Computer Forensic Tools

Keywords: Computers, digital evidence, digital evidence bags, forensics, forensics tools

Computer Forensics Procedures, Tools, and Digital Evidence Bags: What They Are and Who Should Use Them

Brett Pladna

ICTN6870

East Carolina University

Abstract

This paper will try to demonstrate the importance of computer forensics by describing procedures, tools and differences in the use for individuals/small organizations vs. large organizations. The procedures described deal with how to collect evidence and the laws that need to be followed for admission of evidence into a court room. The tools used are the basis for all tools that are available. Tools include, backing up data, authentication, decryption, file auditing, IP tracking, and data recovery and document examination. Smaller organizations might use a variety of these or all of these. The discussion of larger organizations discusses the need for digital evidence bags (DEB) due to their extreme efficiency. A digital evidence bag is used to store information from various applications such as the tools mentioned above.

Introduction

Computer forensics is the application of computer investigation and analysis techniques to determine potential legal evidence. Since computers are vulnerable to attack by some criminals, computer forensics is very important. Understanding computer forensic procedures will help to capture vital information which can be used to prosecute an intruder that compromises a computer or network. Also, deciding on the specific tools for computers or other equipment that is needed to correctly analyze evidence is crucial. These tools are very useful but bigger companies that handle more equipment and information might benefit from something that can combine all these tools into one application.

Procedures for Gathering Evidence

Evidence can be gathered from theft of trade secrets, theft of or destruction of intellectual property, fraud or anything else criminally related to the use of a computer. Evidence, which is also referred to as “digital evidence,” is, “any data that can provide a significant link between the perpetrator and the victim” (Wang, 2007).

Casey (2000) lays out the physical characteristics of digital evidence:

1. It is easily copied and modified, but not easily kept in its original state: an electromagnetic record is stored in a computer system in the binary form—0 or 1. The copied object is exactly the same as the original one, but it is also convenient to proceed

with user modifications. As a result, it is difficult to retain digital evidence in its original status. Confirmation of the original digital source is, therefore, susceptible to doubt.

2. Its source and integrity is not easy to prove: it is very easy to produce an electromagnetic record, so it is also very easy for it to be copied or modified. This makes it very difficult to directly infer the relationship between the evidence obtained and the suspects. That is to say, it is almost impossible to achieve "individualization", unlike the highly efficient methods of fingerprinting or deoxyribonucleic acid (DNA), used to authenticate evidence. Accordingly, it is very difficult to prove whether the evidence has been changed, based on the observation of easy modification of electromagnetic records.
3. The presentation of digital information cannot be well perceived by human senses. This is because the electronic record has been electromagnetically recorded and stored inside the computer system. It is therefore impossible to perceive its content without the help of a suitable toolkit. (P. 2-16)

Before any evidence can be gathered, a warrant must be issued. Just like the need for a warrant to search someone and their property, everyone involved in the computer forensics process needs authorization from the proper authorities to monitor and collect information related to a computer intrusion. Security monitoring tools also have legal implications. Other procedures that need to be followed are the laws that have requirements for safeguarding data. This is not only to keep protected from intruders but to prevent evidence from being dismissed and also to prevent lawsuits or regulatory audits. Three laws[1] that are important for anyone that is involved with computer forensics are the; Wiretap Act (18 U.S.C. 2510-22); Pen Registers and Trap and

[1] These laws can be found in more detail at the U.S. Department of Justice web site http://www.usdoj.gov/criminal/cybercrime/cclaws.html

Trace Devices Statute (18 U.S.C. 3121-27); and the Stored Wired and Electronic Communication Act (18 U.S.C 2701-120). The following is a list of people and organizations that use computer forensic evidence:

- **Criminal Prosecutors** use computer evidence in a variety of crimes where incriminating documents can be found: homicides, financial fraud, drug and embezzlement record-keeping, and child pornography.
- **Civil litigators** can readily make use of personal and business records found on computer systems that bear on: fraud, divorce, discrimination, and harassment cases.
- **Insurance Companies** may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson, and workman's compensation cases.
- **Corporations** often hire computer forensics specialists to ascertain evidence relating to: sexual harassment, embezzlement, theft or misappropriation of trade secrets and other internal/confidential information.
- **Law Enforcement Officials** frequently require assistance in pre-search warrant preparations and post-seizure handling of the computer equipment.
- **Individuals** sometimes hire computer forensics specialists in support of possible claims of: wrongful termination, sexual harassment, or age discrimination.

