# Global Information Assurance Certification Paper

**Computer Forensics:**
**An Emerging Practice in the Battle Against Cyber Crime**

Jonathan D. Isner

Version 1.4

Billions of dollars are stolen each year by criminals, and in today's digitally dominated world, computers are rapidly becoming a vector for those criminals to carry out their crime. Computer forensics is an emerging practice helping victims of computer crime to discover evidence, and prosecute criminals in a court of law.

Dictionary.com defines forensics as, "The use of science and technology to investigate and establish facts in criminal or civil courts of law.[1]" Using this definition, computer forensics would be the application of computer science to a traditional criminal investigation. This paper will define computer forensics; discuss its importance in today's world, and provide proven investigative techniques used to solve crimes committed using computer technology. This paper will also provide an example of software programs used to conduct computer forensic investigations.

Computer forensics is a relatively new practice in the field of law enforcement and private industry. "The term "Computer Forensics" was coined back in 1991 in the first training session held by the International Association of Computer Specialists (IACIS) in Portland, Oregon.[2]" In the years that have passed since then, computers have become more prevalent in society, being used for many functions they were previously not used for, such as on-line banking transactions, data sharing, and stock purchases. Nearly every private home and business is now connected to the Internet in some fashion. "The number of Internet users worldwide is expected to reach 502 million by the end of 2003.[3]" Because of this, companies and private homes are finding themselves victims of computer-savvy criminals on both the inside and the outside of their organization, using computer technology in a malicious manner.

Computer forensics is important in today's world because as the science of computer forensics has been evolving over the years, malicious users and hackers have become smarter and cleverer with their techniques to compromise computer systems, steal money, and confidential, even national security information. Combine that with the lack of computer security implemented by companies and private citizens, leaving their computers extremely vulnerable from both insider and outsider threats, a new breed of cyber criminal has evolved. "The great advantage for criminals using technology is that they don't have to appear in person on the scene of the crime,[4]" said Loek Weerd, police

[1] http://dictionary.reference.com/search?q=forensics
[2] http://www.forensics-intl.com/def4.html
[3] http://www.scmagazine.com/scmagazine/2000_04/cover/cover.html
[4] Ibid

inspector and expert for the computer crime unit of the Haaglanden regional police in the Netherlands.

When one thinks of cyber criminals, the image of a pedophile comes to mind, stalking their prey through Internet chat rooms, or the lone hacker breaking into a bank network to siphon money from the bank to their personal account.

A cyber crime is committed when a computer, or computer technology is used to commit or hide a criminal wrongdoing. Cyber crime has taken many forms, and is used by white-collar criminals to hack into financial institutions, drug dealers, prostitution rings and organized crime. Some of the crimes carried out using computer technology include, fraud, virus and denial of service attacks, information theft and monetary theft. The perpetrator of a cyber crime can come from either inside the organization under attack or from outside the organization. The biggest threat to an organization comes from an insider, someone who has a link to the organization, typically an employee. A disgruntled employee with access to organization computer resources containing proprietary information or money can potentially be extremely dangerous. External threats are also very rampant, especially for organizations with web presence. According to the United States Internet Crime Task Force (USICT) and the CERT Coordination Center at Carnegie Mellon University, business-to-business e-commerce will reach over $1.5 Trillion dollars by 2004. There are over 5 Million websites and over 1 Billion unique Internet web pages, and millions of users of the Internet, which doubles every two years. Thousands of financial institutions in the US alone have websites and many of them are set up to conduct financial transactions on-line[5].

Like traditional forensics, computer forensics is a science, and uses specialized skills, tools and programs. The specialized requirements of computer forensics translate to an expensive cost, which most companies and law enforcement agencies are unable to afford to maintain all the time. This leaves these companies and agencies unprepared to deal with and respond to computer-related security incidents that occur on their systems.

Currently most law enforcement agencies and corporations don't have enough trained investigators to handle the amount of active investigations. According to the Federal Bureau of Investigation (FBI), 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. Professionals are working in many different industries practicing computer forensics. Computer forensics is used by state and local law enforcement, federal law enforcement agencies, other federal government agencies and by private corporations. Corporations that rely on a strong web presence, such as e-commerce companies that conduct business transactions over the Internet especially need the services of trained computer forensic experts because of their exposure to the great risk of hackers from the Internet.

