# Global Information Assurance Certification Paper

SANS Security Essentials GSEC Practical Assignment
version 1.3
Ramon HurlockDick
March 3, 2002

## Analysis of Computer Forensics

## Abstract

Crimes and criminal investigations have been commonplace for years. Many innovative techniques have been developed in order to solve crimes and help keep criminals under control. Before the age of computers, if one were asked to give an example of a crime, you might say "car theft", "assault and battery", "burglary", and many other "conventional" crimes. Law enforcement fully understood them and dealt with them in an appropriate manner. The digital age has dramatically changed the scope of a crime by adding the "electronic" component and with it comes a new form of science, "Computer Forensics".

## Forensics Defined

Forensics in its earliest form dates back to the days of the Greeks. They held contests for public speakers whose abilities were considered central to democracy. These speaking events were eventually associated with the term forensics. Since these events were largely concerned with public advocacy, evidence gathering and presentation in a legal setting also became associated with forensics. This is how the term became common with traditional evidence gathering for traditional crimes and now with non-traditional evidence gathering for computer crimes. This paper will focus on the computer-related aspects of forensics.

## Computer Forensics Defined

The definition of Computer Forensics is " The employment of a set of predefined procedures to thoroughly examine a computer system using software and tools to extract and preserve evidence of criminal activity."

The overall objective of Computer Forensics is to apply a set of procedures and integrate analytical techniques to extract evidence when a computer is used as evidence in a criminal investigation. By working with law enforcement and corporate officers, computer forensics experts must delicately preserve and examine data as it relates to a criminal offense. The expert must be knowledgeable in hardware, software and proficient in applying legal procedures in a criminal investigation.

## Why is Computer Forensics needed?

Computer Forensics is needed due to the complex nature of electronic media. Traditional forensic techniques will not work in recovering and compiling computer based evidence.

Computer network and storage system are fairly complex and requires that the computer forensic scientist/specialist have a high degree of knowledge of hardware, software, operating systems, etc in order to even begin to look for evidence.

When a computer crime is committed, law enforcement must seek the expertise of these computer forensic specialists in order to charge and prosecute crimes involving computer equipment.

There is a tremendous amount of fraud being committed using computers. Everyday thousands of computer users are bombarded with tons of bogus email. There is always someone on the Internet trying to find a new victim to commit a crime against. There are fake websites, phony online auctions, credit card fraud and a host of other crimes. The percentage of fraud is going up and people are losing thousands of dollars to cyber thieves. It does not hurt any less when someone steals money from you using a computer than in person. With the anonymity of the Internet, individuals feel more empowered to send threatening email to other users and groups. Traditional mail can be traced easier and takes longer to reach its intended destination.

Attacks against companies are also very rampant on the Internet. Hackers and other such individuals are always trying to compromise one system or another on the Internet. It may range from a home user to a sensitive government system. Hackers have been known to steal valuable information from e-commerce systems and hold the information for ransom.

All of these various examples are more than enough reason why computer forensics is needed.

**Advantages of Computer Forensics**

Computer Forensics has become a major advantage in investigating crimes, computer and non-computer related. The reason is that most people who are committing crimes, use computers to store and track important information. Computer Forensics can play a major role in retrieving this information, even when the data is intentionally deleted. The science has come a long way in preserving and protecting "computer evidence" in order to work with law enforcement in prosecuting groups and individuals.

**Disadvantages of Computer Forensics**

Although the use of computer forensics has been in use since the mid 80's, only law enforcement and military agencies were using it to investigate computer crimes. The introduction of Computer Forensics to the private sector is relatively new and a few challenges have surfaced. The availability of trained Computer Forensics experts may be one of the biggest problems. Improper procedures and techniques can be challenged and possibly be defeated by sharp defensive lawyers in court cases. Computer Forensics can also be very tedious, time consuming and expensive in order to follow proper procedures as required by law.

**Storage Technology**

The majority of work involved in computer forensics focuses on some sort of storage device. Most storage is done on some sort of magnetic media (ie magnetic tapes, floppy disks, hard-drives, etc), the most common of which is the hard-drive.