(Robbins, 2008)

Besides these characteristics there are also basic requirements for an individual to posses before obtaining evidence using computer forensics. Computer specialists can use various methods (discussed later), to find data that resides in a computer system, or recovering deleted or

damaged file information. Unlike paper evidence, computer evidence can exist in many forms such as a hard drive, disk drive (older computers), USB drive, Zip drive, etc… When a computer system is seized, experts need to protect the system and components so it can be used for prosecution. Experts are careful to ensure that, "no possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer; extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage; a continuing chain of custody is established and maintained; business operations are affected for a limited amount of time, if at all; and any client-attorney information that is inadvertently acquired during a forensic exploration is ethically and legally respected and not divulged" (Robbins, 2008).

When experts are ready to retrieve data they take careful steps to identify and attempt to retrieve data that exists on a computer. If the digital evidence is collected aimlessly then not only will there be inefficient use of resources but the evidence could get compromised, thus liberating a criminal from all possible wrong doing. Before this evidence is submitted it must meet three basic requirements to maintain its reliability: "It must be produced, maintained, and used in a normal environment; be professionally authenticated (i.e. the report from the forensic experts is reliable); and also meet the "best evidence rule." This means that what is produced must be the best evidence available and not a substitute for the evidence offered" (Icove, Seger, & VonStorch, 1995).

There are also procedures that must be followed at the crime scene. Just like any other regular crime scene, a computer has to be kept in the same condition as it was found. Doing this prevents any evidence from being questioned. There are three methods recommended for handling evidence: Acquire the evidence without altering or damaging the original; authenticate the

recovered evidence as being the same as the originally seized data; and analyze the data without modifying it (Wang, 2007). There are also four methods for effective procedures on an investigation utilizing computer forensics. First, one must preserve the evidence. This step is followed after entering the scene of the crime. Digital evidence is fragile and can be changed at any time by just touching a key on the keyboard. Evidence that is damaged or handled improperly will be excluded from evidence and could result in criminals being exonerated. Experts should ask themselves and follow these steps of analysis for the best results of collecting evidence: “Who collected it; How and Where; Who took possession of it; how was it stored and protected in storage; and who took it out of storage and why” (Kruse & Heiser, 2001). After this, evidence must be examined which means data is ready to be retrieved. Once all files are collected the unallocated disk space (free space) is checked. The empty space on the hard drive can contain previously deleted or formatted files. A bit-stream-copy method is used to find deleted files. Deleted files tend to be in strings and the tool will help to rebuild documents. When someone deletes or formats, not all information is wiped; a special format is required for this to happen. When all files are retrieved they need to be protected. Next, evidence is to be analyzed. An analysis consists of the list of the computer system, any relevant data, authorship information, and any indication to try and hide any revealing data. After this analysis, the data is taken to the appropriate place and prepared for presentation. Whenever needed, the forensics expert can provide consultation and/or testimony. Here they will be able to prove their theory of guilt or innocence based on their analysis of the evidence.

If these procedures are followed correctly, criminals will be prosecuted thoroughly. These procedures should be followed not only by law enforcement, but by everyone involved in the collection of digital evidence. When it comes to digital evidence, sensitivity is the keyword. A

digital crime scene follows the same rules as for a regular crime scene; it must be analyzed and preserved in its original form. It is important to realize how imperative it is to follow procedure.

Computer Forensic Tools

There are two basic types of data that are collected, persistent data and volatile data. Persistent data is that which is stored on a hard drive or another medium and is preserved when the computer is turned off. Volatile data is any data that is stored in memory or exist in transit and will be lost when the computer is turned off. Volatile data might be key evidence, so it is important that if the computer is on at the scene of the crime it remain on.

There are a variety of tools used to collect data. Tools can be made by individuals that do not have the experience or reputation in forensics but it is not recommended for the simple reason that it would be hard to convince someone that their software meets all requirements for collecting evidence. Wang (2007 said, "It could also affect the probative force of the evidence gathered." An essential toolkit should consist of various software such as backup, authentication, decryption, disk editing, log file auditing, IP tracking, data recovery, and file examination. When obtaining data, special tools are needed. This tool, known as hardware imaging tool, copies the data bit by bit using a bit-stream-copy method. Regular backups copy all data from the hard drive but not "ambient data." Ambient data is located in the swap file of a windows system. The swap file acts like memory. To retain original evidence, data backup should be considered first. A reliable backup software tool must comply with the requirements of the National Institute of Standards and Technology (NIST):[2]

[2] For more information on the National Institute of Standards and Technology go to http://www.nist.gov/

1. The tool shall duplicate a bit-stream or an image of an original disk or section, where this so-called image refers to saving the content and related storage information as a document.
2. The tool shall not alter the original disk, i.e., the program cannot make changes to the original evidence media.
3. The tool shall be able to verify the integrity of a disk image file.
4. The tool shall log I/O errors; i.e., this program must offer a resolution to fix I/O error messages.
5. The output of the recorded documentation shall be correct in the wake of software operation.

