Global Information Assurance Certification Paper

Computer Forensics: EnCase – The Tool of Choice
Ashish Sawhney, CISSP©, i-Net+, Security+
GSEC Version 1.4b Practical
Submitted: September 1, 2003

Abstract

The term forensics is borrowed from the legal and criminology fields where *forensics* pertains to the investigation of crimes; now it has been expanded to include computers and networks and referred to as computer or network forensics.[1] In the IT world, common misconception with forensics is that it is only used to find data that is surreptitiously stored. That is simply not true. Computer forensics refers to the ability to find and evaluate data; either stored on a media (i.e. hard drive) or traveling through the network, without compromising the integrity of the data. The data does not have to be hidden. It can be unencrypted and in plain sight.

The need for computer forensics arose when computers became part of our daily lives. Our dependency on computers has increased astronomically over the last 10 years. Today computers are a necessity for any business to survive. The information that is stored on the computers can easily be manipulated or sent across the wire, increasing the chances of industrial espionage. Organizations spend millions of dollars a year building an infrastructure to secure their proprietary data and to increase employee productivity and efficiency. Computer forensics is a process that can be used to validate and discover the security breaches.[2] This paper will focus on a product that is commercially available to perform computer forensics in a corporate environment.

Analysis

Corporations have a need to be able to verify the contents of an employee's work computer at any given time. This need arises from situations such as espionage, fraud, unauthorized use of resources, hostile environments (harassment), wrongful termination, etc. Usually the verification process involves three areas of a corporation: human resources, legal and auditing. These areas work together to make sure no employee rights are being violated before the verification process begins.

Now the first question at hand is, what product are we talking about? The answer is Guidance Software's EnCase Enterprise Edition referred to as ERAD (**E**nterprise **R**esponse, **A**udit and **D**iscovery).[3] The following series of questions and answers will help clarify the need for ERAD and its functionality for a large enterprise with a network that is either centralized or distributed. Also, these questions will help understand the application architecture and its communication flow.

Q: Why ERAD?
A: First and foremost, Guidance Software Inc. has been recognized as an industry leader in forensics software since it was founded in 1997.[4] Their software has held up to multiple challenges in a courtroom and has set precedence. Users of ERAD can leverage this precedence if ever the needs arise for trial. Second, ERAD brings the power of a graphical environment to the forensic media analyst. Point-and-click, copy-and-paste and other features of a graphical environment make it one of the best evidence analysis tools available.

Q: How and why is ERAD better for corporations?
A: ERAD allows an investigator to quickly and securely preview, acquire and analyze digital media over a Local Area Network (LAN) or a Wide Area Network (WAN). ERAD gives the investigator anytime/anywhere response capability without ever having to leave his/her desk. Prior to ERAD, the only alternative an investigator had, was to travel to where the media was located or have the media shipped to their location. Use of ERAD has translated into cost savings in travel and shipping of media and a much faster response for corporations.

Q: What are the components of ERAD?
A: ERAD architecture consists of three pieces: SAFE server, Examiner and a Servlet.

Q: What is the function of a SAFE Server?
A: The SAFE (Secure Authentication for EnCase) server has three main functions:

- To authenticate each investigator via PGP public key authentication to each SAFE server.
- To establish access based on the investigators' role (role-based security) Example: Investigator A assigned to the Human resources network segment may not access the Financial Services network segment that is assigned to Investigator B.
- To assign unique rights to investigators for each network device or group of devices. The SAFE server GUI gives the administrator an overall view of all rights for each given investigator and for all network devices the investigator can access.[5]

Q: Does the SAFE have any Role-Based security permissions?
A: The SAFE has three roles: Keymaster, Administrator and Examiner.

Q: What is the function of a Keymaster?
A: Keymaster is the super administrator of the SAFE server. It is the only account that exists after the installation of the SAFE. The Keymaster then must logon and create user accounts for the SAFE administrator and the

examiners. Guidance Software recommends that the Keymaster be a C-level (CEO, CFO, CSO, etc.) or a senior executive due to the power the account possess.

Q: What is the function of the Administrator?
A: The Administrator is the individual who is in charge of the day-to-day administration of the SAFE. Administrator role has the authority to grant permissions to Examiners.

Q: What is the function of an Examiner?
A: Examiner is a general term used to identify the investigators who are permitted to access the SAFE. Examiner is also the GUI that runs on an investigators machine and "talks" to the Servlet.

Q: What is the function of the Servlet?
A: The Servlet runs on a network device to be accessed by an investigator. It runs as a service with administrative privileges on each target machine without any user intervention. It allows the Examiner machine to identify, preview, and acquire local and networked devices.

