The Information Institute

JIST 3(1) 2006

Journal of Information Science and Technology

www.jist.info

Computer Forensics: An Essential Ingredient for Cyber Security

Dr. Richard Bassett, Linda Bass and Paul O'Brien

Western Connecticut State University

Abstract

Computer forensics uses computer investigation and analysis techniques to collect evidence regarding what happened on a computer that is admissible in a court of law. Computer forensics requires a well-balanced combination of technical skills, legal acumen, and ethical conduct. Computer forensics specialists use powerful software tools to uncover data to be sorted through, and then must figure out the important facts and how to properly present them in a court of law. Cyber crime rates are accelerating and computer forensics is the crucial discipline that has the power to impede the progress of these cyber criminals.

Computer forensics is defined by SearchSecurity.com as "the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law" (2005). The goal of computer forensics is to carry out a structured investigation while documenting a chain of evidence to discover exactly what happened on a computer and who was responsible for it. The main priority of computer

Author Notes: This paper was presented at Western Connecticut State University Research Day, which took place on April 22, 2005. This event was sponsored by Western Connecticut State University.

forensics is accuracy. Forensic practitioners must follow strict guidelines and maintain the highest standards of work ethic to achieve accuracy because emphasis must be on evidential integrity and security (The DIBS Group, 2004).

There is a widespread use of personal computers in businesses and homes. Companies are exchanging more information online than ever before, and high-tech crimes are increasing at a rapid rate (Solomon, 2005, p.3). This creates more of a need for crime investigators to have access to computer based information. There is an increased awareness in the legal community of the need for computer forensic services to obtain successful prosecutions which could otherwise fail because of unsatisfactory equipment, procedures, or presentation in court (The DIBS Group, 2004).

Corporate Views Versus Legal Views

Law enforcement officials work with more restrictive rules than corporate employees. Corporate employees and law enforcement officials have different concerns regarding computer forensics (Solomon, 2005, p.9).

Corporate concerns primarily focus on detection and prevention. Increased news coverage of vulnerabilities in software and hardware has caused companies to prioritize security. Efforts are made to implement solutions for intrusion detection, web filtering, spam elimination and patch installation. Therefore, the corporate focus is on minimizing the potential damage caused from unauthorized access attempts through preventing, detecting, and identifying an unauthorized intrusion. This is accomplished by implementing security policies, as well as incident response and disaster recovery plans (Solomon, 2005, p.9).

In many corporate environments, incidents are not reported due to the issue of legal liability. There are some laws that hold management responsible for damages caused by a hacker, and a company may have to prove it took reasonable measures to defend itself from attack (Solomon, 2005, p.10). Management may fear the publicity received from an attack, as this could cause the company to lose customers. Furthermore, if incidents are reported the company risks having critical data and computers seized by law enforcement. An investigation could disrupt employee schedules and cause confusion, leading to interruptions in the work environment (Solomon, 2005, p.11).

Law enforcement agencies focus on investigation and prosecution. Each state has its own set of laws that direct how cases are prosecuted. Evidence has to be properly collected, processed and preserved in order for a case to be prosecuted. Law enforcement must deal with incredible amounts of data. Now that the Internet is involved, crimes can be committed from other states and countries, involving laws and jurisdictions of those regions (Solomon, 2005, p.11). Multiple jurisdictions and agencies can become involved in investigative and analytical activities, each of which may

utilize its own procedures (*Forensic Procedures*, n.d.). This makes the law enforcement official's job that much more difficult.

General Methods in Computer Forensics

A Computer Forensic Specialist (CFS) must follow a rigid set of methods to ensure that computer evidence is correctly obtained. These steps are outlined in Table 1, which also introduces two critical terms: unallocated file space and file slack. The examination of unallocated file space is vital during a computer forensics investigation. When data is written to a storage device, data clusters from the File Allocation Table are allocated to store the data. But when the file is deleted by the user, the data is not erased. A 'delete' operation will incite these data clusters to become unallocated, but they will still hold onto the old data until the operating system reallocates these data clusters at a later time. The data residing in this unallocated file space can potentially contain fragments of files and subdirectories, as well as temporary files used by the application programs or operating systems. All of these types of data may contain sensitive information that can prove to be valuable during an investigation, and so it is necessary to uncover as much data from the unallocated file space as possible. Many criminals fail to recognize that the deletion process does not truly erase the sensitive data, and this is often where incriminating evidence will be discovered.

