

Computer Forensics: An Overview

By Frederick Gallegos, CISA, CDE, CGFM

Many people are shocked by the theft of 40 million records at CardSystems, a third-party processor for payment card transactions for companies such as MasterCard and Visa. Technology has taken the world by storm in recent decades; the advent of the computer has completely revolutionized the way humans live, work and play. Particularly, computers have affected businesses in numerous ways, allowing them to run more efficiently. However, there is a dark side to computers, where individuals use them to carry out malicious assaults. These assaults range from fraud and identity theft to hacking, embezzlement and a wide array of other activities. When these individuals are caught, specialists are called upon to seize and gather information from the computers used in crimes. Computer forensics is the science of locating, extracting and analyzing types of data from different devices, which specialists then interpret to serve as legal evidence.

Computer crimes have been happening for nearly 50 years, since computers have been used in production. Evidence can be derived from computers and then used in court against suspected individuals. Initially, judges accepted the computer-derived evidence as no different from other forms of evidence. However, as data became more ambiguous with the advancement of computers, computer-derived evidence was not considered as reliable. Therefore, the government has stepped in and addressed some of these issues.¹ It is important to note that evidence gathered from computers is subject to the same standards as evidence gathered from any other type of crime scene. Computer evidence is like any other evidence; it must be authentic, accurate, complete, convincing to juries, and in conformity with common law and legislative rules (admissible).² Thus, the evidence gathered from suspected computer-related crimes must conform to the same standards as other evidence to be credible.

Computer-related Crimes

Since computers are everywhere and have virtually penetrated all industries, computer forensics can be helpful when a computer crime has been committed. Criminal prosecutors use computer evidence in a variety of ways for various types of crimes where incriminating documents or files can be found. For example, in instances of homicide, financial fraud, drug and embezzlement record keeping, and child pornography, prosecutors can hire computer forensics specialists to gather data that can be used in court. Insurance agencies have the ability to mitigate costs if insurance fraud has taken place (e.g., computer evidence that pertains to the possibility of fraud in accident, arson or worker's compensation cases). Civil litigations can use personal and business records found on computers and various

media that could possibly bear on discrimination, divorce or harassment cases.³ Corporations sometimes hire computer forensics specialists to gather evidence when certain threatening issues arise, such as the leak of internal and confidential information, embezzlement, theft, sexual harassment or unlawful access to internal computers. Employees may also hire specialists to build a case against a particular corporation. For example, an employee may try to gather evidence to support a claim of age or race discrimination, sexual harassment or wrongful termination.⁴ Should incriminating evidence be discovered from any of the instances mentioned above, it can be used against the accused party in court.

Computer criminals can infiltrate systems on various platforms and commit a wide array of crimes. Typically, the systems that the criminals attempt to penetrate are protected with some type of security device to inhibit access. Some of these crimes include hacking web sites for bank account information, credit card information and personal identification, or stealing trade secrets from a company or government institution. For virtually any crime that is committed using a computer in some form, forensics specialists can be called upon to gather evidence against the accused individuals.

Criminals can use computers in two ways to carry out their activities. First, they may utilize the computer as a repository, also known as a database, to house the information they have acquired.⁵ For example, if a criminal is collecting credit card or personal identification information, he/she might create flat files, such as a text file, to copy and record the retrieved information for later use. The criminal can also create a database if he/she has a large list of information to easily run queries against to extract the type of information desired.

Criminals also use computers as a tool to commit crimes. They utilize their ability to connect to the Internet and various other types of networks. The computer simply needs a modem or Ethernet card to connect. The criminal may then connect to bank networks, home networks, office networks or virtual private networks (VPNs). The individual can utilize a number of tools to gain access to these networks and their data.⁶ The criminal might also use ghost terminals, which are machines not owned by the individual but used to carry out unlawful activities. For example, a hacker may connect to a computer that he/she hacked on a university campus, and then launch attacks from that computer and possibly store data on it. Agents should consider the possibility that the computer user has stored valuable information at some remote location.⁷ Specialists will need to survey and assess various avenues during an investigation, even those that are not immediately obvious at the crime scene.

