Global Information Assurance Certification Paper

Computer Forensic Software in a Corporate Environment
Shannon C. Perkins
June 16, 2003

Abstract

In a corporation, employees can use the computer network to commit a wide variety of crimes and misconduct. Therefore, the recovery of digital evidence has become more and more important to corporations in civil and criminal prosecutions as well as assisting in the dismissal of employees. Digital evidence can assist in proving fraud, theft, blackmail, child pornography, identity theft, sending harassing or threatening emails, hacking into others computers, sexual harassment, industrial espionage, employee misconduct and intellectual property theft.

This paper will explore one way a corporation can forensically gather evidence to support an electronic investigation using EnCase Forensic Edition and Encase Enterprise Edition.

What is Computer Forensics?

As in any investigation, establishing that an incident has occurred is the first step. Then, the incident needs to be evaluated to determine if computer forensics is needed. In my research I have come across a number of definitions for computer forensics. It seems the definition has evolved over the years. A simple definition of computer forensics is "the processes of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable (McKemmish, 1999)." You can think of computer forensics as solving a computer mystery. According to Rodney McKemmish (1999), forensic computing has four key elements:

1. Identification of digital evidence – knowing what evidence is present, where it is stored and how it is stored.
2. Preservation of digital evidence – it is imperative that any examination of the electronically stored data be carried out in the least intrusive manner.
3. Analysis of digital evidence – the extraction, processing, and interpretation of digital data.
4. Presentation of digital evidence – the actual presentation in a court of law. This includes the manner of presentation, the expertise and qualifications of the presenter and the credibility of the processes employed to produce the evidence being tendered.

Forensic investigators can use several methods for discovering the data that resides in a computer system, and recover deleted, encrypted, or damaged file information, preserve it, analyze it and present it in a court of law.

Why is Computer Forensics Needed?

According to Peter Sommer (1997) computers have appeared in the course of litigation for over twenty-five years. In 1977, there were 291 US federal cases and 246 state cases in which the word "computer" appears and which were sufficiently important to be noted in the Lexis database (Sommer, 1997). A specialized computer forensic unit may be important to a large company to assist in a possible litigation and to deal with incident response.

Incident Response means actions taken to deal with an incident that occurs (Schultz, 2002). Incident response in a company's computer network could mean the actions taken to deal with harassment via email, pornography trafficking, organized crime activity, industrial espionage, employee misconduct and intellectual property theft.

Companies have a couple of options when it comes to dealing with computer forensics for incident response. The company can either hire a private sector forensic expert to come in and do the forensic investigation as needed or the company can train and employee their own computer forensics experts. The cost

There are a few computer forensic software products such as EnCase, SafeBack Mirror Image Backup Software and iLook (used by law enforcement only) that could be used to aid in performing a forensic investigation. While SafeBack's primary use is to preserve computer related evidence on computer hard disk drives, it can also be used covertly to duplicate all storage areas on a computer hard disk drive[1]. While SafeBack is limited to copying and preserving evidence, Guidance's EnCase products offer a single software tool that addresses all aspects of the investigation. EnCase has a graphical interface to view and manager all of the evidence on a hard drive. EnCase also allows for forensic investigations to be performed over a network or in a stand-alone version.

Computer evidence, unlike paper evidence can often exist in many forms, with earlier versions still accessible on a computer disk. Knowing the possibility of their existence, even alternate formats of the same data can be discovered. A computer forensics professional is needed to ensure that a subjects computer system is handled properly, that no evidence is damaged, destroyed, or compromised by the procedures used to investigate the computer.

When investigating a hard drive, the analysis should be performed on a copy of the hard drive and never, except under the most extraordinary circumstances, or during a live analysis, on the original. The copy should be made in such a way as to not alter the original information in any way and the copy must be authenticated as an exact duplicate of the original. The analysis process should not alter the information in any way.

[1] New Technologies Inc. http://www.forensics-intl.com/safeback.html

Guidance Software Inc. offers 2 forensic products: a stand-alone version called EnCase Forensic Edition and a network version called EnCase Enterprise Edition (EEE). Using EnCase Enterprise Edition or the Forensic Edition will allow a forensic investigator to adhere to all of the above restrictions. Both products will allow for forensic analysis that will hold up in a court of law.