(Wang, 2007)

Authentication software is used to prove that the evidence has not been changed. Programs like MD5 or SHA-1 are required. MD5 produces hash code that is encrypted. "MD5 adopts an implied mathematical calculation method to save the data to the drive or document. The hash value produced by this mathematical equation can select any one of the data and it is in low possibility to have the same hash code for different data input; to find two identical hash codes would require approximately 264 times calculations. In addition, to recover through hash code operation requires approximately 2128 times calculations" (Stallings, 2003). This is used to confirm that the copy data and the original data are the same.

Decryption tools are needed to gain access to password protected computers, files, or both. If data recovered from a suspect's computer is encrypted then certain methods must be considered.

If there is a password and it can't be found then there are two methods to break it; guessing the password and using a system vent. Since most computers use a one-way function to protect passwords, brute force and dictionary attacks could work. If the code is still unbreakable then you will need to use a high speed computer with decrypt software because the time to find the password can be long. A back way to get into the Operating System is known as a system vent. An example would be causing a buffer overflow by sending it a notify command which can take control of any part of the operating system. Also there are methods to gain access to a computer if it is password protected on boot up. You can use the universal BIOS password that will work not matter what password you have. It is assigned by the manufacturer. Knowing this, a suspect is more than likely going to have other protective means to prevent access to data that is needed for evidence. Also by clearing the CMOS you return all setups to default. Usually there is a jump that is located on the motherboard. If the jump can't be found then the battery can be removed. It just needs to be put back later. Screensavers, Documents, PDF files, and compressed files all have various programs that can be used to break passwords.[3]

As discussed earlier, when data is deleted it still remains on the hard drive. An identity code is attached to the title of the document to represent the fact that it was deleted. A disk data editing and searching tool is appropriate to find this information. It works by searching strings of code that is embedded in the hard drive as well as documents when they are deleted. Searching for these strings of code would take a very long time without a program like *Winhex Editor*. It searches for strings of code on the hard drive to find data that is worth recovering.

[3] A list of programs can be found on Page 220-221 of (Wang, 2007). Also there are many that can be found on the Internet.

The next tool is a daily audit log file tool which is an example of what the event monitor does on a Microsoft Windows computer. Large computers or Intrusion Detection Systems (IDS) have a daily audit file that records important activity on a computer such as who logs on and off and what files have been changed or deleted. Other sources of audits come from internet browsers. Forensic experts can look at cookies to identify accounts that a suspect logged on.

There are three other tools that are helpful once a forensic expert is inside of a computer's operating system. Tracking an IP address by using the ping command on a Windows based computer can be used, and two pieces of other software (*Whois* and *traceroute*) can also be used to find additional information on the IP address. Recovery of other data such as email is similar to the process of recovering deleted files on a hard drive. A tool like *R-Mail* can be used to recover the messages. A final tool used should be a document examiner. There are many document formats and it can become very tedious to try and find the correct program to read the file. A program such as *Quick View Plus* is a document read that will read many different file formats.

These are many tools that can be used to help collect evidence from a computer. There are many programs that can fit into these categories but it is best to choose the ones that are from a reputable vendor. This will lessen the chance of evidence being damaged and having it inadmissible. The software mentioned is useful for companies of any size but larger companies should find an efficient way to manage the data that is collected from all software applications. Smaller companies or perhaps an individual would be better suited to use each application independently. This does not mean smaller companies cannot use a tool that manages these applications; it might cost more than it is worth.

Computer Forensics for Companies

From an organization stand point, computer forensics is important because it can save money. Managers are allocating a good percentage of their technology budget for computer and network security. In 2005 the International Data Corporation (IDC) reported that "the market for intrusion-detection and vulnerability-assessment software will reach 1.45 billion dollars in 2006" (US-CERT, 2005). Even though that data is 3 years old, the amount of money spent is significant. After looking for more information from the IDC[4], no further statistics were documented. More and more organizations are deploying network security devices such as intrusion detection systems (IDS), firewalls and proxies. Businesses have their own computer incident response teams and network investigators or may have them outsourced. These teams are often assembled at very short notice when an incident occurs. When an incident does occur, little may be known and usually the goal is to restore the system to normal by the System Administrator (SA) with help from the helpdesk. In most cases the incident is minor but in cases where there is a more serious problem a more rigorous investigation is needed. The problem with the investigation is that sometimes the SA might have not recorded the details of the incident accurately which could inadvertently could cause the blame to be put on that individual.

