Global Information Assurance Certification Paper

Electronic Discovery
&
Computer Forensics

GSEC Practical Assignment
Version 1.4b Option 1

Drew Fahey

January 22, 2004

1.1 – Abstract.

Computer Forensics is an industry buzz word that has been around for the last couple of years. There are very few organizations that have qualified people who can conduct computer forensics, yet it is a prevailing topic among computer professionals. Once an emanate domain for law enforcement, computer forensics is rapidly becoming one of the most sought after training programs. However, most of the training for computer forensics is still only available to law enforcement. So how does someone go about getting the computer forensics assistance they need?

This paper will look at electronic discovery and computer forensics in the legal environment. More specifically, it will be a guideline for what companies, law firms, and individuals, need to look for when evaluating computer forensics firms, as well as appropriate case law governing electronic discovery and computer forensics.

1.2 – What is Electronic Discovery?

Law firms, attorneys, and courts are faced with a brand new world of evidence: evidence that is processed, stored, viewed, and transmitted electronically. Although the paperless office has not quite come to pass, almost everything we do in society has taken some part in the electronic revolution. The computer has had a remarkable impact on how businesses function today. No longer do businesses use typewriters, carbon paper or even notepads. This has led to a dichotomy in the discovery process.

The evolution of electronic information greatly impacts the legal community more than ever before. The legal community has yet to fully understand the importance of electronic discovery. As people and businesses conduct more of their business electronically, the legal system and courts need to recognize this and require the exchange of electronic information in discovery following the same principles applied to paper evidence. Likewise, forensic investigations rely heavily on the use of electronic information as evidence to build more complete cases.

All email, documents, spreadsheets, and electronic files are potential evidence for attorneys, investigators, and legal professionals. Courts have uniformly agreed that electronic evidence is as admissible as paper evidence. However, collecting and reviewing electronic evidence is a challenge that requires a great deal of technical expertise and knowledge.

1.3 – What is Computer Forensics?

Forensics, as defined by thinkquest[1], is "any science used for the purposes of the law, and therefore provides impartial scientific evidence for use in the courts of law, and in a criminal investigation and trial. Forensic science is a multidisciplinary subject, drawing principally from chemistry and biology, but also from physics, geology, psychology, social science, etc."

As such, computer forensics is simply the application of computers in forensics. The most important aspect is the impartial computer investigation and analysis of electronic media. Along with other forensic disciplines, the techniques used in computer forensics to determine potential legal evidence requires specialized training. With an estimated 93% of the world's data being created by computers, computer forensics offers many challenges and opportunities to the legal arena. Electronic evidence might be sought in a wide range of computer crimes or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud. [2]

Computer forensics has a few rules that are designed to facilitate a forensically sound examination of computer evidence. These rules will enable a forensic examiner to testify as to their handling of a particular piece of evidence. The four rules are that the exam is to be fully documented, and that it must be repeatable, reproducible and verifiable. The results must be repeatable and reproducible such that any qualified expert who completes an exam of the evidence employing the same tools and methods will arrive at the same results.

1.4 – Why the need for Electronic Discovery and Computer Forensics?

Computers have appeared in the course of litigation for over twenty-five years[3]. In fact, some of the first case history for computer crime appeared in 1977, in which there were 291 US federal cases and 246 state cases in which the word "computer" appeared and which were sufficiently important to be noted in the LexisNexis[4] database.

For all intents and purposes, computers in the legal arena did not create any immediate difficulties; judges and courts sought to allow computer-based evidence on the basis that it was not any different from other forms of evidence with which they were already familiar such as documents, books, film and audio tape. However this process could not continue without new laws and processes being required. As technology advanced, it became apparent that new situations would not fit with more traditional analogous evidence material. Many of these

[1] http://library.thinkquest.org/TQ0312020/whatisforens.htm
[2] http://www.computerforensics.net/forensics.htm
[3] http://www.virtualcity.co.uk/vcaforens.htm
[4] http://www.lexis.com/

problems were solved by changes in rules of evidence[5], but many were addressed in court rulings. Not all of the key cases dealt directly with computers and computer crime, but have a direct bearing on them as they contained key characteristics of computer-originated evidence.

