

Computer Forensics:  
Breaking down the 1's and 0's of  
cyber activity for potential evidence.

Joseph Coward  
Spring 2009

## **Abstract**

This paper will take an informative look at Computer Forensics. It will discuss the impact Computer Forensics has on the legal aspects of today's crimes. This paper will explain how digital evidence is collected, handled, preserved, and analyzed. Finally, I will explain what tools are used and use real examples of computer forensics in action.

## **Keywords**

Computer Forensics, Preserving digital evidence, computer forensics tools.

Computer systems today provide the foundation of data storage for many businesses and a must have convenience for individuals. Customer records, account data, transaction records, personal identifying information, and other data rich information are available for use or to be protected from use or loss. In any case, an event that leads to the loss, theft, access (authorized or not), transmission or other use may be called into question to answer who, what, when, where, why, and how. In the mentioned situations, computer forensics comes to the light in order to search, find, and protect system logs or application logs. This is because information regarding the location of the actual data or information relating to the actual data is very valuable in various instances.

Computer Forensics, thanks to the ever increasing use and dependence on computers, is becoming a growing and valuable field. Computer Forensics refers to "the use of analytical and investigative techniques to identify, collect, examine and preserve evidence/information which is magnetically stored or encoded" [1]. There are many instances of where crimes involving a computer need to be investigated. These crimes range from child exploitation to a network breach resulting in the theft of personal data or the destruction of digital information. In today's digital world, it is important to put a real person behind the keyboard of any type of cyber event, primarily in instances of cybercrime. Computer Forensics attempts to do exactly that. "The core goals of computer forensics are fairly straightforward: the preservation, identification, extraction, documentation, and interpretation of computer data [2]." In order to do this, there are generally two types of data that are collected in computer forensics. *Persistent data*, which is data stored on a local hard drive or another medium. This type of data is preserved when the computer is powered off. There is also *volatile data*, which is any data stored in memory, or exists in transit. This refers to data that is lost when the computer loses power or is turned off. This type of data resides in cache and RAM [3]. Depending on the nature of the crime, skill or knowledge the cybercriminal has relating to computers or origin of the cyber event, the digital evidence remaining as proof of the event may be limited. Also, what little evidence that is recovered, or could be recovered, becomes a vital part of the legal proceedings that could follow.

According to a guide by the US Department of Justice, any electronic data that is potential evidence is often not obvious, has the possibility to transcend borders with ease and speed, is fragile and can be easily altered, damaged, or destroyed, and is time-sensitive in most cases [4]. With such importance and fragileness placed on this information, it is easy to understand why a high level of care and accuracy is placed on the identification, preservation, extraction, documentation, and interpretation of this information. From a legal standpoint, Computer Forensics has become a cornerstone of many court cases. Even if the case does not necessarily involve a computer crime, Computer Forensics may be used to shed light onto certain details of the case. For example, if it was a murder case, or

missing person's case, a computer might be examined to create a link to other people that were talked to or to gain clues by examining what someone searched for in a search engine like Google or Yahoo. The highly televised case involving the whereabouts of a missing child Caylee Anthony is a perfect example. In this case, a child was missing and the mother became a primary suspect. During several efforts to investigate her, the mother's computer was seized and examined for relative information. In this case, the most damaging evidence came from search engine data. Topics like breaking someone's neck or how to make chloroform, a chemical that can incapacitate someone, was found as part of searches conducted on the mother's computer. This information was used to bring evidence to support reasoning for the mother to remain a suspect, and also helped in bringing charges against her, even before a body was found [5].