In November 2000 the FBI opened the first Regional Computer Forensics Lab (RCFL) in San Diego, California. An RCFL is a single service forensic laboratory devoted entirely to the examination of computer evidence in support of

[5] https://www.usict.org/resources.asp

criminal investigations. RCFL examiners combine the talents and experience of Federal, State, and Local law enforcement agencies. Normally, an RCFL consists of 15 people: 12 of the staff members are examiners and 3 staff members support the RCFL. The RCFL's duties may include seizing and collecting digital evidence at a crime scene, conducting an impartial examination of submitted computer evidence, and testifying in court[6]. A second RCFL was opened in North Texas in 2001, and three are planned to open in 2003 in Chicago, Kansas City and San Francisco. RFCLs bring together multiple agencies, across multiple jurisdictions responsible for acquiring, archiving, and analyzing digital evidence in support of criminal investigations. RFCLs are very important to the progression of the computer forensics industry, and vital to the success of current and future investigations.

"Electronic or computer evidence used to mean the regular print-out from a computer.[7]" This is no longer the case, as computer forensics is the process of examining computers and computer media such as hard drives, tapes and diskettes. The goal of the forensic process is to obtain evidence that will stand up in court and be convincing to a jury. Computer forensic evidence is used by criminal prosecutors; in civil litigation cases such as divorce and harassment; by corporations to investigate fraud, embezzlement; and by corporate espionage and by law enforcement. Computer evidence must be "authentic, accurate, complete, convincing to juries and in conformity with common law and legislative rules.[8]"

Electronic records such as audit logs; e-mails, word processing files, and image files provide law enforcement and the government with important evidence in criminal cases. Evidence needs to be discovered and gathered as soon as possible in order to keep it from being contaminated. Evidence contamination is a major deterrent to a successful investigation. A chain of custody needs to be established and documented in order to account for all that happens to evidence from the time it was collected to when it is due to be used in court. The complex process of computer forensics requires that law enforcement agents and prosecuting attorneys be well versed in the techniques and the legal aspects of obtaining electronic evidence from computers and computer media.

Of course law enforcement personnel can't just go around seizing computer property. There are laws that govern computer forensic investigation. The laws that govern computer forensic investigation are the same ones that govern any law enforcement investigation. Two primary laws governing the seizure of electronic evidence from computer systems are the Fourth Amendment of the U.S. Constitution and the statutory privacy laws codified at 18 U.S.C. §§ 2510-22, 18 U.S.C. §§ 2701-12, and 18 U.S.C. §§ 3121-27. The Fourth Amendment restricts the power of law enforcement agents to conduct searches without a warrant. The Fourth Amendment states:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and

[6] http://www.nporcfl.org/2.shtm
[7] Vacca, p.3
[8] Ibid, p.26

no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[9]" One question that arises in Fourth Amendment cases is whether or not an individual has a right to privacy of the information stored on computers, or electronic media. "When confronted with this issue, courts have analogized electronic storage devices to closed containers, and have reasoned that accessing the information stored within an electronic storage device is akin to opening a closed container. Because individuals generally retain a reasonable expectation of privacy in the contents of closed containers, see United States v. Ross, 456 U.S. 798, 822-23 (1982), they also generally retain a reasonable expectation of privacy in data held within electronic storage devices.[10]"

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) went into effect in October 2001. This act widened the authority of law enforcement agents to make searches and seizures of computers in gathering electronic evidence. A major principle behind this piece of legislation is to fight money laundering that is believed to finance terrorist organizations.

The goal of evidence collection is to preserve the evidence for future use. Electronic evidence is volatile, and can easily be altered and lose is value and usability over time. There are difficulties that exist with electronic evidence that aren't found when dealing with regular physical evidence. The paper trail that is oft used to track criminals in non-electronic cases is much harder to track in electronic environments because it can be easily covered or altered.

These factors make it imperative for investigators to conduct their investigations according to a rigorous methodology and process. A good forensic technician will follow a "careful methodology of approach, including record keeping, sound knowledge of computing, sound knowledge of the law of evidence, sound knowledge of legal procedures, access and skill in use of the appropriate utilities.[11]" A general, simple outline for an investigation involves four steps: Identification of Evidence, Preservation of Evidence, Analysis of Evidence and Presentation of Evidence[12].

Identification of Evidence aims at finding where the pertinent evidence exists on a computer system. An investigator must be able to tell the difference between quality, usable evidence, and data that is not usable. The investigator must be skilled at searching, and know the right places to look.