I will take a moment to explain what a hard-drive is and its related technologies. Hard-drives are electronic storage devices. It takes the information that a user creates, whether it's an email, word document or excel spreadsheet and electronically stores it. This is also where the operating system and other essential data are stored. A computer may have one or more hard-drives. Hard-drives come in a variety of sizes and types. The most common type is IDE, but there are other types such as SCSI, Fiber Channel and a new technology called FireWire.

All hard-drives operate in a similar manner. They have partitions, able to access data directly and have a way to associate the file with the physical storage. At the physical or hardware level, the drive is composed of tracks, cylinders and sectors. When a drive is formatted, the physical tracks are formed so that data can be stored in them. Sectors are portions of the tracks and normally are segmented in 512K increments. At the software level the way the files are organized are based on the particular operating system used. Two of the most popular operating systems are Windows and Unix.

Once an operating system is in place, clusters can be formed based on logically grouping the physical sectors together. A cluster is the smallest unit of storage that the operating system can use to store a file and each cluster must be used completely. In other words, you cannot have a cluster that is only partially full. A Windows Dos based file structure is normally a group of partitions that logically map to a drive letter such as "A", "C", "D", etc. A Unix based file structure also has partitions, but uses a concept called a "file system" and mount points "/","/usr", "/var", etc. A Windows Dos based system tracks files using FAT or File allocation Table. There are entries in the FAT that point to the various clusters on the system. The Unix equivalents of FAT are inoeds or "index nodes".

From a Computer Forensic point of view, this is what happens when a file is stored and deleted. For purposes of this example, we will use the Windows file system. If a user wants to create a 2K file, the system will have to allocate a minimum of one cluster to accommodate this file. Since the file is smaller than one cluster and we know that a cluster has to be completely full, the system will take "random data" from areas such as memory, swap, and "fill" the rest of the cluster. This extra space that Windows had to fill up demonstrates the concept of "File Slack". This random information could have been anything at all. This is an important concept for the forensic investigator as the contents of that file slack could be an important clue to solving a problem or question. If the user now deletes that file, the file is not physically deleted, only the entry in the FAT is removed and using special forensic tools, partial data or the complete file may be recovered.

**Computer Forensic Tools**

Net Threat Analyzer

This is a forensic tool that is designed to help school educators; police and other law officials analyze the Internet history of computer users. This tool can look through a computer's hard-drive and retrieve various Internet related information such as email and web sites visited. The tool works by booting from a floppy drive, scans the hard-drive and flags any information that may be suspect. This tool may have been helpful in the case of the Columbine High School Shooting where the Internet was used to research data on building weapons.

GetSlack

This tool is used to retrieve file slack information. As mentioned before, file slack contains very valuable information and can be very helpful to investigators. The program is small enough to fit on a floppy disk. It is DOS-based, able to convert hidden information into readable format automatically, and does not leave any trace evidence behind. It can be used either in an investigative mode or auditing mode for slack file analysis. GetSlack is a small and helpful piece of software.

F)orensic (R)ecovery of (E)vidence (D)evice - F.R.E.D. Sr

This is a complete solution for the top-notch computer forensic investigator. F.R.E.D. is a hardware and software toolkit. Instead of attempting to search the workstation and boot from floppies the investigator can take the storage device and attach it to F.R.E.D.. This tool can accept several types of devices: 3.5 floppy, SCSI and IDE hard-drives, Jazz and Zip drives, etc. Basically, you can just plug in the media and it can read it. Once the media being investigated is connected to F.R.E.D, one of several forensic software tools (DriveSpy, Image, PDWipe, PDBlock and PART ) can be used to analyze the data. A very unique feature of the F.R.E.D. system is the SCSIBLOCK system. Forensic investigators have to be careful about unwanted writes occurring during any ongoing analysis. The SCSIBLOCK system will prevent unwanted writes at a hardware level from SCSI devices to the installed IDE drives.

DriveSpy

This tool can perform a variety of forensic functions. It can be installed to collect evidence as it occurs, examine disk partitions, process hidden and deleted file, create exports and a host of other features.

PDWipe

This tool is designed to properly wipe a hard-drive clean. It is capable of doing a de-classification level wipe in accordance with NAVSO P5239-10 standards.

