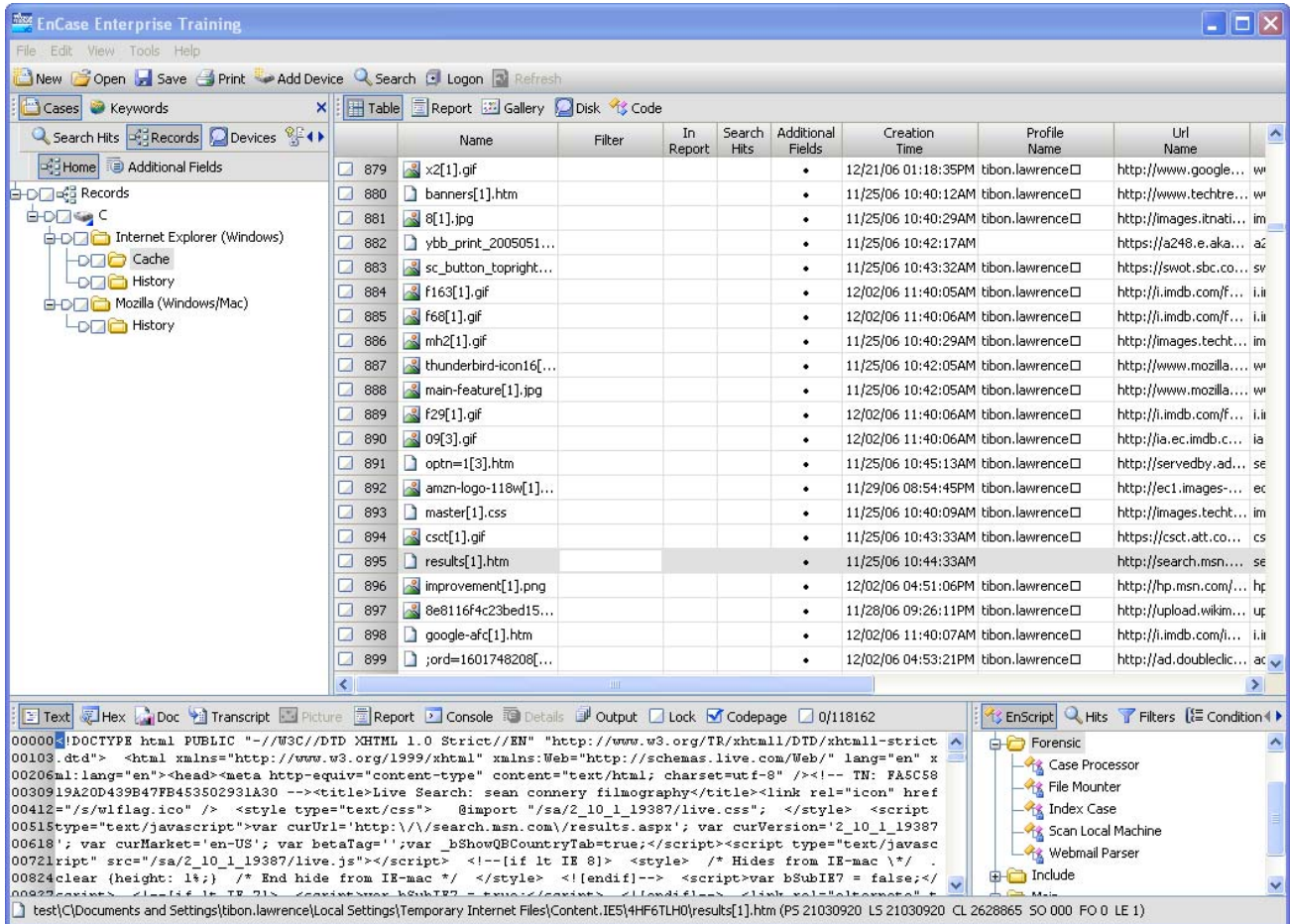
- Internet Explorer
- Mozilla (Firefox)
- Opera

© 2007 Guidance Software. All Rights Reserved.