Generally, I would not view a blog as a valid source of information, but in this cause, the information is used only to document a well known case of Computer Forensics being used in non-computer related crimes. In cyber-related crimes, Computer Forensics is more important because, generally, there may only be digital evidence. So before you can place a person behind the cyber event, you must evaluate what evidence may be available. This evidence can be located on PCs, laptops, PDAs, cell phones, removable drives, or CD's at any location. This evidence may even be found far away from the physical cyber crime location, as is the case with Internet Service Provider data relating to transmission logs. Furthermore, skilled cyber criminals may also possess enough knowledge to cover their tracks very well. Data can be overlaid or hidden within other file types using widely available types of steganography software. It can be edited, deleted, or outright destroyed. Also, the attacker could begin using anti-forensic techniques to hide evidence of a cyber crime. They may hide folders, rename files, delete logs, or change, edit or modify file data [6] (p.77 - 85). "A rudimentary way to hide evidence in a Windows environment is changing the file extension and placing the file in a nondescript directory" [14] (p. 754). Microsoft Vista has a feature that provides AES encryption on data. This feature is called BitLocker and could mean more encrypted data making its way to computer forensic examiners. The silver lining of this is that this feature is not enabled by default, and is available on the upper versions of Vista [16]. The same way a savvy cyber criminal can cover their tracks, an unskilled cyber criminal may leave evidence for the forensic investigator. There is a misconception that when you delete a file it is gone for good if you empty your recycle bin. The reality is your computer moves the file to a new directory, in essence hiding it from you, to make it appear to have been deleted. When you empty the recycle bin, your computer makes the space occupied by that file available again. The file will remain there until the computer writes new data on that sector of the drive. This could take months for this to happen. There is commercial software, even freeware, that will recover deleted files and in some cases files that have been written over [7]. To put it in another way, imagine the data you wish to delete was a book. When you delete the data, associate that with ripping the cover off the book and placing it back on the shelf. The

book would remain on the shelf until that space is used by books with covers. This is why many organizations have a procedure to fill a hard drive with arbitrary data several times before formatting it for discard. This is done to protect the sensitive data from being recovered by unintended people. All of this makes Computer Forensics a difficult task. In extreme cases, data needs to be recovered from hard drives submerged in water, computers shot with guns, or computers burned in incinerating fires, or CD's shattered into several pieces. It all is done through Computer Forensics. Not only must it be recovered, it must be handled, analyzed, processed, and documented in a manner to be used and upheld in a court of law. To be able to use evidence from a computer in court, the evidence must be authenticated or be able to prove that the information presented as evidence came from the suspect(s) computer and that it has not been altered in any way [7]. It must be collected and processed, just as a drop of blood or discarded weapon used in the committing of a crime. If not, doubt could loom over the accuracy of the evidence and there is not much of a case against a criminal. For the remainder of this paper, I will focus more on Computer Forensics used as a part of computer crime and not other types of crimes when it has been used in the past.

In 2003, a survey conducted by the FBI indicated that "the average bank robbery netted \$6,900, whereas the average computer crime netted \$900,000" [8] (p.5). I am certain this amount has only increased in the years since that survey was conducted. The Identity Theft Resource Center claimed that the number of **publicly** reported data breaches in the United States was 446 for the year 2007. This seems like a very low number, but these are cases of **reported** instances. Many times, the actual number would not be known because people fail to notice, much less, report it [9]. The actual number of breaches could be in the millions per year. With huge amounts of rewards in financial gain or with personal data gain, it is easy to see how cyber criminals would be tempted to commit these crimes and why it is so important to bring them to justice. Once there has been a crime suspected, it is important to find appropriate evidence to first identify what crime has been committed, what the outcome of the crime was, and who is responsible for the crime. When that evidence turns out to be in a digital format or on a computer, there are processes and methods used to identify, collect and preserve that information properly in order for it to be effective in court.

First, let's focus on the idea of identifying what is potential evidence in a cyber related crime. With computer related crimes, there are various locations evidence can be. "Computer evidence [can be] represented by physical items such as chips, boards, central processing units, storage media, monitors, and printers" [10]. It can be found on site in the form of hard drives in computer or laptops, flash drives, CD's or diskettes at the scene or at another location, it can be stored on PDA's, iPods, cell phones, smartcards and other electronic devices. Computer Forensic Specialists could find useful information stored in the Cookies folder, temporary Internet Files folder, examining stored Bookmarks, or other folders on the computer.