Preservation of data aims at keeping the evidence in a usable form. The evidence should be preserved to as close to its original state as possible. Preserving the evidence could mean the difference between a successful case and a failure. Computer evidence could very easily be lost to erasure from many different causes. The best course of action to follow in order to preserve data is not to immediately examine the computer suspected of containing evidence. First, identify all devices that could hold evidence, for example laptops, PDAs,

[9] http://caselaw.lp.findlaw.com/data/constitution/amendment04/
[10] http://www.cybercrime.gov/ip.html
[11] Ibid.
[12] Vacca, p.128

and Zip drives. Secure all removable media such as Zip disks, floppy disks and CDs. Do not allow anyone to use these devices or media, and take an image of all devices and media.

Analysis of Evidence aims to make sense out of the data extracted from the computer system. The investigator must be able to pull out the meaningful evidence from all the data taken off the system.

Presentation of Evidence aims to put the evidence in a manner that is understandable. The understanding of the evidence can't just be restricted to other law enforcement personnel or forensic specialists. The presentation must be able to speak to people outside the forensic realm, such as lawyers, judges and jurors.

A computer forensic investigator's most powerful tools are the software programs used to collect and analyze evidence during investigations. There are many types of computer forensic software available to investigators that perform many functions of an investigation. Forensic tool software programs are used to gather or copy data from computers and computer media, decrypt computer information, or analyze computer media to locate information. Some of the available software is freeware, and some is very expensive and sold commercially. These software tools serve the full range of investigations. They are useful for a novice investigator searching one computer, to an experienced FBI task force searching the entire computer network of a major corporation or criminal ring. "The nature of the forensic examination and the goal of the investigation will determine the most appropriate tools to be used.[13]" These forensic tools aid the investigator in accomplishing the ultimate goal of the investigation, preserving the data in its original form.

One comprehensive piece of software that is used in forensic investigations is the EnCase Forensic Edition by Guidance Software. The EnCase software is loaded on the investigators' computer, which connects to the target computer. The target computer is the computer that has been compromised and is being investigated. The investigator next selects the media they'll investigate. EnCase is compatible with, and can be run on multiple operating system platforms including Windows, MAC OS, Linux, Solaris, and HP UX. Encase can analyze a plethora of computer media, including hard drives, Zip drives, USB devices, even Palm devices. EnCase uses an easy to navigate graphical user interface (GUI) so investigators can conduct intricate investigations with organization and precision.

The EnCase program creates a binary duplicate of the original media, including all slack space. The new image is verified for authenticity by comparing MD5 hash values of the original media and the duplicated copy. This ensures the preservation of the data, which is vitally important to the investigation. The analysis of the data is performed using the features of the EnCase software. Analysis is supported with different views that enable the investigator to quickly find specific information. EnCase allows investigators to work on multiple cases simultaneously. For example, while an investigator is acquiring data from a computer's hard drive, the investigator can search and acquire data from the

[13] http://www.securityfocus.com/guest/16691

computer's Zip or floppy drive. The Encase reporting function allows the investigator to document the results of their investigation in formats acceptable for court presentation.

EnCase allows the investigator to search a full range of file systems. The following file systems are currently supported by EnCase Forensic Edition: FAT12 (Floppy), FAT16, FAT32, NTFS, HFS, HFS+, UFS, Sun Solaris, EXT2, Reiser, Palm, CDFS, Joliet, UDF and ISO 9660.

Criminals will often try to cover their tracks by changing the character set of the data or document they are working with, or write the data in a foreign language. EnCase has full support for Unicode. It can display the characters of foreign languages, and allows for keyword searches in those foreign languages.

EnCase Supports different dynamic disk configurations, RAID 0, RAID 1, RAID 5, Spanned and Basic. A RAID drive is a configuration that employs two or more drives in combination for fault tolerance and performance. The EnCase software automatically detects the disk configuration and will map the drives.

Important evidence is often found in emails. Even though emails may have been deleted, it doesn't mean they are gone forever. EnCase features email search support by reading PST files, which is the file format associated with Microsoft Outlook, one of the most common email applications used the world over. Encase can bypass PST file passwords, read PST files and extract emails for plain text searches.

One of the superlative features of EnCase is the Enscript feature. It is a macro programming language built into the EnCase software. The investigator can customize scripts for specific tasks, and automated routine tasks.

When conducting a computer forensic investigation, time is of the essence. The EnCase Forensic Edition is a valuable software program that streamlines many tasks involved, giving the investigator crucial time to conduct analysis and ensure the evidence is preserved to its original format.