Method	*Description*
1 – Protect	Protect subject computer system from alteration, data corruption, virus infection, and physical damage
2 – Discover	Uncover all files: normal, hidden, deleted, encrypted, password-protected
3 – Recover	Recover as many of the deleted files as possible
4 – Reveal	Reveal the contents of hidden and temporary files
5 – Access	Access the protected and encrypted files, if legal
6 – Analyze	Analyze all relevant data, including data located in unallocated file space and file slack
7 – Report	Print out a listing of all relevant files, and provide an overall opinion on the system examination
8 – Testimony	Provide expert testimony or consultation, if required

Table 1. General Methods Used in Computer Forensics

File Slack is another source of vital data that criminals may overlook. When files are created, they are usually stored in clusters of fixed length. File sizes frequently do not match the cluster length exactly, and so the data storage space that exists from the end of the file to the end of the cluster is known as file slack. This file slack is often filled with randomly dumped data from the computer's memory, so there is the potential that it could include data related to network logon names, passwords, and private personal information. Since it is so important to access and reveal the contents of unallocated file space and file slack, software utilities used in computer forensics have been designed to efficiently and accurately uncover this important data.

Ethical Predicaments

These general methods show that sensitive data must be handled all the time in Computer Forensics. Consequently, there are many ethical dilemmas that a CFS must be prepared to deal with during an investigation. The most common ethical problem is managing the discovery of confidential data that is irrelevant to the case at hand. For example, if an investigator is searching through a mirror-image copy of a suspect's hard drive, he may come across a personal email that contains incriminating evidence of adultery or some other sort of inappropriate behavior that is not relevant to the ongoing case. The question of what to do with this information then arises. Computer Forensic Specialists must deal with this constantly, and the general code of ethics to follow is that this information must be ignored because it is not relevant to the investigation. However, it is not always easy to ignore this kind of information and any secrets that may be uncovered can weigh heavily on the mind of a CFS.

Acknowledgement of errors is another ethical dilemma that may be harder to overcome. If a CFS accidentally tampers with the data on the subject computer, this evidence would not be admissible in court, and the investigation would be compromised. Many Computer Forensic Specialists find it hard to admit these mistakes because one major screw up could lead to immediate unemployment (*Code of Ethics and Conduct*, 2004).

It is also necessary to remove all bias during an investigation. If a CFS goes into an investigation with the hope that the suspect is found innocent, he may ignore all evidence pointing towards culpability of the suspect and instead only report evidence that suggests innocence. This ethical problem can easily arise if the CFS has something to lose if the suspect is determined to be guilty.

Another ethical decision concerns the time-consuming nature of computer investigations. If the CFS has outside stresses to worry about, such as family problems, he may not spend the required time to thoroughly and completely investigate a subject computer. It is important to completely analyze the machine with proficient execution, and any insufficiencies in this endeavor can ruin the entire case in a split-second.

Maintaining control and responsibility for forensics equipment can also become an ethical issue. This can occur if the friend of a CFS suspects there is some fishy business going on with his computer and asks as a personal favor for the CFS to check out his machine and see what can be unearthed. This is unprofessional, unethical, and it shows a poor sense of responsibility for the forensic equipment with which Computer Forensic Specialists are entrusted. However, people are generally sympathetic towards their friends and will often act outside the bounds of logic and ethics to comply with a friend's requests.

Software Tools

Computer examiners use several different types of tools to identify and attain computer evidence. There are many different tools available to use for forensic analysis. The following is a description of three of the tools available.

One type of software available for forensic analysis is EnCase (www.encase.com/products/ee_index.asp). EnCase was originally developed for law enforcement personnel, but has matured to support commercial needs, as well. The EnCase Enterprise Edition is a network-enabled incident response system which offers immediate and complete forensic analysis of volatile and static data on compromised servers and workstations anywhere on the network, without disrupting operations. It consists of three components. The first of these components is the Examiner software. This software is installed on a secure system where investigations and audits are performed. The second component is called SAFE, which stands for Secure Authentication of EnCase. SAFE is a server which is used to authenticate users, administer access rights, maintain logs of EnCase transactions, and provide for secure data transmission. The final component is Servlet, an efficient software component installed on network workstations and servers to establish connectivity between the Examiner, SAFE, and the networked workstations, servers, or devices being investigated.