One of the treasure troves of information can be found in a little known temp area known as file slack. File slack consists of "raw memory dumps that occur during the work session as files are closed. The data dumped from memory ends up being stored at the end of allocated files, beyond the reach or the view of the computer user" [21]. There is also valuable information that can be found on computer hardware equipment in a totally different location like the equipment of an ISP or within equipment at another business or home. The Stored Wire and Electronic Communication Transactional Records Act of 1996, requires Internet Service Providers to keep logs on user's Internet request activities for 90 days [11]. Furthermore, there is a push by lawmakers now, to extend this to Wi-Fi networks as well [12]. Once potential evidence has been found, it must be collected. Even your favorite search engine companies like Google or Yahoo, have some method of tracking who runs searches and what they search for and since IP Addresses are unique identifiers, tracing crime related searches is not a far-fetched idea.

Collecting information/evidence from computer media is similar and different, at the same time, as other physical evidence collection. First, it must be collected and handled in a manner not to damage it. Secondly, it is important to document every aspect of the evaluation and processing of the computer. Not only do you document the evidence found, but you document all of the software and versions used in the extraction of the evidence. The more documentation you have on the processes and methods used that leads up to the evidence that is found makes it creditable in court. This process is known as chain of custody, and it is a vital part of computer forensics and the legal system [13] (p.373-374). Many times, a computer forensic investigator has to make a difficult decision. Do they risk losing vital evidence by pulling the plug on a computer, or risk damaging it by attempting to collect data on a live computer? If they chose to work with the live system, it is important that the system activity and contents are captured. This means checking CPU activity and system memory, evaluate the active processes that are running at the time, documenting network connections, and evaluating open files. On the other hand, if the system is analyzed while the power is off, a more representative backup can be made, because the normal boot process changes to drive media, makes changes to files or temporary file information. This forensic backup differs from a normal backup, because this will image the entire drive[14] (p.748-751). There are many computer forensic tools on the market which will assist in collecting digital evidence. Tools like EnCase, Forensic Toolkit, and SleuthKit. EnCase can search a pc for Word documents that are password encrypted, extract Windows registry information, or recognize file types by their internal structures rather than by the file type extension [17] (p.59-62). Forensic Toolkit is one of the more powerful tools available. Not only can it analyze registry entries, decrypt files, and crack passwords using dictionary attacks. One of the more promising features is the ability to identify steganography [18]. The main concern with this powerful product is the potential use in negative ways, by hackers or

other attackers. After all, this is a powerful decryption/password cracker tool. SleuthKit is an open source tool that focuses more on Unix computers, but it can show files, examine disk layouts and locate and extract partitions; even deleted ones [19]. After the task of collecting information/information, the real challenge is preserving it. One of the more promising freeware software options that can recover deleted files or partions is called Recover My Files. It is free to try and \$69.99 to buy. It can even recover files lost in a computer format [20]. I was skeptical of this claim, but I was able to verify this after running it on my own computer. The software was able to find several virtual machines that I had created and deleted to test various Desktop and Server Operating Systems for other classes. Furthermore the software was able to recover the whole deleted virtual machines, as well as other files dating back eight months. This surprised me, considering when you delete a virtual machine file; the file is too large for the recycle bin and is lost beyond recovery. I assumed those files too large for the recycle bin were not kept in a temporary location, like other deleted files.

Preserving the information in the original state is the most important aspect of Computer Forensics. Some of the steps to preserving digital information as evidence include the following items: Evaluate the risk of turning off the computer system. There is potential useful information that is stored in memory (RAM) and will be lost. Disconnect the system from the network, because if it stays connected, an individual could cover his/her tracks by deleting log files and other data that could be used as evidence. This could cause issues if the computer is a vital part of day-to-day operations, like a server for example. Do not use the system in question to do anything. You could inadvertently overwrite valuable data. In some cases, the cyber criminal might have planted a program that will erase data when triggered by some event (such as opening or closing a program). The issue is further clouded because digital information is easily manipulated. For instance, just opening a file changes the date and time stamp of a file. This can be exploited by a trained law professional to raise doubts about the validity of the evidence collecting process or the evidence itself [15]. It is my opinion that if trials for which computer related evidence was admitted, it would be easy to raise doubt in a jurors mind about the authenticity of the evidence, because the average person is weak at understanding technology and may be easily convinced to doubt the evidence.