EnCase is an example of a high-end, expensive solution used for large-scale investigations by larger organizations. There are many other solutions available to investigators who represent smaller organizations with smaller budgets. Most software companies will allow their prospective customers to use a trial version of their program to aid the customer in making the correct decision for their forensic tool needs.

DataLifter is a collection programs for computer forensic specialists to use in an investigation. DataLifter consists of nine different procedures that perform many functions of an investigation. Some of these procedures are explained in the following paragraph.

Disk2File will scan all files and folders from the path you choose on a target computer. While scanning the target computer or media, important file information as filename extension, last access date, creation date and time, modification date and time and file size. The Image Linker procedure was developed to deal with the ART file format. ART files are graphic images used by America Online. The File Extractor procedure will retrieve files from unallocated disk space. Often, evidence can be found in file slack and

unallocated file space. File slack can contain random bytes of data from the computer's memory. This occurs because Windows writes data in 512 byte blocks called sectors. Clusters are made up of blocks of sectors. If there isn't enough data in the file to fill the last sector, Windows pads the remaining space with data from the memory buffers of the operating system. The data randomly selected from the memory buffers is called RAM slack. RAM slack can contain information that may have been created, viewed, modified, downloaded, or copied during work sessions that have occurred since the computer was last booted. This kind of data is called ambient data. As much as 50% of computer hard disk drive may contain this ambient data – email fragments, word processing fragments – other fragments from previous work sessions[14]. The Internet cache and history agent allows the investigator to read the cache and history folders and files of Netscape and Internet Explorer. The Email Retriever procedure provides a means to view Email created by the Microsoft Outlook Express, Netscape, Eudora, and Pegasus without having to run the Email client. Some DataLifter procedures are designed to work with other forensic programs, such as the aforementioned Guidance Software's EnCase software.

LC-Tech offers a set of forensics tools developed to recover lost and deleted data, packaged as their Forensic Utility Suite. FILERECOVERY for Windows works across all Windows operating system platforms to recover files that have been deleted. FILERECOVERY Professional allows an investigator to recover data from damaged disk drives. Drives are automatically detected even though they may not be visible in Windows Explorer. FILERECOVERY for Digital Media allows an investigator to recover lost files from digital media such as flash cards, memory sticks, and DVDs.

One important practice during an investigation is to create a mirror image backup of systems being investigated. Mirror image backup software is important and should be used to preserve data. SafeBack is an evidence preservation tool developed for use by federal law enforcement agencies. It is used to make mirror image backups of entire hard drives or hard drive partitions and can write to almost any magnetic storage device such as tape drives.

Vogon, International is another company that produces imaging software and hardware designed to capture large amounts of data off a system quickly, assuring the integrity of the data. Their Dual DAT Imager is designed to capture a large volume of data on the site of an investigation. The hardware produces both evidential and working images, and keeps an audit log, which can be used in conjunction with the evidence in a court of law. The Dual DAT Imager is directly attached to the suspect computer via a SCSI or parallel connection.

Even though disk imaging can be quite a lengthy and challenging process, it doesn't have to be expensive. The Data Dumper tool is a command line tool developed for UNIX systems and is freely available. The tool can make exact copies of UNIX files systems for analysis. Being a command line tool it requires knowledge of the UNIX file system structure and commands.

Foundstone, Inc. offers a set of forensic tools that are free for anyone to download. The Vision tool is a host-based utility, which when run, displays all the

[14] Vacca, p.38

open TCP and UDP ports on a system, the service that is running on that port, and the application associated with that service. NTLast is a Windows Event Log analysis tool. It is a command line tool that can search local and remote NT security event logs to display entries in an on-screen report. NTLast can filter out and display Internet Information Server (IIS) logons. This is a good tool for investigators to quickly analyze security and system audit logs. The Forensic Toolkit™ is a set of Win32 command line tools that can examine NTFS file partitions. AFind lists all files by their last access time. HFind scans a drive for hidden files.

Some forensic tools are meant for use in a situation when the investigator wants to analyze a computer while it is still running. One of these tools is the built-in Windows command, netstat. The netstat command lists all active connections, and ports that are actively listening. It can give statistics on IP, TCP, ICMP and UDP. Examples of the statistics output are IP packets received, IP address errors, ICMP messages sent and received, failed TCP connection attempts, and UDP datagrams received and sent.