Image

This tool is designed to create copies of floppy disks that are suitable for forensic analysis. It uses a MD5 checksum to maintain integrity.

PDBlock

This tool is designed to block physical writes to disk drives during an investigation. It operates on a software level instead of a hardware level like SCSIBLOCK.

BMAP

The tools so far focus mainly on Windows file systems. This tool is designed to recover evidence from a Unix file system. It can be used to store (i.e. "hide" information), view hidden information and retrieve data.

FBI Carnivore

In order to deal with serious computer related crimes and issues such as terrorism, espionage, information warfare, fraud, child pornography and sexual and exploitation of children, the FBI has created a program called Carnivore. This is complex software that is designed to work with Internet Service Providers and capture all information that passes through them. Based on controls that have been programmed into the software, it will only pick out information that the FBI has legal right to "listen" to. This tool is very controversial based on some public belief that it could be used for abuse of privacy issues. It will allow the FBI to be much more effective in their computer crime investigations.

These are just a few of several tools that are available for Computer Forensic Analysis. Most of the tools perform similar analysis using independent techniques. It is common practice to use several independent tools to perform the same analysis in order to prove accuracy.

**Techniques**

Proper forensic procedures and techniques go hand in hand with good forensic tools. Without proper training with regards to handling evidence and use of forensic tools, the evidence may be compromised or destroyed.

The first step would be safe seizure of the evidence. The computer should be shutdown immediately. No programs should be executed as they could destroy evidence or trigger data destroying programs. Anyone operating the computer at the moment of seizure should be immediately removed from the scene. The next step should be to document everything regarding the configuration of the hardware, times, dates and circumstances of the actual seizure.

After the first two steps are completed, a specialized kind of backup called a bitstream backup should be completed. Normal backups are not appropriate when backing up data that will be used for evidence; their archiving process changes the data slightly and bitstream backups maintain the original state of the data as required by law. Using some of the tools mentioned before, a backup should be created that does not alter the original data in any manner.

After the backups are performed the original evidence should be stored in a locked facility and then the analysis can be performed on the copies. Any analysis should be performed more than once with independent tools. This will help prove the integrity of the various tools and validate the results.

Recommended Evidence Handling

- Shut down the computer
- Document the hardware configuration of the system
- Transport the computer system to a secure location
- Make bitstream backups of hard disks and floppies
- Perform an integrity check of all data via hashes
- Document the system date and time
- Make a list of key search words
- Evaluate the swap File
- Evaluate file slack
- Evaluate unallocated space
- Search file, file slack and unallocated space for key words
- Document file names, dates and times
- Identify file, program and storage anomalies
- Evaluate software functionality found in the system
- Document your findings

## Legal Implications

As with any forensic science, there are legal standards which govern the way crimes can be investigated. On October 26, 2001, the Patriot Act was implemented to govern the way computers are seized and evidence gathered. Prior to this act there were several loopholes that hindered investigators in the prosecution of certain computer crimes. This act closed several of those loopholes with the following amendments. Here are some of the modifications with some explanations.

· Section 202 Authority to Intercept Voice Communications in Computer Hacking Investigations
This section allows investigators to obtain wiretaps for violations of the Computer Fraud and Abuse Act

· Section 209 Obtaining Voice-mail and Other Stored Voice Communications
This section allows investigators access to voice mail without the requirement of a wiretap.

· Section 210 Scope of Subpoenas for Electronic Evidence
This section allows the ability of investigators to gather evidence related to the Internet such as session information and Internet Service payment records.

· Section 212 Emergency Disclosures by Communications Providers
Allows communications provider the permission to report information of any imminent terrorist-like attacks immediately.

· Section 217 Intercepting the Communications of Computer Trespassers
Allows computer owners to authorize law enforcement officials to intercept computer hackers that are trying to break into their systems.