Methods and Techniques

At times, individuals might attempt to hide data that contain incriminating information they do not want others to find. One commonly used method to hide data is to rename a file of a particular type to another type by changing the extension of a file. For example, an individual with pornography on his/her computer might not want others to find it. Therefore, it is possible that he/she might change the .jpg extension to .xls for Microsoft Excel. Renaming the file makes it nearly impossible for someone to search through and determine the correct file type. In cases such as this, EnCase can be utilized to flag suspicious file types. Running a hash analysis of the hard drive will interpret the file headers and mark them as containing incorrect header information.⁸ Thus, after the file has been flagged, the analyst can read the file header information and make a determination of the correct file type.

Computer forensic specialists can gather evidence against a criminal in several ways. They can image a hard drive or other media on which the illegal information might be stored. For example, if the attacker has saved the database to a floppy and formatted the floppy disk, the specialist can most likely retrieve the illegal data from the drive. Specialists can decrypt and crack passwords that have been imposed on files, as criminals might encrypt their files and set passwords to inhibit others from gaining access to the illegal files.

The science of computer forensics is meticulous and requires patience and dedication. Specialists must be extremely careful to preserve the original file or device, for that is all with which they have to work. Therefore, it is extremely important to first create exact images of the information and work with that information on a different medium. Specialists work hard to find vital information and gather enough evidence for prosecution or disciplinary action.⁹

Often, these specialists investigate under extreme secrecy so other individuals do not know exactly what they are doing or what information they have gathered. Once they have thoroughly gathered all the information and evidence that they can, specialists compile a report to be used in court. At times, specialists themselves testify in court when an independent opinion is needed on complex technical issues, since these individuals are specially trained, have an extensive background working with computers and dealing with technical issues, and are familiar with gathered information and the methods used to acquire that information.

Computer Forensics in Business

Computer forensics specialists are especially important to business. Businesses frequently call upon these specialists to assist when an incident occurs and computer crime expertise is needed. For example, an employee of a company is using the company's computer for personal reasons on the company's time. The employee might be surfing the web to access adult web sites, search through auction sites, engage in peer-to-peer file transfers, swap music and movies using company bandwidth, or perform a number of other activities where the individual engages in agency conflict. In recent years, these

activities have been considered illegal and, although it is still a gray area, most companies do not allow their employees to engage in these types of activities.¹⁰ If an employee has been suspected of engaging in such activities, he/she might try to delete information and cover the tracks in the hope that no one will find the files or other evidence and he/she can keep the job. This is where the forensic specialist becomes involved. Companies can hire specialists to gather various types of information from the employee's computer. Specialists can recover deleted files, track network activity and create reports that contain a summary of all of the employee's activities. This is important for corporations because they will then have legal, binding evidence against an employee and will be able to terminate him/her and take other actions legally. The employee will not have a leg to stand on once such evidence has been gathered.

Angry employees are more likely than independent hackers and competitors to commit a crime against a firm. The individuals who launch these attacks may have a specific type of attack in mind. In recent years, malicious-minded individuals have assaulted numerous e-commerce web sites with denial-of-service attacks and have imposed several other malevolent acts on corporations and governments including, but not limited to, viruses, wiretapping and financial fraud. These attacks can cause financial hardships to companies, especially their e-commerce activities. Cybercrime potentially costs millions, if not billions, of US dollars in unrealized profits and exposes organizations to significant risk.¹¹ For example, if a disgruntled employee finds an exploit in the company's

financial securities and begins stealing the company's money, this could potentially hinder the viability of the company. If someone is suspected of embezzlement, a computer forensics specialist could be hired to analyze and gather evidence against the suspected individual. It is important to realize the ramifications that can occur from a computer attack. If prosecuted, depending on the crime, a person can face stiff fines and jail time.

Challenges of Computer Forensics

For the IT professional—especially IT audit and security—computer forensics is an exciting, developing field. IT professionals can work in the field of computer forensics or side-by-side with computer forensics specialists, supplying insight into a particular system or network. The specialists can ask the IT professional questions pertaining to the system and get a response faster than by doing research on their own and figuring everything out blindly. Although specialists are highly trained and can adapt to most systems or platforms, collaboration can make the jobs of the forensics specialist and the IT professional easier and more efficient.

Since its birth in the early 1970s, computer forensics has evolved into what is now a large field. New technologies and enhancements in protocols are allowing engineers and developers to create more stable and robust hardware, software and tools for the specialist to use in computer-related criminal investigations. As computers become more advanced and more

*It is extremely
important to first
create exact images
of the information.*

abundant, so do criminal activities. Therefore, the computer forensics niche is in constant progression along with the technological advancements of computers.