- Safari

The browser history information is placed in a common interface that is easily navigated to quickly find relevant evidence, such as:

- **URL** - Complete URL address of History entry
- **Host** - Domain Host of the URL
- **User** - Current user that was logged on at the time of visit
- **VisitCount** - Number of times site was visited by the user
- **FirstDate**- Date and time of last visit of user (may or may not be GMT offset)
- **HistoryPath** - Location of the .DAT file from where the entry was parsed



## Internet History Keyword Search

Often, examiners want to only to identify sites visited that have a particular keyword, such as “theft” or “hacking.” The Internet History Keyword Search searches out all browser history artifacts (in allocated space) and writes it in HTML format, letting investigators view the same sites visited by the subject, quickly and easily.

## Web Cache Analysis

Most browsers automatically save cached copies of each Web page viewed, including related pictures, text and multimedia elements. This information is typically referred to as Web cache. EnCase has the ability to automatically find, parse, analyze, display and document various types of Web cache from these popular browsers:

- . • **Internet Explorer**
- . • **Firefox**
- . • **Opera**
- . • **Safari**

The Web cache information is placed in an easy-to-navigate common interface that lets users quickly find relevant information. The Web cache analysis provides wealth of information to the examiner such as:

- **URL Name** - Complete URL of the site viewed.
- **URL Host** – The host URL site.
- **Host** - Domain Host of the URL
- **Cached date** - Date and time the artifact was cached on the local drive
- **Cache path** - Location in which the cached file is located
- **Browser Record Type** – The time span the browser is set to keep history for.
- **Visit count** – The number of times the site was visited.
- **Browser type** - The browser that was used to view the site.
- **Plus many more.**

## HTML Carver

Offers a powerful search and export function that looks for HTML files independent of the browser or Internet enabled application. The HTML carver not only looks for HTML files in allocated space, but also searches unallocated space for HTML file headers to rebuild pages when possible. By searching allocated and unallocated space automatically, EnCase Enterprise saves a tremendous amount of time and yields better search results. This feature can be customized in a variety of ways. Users can, for example, automatically export all HTML pages found and create an index that lets the examiner walk through pages as the person did. The HTML Carver can also search all HTML pages using keywords such as "Hotmail." The HTML Carver gives users flexibility when searching and displaying results and automates tedious, time-consuming manual processes.

## Kazaa Toolkit

Searches a case for a rich set of Kazaa artifacts such as .dbb, .dat files, setting from registry, records in unallocated space and automatically documents them. The feature can reveal a wealth of information on related suspect activities.

## HTML page reconstruction

EnCase can render HTML Web pages from within the Examiner for easy viewing and quick analysis without exporting pages or using external viewers. EnCase can display and document cached HTML pages with readable text, and the associated images.

## Instant Messenger Toolkit

Searches media for Instant Messenger artifacts and automatically documents them. EnCase provides built-in tools to identify and analyze artifacts for AOL, Yahoo and Microsoft Instant

© 2007 Guidance Software. All Rights Reserved.

Messenger applications. Each of these artifacts provides information about the configuration. It reveals which individuals the user communicated with and other relevant information such as chat logs and file transfers.

## **EnScript™**

Many of the powerful automated features and tool sets within EnCase Enterprise (including many of the features previously described) are driven by EnCase EnScript technology. EnScript is a powerful programming language that follows standards consistent with C++ and Java. EnScript lets users automate complex or repetitive tasks. EnScript can also allow communications and with external systems, such as intrusion detection systems and Windows systems through WMI. EnScript allows the investigator to build custom scripts for specific investigative needs and/or automate complex and routine tasks. EnScripts can save investigators days or months of analysis by automating almost any investigative task. EnScripts can also be made into packages, allowing for version licensing and source code protection.

## **Security and Administration**

EnCase Enterprise has the power to reach across and deeply analyze many different facets of any organization, giving users the power to investigate their entire networks. That might include a computer investigation to identify fraud, or an investigation of employees suspected of misconduct or an audit of computers used for financial activity, or a response to a computer-related incident,. Many situations require an organization to control and audit who can access information and whether they're authorized to see that information. EnCase Enterprise provides a number of mechanisms to ensure EnCase users are not only authenticated but also authorized for the functions they are able to perform. Role-based permissions and event logs let users track and control which materials examiners can analyze and what EnCase functions they can use.