· Section 814 Deterrence and Prevention of Cyber-terrorism
    · A. Section 1030(c) - Raising the maximum penalty for hackers that damage protected computers and eliminating mandatory minimums.
    This section raises maximum time for first time offenders that damage protected system to ten years and to twenty years for repeat offenders.
    · C. Section 1030(c) - Aggregating the damage caused by a hacker's entire course of conduct.
    This sections allows investigators to add up the cost of the damage to all the computers a suspect has caused and charge them with the appropriate charges.
    · D. 1030(c)(2)(C) - New offense for damaging computers used for national security and criminal justice.
    This section allows hackers to be prosecuted if they attack any computer used for National Security or similar even if the damage is under the minimum amount $5,000.

**Analysis of Actual Case Studies using Computer Forensics**

- Apparently several employees at Anderson Consulting were ordered to delete email that was connected with the Enron Corporation. This is very similar to the popular document shredding that Anderson was also involved with. Unfortunately or fortunately (depends on your point of view) email evidence is much easier to retrieve than paper evidence. Investigators were able to use forensic techniques and software to recover quite a bit of deleted files from employees workstations, email servers and backup tapes. The details of the emails are not available at the moment, but the fact remains that simply deleting email will not protect even a large firm as Anderson Consulting.

- A public company was dealing with a wrongful dismissal claim involving an employee who was fired for visiting pornographic Internet web sites while at work. The subject employee alleged that he should not have been fired because the executive who fired him

was also browsing Internet web sites which had pornographic-based content. There were also other allegations that this executive was misappropriating company funds and resources. Computer Forensics found evidence to support the allegations concerning this executive and the focus of the investigation shifted towards the executive.

- A Computer Forensics expert assisted in the conviction of Rev. William Guthrie, former Pastor of Wolsey's First Presbyterian Church, who was charged with the first-degree murder of his wife, Sharon Guthrie, who had drowned in the bathtub of their home. An autopsy revealed that she had taken an overdose of the sleeping pill Temazepan. The Rev. used the Internet as an information resource to gather information for painless and surefire killing methods. The computer detective had found detailed notes about sleeping pills and household cleaning agents. By combing files stored on the Rev's computer, the forensics expert was able to submit his findings as evidence in the murder trial.

- After years of service, a senior executive was terminated very close to his vesture date. He believed that the dates of his termination and vesture date were too close to be a coincidence. He filed a lawsuit for age discrimination against his former employer and the company denied all charges. Computer Forensics experts were able to prove that a recent search had been performed on the company database for employees within a certain age group. The company settled the case out of court.

- A fast living con artist was filing for bankruptcy. While the case was being processed and his assets were being evaluated, he was living on a multi-acre ranch with a girlfriend. His creditors inquired if he owned the property. He provided a letter that he had given the property to his girlfriend as a gift, three years prior. Computer Forensics experts proved that the letter, stored on his computer, was false due to "back dating".

## Summary

Computer Forensics is not just a set of fancy tools that can retrieve deleted files and crack passwords. Computer Forensics is a complete science just like the other forensic science. Experts have to learn how to handle the data and what to do with the data once it is retrieved. Strict procedures must be followed or evidence can be thrown out of court as invalid.

Due to the wide use of technology and information being stored on computers, having trained experts at retrieving and analyzing computer information is invaluable to many modern court cases. Even when the case does not seem to be remotely computer related, some critical information might be stored on a computer. The importance, understanding and support of Computer Forensics cannot be stressed enough. Computer Forensics is becoming as important to the legal community as any other type of forensic science.

**Sources**


1. American Forensics Association, " What is Forensics?", http://www.americanforensics.org/what.html

2. Robbins Judd , " An Explanation of Computer Forensics", 5 December 2001.,http://www.computerforensics.net/forensics.htm

3. Alex Salkever, "Hot on the E-Trail of Evidence at Enron", http://www.businessweek.com/bwdaily/dnflash/jan2002/nf20020129_3701.htm

4. *Dan Caterinicchia* , " New software will help school, police identify threats and hate crimes on the Net ", http://www.cnn.com/TECH/computing/9907/06/netthreat.idg/

5. *New Technologies Inc.* , "File Slack Defined", http://www.forensics-intl.com/def6.html

6. *New Technologies Inc.* , " GetSlack - Forensic Data Capture Utility", http://www.forensics-intl.com/getslack.html