It has been stated that just gathering evidence alone won't make for a case in court. The evidence must be connected to a person who committed the crime. This is often the most difficult part of the analysis of forensic evidence, tying that evidence to a perpetrator. One form of identification for computers is its IP address. The IP address is the identifier for every computer or device connected to the Internet. A domain name is a common name that identifies an IP address making it easier to search for computers and devices on the Internet. A utility called Whois allows an investigator to search an IP address and will return a domain name, and vice versa. This utility would be helpful in identifying computers that attacks have originated from, or identifying web sites visited by a suspect who has attempted to cover the tracks of their web usage.

As the practice of computer forensics has emerged, so has the need for professionals to be trained and kept up to date with the latest industry technology and processes. Training is extremely important for computer forensics investigators. The proper training could mean the difference between catching a cyber criminal, and that criminal going free. There are many different means to receive training in the process of computer forensics. Some are short courses meant to introduce a student to the industry and its techniques and practices. Other courses are taught by companies to teach students to use and become experts in their forensic software package. New Technologies, Inc. (NTI) offers a range of courses from a 3-day hands-on class meant to immerse students in situations in which a forensic response is necessary. NTI also offers more specialized courses such as a class on the practice of data hiding, a class specializing in the forensic investigation of Microsoft Windows computer systems, and a class specializing in preparing students to present evidence and testify in court.

Colleges and Universities around the country have recognized the importance of computer forensics, and many college-level curriculums have surfaced as a result. The George Washington University department of Forensic Science offers a Master of Arts degree in Computer Fraud Investigations. The

program combines study of risk management, security management, forensic science practices such as techniques for investigation and evidence collection and analysis. The program also offers courses in criminal law to cover the legal issues that pertain to computer investigations.

Of course if one doesn't have the time or resources to take a class or enroll in a full degree program in computer forensics, a good way to learn about the industry and its tools is to download some of the freely available tools previously mentioned in this paper, and experiment with their features and functions.

In conclusion, as computer technology has become more advanced it has permeated society in business and private homes. Computers are now used for financial transactions, banking, stock purchases and retail purchases involving credit cards. As computer technology has become more advanced, criminals have become computer savvy. Criminals now use computers to carry out a variety of crimes, from viral attacks, to financial fraud. Computer forensics is an emerging practice and industry for law enforcement and private corporations to combat the threat of these computer savvy criminals. Computer forensics involves the application of computer science to traditional criminal investigation. Its purpose is to collect evidence from computer systems and computer media that can be preserved and analyzed by the investigator, and can be presented in court to aid in prosecution of criminals. There are many software programs available to computer forensic specialists to aid in conducting investigations. These programs can help to retrieve data and automate some tasks of an investigation, helping with the preservation of data and speeding up the process of the investigation. There are laws that govern the search and seizure of computer resources in a criminal investigation, with the Fourth Amendment of the Constitution being the primary governing law. Recently, lawmakers have passed legislation giving investigators more power to conduct searches and seizures of computer related technology. Lawmakers in the United States have obviously realized the growing threat of cyber crime and the need for law enforcement agents to be able to quickly respond to incidents.

Computer technology will only continue to advance and pervade society, and criminals will only continue to get smarter in the ways they use computers to carry out crimes and hide information. Trained computer forensic professionals in both law enforcement and private industry will prove to be extremely valuable in the years to come fighting cyber crime.

## References


Dictonary.com
http://dictionary.reference.com/search?q=forensics

New Technologies, Inc.
http://www.forensics-intl.com/def4.html

Armstrong, Illena, "Computer Forensics." SC Magazine, April 2000.
http://www.scmagazine.com/scmagazine/2000_04/cover/cover.html

The United States Internet Crime Task Force, Inc.
https://www.usict.org/resources.asp

Regional Computer Forensics Laboratory, National Office
http://www.nporcfl.org/2.shtm

Find Law
http://caselaw.lp.findlaw.com/data/constitution/amendment04/

Computer Crime and Intellectual Property Section of the Criminal Division of the US Department of Justice
http://www.cybercrime.gov/ip.html

Morris, Rod, "An Introduction to Computer Forensic Tools." Security Focus – Guest Feature, October 10, 2002.
http://www.securityfocus.com/guest/16691

LC Technology, International
http://www.lc-tech.com/forensic_suite.htm

George Washington University
http://www.gwu.edu/~mastergw/programs/crime_commerce/index.html

Foundstone
http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/freetools.htm

Vacca, R. John. Computer Forensics: Computer Crime Scene Investigation. Charles River Media, May 2002.