### **Role-Based Permissions**

EnCase Enterprise uses a PKI scheme based on open PGP encryption standards to provide secure authentication and entitlement. This solution for entitlement has proven to be robust and secure since its introduction in 1991. The EnCase Enterprise use of role-based permissions provides granular control to ensure proper enforcement of policies and procedures. Every user or user group has a role or multiple roles assigned to them. Those roles determine which materials and functions they can access through EnCase. Roles can be created with various restrictions or limitations. For example, only the incident response team might be allowed to conduct a Snapshot analysis on the Web server farm. Likewise, only the senior investigator is allowed to perform keyword searches on management personnel's computers. The EnCase SAFE security platform provides tremendous flexibility to support your organization's evolving investigative requirements.

### **Logged Events**

Besides administering users and permissions, the SAFE also keeps logs of examiner activity. The logs are stored in an encrypted format and only authorized individuals have access to view log files. These logs provide a key role in chain of custody and understanding the usage and auditing of EnCase Enterprise. For each examiner that performs an investigation of a system, a record is created that shows when they logged in, machines they accessed and which role or roles were used. Macro Logging keeps track of actions that were taken by the investigator through the SAFE. When an examiner performs a preview, acquisition or search on the nodes, the following information is logged: time, user, role, message, status, start and stop time. When the acquisition information is displayed, the hash values are also shown in the report log. EnScript programs that

are run by the investigator will also be logged. The logs are essential for management to understand overall usage of the system and keep track of what investigators are doing. All logfiles are stored on the SAFE machine.

## **EnCase Enterprise Professional Suite**

*A powerful, integrated tool suite that provides flexibility and convenience during enterprise investigations.*

Computer investigations often require that evidence be shared among investigators or with third parties during inter-agency investigations, regulatory audits and other situations. Executives from all departments have a vested interest in computer investigations, as mounting legislation and regulations hold management accountable for self-regulation, financial authenticity and disclosure. Thus, evidence captured by EnCase Enterprise may need to be reviewed by legal, audit or human resources teams – or possibly outside parties. EnCase Enterprise Professional Suite lets you present case findings to non-EnCase users within formats or applications they already use.

In addition to the challenges of viewing and sharing data, dealing with encrypted and password-protected data poses another obstacle. Investigators often spend valuable time attempting to decrypt and unlock protected files, thus redirecting focus away from analysis. EnCase Professional Suite quickly deciphers EFS encrypted files and displays passwords stored in the Windows Registry. The EnCase Enterprise Professional Suite also lets examiners “boot” Windows and non-Windows operating systems from EnCase evidence files using VMware. Investigators can then interact with the operating system as the user did in a read-only state without altering data.

The EnCase Enterprise Professional Suite is a powerful combination of integrated tools that allows seamless sharing of evidentiary data and solves the resource drain of encrypted data. The modules provided in the EnCase Enterprise Professional Suite can be used in conjunction with the powerful network capabilities of EnCase Enterprise. This provides investigators, auditors and/or security professional’s maximum flexibility during investigations and helps mask complexity when forensic data is shared with untrained individuals. Forensic data can be served from EnCase to Microsoft Windows as read-only for further analysis by common applications such as Windows Explorer, third-party Windows utilities or other analytical tools. This allows evidence to be viewed and analyzed in a format familiar to non-EnCase users or non-investigators.

The Encase Enterprise Professional Suite includes additional modules to extend investigative reach, including EnCase Virtual File System (VFS) Server, EnCase Physical Disk Emulator (PDE) and EnCase Decryption Suite (EDS):

### **FastBloc SE**

Fast Bloc SE provides all of the functionality of a hardware write blocking device, but built into the EnCase Examiner. FastBloc SE provides the ability to write block IDE, SCSI, USB, and firewire devices, eliminating the need to stock bulky hardware write blockers. FastBloc SE also give investigators the option to wipe devices attached to controller cards controlled by FastBloc SE, as well as to restore drives while maintaining the hash value of the logical evidence file.