7. *FBI Press Room* , " Congressional Statement 200 Carnivore diagnostic tool", http://www.fbi.gov/congress/congress00/kerr090600.htm

8. *New Technologies Inc.* , " GetSlack - Forensic Data Capture Utility", http://www.forensics-intl.com/getslack.html

9. Digital Intelligence, Inc., " F.R.E.D. Sr ", http://www.digitalintel.com/fred_sr.htm

10. Michael R. Anderson, " Digital Intelligence, Inc. ", http://www.forensics-intl.com/art5.html

11. National Fraud Information Center, "2001 Internet Fraud Statistics ", http://www.fraud.org/

12. United States Department Of Justice, "Computer Crime and Intellectual Property Section (CCIPS) ", http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm

13. Computer Forensics Inc., "Case Histories", http://www.forensics.com/casehistories/frame.htm

14. Linux Security.com, "Linux Data Hiding and Recovery", http://www.linuxsecurity.com/feature_stories/data-hiding-forensics.html

Last Updated: July 25th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Boston 2017 | Boston, MA | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| SANS Prague 2017 | Prague, Czech Republic | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| Community SANS Omaha SEC401* | Omaha, NE | Aug 14, 2017 - Aug 19, 2017 | Community SANS |
| SANS New York City 2017 | New York City, NY | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS Salt Lake City 2017 | Salt Lake City, UT | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS Adelaide 2017 | Adelaide, Australia | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style | Virginia Beach, VA | Aug 21, 2017 - Aug 26, 2017 | vLive |
| SANS Chicago 2017 | Chicago, IL | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| SANS Virginia Beach 2017 | Virginia Beach, VA | Aug 21, 2017 - Sep 01, 2017 | Live Event |
| Community SANS Pasadena SEC401 @ NASA | Pasadena, CA | Aug 23, 2017 - Aug 30, 2017 | Community SANS |
| Mentor Session - SEC401 | Minneapolis, MN | Aug 29, 2017 - Oct 10, 2017 | Mentor |
| SANS San Francisco Fall 2017 | San Francisco, CA | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| SANS Tampa - Clearwater 2017 | Clearwater, FL | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| Mentor Session - SEC401 | Edmonton, AB | Sep 06, 2017 - Oct 18, 2017 | Mentor |
| SANS Network Security 2017 | Las Vegas, NV | Sep 10, 2017 - Sep 17, 2017 | Live Event |
| Community SANS Albany SEC401 | Albany, NY | Sep 11, 2017 - Sep 16, 2017 | Community SANS |
| Mentor Session - SEC401 | Ventura, CA | Sep 11, 2017 - Oct 12, 2017 | Mentor |
| Community SANS Columbia SEC401 | Columbia, MD | Sep 18, 2017 - Sep 23, 2017 | Community SANS |
| Community SANS Dallas SEC401 | Dallas, TX | Sep 18, 2017 - Sep 23, 2017 | Community SANS |
| Community SANS New York SEC401 | New York, NY | Sep 25, 2017 - Sep 30, 2017 | Community SANS |
| Rocky Mountain Fall 2017 | Denver, CO | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS London September 2017 | London, United Kingdom | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS Baltimore Fall 2017 | Baltimore, MD | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS Copenhagen 2017 | Copenhagen, Denmark | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| Community SANS Boise SEC401 | Boise, ID | Sep 25, 2017 - Sep 30, 2017 | Community SANS |
| Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style | Baltimore, MD | Sep 25, 2017 - Sep 30, 2017 | vLive |
| SANS DFIR Prague 2017 | Prague, Czech Republic | Oct 02, 2017 - Oct 08, 2017 | Live Event |
| Community SANS Charleston SEC401 | Charleston, SC | Oct 02, 2017 - Oct 07, 2017 | Community SANS |
| Community SANS Sacramento SEC401 | Sacramento, CA | Oct 02, 2017 - Oct 07, 2017 | Community SANS |
| Mentor Session - SEC401 | Arlington, VA | Oct 04, 2017 - Nov 15, 2017 | Mentor |
| SANS Phoenix-Mesa 2017 | Mesa, AZ | Oct 09, 2017 - Oct 14, 2017 | Live Event |