The 2002 American Bar Association (ABA) Survey on Litigation and Courtroom Technology[6] revealed some very interesting statistics that, astoundingly, have not changed very much from years past. According to the study only 19% of lawyers have received an electronic discovery request. Only 53% of lawyers have conducted their own form of electronic discovery. The survey also shows that a majority of the electronic discovery is conducted by only the larger firms in the largest cities. The Federal Rules of Civil Procedure, and most of states' laws, consider electronic discovery critical in any discovery request. Based upon these numbers it can be assumed that many attorneys are technically not in compliance with discovery requests by failing to disclose documents that may exist in electronic format. Because of non-compliance with the electronic discovery process an individual could face ethical and/or legal dilemmas.

One of the major problems in electronic discovery and computer forensics is that many lawyers are under the false impression that electronic discovery is expensive. This is one of the myths that needs to be quickly dispelled. Electronic discovery and computer forensics is often cheaper and quicker to conduct than traditional discovery methods. Computer forensic tools, used by properly trained specialists, allow the cost effective and safe recovery of deleted, hidden and temporary files normally invisible to the user, as well as active files. The types of cases using electronic discovery include but are not limited to: computer crimes, intellectual property theft, trade secrets, defamation, sexual harassment, divorce cases, fraud cases, and spoliation of evidence.

Another problem is determining when computer evidence relevant? As can be seen from the ABA survey results, at least half of the people in the legal community are not conducting electronic discovery. This means that many lawyers and law firms simply do not understand or recognize computer evidence. When at least 97% of lawyers use email on a daily basis it is easy to see why this is startling.[7] Since email is used by so many people it is one of the key elements to look for when conducting computer forensics for electronic discovery. Electronic discovery and computer forensics are not limited to high profile cases like Enron but can be utilized on all cases as previously stated.

The legal community needs to understand that there is a tremendous amount of information available in electronic form that could be the difference between winning and losing a case. Law firms that understand electronic discovery and computer forensics will have an advantage over those that do not understand

[5] http://www.access.gpo.gov/uscode/title28a/28a_5_.html
[6] http://www.lawtechnology.org/surveys/2002survey/2002survey_exec.pdf
[7] http://www.lawtechnology.org/surveys/2002survey/2002survey_exec.pdf

how to properly request and respond to it. Traditional paper based discovery will become the exception and electronic discovery the rule.[8]

1.5 – How Electronic Discovery and Computer Forensics go together

The first and most important rule in electronic discovery and computer forensics is the same as in traditional evidence gathering: Do not alter the evidence. One of the largest problems in electronic discovery is the tampering of the original evidence. Digital evidence is even more difficult to preserve because of the manner in which data is stored on a computer's hard drive. Continued use of a drive or a system can permanently delete, destroy or corrupt the original evidence. Many in the legal community feel compelled to conduct their own analysis, discovery and forensics and end up causing more problems then solutions. People generally do not treat electronic data stored on a computer as they would other evidence. One would not think of conducting a DNA test on their own without an expert, so why is it different for computer evidence? This is apparent time after time when an individual will power up a computer, that contains the evidence, to extract the data they need for their case without thinking about the repercussions. Simply put, people use computers everyday so they falsely assume they know what they are doing when it comes to electronic discovery and computer forensics. Nothing could be further from the truth.

Electronic discovery and computer forensics go hand in hand and both require a good deal of knowledge, skill and training. Computer forensics is not a new concept. Computer forensics has, however, traditionally been in the domain of law enforcement, and even today there are very few organizations that will provide training to a non-law enforcement individual. Unfortunately, there is no governing body that oversees the standards of conduct for computer forensics like exist for other forensic sciences, even among law enforcement agencies.

The obvious question to ask --What qualifications should a person or company who conducts electronic discovery and computer forensics have? The easy answer is to look at their backgrounds and training and how long have they been conducting computer forensics? Some of the training organizations that certify individuals for computer forensics are:

For law enforcement:

- International Association of Computer Investigative Specialists (IACIS)
- DoD Computer Investigations Training Program (DCITP)
- Seized Computer Evidence Recovery Specialist (SCERS)
- Federal Bureau of Investigations (FBI)

[8] http://www.onlinesecurity.com/Community_Forum_detail.php?article_id=90

- National White Collar Crime Center (NW3C)

For non-law enforcement:

- SysAdmin, Audit, Network, Security (SANS) Institute
- New Technologies Inc.
- High Tech Crime Network

This is by no means an all inclusive list as there are other companies that teach law enforcement and non law enforcement in product usage, such as Guidance Software which teaches Encase, and AccessData which teaches FTK. There is a distinct difference between teaching the forensics process as opposed to a forensics tool.