Q: Does ERAD provide any logging?
A: ERAD does provide some logging capabilities. The log stores information on all transactions conducted by a specified user on a particular SAFE server. This log can be used as an initial Chain of Custody log by indicating the date and time a particular machine was previewed or acquired. ERAD also provides a certain level of auditing which allows the administrator of the SAFE server to determine if a user is misusing the system.

Q: How does ERAD work over LAN/WAN?
A: ERAD is a three-tier client/server application. The Servlet is placed and executed on a client machine and the communication session is established between the client and the examiner. The client can be located anywhere geographically; as long as there is IP connectivity, communication can be established.

Q: How does the communication flow in ERAD?
A: For any components of ERAD to communicate, they must first complete an authentication process involving high-level public key encryption. ERAD uses 128-bit AES encryption. The examiner first authenticates to the SAFE server using public/private key encryption. Once the Examiner is authenticated, SAFE verifies the investigators authority to access the particular network device.[6]

If the investigator has the authorization to access the network device, the SAFE opens a secured communication channel on a predetermined port

to the Servlet on the network device and “hands-off” the communication to the Examiner. This enables the investigator to securely identify, preview and acquire the target machine. Once the investigator is done examining the target machine, the communication is simply terminated and the Servlet returns to a passive state till the next time an examination needs to take place.

This client/server approach to forensics allows the investigators to be located anywhere geographically but still limits their authority by having all access controlled at a centralized server. See Figure 1 for the communication flow diagram.

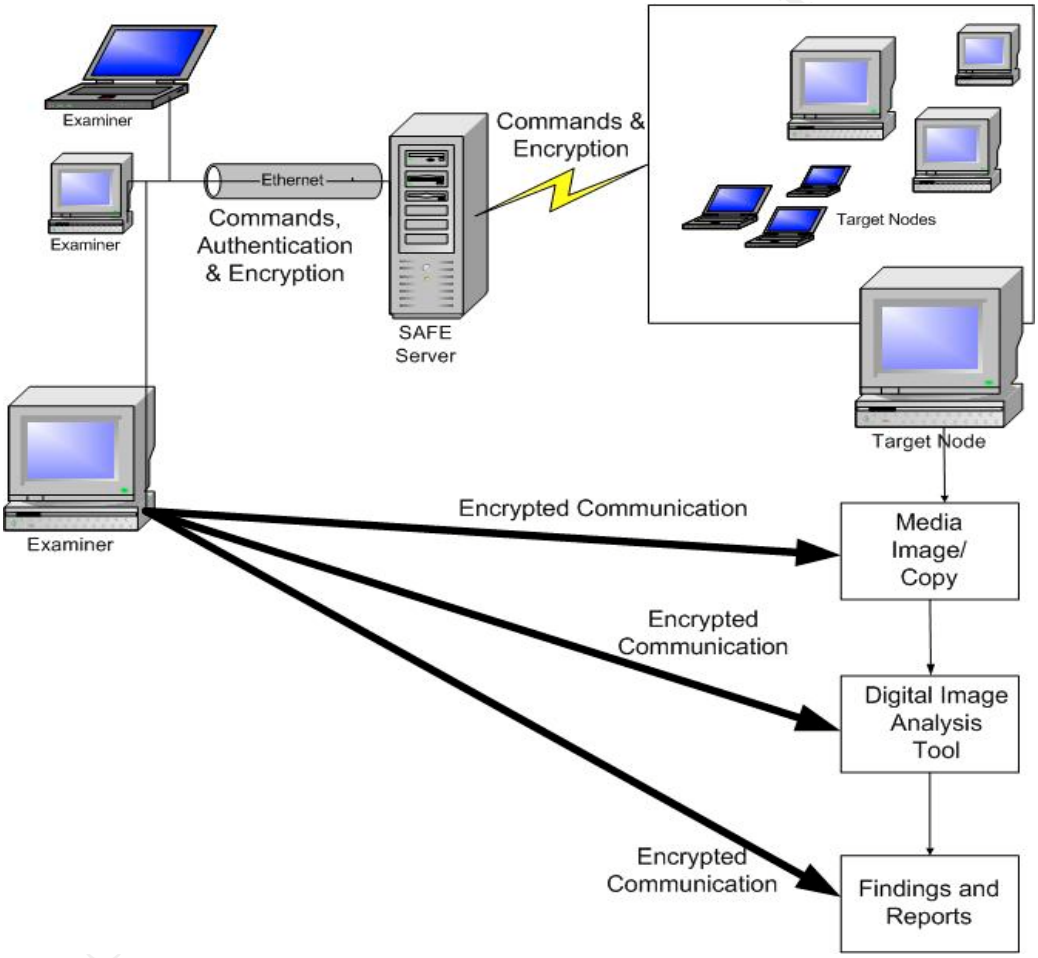

Figure 1

Q: What capabilities does an investigator have on the target machine while using the Examiner?