These components work to provide the acquisition and analysis of volatile data on workstations and servers suspected to be compromised. This includes running applications, open files and other data in RAM, as well as acquiring and analyzing attached drive media, including files, operating systems artifacts, and data in file slack and unallocated spaces. It quickly isolates, identifies, assesses and rectifies both internal and external security breaches and provides non-intrusive forensic functionality to ensure that investigations withstand internal or external scrutiny regarding thoroughness, accuracy and authenticity.

In summary, the EnCase Enterprise Edition conducts comprehensive investigations, uncovering information and evidence pertaining to incidents that other tools cannot find. EnCase will find information despite efforts made to hide or delete it.

Also available is Paraben's P2 Examination Process (www.paraben-forensics.com/catalog/). This is a software suite consisting of nine different software applications, each of which takes a different role in the examination process. They are: Forensic Replicator, Forensic Sorter, E-mail Examiner, Network E-mail Examiner, Text Searcher, Case Agent Companion, Decryption Collection Enterprise, Chat Examiner, and PDA Seizure.

Forensic Replicator replicates exactly drives and media. Once that has been done, Forensic Sorter classifies data into different categories, recovering deleted files, and overall making the examination easier to manage, faster to process and easier to find the information desired. Next is the E-mail Examiner, which can recover active and deleted mail messages from America Online, USENET groups, Outlook Express, Juno, MSN mail, and many others. Network E-mail Examiner will examine thoroughly network e-mail archives. Text Searcher is a fast and methodical searching tool which allows the examiner to search for specific terms in any text. It supports multiple languages, has full searching capabilities for specific file types as well as slack and unallocated space, and has an easy to use interface and report output. Case Agent Companion includes a file viewer which helps to organize examination results by case, logging all parts of analysis into a detailed log file.

Also included in Paraben's forensic software suite is Decryption Collection Enterprise, which recovers passwords and decrypts encrypted data. Chat Examiner analyzes chat logs. However, AOL Instant Messenger is not supported by Chat Examiner because it does not have traditional data stores or logs. The final piece of Paraben's suite is PDA Seizure, which acquires, views, and reports on data from a PDA.

Another software tool available is the Forensic Toolkit (www.accessdata.com/Product04_overview.htm). FTK offers law enforcement and corporate security the ability to perform complete, thorough computer forensics examinations, featuring powerful file filtering and search functions. Customizable filters allow the user to sort through thousands of files quickly to find the evidence needed. FTK is recognized as the leading forensic tool to perform e-mail analysis, recovering deleted and partially deleted e-mail. The Forensic Toolkit also will identify and flag known child pornography and other potential evidence files, as well as identifying standard operating system and program files. FTK also yields instant text search results, performs advance searches for JPEG images and Internet text, recovers deleted files and partitions, and targets key files quickly by the creation of custom file filters. It generates audit logs as well as case reports, and allows quick navigation through acquired images.

The EnCase Enterprise Edition, Paraben's P2 Examination Process, and Forensic Toolkit software packages have been highlighted because they illustrate the vast amount of functionality that is mandatory for investigating cyber crime. The methodologies of computer forensics are rigorous and thorough, and a software tool that can only create disk images is not sufficient for completion of the investigation. A dependable forensic

software product should include high-quality implementations for every single method outlined in Table 1, as well as auditing capabilities so that the user can keep track of the details of the investigation. EnCase, Paraben's suite, and FTK are all examples of this brand of multifaceted forensic software that is necessary for viable use in the computer forensics process.

No matter what forensic software is used during an examination, it should be noted by its version and be used in accordance with the licensing agreement. Any software should be tested and validated for its forensic use by the examiner before an examination is undertaken.