Regardless of the training, one thing is certain: digital evidence is fragile by nature and must be treated very carefully to prevent evidence spoilage or even the appearance of improper handling or usage.[9] This is due in part to the complexity of computer operating systems and applications, as well as to the users who use them. One of the many problems in electronic discovery and computer forensics is the issue of over-complicating or simplifying the relevancy of information technology. As such, many times common sense does not prevail, hence the requirement for a computer forensics expert. An expert is required for the acquisition and analysis of digital data.

Many times a systems or network administrator is identified as an expert simply because they had some computer skills and the title. The problem with using these individuals as experts is that their methodology is not consistent with the accepted standards of computer forensics and data recovery. Using this type of expert almost always results in irreversible corrupted evidence. By choosing someone who does not have specific computer forensics training you can taint the objectivity of the investigation and more importantly, corrupt the usability of the recovered evidence.

In addition to the acquisition and analysis of computer data, it is extremely important to have sound procedures and methodologies in place for the storage and security of computer evidence. Improperly preserved computer evidence can be worse than having no evidence at all.[10] This has been all too apparent in past cases that have been thrown out of court due to improper chain of custody issues.

[9] http://www.onlinesecurity.com/Community_Forum_detail.php?article_id=91
[10] http://www.onlinesecurity.com/Community_Forum_detail.php?article_id=91

1.6 – What are some of the legal issues?

Rule 34 of the Federal Rules of Civil Procedure states that documents stored on computer equipment can be discovered just as documents from a file cabinet.[11] There are a few significant differences that must be realized. First and foremost, computer evidence needs to be processed, analyzed and presented by computer forensic experts because much of it can only be recovered through the use of specialized software and training. Second, files on a computer can easily be erased and overwritten just through the normal operation of the computer.

One cause for impeachment of computer evidence is mishandling in the seizure and acquisition of the evidence. Many individuals make the critical mistake of exploring a computer to find potential evidence before they call in a computer forensic expert. Some people even make the mistake of installing software on the computer to recover deleted files or do their own analysis. This can damage and/or destroy the evidence. A classic example of this is now set in case law: *Gates Rubber Co. v. Bando Chemical Industries.*[12]

Another cause of electronic evidence being impeached is not having proper documentation. Seized data, electronic evidence and entire cases have been thrown out because there was never a chain of custody established or continued. A classic example is the CD Universe case,[13] in which the three companies: Network Associates, Kroll O'Gara and Infowar.com failed to establish a proper chain of custody. The chain of custody needs to document from where the computer came, who took possession, and who had access to it. In addition to a complete chain of custody, there should be a detailed inventory of the media involved, including make, model, serial number, condition and capacity.[14]

Rule 53 of the Federal Rules of Civil Procedure states that a court which has a pending action may appoint a special master. In this case a special master serves as referee, auditor, examiner, and an assessor. [15] This can be extremely beneficial when dealing with electronic evidence as a computer forensics expert can be appointed as a special master and work as an independent, neutral party that works for the court and presents the findings to all sides.

1.7 – Frequently Asked Questions

Is there really any value to electronic data's value to litigation?

Recent surveys confirm that more than 93 percent of all documents produced since 1999 were created in digital form. It can be assumed this number has only

[11] http://www.law.cornell.edu/rules/frcp/Rule34.htm
[12] http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/gates.html
[13] http://zdnet.com.com/2100-11-502482.html?legacy=zdnn
[14] http://www.renewdata.com/LTNarticle.html
[15] http://www.law.cornell.edu/rules/frcp/Rule53.htm

increased. Some statistics show that at least 70% of electronic data is never produced to hard copy. So simply stated if you choose to ignore the electronic evidence, you are choosing to ignore a majority of the evidence. The equivalent in normal discovery terms would be reviewing 3 out of every 10 filing cabinets.