EnCase Forensic Edition

EnCase Forensic version is a stand-alone copy of EnCase. Guidance developed EnCase on specifications and requirements from law enforcement. Guidance tried to simplify the process of searching a computer, documenting the search and making forensic evidence copies by developing EnCase. EnCase is a non-invasive way to perform a forensic investigation on a suspect machine.

With EnCase, you can save an exact snapshot of the hard drive or CD-ROM and save it to an evidence file. You can also view the hard drive image, view files without changing the file contents or date-time stamps, analyze the file structure and perform keyword searches, GREP searches and bookmark your findings for a report.

With the EnCase Forensic version, investigators start by placing a suspect's hard drive in a forensic computer and then make a bit-by-bit image of the drive. To do this, you acquire the hard drive either in DOS or Windows. EnCase Forensic Edition makes a mirror image of the hard drive that is read only. This read only image prevents investigators from altering the data or invalidating any possible evidence.

EnCase Enterprise Edition

EnCase Enterprise Edition is an enterprise response, auditing, and discovery (ERAD) solution. EnCase Enterprise Edition is the first ever network-enabled computer forensic software that enables investigators to immediately preview, acquire and analyze all digital information connected to a wide-area-network[2]. The EnCase Enterprise Edition is based upon the same technology as the standalone forensic edition; only it is modified to run in a live enterprise environment to provide a real-time response, recovery and analysis capability. EEE is not completely identical to the stand-alone version. The enterprise edition offers numerous advantages over the stand-alone version. It allows for the remote analysis of files over the network, and provides the only available mechanism for live, disk-level analysis of remote drives.

There are three parts to EEE: the SAFE server, examiner machine, and the servlet. The SAFE controls all the access and is a secured server that

[2] Guidance Software Inc.
http://www.guidancesoftware.com/products/software/encaseenterprise/prodbrochure.shtm

authenticates the users. The way the SAFE authenticates a user is on public key encryption. To control access, user accounts can be set up and can be granted different role based permissions. You can allow a role to have all permissions including permission to acquire a computer, create users and roles, edit network layouts, and view logs. While other roles may only be allowed to acquire a computer and nothing else.
The servlet is generated when the SAFE server is installed. That servlet is then placed on a machine you wish to acquire, or access with the Examiner. The servlet runs as a service and has local system account privileges. The SAFE sends the servlet commands and the servlet uses port 4445 to listen for the commands. The servlet is set to automatically start every time the user turns on their system.

The Examiner is a workstation that has the EnCase software installed on it. From the Examiner you can manage the SAFE server. The Keymaster, or super administrator, has the ability to create users and roles and add network devices. The Keymaster shouldn't perform investigations, so s/he will create user accounts and can delegate the Keymaster responsibilities to an administrator of the SAFE. According to Guidance Software Inc. the Keymaster should be a C-level of the company (CEO, CFO, CIO), or a senior executive not likely to leave the company that has corporate liability[3]. From the Examiner you can also perform a preview of a device over the network as well as an acquisition of a hard drive or a keyword search.

Both versions of EnCase allow an investigator to view all of the data that the operating system alone could not let you view – including file slack, unallocated space and deleted files. File slack is the space between the logical end and the physical end of a file. Remnants of previous files or folders could be found in the file slack. Ram slack is the space from the end of the file to the end of the containing sector. It is random data plucked from the system's RAM to fill in the space left between end of a file and end of a sector. For example, if you have a 512-byte sector and 300 bytes of data, you will have 212 bytes of RAM slack. By viewing the data in the unallocated space, you may see some deleted file data, which can be very beneficial.

Free space is basically any information on a hard drive that is not allocated to a file. This includes both space that has never been allocated to a file and space that is considered unallocated after file deletion. By comparing known file signatures with file extensions EnCase allows an investigator to determine if a person has tried to hide evidence. Most files have a unique 'signature' within their header and/or footer made up of a few bytes at the beginning of the sector. File signature analysis compares the evidence file signatures against a database of known signatures.

[3] Guidance Software EnCase Enterprise Edition Administrator Manual, p.9.