Using EnCase to Capture a Criminal

The application of these software tools has helped bring many cyber criminals to justice. One recent case involved PayPal Inc., which is an online payment processing company. They observed that ten names were creating sets of at least forty accounts that were being used to buy expensive goods on eBay.com auctions. A mock PayPal site was discovered that was used by the criminals to grab user log-ins and passwords, and this led to the theft of tens of thousands of credit card numbers. The clever scam involved the criminals acting as sellers and buyers in the same eBay auctions, and then essentially paying themselves with stolen credit cards. A fraud investigator later discovered that the IP address of the people running the mock site exactly matched the IP addresses of the questionable PayPal accounts. When the perpetrators were eventually brought into custody, mirror-image copies of their hard drives were subjected to EnCase's keyword and pattern searching mechanism. Special care was taken to have EnCase uncover as much data from the file slack and unallocated file space as possible, and the fraud investigator John Kothanek reported that "We were able to establish a link between their machine's IP address, the credit cards they were using in our system and the Perl scripts they were using to open accounts on our system" (Radcliff, 2002). Alexey Ivanov and Vassili Gorchkov were the criminals accused of wire fraud, and Gorchkov was sentenced to three years in prison, while Ivanov was sentenced to four years in prison. The use of software tools such as EnCase alleviated some of the inherent complexity in gathering the necessary evidence to convict these two dangerous criminals.

Problems Computer Forensics Must Address

This case illustrates that the most reliable forensic software tools are immensely helpful in stopping cyber crime. However, there are many problems that have not been solved in the field of computer forensics. Hard drive sizes are increasing exponentially. This has the twofold effect of not only dramatically increasing the duration of the disk-imaging process, but also of increasing the amount of time that must be devoted to data analysis,

since more data is being uncovered. The real problem is that while the software may be great at uncovering the data, human ingenuity is required to mine through this huge pile of data and pick out the tidbits of incriminating evidence that may or may not even exist. This task is profoundly difficult to accomplish and the inevitable frustration a CFS faces here is not desirable. One possible solution to this obstacle is to find a way to automate much of the data analysis processing. However, coming up with a model or algorithmic procedure for this is a daunting task in itself, and this has yet to be resolved.

Another hindrance that a CFS faces is the limitations of the software tools in existence. These tools are quite reliable at disk-imaging and data discovery. However, the data recovery capabilities of the present tools are quite limited. The main problem is that "none of the software tools, commercial or non-commercial, are able to guarantee the recovery of unreferenced files" (Arthur, n.d.). These software tools are also plagued by limited extensibility beyond the standard desktop computer. Cyber criminals will jump on this vulnerability, and therefore the next step for this field is to implement reliable and high-quality forensic software tools for digital cameras, PDAs, routers, and so forth.

Commercial software tools are also a problem because software developers need to protect their code to prevent competitors from stealing their product. However, since most of the code is not made public, it is very difficult for the developers to verify error rates of the software, and so reliability of performance is still questionable. For example, one common way to calculate an error rate is to keep a history of all the bugs encountered and the severity of these bugs. However, if the source code is not open to the public, the developer could simply fix a bug without ever publicly documenting it, and so this bug would not be accounted for in the error rate (Carrier, n.d.). Therefore, the commercial interests of the software developers will often take precedence over the quality of software, and this is not good news for the CFS whose investigations are dependent upon the reliability of the software. The general mindset is that open-source forensic software would be an ideal fix for this conflict. However, most software developers are out to make a profit, and consequently they do not see many benefits in joining the open-source code movement.

This financial motivation is also strongly entwined with the major problem that corporations have with the field of computer forensics. The specialized tools used by a CFS are viewed as intolerably expensive by many corporations, and as a result many corporations simply choose not to invest any meaningful money into computer forensics. This trend amplifies cyber crime rates because "This leaves these companies and agencies unprepared to deal with and respond to computer-related security incidents that occur on their systems" (Isner, 2003). Education and training are the keys to solving this problem. Many corporations depend on the Internet for daily transactions, and they need to become

more aware of the fact that security may seem like an expense, but in the long-run it will yield a profit by decreasing the amount of damage done by cyber criminals.

In addition to all these problems, Computer Forensic Specialists also must find a way to overcome the general lack of knowledge that may exist in a courtroom setting. Nothing is more frustrating than for a CFS to put in a painstaking number of hours scrutinizing every detail of a hard drive, only to find out that his efforts were fruitless because he could not convey his findings to judges and lawyers in an adequate manner. Part of this problem hinges on the general lack of awareness that still exists in the courtroom setting in regards to computer evidence. Many people still lack familiarity with common computer concepts, and so it is difficult to fully explain the depths of the investigative findings without getting overly technical. So in addition to mastering the software and hardware knowledge necessary to be a skilled CFS, it is also necessary to know how to clearly articulate important findings in the courtroom.