Can information be permanently deleted from a hard drive?

The simple answer is yes. When a file is deleted the data does not really go away. The file, is instead, marked for deletion and the operating system is free to use its space for new files. To permanently delete information from a hard drive requires the space that the data resides in to be overwritten numerous times. There are several programs available that will do this task very simply. However, it is important to know if you have a duty to preserve any evidence before you permanently delete a file. The reason this is important is that it is possible to determine if a software tool was used to wipe files from a hard drive. If there was a duty to preserve evidence and a software wiping tool was found to have been used, a court could impose legal sanctions.

Can data on a hard disk be recovered if the drive is physically destroyed?

There are very few means to absolutely destroy electronic data. It is definitely possible to recover data from a hard disk that has been physically destroyed. Data has been recovered from drives that have been burned in fires, submerged in water, dropped from a building, and even shot.

How do passwords and encryption impact the discovery process?

It definitely slows down the discovery process but does not stop it. Password and encryption cracking of protected documents or data are routine in computer forensics. Given enough time, almost any password or encryption can be broken. A cost-benefit analysis should be done to determine how much time should be allocated to breaking the passwords and or encryption.

What is meant by preservation of digital evidence?

When litigation is pending, ongoing, or expected a duty to preserve all evidence relevant to litigation exists. This preservation duty includes traditional paper documents as well as any digital data relevant to the case. The electronic data can be electronic versions of the printed paper material, email, backups, and even entire computer systems.

The biggest problem with digital evidence is that it does not require an overt act, such as shredding a paper document, to destroy it. Digital evidence can be destroyed rather unknowingly and unwittingly by people doing their normal day to day activity. In fact, corporate policy, which may include the recycling of backup tapes, is routine and destroys data without a lot of overt planning. This is very

important to consider because organizations could face sanctions for the spoliation of evidence by simply conducting daily business operations.

What is lost when information is converted from digital form to paper?

You will lose the metadata that potentially exists in the document. Metadata can be a very important element of potential evidence. So what is metadata? It is in the simplest terms a definition or description of data. Metadata can not be viewed or included in printed versions of documents. It can be important because it can reveal a lot of information about a document, such as who the author was, when it was last saved and or printed, what changes have been made to it, and who the last individuals to review it were.

Are courts equipped for electronic data discovery issues?

The simple answer is yes. Electronic information is equally as discoverable as paper documents. The real question is do courts understand it? Courts see electronic discovery as the ability to view documents in electronic format that is conducive to all parties. However electronic discovery can be and is so much more.

What types of evidence exist on computers?

There are three main types of data that can exist on a computer that can be evidence. They are:

Active Data: These are the current files on the computer, still visible and available to applications. Active data is the most common type of data and what most people work with on a daily basis.

Latent Data: Latent data are deleted files and other non-logical data types such as memory dumps, swap files, temporary files, printer spool files, and metadata that can be retrieved. This data is generally inaccessible without the use of specialized tools and techniques.

Archival Data: This is data that's been backed up to secondary media such as, tapes, CDs, DVDs, network servers, and less commonly floppy disks. This type of data can be extremely voluminous.

One of the best types of evidence that can exist in all three types of data from above are the date and time stamps of the files themselves. Date and time stamps are recorded by Last Accessed Date, Last Modified Date, and Date Created. In some case date deleted is also possible.

1.8 – Important Case Law

The following case law is included to demonstrate the relevance of electronic discovery, and computer forensics in legal proceedings.

Adams v. Dan River Mills, Inc., 54 F.R.D. 220, 222 (W.D. Va. 1972) [16]

This case made it clear that computer tapes can be a part of the discovery process. Older backup tapes that may contain the needed evidence can now be included as part of the normal discovery process even though the computer systems may no longer contain the evidence.

Anti-Monopoly Inc. v. Hasbro Inc (S.D.N.Y. 1995) 1995 U.S. Dist. LEXIS 16355 [16]

This case made it clear that electronic data and documents are discoverable even if the hard copies (paper) are provided. In addition the responding party was responsible to design whatever programs were necessary to extract the needed data. This case set the standard: "today it is black letter law that computerized data is discoverable if relevant."