With EnCase, you can view the data by table, gallery, timeline or report view. The table view is similar to a spreadsheet format. You can sort files by name, date, or size. With the gallery view, you can see all graphical images on the hard drive. The timeline view allows you to see event times from days, to months to years. EnCase allows you to view all files on a hard drive and even recover deleted files. You are able to tell when the last time a file was modified, and where it was located on the computer. Performing a keyword search allows an examiner to find any file that may have that word in it anywhere on that physical or logical drive.

Other features of EnCase are the filters, bookmaking and reporting. Filters are used to limit the information you see in a case. For example, you could filter the files to see only those whose hash category is unknown. The bookmark feature allows you to save files, folders, or sections of a file by highlighting them and saving them. This allows for easy reference. If you perform a keyword search for "credit card" and those words were found in a Word document, you can highlight just that section or text fragment and bookmark it. You can then add that bookmark to the report. The report will then show the text fragment, and list what file the bookmark was made from. You can also bookmark any notable files, and folder information.

When you are done with the forensic examination, you can report their findings with EnCase's reporting function. You can choose what method you want to do the report in. You can do a report that is broken up into sub-reports or you can do a paperless report that includes hyperlinks and supporting documentation and files all burnt to a compact disk or DVD. Reports can be customized to the liking of the examiner. Reports can also contain recovered Outlook email text and attachments. The report can also contain the file properties such as file name, file extension, type, signature, last accessed, last written, file created, entry modified, original path and if the file was deleted or not. The original path will indicate where the deleted file originally came from.

EnCase Enterprise also has a feature called Wipe Drive. This command will allow you to wipe the drive, overwriting all sectors on the drive. This will destroy all data on the drive. You will only want to do this when the case is closed and all evidence is gathered. You may want to consult with your companies Legal department before doing the hard drive wipe.

Acquiring Different Types of Drives

Using EnCase Enterprise version, you can acquire a hard drive directly into Windows over the network using the EnCase application. But, if you are using the EnCase Forensic Edition, acquisitions can be performed several different ways: DOS acquisition with a parallel port or network cable, drive to drive and FastBlock acquisition.

I have found that FastBlock acquisitions tend to be the fastest. The FastBlock is a write-blocked device. You can preview and acquire the subject drive quickly and safely in a Windows environment. The FastBlock device is compact and portable. You attach the subject drive to the FastBlock and can add that device within EnCase. When adding the device you will add a local drive and then choose the FastBlock device. Before previewing and acquiring the drive, you can edit the device name, notes and other properties.

The DOS acquisition requires you to make an EnCase boot disk before you can acquire in DOS. The computer must then be booted with the EnCase boot disk. The subject hard drive must be connected to the forensic computer with a parallel port or crossover cable so you can acquire it. Once the drive has been connected, EnCase can be booted up in DOS mode by typing 'en' at the DOS prompt. EnCase locks all local hard drives when it is launched, therefore, you must unlock the hard drive where you will be storing the evidence or where you will be acquiring the drive to. DOS displays physical disks on the left hand side of the screen and logical volumes on the right side.

A drawback for DOS is that it can only recognize certain file systems: FAT32 and FAT16. FAT stands for File Allocation Table. FAT file system was invented in 1977 as a way to store data on floppy disks. Although originally intended for floppy disks, FAT has been modified to be a fast, and flexible system for managing data on both removable and fixed media. A file system is the overall structure in which files are named, stored, and organized. NTFS, FAT, and FAT32 are types of file systems.

Once the acquisition is complete, the subject hard drive should be removed. The computer can then be rebooted and EnCase can be opened in Windows to view the evidence file.

Another way of acquiring the drive in DOS is to do a drive-to-drive acquisition. To do this, you would place the subject hard drive in the actual forensic computer (i.e. both hard drives are on the same motherboard). Drive-to-drive acquisition would be second fastest to the FastBlock acquisition.

No matter which type of acquisition you choose to do, during the process you will be prompted to enter certain information about the acquisition such as compression, output path, file segment size and if you want to generate an image hash. At this point, you can password protect the file if you chose.