With new, complex advancements, there are also complicated challenges. One of the challenges that will be facing the field of computer forensics is the advancement of encryption. As encryption standards rise and the algorithms become more complex, it will be more difficult and more time-consuming for specialists to decrypt and then piece together encrypted files into meaningful information. Another major challenge is maintaining credible certifications and industry standards in the field. Currently, there are a few cardinal rules that specialists tend to follow:

- Ensure that no forensics evidence is damaged, destroyed or otherwise compromised by the procedures used during the investigation.
- Never work on the original evidence.
- Establish and maintain a continuing chain of custody.
- Document everything.¹²

These rules are especially important because they help ensure that the data will be gathered in a structured manner even though there is not a solid set of standards. Currently, the National Institute of Standards and Technology (NIST) creates the various standards for the technology industry in the US. More standards need to be adopted for this field to make the gathered evidence and the compiled information used in court more credible in the eyes of the judge, jury and opposing attorneys. Once better standards are addressed and adopted, information gathered by specialists will be more reliable in court and to the general public.

Education and Training

Computer forensics specialists are highly trained consultants who have the ability to solve complex computer crime-related issues. Professional organizations such as the Information Systems Audit and Control Association (ISACA), the High Technology Crime Investigation Association (HTCIA), the Institute of Internal Auditors (IIA), the Association of Certified Fraud Examiners (ACFE) and the Information Systems Security Association (ISSA) have offered training support in this evolving area. The specialists are trained extensively on knowledge of software packages and utilities used to obtain data. Individuals seeking a career in computer forensics can obtain training from universities, technical schools and seminars. Specialists typically hold degrees in computer science, computer engineering or computer information systems. As mentioned previously, there are various professional organizations that people in the industry can join to further their networking and education in this field. Certifications are available from software vendors for their products. Individuals must go through rigorous training and have a solid working knowledge of the software to be competent enough to pass the test. Nonvendor certifications, such as Certified Information Systems Auditor™ (CISA®) and Certified Information Systems Manager® (CISM®), are also available.

At the university level, University of Tulsa (Oklahoma, USA), Purdue University (Indiana, USA), University of Texas

(USA) and many others have developed state-of-the-art training programs and facilities to teach future practitioners in this field. A recent article by Patricia Y. Logan, Ph.D., from Marshall University of West Virginia (USA) is worthwhile reading for the challenges of the field and the use of forensics as a tool. The document, titled “Corporate Computer Forensics: Opening Opportunities for Students,” was presented at the 9th Annual Colloquium of Information Systems Security Educators and is available in its proceedings.

Demand for Computer Forensic Services

As computers become more prevalent in the world, more computer crimes will occur. Thus, the need for computer forensics specialists will continue to grow as long as computers are being implemented in society. Currently, the need for computer forensics is growing exponentially. The need is particularly acute at local, state, federal and military law enforcement agencies that house computer forensics divisions.¹³ It is important for companies to identify and take proper action against those who engage in agency conflict. Once an individual is suspected of any type of computer crime, whether it is embezzlement, file sharing or fraud, it is in the organization’s best interest to hire a computer forensics specialist to gather evidence that could possibly prove that the suspect is guilty of the accused crime.

In recent years, corporations have started taking the initiative and imaging the contents of an employee’s computer when he/she leaves the company. As such, an employee’s hard drive is imaged upon resignation, termination or internal transfer. Archiving these images is important, as issues such as theft of trade secrets or intellectual property, harassment and wrongful termination claims often do not surface until months after an employee leaves his/her position.¹⁴ Therefore, it is important for companies to archive the information in the event that it needs to investigate the activities on the employee’s computer. With the increasing importance of computer forensics, the Big 4 accounting firms have stepped up their efforts to recruit and hire professionals with forensics skills.

The Future of Computer Forensics

The science of computer forensics has a seemingly limitless future, and as technology advances, the field will continue to expand. Such evidence has to be handled in the appropriate manner and must be documented for use in a court of law. Any methodology, process or procedural breakdown in the application of forensics can jeopardize the company’s case.

Organizations are beginning to rely on the findings that computer forensics specialists gather when a cybercrime is committed. Computer forensics quickly is becoming standard protocol in corporate internal investigations by expanding beyond the realm of specialized, computer incident response teams. As the overwhelming majority of documents are now stored electronically, it is difficult to imagine any type of investigation that does not warrant a computer forensic investigation.¹⁵ It is becoming a standard for electronic crime investigations.