Playboy Enterprises v. Welles (S.D. Cal.1999), 60 F. Supp.2d 1050 [16]

This case showed that by requesting documents under the Rules of Civil Procedure the requestor automatically requests electronic evidence. This meant that the request for documents also included email and hence an expert was allowed to image the hard drive. This case also held that a protective order would be in place upon the expert for privileged information.

Daewoo Electronics Co, Ltd. v. United States, 650 F. Supp. 1003, 1006 (C.I.T. 1986) [16]

This case set that electronic data should be translated into a form usable by the discovering party at the burden of the respondent unless extraordinary hardship can be shown.

Gates Rubber Co. v. Bando Chemical Indus., Ltd 167 F.R.D. 90, 112 (D.Colo. 1996) [16]

This case set many precedents. The expert that was hired by Gates installed software on Bando's computer to search for deleted files. Under the Rules of Civil Procedure 37 the court imposed sanctions for destruction of evidence and permitted expedited discovery on the computerized files.

Simon Property Group v. mySimon Inc.(S.D.Ind.2000), 194 F.R.D. 639 [16]

This case set forth a process for discovery by which an expert was chosen to inspect the computers. The expert was designated as an officer of the court and asked to conduct forensics and provide a report to the court. The court, in turn, provided the report to the responding party to identify responsive and non-privileged documents and to create a privilege log and produce that material to the requesting party.

[16] http://californiadiscovery.findlaw.com/electronic_discovery_legal_authority.htm

References :

[1] 2003 ThinkQuest USA "Exploring Forensics", URL: http://library.thinkquest.org/TQ0312020/whatisforens.htm

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

[3] Sommer, Peter. "Computer Forensics: an introduction", URL: http://www.virtualcity.co.uk/vcaforens.htm

[4] LexisNexis Research System Home Page, URL: http://www.lexis.com/

[5] U.S. Code Title 28 - Federal Rules of Evidence., URL: http://www.access.gpo.gov/uscode/title28a/28a_5_.html

[6/7] 2002 American Bar Association Annual Technology Survey. "Litigation and Courtroom Technology", URL: http://www.lawtechnology.org/surveys/2002survey/2002survey_exec.pdf

[8] Barsocchini, Albert. "Electronic Discovery Still Off the Radar Screen For Most Attorneys", URL: http://www.onlinesecurity.com/Community_Forum_detail.php?article_id=90

[9/10] Laykin, Erik. "What are the first steps in securing digital evidence?", URL: http://www.onlinesecurity.com/Community_Forum_detail.php?article_id=91

[11] Cornell University LII. "Federal Rules of Civil Procedure", URL: http://www.law.cornell.edu/rules/frcp/Rule34.htm

[12] cyber.law.harvard.edu. Civil Action No. 92-S-0136, URL: http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/gates.html

[13] MSNBC. "CD Universe evidence compromised", URL: http://zdnet.com.com/2100-11-502482.html?legacy=zdnn

[14] Larsen, L.M. "Here's How to Avoid Nasty Bytes", URL: http://www.renewdata.com/LTNarticle.html

[15] Cornell University LII. "Federal Rules of Civil Procedure", URL: http://www.law.cornell.edu/rules/frcp/Rule53.htm

[16] Best, Richard E. "Legal Authority for Electronic Discovery", URL: http://californiadiscovery.findlaw.com/electronic_discovery_legal_authority.htm

Additional References:
(Web Sites for Training Organizations)

International Association of Computer Investigative Specialists (IACIS):
http://www.cops.org/

Department of Defense Computer Investigations Training Program (DCITP):
http://www.dcitp.gov/DCITP.htm

National White Collar Crime Center (NW3C):
http://www.nw3c.org/training_courses.html

Federal Law Enforcement Training Center (FLETC):
http://www.fletc.gov/ffi/SCERS_Ovr.htm

Federal Bureau of Investigations (FBI):
http://www.fbi.gov/

New Technologies Armor, Inc (NTI):
http://www.forensics-intl.com/intro.html

Guidance Software, Inc.:
http://www.guidancesoftware.com/

High Tech Crime Network (HTCN):
http://www.htcn.org/index.htm