A: While using the Examiner, an investigator can preview the entire machine as if he/she had physical access to it. The investigator has the capability to extract individual files or duplicate the entire drive at a bit level;

meaning, all data is duplicated including anything that has been deleted. Investigator can also recover deleted or damaged files and track and follow a trail of events; all from the Examiner machine.

NOTE: *At no point does the investigator have the capability to alter any information on the target machine. This ensures data integrity*.

Q: How does EnCase ensure drive image that is created is not contaminated or tampered with?

A: For each case being worked on, EnCase creates an Evidence File. The evidence file consists of three parts: header, checksum and data blocks. When the evidence file is created, user inputs information pertinent to the investigation. This information, along with contents of the disk, is stored in the evidence file.

Every file is an exact sector-by-sector copy of the media being examined. The media could be a hard drive or any removable media (floppy, flash cards, jazz, etc). Each and every byte of the file is verified using a 32-bit Cyclical Redundancy Check (CRC)[7]. EnCase computes a CRC for every block of 64 sectors rather than computer a CRC value for the entire disk image.

Additionally, EnCase also calculates a MD5[8] Hash when a physical or a logical volume is acquired. The calculated hash value is written into the evidence file and becomes a permanent part of the case documentation. When an evidence file is added to a case, EnCase automatically verifies the CRC values, and re-computes the hash value. These re-computed values along with the values from when the media was acquired are both added to the EnCase report for confirmation that Evidence File was not altered since its' acquisition.

Q: What is hash analysis?

A: Hash is a number generated based on a string of text. Then generated number itself if very small compared to the size of the file. A file hash is similar to fingerprint; for all practical purposes it is considered unique. EnCase uses MD5 algorithm to generate hash values. With the use of MD5 algorithm likelihood that any two files have the same have value is 2^{128}.

EnCase stores hash values of known files internally in hash libraries. Since the hash value is computed based on the contents of the file and the file name has no bearing on it, EnCase can use hash values for comparison and aid the investigator in finding or ignoring specific files.

Example: If an investigator is looking for the SubSeven[9] executable, he/she would generate the hash value of the executable and add it to the

EnCase hash library. Next, by executing the hash analysis EnCase will scour the storage media in an attempt to match the SubSeven hash value with the hash value of every file (regardless of its' name) on the storage media.

Another helpful use of the hash analysis is when an investigator might choose to ignore a set of files as part of an investigation. This is especially helpful in corporate environments where an enterprise base load is created for all computers. By generating hash values for all the files in the base load and adding them the hash library, an investigator may be able to omit thousands of files from the investigation without affecting the outcome of the investigation. This results in time saved, which translates to money saved.

Q: What is signature analysis?
A: Every file has a signature, also known as a file header, which defines what type of file it is so that a program can properly recognize and associate it. There are several thousand file types and out of those many have been standardized by the International Standards Organization (ISO), and the International Telecommunications Union, Telecommunication Standardization Sector (ITU-T).

Examples:

File Signature	File Extension	Description
47 49 46 38 37 61	GIF	GIF87a Graphics interchange format file
47 49 46 38 39 61	GIF	GIF89a Graphics interchange format file
E3 82 85 96	PWL	Windows Password File
89 50 4E 47 0D 0A 1A 0A	PNG	Portable Network Graphics File
52 45 47 45 44 49 54 34	REG, SUD	Windows NT Registry and Registry Undo files

Table 1 - File Signatures[10]

Some users are known to deliberately change the file extensions to hide data. When a file extension is changed the file signature does not change but most programs won't recognize what the file is. Meaning if a JPEG file extension is changed from .JPG to .DLL, most programs won't be able to recognize it as an image file. To make sure there are no data that is being surreptitiously stored, it is important to perform signature analysis[11].

EnCase contains a table of known file signatures, which can be modified or added to as the need might arise. EnCase, with click of a button, allows the investigator to compare the file signatures with its' internal

table. After the comparison is finished, Encase labels the files in one of 4 ways:

- !Bad Signature
- *[Alias]
- Match
- Unknown

!Bad Signature – indicates the extension exists in the file signature table but the header is incorrect, and the header is not in the file signature table

***[Alias] –** indicates the header is in the file signature table and the extension is incorrect. This is an indication that the extension of the file has been changed.

Match – indicates the header matches the extension

Unknown – indicates neither the header nor the file extensions are listed in the file signature table.

Q: What is EnScript?