## **eDiscovery Suite**

The EnCase Enterprise eDiscovery suite is a powerful tool provides thorough identification, collection and processing of relevant data on servers, workstations and laptops anywhere on a global network, without disrupting business operations. It eliminates the need for cumbersome and inefficient manual processes that are very costly. You can conduct automated, targeted searches that cull at the point of collection, capturing only potentially relevant data. Then data is automatically processed and uploaded into a review platform. This streamlined process reduces hard costs — by up to 90% — while improving compliance with a very defensible process. The eDiscovery solution combined with the expertise of our professional services group also enables basic, proactive electronic records management audits. All outdated records on the network can be located, categorized and, if desired, erased.

## **AIRS**

Guidance Software has engineered an incident response solution that integrates with alerting and content monitoring tools to field alerts and provide real-time response. It enables incident responders to zero in on compromised machines with unparalleled speed. The Automated Incident Response Suite (AIRS) fields alerts, filters out false positives and assesses whether a machine was actually compromised. As alerts are generated, a real-time "Snapshot" is taken of the target hosts. Immediate analysis from the source and target reveals event details.

For specific events, subsequent automated Snapshots are triggered shortly after the event to show attack results in time slices, revealing whether the event actually occurred, and if so, its impact and origin. The aggregation of IDS event data and EnCase® Snapshot data into a central location, in real time, gives incident responders, security analysts and others the information they need to truly understand whether an incident occurred and its impact.

## **Summary**

It is evident that organizations *must* have a procedural and technical infrastructure in place to immediately respond to computer security breaches and investigate malicious activity and employee malfeasance. Regardless of precautionary measures, computer-related incidents will occur and organizations must be prepared. An organization without an enterprise investigation capability not only has an incomplete security solution, but is also exposed to high levels of risk, potential liability, and at worst case, financial loss.

This paper discussed the numerous benefits, capabilities and detailed features of EnCase Enterprise. It's a powerful network-enabled multi-platform enterprise investigation solution, that enables immediate response to computer related incidents and thorough computer forensic analysis. Immediate response is critical to maintaining business continuity and reducing the impact of incidents or attacks. EnCase Enterprise reduces the incident response time from days or weeks down to seconds. It lets investigators capture critical information and quickly determine the scope and magnitude of security breaches and helps contain and remediate those attacks.

Security professionals, investigators and incident response teams can now reach any part of the enterprise in seconds, conduct thorough investigations, preserve vital forensic data, and produce

© 2007 Guidance Software. All Rights Reserved.

detailed reports of their findings -- without interrupting business operations or taking systems out of service.

## **Additional Resources and Information**

The Guidance Software Web site contains a wealth of information about our products and services, and offers legal resources, white papers, Webinars and more. Visit [www.guidancesoftware.com](http://www.guidancesoftware.com)

### **About Guidance Software**

Guidance Software is the leader in computer forensics and incident response solutions. Founded in 1997 and headquartered in Pasadena, Calif., Guidance Software has offices and training facilities in California, Virginia, New York, and the United Kingdom. More than 13,000 corporate and government investigators depend on EnCase software, while more than 3,500 investigators attend Guidance Software's forensic methodology training annually. Accepted by numerous courts and honored with eWEEK's Excellence Award and SC Magazine's Annual Award, EnCase software is considered the standard forensic tool. For more information, visit [www.guidancesoftware.com](http://www.guidancesoftware.com)

### **Guidance Software Professional Development and Training**

Guidance Software trains more than 3,500 investigators each year and offers a wide curriculum for corporate investigators and security professionals. Classes range from introductory to expert, covering computer forensics and incident response. Other courses focus on Internet and e-mail investigations, network intrusion, NTFS, Linux/UNIX and EnScript programming.

### **Guidance Software Professional Services**

Guidance Software's Professional Services Division offers unparalleled expertise in computer forensics and enterprise investigations. Our consultants include former leading law enforcement, government and corporate cybercrime veterans who are EnCase experts. With unrivaled experience and in-house knowledge our Professional Services Division is the clear choice for investigations, implementations and incident response.