Conclusion

Computer forensics is an increasingly important field that requires one to possess an intricate mix of technical skills, legal knowledge, and ethical behavior patterns. Specialists in this field have very powerful software tools at their disposal which will uncover a myriad of data to be sorted through, and it is up to the specialist to figure out what the important facts are and how to present them appropriately in a court of law. Even though the software tools are generally praised for their effectiveness, the statistics show that an improvement in the overall methodologies used in computer forensics is required. The FBI has made it known that “in the year 2000 there were 2,032 cases opened involving cyber crime. Of those cases, only 921 were closed. Of those closed cases only 54 convictions were handed down in court” (Isner, 2003). This is an alarming statistic, but it should not be surprising considering that the field is still in its infancy. As technologies expand, more powerful and versatile software tools will be required, and more well-trained Computer Forensic Specialists will be needed because cyber crime is exploding and computer forensics is the vital discipline that has the power to control this outburst.

References

Access Data. (2003). *Forensic Toolkit*. Retrieved February 4, 2005, from http://www.accessdata.com/Product04_Overview.htm

Arthur, K. K. (n.d.). *An Investigation Into Computer Forensic Tools*. Retrieved February 8, 2005, from http://www.infosecsa.co.za/proceedings2004/060.pdf

Carrier, B. (n.d.). *Open Source Digital Forensics Tools*. Retrieved February 7, 2005, from http://www.cerias.purdue.edu/homes/carrier/forensics/docs/opensrc_legal.pdf

CyberSecurity Institute. (2004). *Code of Ethics and Conduct*. Retrieved February 14, 2005, from http://www.cybersecurityinstitute.biz/training/ethicsconduct.htm

Guidance Software. (2005). *EnCase Enterprise Edition*. Retrieved February 4, 2005, from http://www.encase.com/products/ee_index.asp

IACIS. (n.d.). *Forensic Procedures*. Retrieved February 6, 2005, from www.iacis.com/html/procprint.htm

Isner, J. D. (2003) *Computer Forensics: An Emerging Practice in the Battle Against Cyber Crime*. Retrieved February 8, 2005, from http://www.giac.org/practical/GSEC/Jonathan_Isner_GSEC.pdf

Paraben Corporation. (2005). *Paraben Forensic Tools*. Retrieved February 4, 2005, from http://www.paraben-forensics.com/catalog/

Radcliff, D. (2002). *Cybersleuthing Solves the Case*. Retrieved February 9, 2005, from http://www.computerworld.com/securitytopics/security/story/0,10801,67299,00.html

Robbins, J. (n.d.). *An Explanation of Computer Forensics*. Available at http://www.computerforensics.net/forensics.htm

SearchSecurity.com Definitions. (Jan.14, 2005). Retrieved February 2, 2005, from http://searchsecurity.techtarget.com/sDefinition/0,sid14_gci1007675,00.html

Solomon, Michael G., Barrett, Diane and Broom, Neil. (2005). *Computer Forensics Jump Start*. San Francisco: Sybex.

The DIBS Group. (2004). *The DIBS Methodology*. Retrieved February 5, 2005, from www.dibsusa.com/methodology/methodology.html

Author Biographies

Dr. Richard A. Bassett D.P.S. is an Assistant Professor of Management Information Systems at Western Connecticut State University. He was founder and CEO of Bassett Computer Systems, Inc. for 17 years where he was involved with the design and implementation of information systems for hundreds of small and midsized businesses. He has authored several articles including: The Security threats faced by Telecommuters, Minimal Steps required to secure a Local Area Network, The Security Concerns faced by Telecommuters and The Technology Decision Challenges which Growing Companies Face. He has is actively involved with technology endeavors of numerous organizations including: The Children's Center, Bridges of Milford, North Haven Rotary Communicare and the Amber Alert System.

Linda Bass is a Junior at Western Connecticut State University, where she is pursuing a BBA in Management Information Systems with a concentration in Information Security Management.

Paul O'Brien graduated Summa Cum Laude from Western Connecticut State University with a BA in Computer Science and a minor in Information Security, as well as Mathematics. He is specifically interested in modern cryptology, advanced number theory, and watching the New York Yankees win every World Series.