Authentication of the Data

Federal Rule of Evidence 901(a) states that the authentication of a document (including a computer file) is "satisfied by evidence sufficient to support a finding that the matter in question is what the proponent claims (Patzakis)." Where direct testimony is not available, a document may be authenticated through

circumstantial evidence. A computer forensic examination is often an effective means to authenticate electronic evidence through circumstantial evidence. The examiner must be able to provide competent and sufficient testimony to connect the recovered data to the matter in question[4]. Using EnCase does not modify any of the electronic evidence. The Evidence File consists of four parts: the file header, the checksums and the data blocks and the MD5 block. These parts all work together to provide a secure and self-checking "exact snapshot" of the computer disk at the time of analysis.

The EnCase process is the documented chain of custody information that is automatically generated at the time of acquisition, and continually self-verified thereafter. The time and date of acquisition, the system clock readings of the examiner's computer, the acquisition MD5 hash value, the examiner's name and other information are stored in the header to the EnCase Evidence File.[5] This information cannot be modified and will hold up in a court of law.

Checksums are very important during a forensic examination. A checksum is a count of the number of bits in a transmission unit that is included with the unit. With this, the receiver can check to see whether the same number of bits arrived. If the counts match, it's assumed that the complete transmission was received.

The most commonly accepted and used checksum is the MD5 algorithm. The MD5 algorithm creates a 128-bit checksum from a file. The checksum is also known as a hash value. If the file content is altered, so is the hash value. The hash value does not change if only the file name is altered. The MD5 hash value is generated to verify the integrity of the files and data and to cut down on the amount of data that needs to be investigated. MD5 was developed by RSA and is publicly available. If the hash values of two files match, it is almost certain that the two file contents match exactly.

The MD5 has value is used to determine whether or not the contents of a file have been altered. MD5 can also be used to identify files with identical contents (regardless of the names that have been given to the files).

For pre-incident preparation, create a baseline of checksums for critical system files or the complete base load for a computer system. This can be used to verify a compromised system and prevents you from having to verify a file line by line.

EnCase automates generating the hash values. With EnCase you can verify that the evidence file EnCase created is the same as the original. With EnCase, an investigator can even create their own hash sets to be used with other investigations. Hash analysis will be used to identify files, which are not of interest such as operating system files, or files that may be on the computers

[4] Guidance Software Legal Journal http://www.guidancesoftware.com/support/downloads/legaljournal.pdf
[5] Guidance Software Legal Journal http://www.guidancesoftware.com/support/downloads/legaljournal.pdf

base load for your particular company. Hash analysis can also be very helpful in determining if child pornography is saved on a computer system.

Live Response

Earlier I mentioned that analysis should be performed on a copy of the hard drive. This is usually true except in certain circumstances when live analysis is necessary. There are several reasons why you would want to do a live analysis of a machine. Brining down a system or server can cause damage to the business operations and the company could lose money. Doing a live analysis may be cost beneficial to your company.

Another reason to do live analysis is to access pertinent, volatile data that would be lost or disappear if the system were shut down. With a live analysis, you can see process that are running, open ports, and data in RAM. Evidence may be lost between the hours it takes to get the hard drive after an incident has been found. Depending on the size of the company, the computer system may not even be located in your state. Being able to do a quick preview over the network will save on travel and time.

EnScripts and Filters

I have found that the EnScripts and filters are very helpful during an investigation. EnScript is a programming language that is consistent with C++ and Java Script. EnScript automates searches. For example, you can run a script that will find a unique email address or Internet history for that system. Another EnScript can search for either .doc or .xls files in all files including unallocated clusters. One of the EnScripts that I use the most is the graphic file finder. With the graphic file finder, it bookmarks every JPG, GIF, BMP and EMF file. It searches the unallocated clusters and files with a specific extension. This is very helpful because it finds the files that are in the unallocated clusters. These are files you may not see with a cursory review of the hard drive. Another EnScript is the MSN and Yahoo messenger parsers. The MSN Messenger script looks for "Session Start" and "Session Close" and bookmarks it. The Yahoo messenger script parses the Yahoo messenger archive and history files from allocated clusters.

Filters will filter the information displayed in the EnCase table, gallery, timeline and report. You are able to write your own filter, but there are also some that come with EnCase. You can also download updates from their website. Some of the filters can be used to search the registry files, log files and Internet files. They are similar to EnScripts, but they are much shorter in syntax.