As computers become more prevalent in the world, more computer crimes will occur.

Computer forensics is not only used for cybercrime cases, but the techniques and methods are also adopted for noninvestigative purposes. Examples include data mapping for security and privacy risk assessment, and the search for intellectual property for data protection.

Computer forensics is transitioning from an investigation and response mechanism to one of prevention, compliance and assurance.¹⁶ By utilizing computer forensics techniques, companies can better protect themselves against potential threats from hackers and angry employees. Additionally, computer forensics schemes can be used when critical files have been deleted accidentally or through hardware failure. Thus, there are several additional applications pertaining to the science of computer forensics in addition to utilizing the methods to investigate computer-related crimes.

Conclusion

The role of computer forensics will play a large role in society as computer technology emerges. It is an extremely hot topic and is used widely among all industries. Corporations and government agencies hire computer forensics specialists whenever they need a computer-related crime investigated. The specialists gather evidence from various media and present the evidence to whomever has ordered it or in some cases, in a court of law.

Endnotes

- ¹ SANS, "Interfacing with Law Enforcement—Frequently Asked Questions," 2005, www.sans.org/score/faq/law_enf_faq/
- ² Vacca, John R.; *Computer Forensics—Computer Crime Scene Investigation*, Charles River Media Inc., 2002
- ³ Pidanick, Ryan; "An Investigation of Computer Forensics," *Information Systems Control Journal*, vol. 3, 2004, p. 47-51
- ⁴ *Op. cit.*, SANS
- ⁵ Lunn, Dorothy A.; "Computer Forensics—An Overview," 20 February 2001, www.sans.org/rr/incident/forensics.php
- ⁶ *Op. cit.*, Pidanick
- ⁷ *Op. cit.*, SANS
- ⁸ Andrews, Ryan; Personal Interview, 6 June 2003
- ⁹ Vagon, "Computer Forensic Services and Systems," 2003, www.vogon-computer-evidence.us/

¹⁰ *Op. cit.*, Pidanick

¹¹ *Op. cit.*, Vacca

¹² *Op. cit.*, Lunn

¹³ *Op. cit.*, Vacca

¹⁴ Barbin, Douglas; John Patzakis; "Cyber Crime and Forensics," *Information Systems Control Journal*, vol. 3, 2002, p. 25-27

¹⁵ *Ibid.*

¹⁶ *Ibid.*

References

Beeson, Chris; "FBI/CSI Computer Crime and Security Survey," 1999, www.cbc.ca/news/indepth/hackers/csi-fbi2000.pdf

Fisher, Dennis; "Feds Move to Secure Net," *eWeek*, 10 March 2003, p. 1

Heiser, Jay; Warren Kruse; *Computer Forensic—Incident Response Essentials*, Addison-Wesley, 2002

Logan, Patricia Y.; "Corporate Computer Forensics: Opening Opportunities for Students," Proceeding of the 9th Annual Colloquium for Information Systems Security Education, June 2005

Security Focus, "An Introduction to Computer Forensic Tools," 10 October 2002, www.securityfocus.com/guest/16691

US Department of Defense, "Department of Defense: Computer Forensics Laboratory," 2003, www.dcfl.gov/DCFL/aboutdcfl.asp

Yang, John; "Government Jobs at Cyber Crime," 22 July 2001, <http://abcnews.go.com/sections/wnt/DailyNews/cybercrime010721.html>

Frederick Gallegos, CISA, CDE, CGFM

is an adjunct professor for the Computer Information Systems Department, College of Business Administration, California State Polytechnic University, Pomona, California, USA. He has more than 30 years' experience in the information systems audit, control and security field. He has taught undergraduate and graduate courses in the IS audit, security and control field and is published widely.

Information Systems Control Journal, formerly the IS Audit & Control Journal, is published by the *Information Systems Audit and Control Association*, Inc. Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of the Information Systems Audit and Control Association and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *Information Systems Control Journal* does not attest to the originality of authors' content.

© Copyright 2005 by Information Systems Audit and Control Association Inc., formerly the EDP Auditors Association. All rights reserved. ISCA™ Information Systems Control Association™

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by the Information Systems Audit and Control Association Inc., for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org