Turner (2007) says:

"The SA usually has a vast range of tools available at their disposal to monitor system performance, determine system configuration or to fault find system problems. The majority of these tools and utilities are very focused in the function they performed the information they

[4] For more information on the IDC go to http://www.idc.com/home.jhtml

provide. Many of these tools are console applications and run as command line utilities. Furthermore, they are often packaged with the operating system.

The problem with these tools is they are designed to provide information, but are not designed to provide any form of integrity assurance or record when those utilities were executed. From a forensic perspective they provide no audit record about the timestamp or actions taken, or results returned from running those utilities."

(P.31)

What needs to be done is to filter the action of these tools into one program so they can be used in one instance. System Administrators "would be able to execute their favorite tools and utilities" The recommended process is the use of a Digital Evidence Bag[5] (DEB). A DEB is a "universal container for digital evidence from any source. It allows the provenance to be recorded and continuity to be maintained throughout the life of the investigation" (Turner, 2007). In other words a DEB is part of a software application that would be able to save information from each forensic tool that is executed. A DEB consists of a tag, index, and bag files. The index and bag files are known as Evidence Units (EU). "DEBs were originally conceived to be used in the traditional role of static digital forensic investigations. In this role they permit more advanced data capture techniques to be supported, for example selective and intelligent imaging methodologies" (Turner, 2006). However, they can also be used to store forensic images of command line utility output, digital media, memory dumps, network packet captures and all associated meta-data. The function of DEBs would be more effective in a dynamic environment such as incident response, system administration and network forensics. When an investigation

[5] For more detailed information on DEBs you can read the research of Philip Turner.

begins a DEB would be created by the user. All a user would be required to do is open the DEB and applications that you execute start collecting information and storing it.

Besides the tools mentioned in the previous section, other advanced tools can be executed in a DEB. A DEB can contain anything that a company needs to ensure incident response is handled efficiently. An example of a more advanced technology to add to a DEB would be a way of analyzing magnetic card cloning devices. From a forensic stand point this is significant due to the ease of manipulating these devices. “There are many magnetic stripe card readers or skimmers, as they are commonly known, produced by a small number of manufacturers. These devices are marketed for use by legitimate commercial retail purposes. They also have become increasingly used for illegal fraudulent activities” (Masters & Turner, 2007). The problem with these devices, besides being easily manipulated, is that there is a very limited way of collecting data evidence. Some of the applications attached that are programmed into the devices delete card information once it is downloaded to a PC. If added to the function of the DEB software, a company would be able to execute the magnetic reader program to add information to the DEB.

Conclusion

Computer forensics is important. The procedures are important to follow, because doing so ensures evidence will be admitted and suspects will be more likely to face the consequences if found guilty. Following these procedures also means using the proper forensic tools to analyze data correctly. The tools used depend on what is being analyzed. Smaller companies or an individual user might not need many resources to secure their computers but perhaps a big organization might need many different types of applications to monitor hundreds of computers and dozens of sub-networks. This might require a digital evidence bag for more efficient

collection of data. Also, certain technologies would benefit from a digital evidence bag such as magnetic card readers due to specific programs associated with the device to operate and process information.

References

*Casey, E. (2000). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* San Diego, CA: Academic Press.

*Icove, D., Seger, K., & VonStorch, W. (1995). *Computer Crime.* O'Reilly & Associates.

*Kruse, W. G., & Heiser, J. G. (2001). *Computer Forensics: Incident Response Essentials* . Addison Wesley.

*Masters, G., & Turner, P. (2007). Forensic Data Recovery aand Examination of Magnetic Swipe Cloning Devices. *Digital Investigation , 4* (1), 16-22.

Robbins, J. (2008). *An Explanation of Computer Forensics.* Retrieved April 9, 2008, from http://computerforensics.net/forensics.htm

*Stallings, W. (2003). *Cryptography and Network Security 3/e.* Prentice Hall.

*Turner, P. (2007). Applying a Forensic Approach to Incident Response, Network Investigation and System Administration using Digital Evidence Bags. *Digital Investigation , 4* (1), 30-35.

*Turner, P. (2006). Selective and Intelligent Imaging Using Digital Evidence Bags. *Digital Investigation , 3* (1), 59-64.

US-CERT. (2005). Computer Forensics. *US-CERT , 1* (2).

*Wang, S.-J. (2007). Measures of Retaining Digital Evidence to Prosecute Computer-Based Cyber-Crimes. *Computer Standards & Interfaces , 29* (2), 8.