I find the EnScripts and filters to be extremely helpful. What evidence you would look for depends on the type of investigation you have. If you have a case of suspected pornography, the graphic file finder will be very valuable since it can

find the files in the unallocated clusters. If you have a case where you are investigating some kind of fraud, the document file finder and the unique email finder will be helpful. No matter what the investigation is, there will be a script or filter that you can run. In the worse case scenario, you can write your own.

INFO2

EnCase is able to find files that were once in the recycle bin. The files are called INFO2 files. The date and time the file was deleted is recorded in the INFO2 file. They can be recovered from allocated and unallocated clusters. You will need to run an EnScript to recover the INFO2 file. Once they are recovered, they will appear under the bookmark tab. I have found this to be very valuable in investigations. If the suspect knows someone is watching them and is trying to destroy computer evidence, INFO2 is a good place to look.

Skills

EnCase is just one forensic tool to use for computer forensic examinations. For a well-rounded forensic examiner, one should possess most, if not all, of the following skills:

1. A good understanding of basic rules of evidence, as they relate to:
    a. The seizure or acquisition of magnetic media
    b. The handling, marking and storage of electronic evidence
    c. The "chain of custody" and The "right to privacy"
2. A good understanding of how to wipe, verify and validate media
3. A good understanding of how to protect the original media for accidental writes
4. A good understanding of how to make and verify exact copies of media
5. A basic understanding of PC hardware and networking
6. A good understanding of Microsoft FAT file system data storage and recovery
7. A good understanding of Microsoft Office applications and how to access the metadata that is stored within MS Office documents
8. A basic understanding of common data formats by header, appearance, etc.
9. A basic understanding of how to defeat passwords
10. A basic understanding of Internet issues, such as doing a "who is", and determining ownership of a domain name
11. The ability to write clear understandable reports
12. The ability to organize and present exhibits in or as an attachment to reports

In addition to the above skills, a forensic examiner should possess logical thinking skills, be able to uncover and understand the cause and effect of a computer's actions, and possess an open mind.

Summary

Unless you work for a large corporation or a financial institute, having your own forensic investigation unit may not be cost beneficial. It may be less expensive for a company to contract out by the hour when an incident happens rather than have several salaried employees that they must keep trained and up to speed on the latest advances in computer forensics.

Despite the cost, corporations can benefit from computer forensics by assisting in civil and criminal prosecutions. Whether a company is looking for forensic evidence to terminate an employee for wrongdoing or to preserve digital evidence for possible future litigation, forensic software can play a key role. As people get more sophisticated in committing computer crimes, forensic computing may become more utilized. The evidence gathered must be forensically sound to stand up in a court of law. To do an accurate investigation, a company needs to make sure all the steps of acquiring, preserving, retrieving and presenting data has been done correctly. A valid and reliable method to recover data is necessary. Using EnCase is a way to do just that.

References

Commercenet Research Council (1999). "2000 Industry Statistics" Available at: http://www.commercenet.com/research/stats/wwstats.html

Guidance Software Inc. EnCase Enterprise Edition Administrator Manual. 2002 pg. 9

Guidance Software Inc. "EnCase Enterprise Edition: Product Information." Available at: http://www.guidancesoftware.com/products/software/encaseenterprise/prodbrochure.shtm (2003)

Guidance Software Inc. "Guidance Software Legal Journal" Available at: http://www.guidancesoftware.com/support/downloads/legaljournal.pdf (2003)

Hijazi, Nesrin. "GIDEON Alert: Trading Privacy for Personalization." Available at: http://www.commercenet.com/research/facts-figures-forecasts/2000/00_01_fff.html#B2B (2000)

McKemmish, Rodney. "What is Forensic Computing" Trends and Issues in crime and criminal justice. Available at: http://www.aic.gov.au/publications/tandi/tandi118.html (1999)

New Technologies Inc. Available at: http://www.forensics-intl.com/safeback.html (2003)

Patzakis, John "Evidentiary Authentication Within the EnCase Enterprise Process." Available at: http://www.guidancesoftware.com/whitepapers/EEEauthentication.pdf

Schultz, Eugene E. & Shumway, Russell. Incident Response: A Strategic Guide to Handling System and Network Security Breaches. New Riders Publishing, Indianapolis, Indiana (2002)

Sommer, Peter. "Computer Forensics: An Introduction." Available at: http://www.virtualcity.co.uk/vcaforens.htm (1997)