A: EnScript is a macro-programming language designed to work within the EnCase environment. The EnScripts are same as executable files. With the use of EnScripts, an investigator can create and delete files/folders on local drives; hence, caution must be used when using EnScripts.[12]

EnScripts, when used properly, can be a very powerful and helpful tool for an investigation. Some of the prepackaged EnScripts allow an investigator to perform actions such as find and extract all graphic files on a given media regardless of the fact the files might now exist in the unallocated clusters. Another example of a prepackaged EnScript is one that recovers every HTML link a user visited.

Q: Can keyword or phrase searches be performed in ERAD?

A: ERAD provides the capability to perform keyword, phrase and GREP[13] searches. It allows the investigator to control the search location by selecting individual files, folders or the entire case that can contain multiple storage media. It performs the searches on each term byte-by-byte from start to finish at both logical and physical level. ERAD also allows the keywords and phrase searches to be case sensitive.

An investigator can use GREP expressions to perform searches within ERAD. GREP is a search utility with very powerful and flexible syntax. It enables an investigator to limit the false hits by being extremely specific or allows the search results to be very broad by allowing wildcards, in the search criterion. Any and all search results can be bookmarked. Bookmarking gives an investigator opportunity for an in-depth review at a later time. It also allows provides for the option to add bookmarked material to the final case report.

Q: What type of reporting does ERAD provide?
A: ERAD provides the investigator with the ability to create a final case report in either a Rich Text Format (RTF) or a HTML format.

The report itself can contain anything from found images or text fragments from files and emails. The report also contains information regarding physical and logical characteristics (partitions, size, sectors, etc.) of all media being examined. It lists the investigators name, the acquisition hash value and the verification hash value. The investigator might also choose to include the folder structure for the entire drive.

Q: Are there any product limitations of ERAD?
A: Unfortunately ERAD Servlet only works on Windows 95, 98, ME, NT, 2000 and XP. Support for UNIX platforms is currently under development.

As powerful of tool as ERAD is, it does have its' share of bugs. It appears as though there is a new version of ERAD released every few weeks. On the surface that might appear as if the Guidance Software is being extremely diligent in producing a robust product, but that is not the case. Guidance Software is a company of approximately 100 employees, which apparently is not enough to provide a decent level of Quality and Assurance on their products before they are released.

With every new release that adds functionality to the product, something else stops working. I believe Guidance is still trying to accept the fact that large corporations will be using their product. It might be easy for small shops to upgrade their software, but for a large corporation it is a monumental task. For every new release, corporations have to retest the ERAD software to ensure compatibility with other enterprise applications. I have experienced problems with ERAD (first hand), where a newer version starts to crash windows machines but the old one works fine. After some testing it was discovered the new release was checking for a specific connected device and if the device were not found, machine would crash. This is the kind of problem that should be discovered during Q&A.

Everything considered, Guidance Software, Inc. still shines brightly above the rest of the pack. EnCase ERAD is a product that provides digital risk management by allowing anytime/anywhere response. Guidance Software, Inc delivers a service that is desperately needed by corporations and law enforcement.

Conclusion

Corporations have finally started to embrace computer forensics as an incident response and an enterprise investigation tool because reality of perimeter security breaches and internal threats are finally becoming more apparent. New legislation in many cases is starting to mandate corporate practices. For comprehensive security and risk management, corporations must have enterprise-wide incident response, policy auditing and discovery capabilities. ERAD, with its' client/server architecture, enables corporations for immediate response without costly travel and expense charges. This also enables quick response to incidents, reducing response time to hours instead of days or weeks.

References

[1] Robbins, Judd. An Explanation of Computer Forensics [Online]
URL: http://www.computerforensics.net/forensics.htm

[2] King, N. & Weiss, E. (2002, February) ANALYZE THIS! Network forensics analysis tools (NFATs) reveal insecurities, turn sysadmins into systems detectives. Information Security, [Online] URL: http://www.infosecuritymag.com/2002/feb/cover.shtml

[3] URL: http://www.guidancesoftware.com/products/EnCaseEnterprise/productinfo.shtm

[4] Tullett, J. (2003, January). Product Selection: EnCase Enterprise Edition. SCMagazine, [Online]
URL: http://www.scmagazine.com/scmagazine/2003_01/review_1/

[5] URL: http://www.encase.com/products/EnCaseEnterprise/productinfo.shtm

[6] URL: http://www.encase.com/corporate/whitepapers/downloads/EEEInside.pdf

[7] URL: http://www.amherst.edu/~leneel/crchow.html

[8] URL: http://www.ietf.org/rfc/rfc1321.txt

[9] URL: http://www.subseven.ws/

[10] URL: http://www.garykessler.net/library/file_sigs.html

[11] URL: http://www.securityfocus.com/infocus/1294

[12] URL: http://www.encase.com/support/enscript/index.shtm

[13] URL: http://logidac.com/abuseEmail/grep/aboutgrep.html