With technology overtaking the face of businesses or personal life, it is time IT Professionals understand the importance of the data they contain. In the event of any cyber related crime, or potential crime, it is important to understand who, what, when, where, why, and how of the situation. Once that happens, you begin to realize that all those answers could be contained in a digital format located within the hardware and software of a computer system or network. If you are apart of a business and suspect some cyber crime has been committed against your organization, there needs to be a plan that has been tested and is in place. It needs to have procedures on

who you should contact, how you should proceed until a trained forensic examiner can arrive, how your consumers must be notified and what you should or should not do regarding the affected system or device, keeping in mind that these systems or devices contain the evidence of the wrongdoing. This evidence is very sensitive and exploitable, so it must be handled with the same care and precision needed to preserve the frailest object. The first instinct may be to pull the plug or something else, but that might destroy all the evidence. Furthermore, as we become more and more dependent upon computers, the stakes become higher for cyber criminals to free themselves of the tell-tell information left behind during their crimes or acts of illegal activity.

## Works Cited

- [1] Computer Forensics World. "Computer Forensics Basics: Frequently Asked Questions". (Online) Retrieved April 3rd, 2009, from <http://www.computerforensicsworld.com/>
- \*[2] Dixon, Phillip D. "An overview of computer forensics". 2005 Potentials, IEEE. Volume 24 Issue 5. IEEE International.
- [3] United States Computer Emergency Readiness Team. "Computer Forensics". (Online) Retrieved April 3rd, 2009, from [http://www.us-cert.gov/reading\\_room/forensics.pdf](http://www.us-cert.gov/reading_room/forensics.pdf)
- [4] United States Department of Justice. "Crime Scene Investigation: A Guide for First Responders". (Online) Retrieved April 2nd, 2009, from <http://www.ncjrs.gov/pdffiles1/nij/187736.pdf>
- [5] CNN News. "Caylee Blog". (Online) Retrieved April 2nd, 2009, from [http://www.cnn.com/2008/CRIME/09/08/NGfindcayleeblog/index.html?i\\_ref=newssearch](http://www.cnn.com/2008/CRIME/09/08/NGfindcayleeblog/index.html?i_ref=newssearch)
- [6] Marcella Jr., Albert J. *Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes*". 2008. Taylor & Francis Group, LLC. Auerbach Publications.
- [7] How Stuff Works. "How Computer Forensics Work". (Online) Retrieved April 5th, 2009, from <http://computer.howstuffworks.com/computer-forensic4.htm>
- [8] Vacca, John. *Computer Crime Scene Investigation: Second Edition*". 2005. Cengage Learning. Charles River Media, Inc.
- [9] Information Week. "Data Breaches: Getting Worse Or Better?" (Online) Retrieved April 4th, 2009, from <http://www.informationweek.com/news/global-cio/showArticle.jhtml?articleID=205207382>
- \*[10] Federal Bureau of Investigation. "Forensic Science Communications". Volume 2 Number 4. (Online) Retrieved April 3rd, 2009, from <http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm>
- [11] US Department of Justice. "Stored Wire and Electronic Communication Transactional Records Access" (Online) Retrieved April 4th, 2009, from [http://www.usdoj.gov/criminal/cybercrime/ECPA2701\\_2712.htm](http://www.usdoj.gov/criminal/cybercrime/ECPA2701_2712.htm)

- [12] CNN News. "Bill proposes ISPs, Wi-Fi keep logs for police". (Online) Retrieved April 5th, 2009, from <http://www.cnn.com/2009/TECH/02/20/internet.records.bill/index.html>
- [13] McQuade, Samuel C. "*Understanding and Managing Cybercrime*". (2006). Pearson Education, Inc.
- [14] Bragg, Roberta Rhodes-Ousley, Mark and Strassberg, Keith. "*Network Security: The Complete Reference*". (2004). McGraw-Hill.
- [15] TechGenix. "Bill Preserving Digital Evidence to Bring Hackers and Attackers to Justice". (Online) Retrieved April 12th, 2009, from <http://www.windowsecurity.com/articles/Preserving-Digital-Evidence.html>
- \*[16] Hayes, Darren R and Qureshi, Shareq. "A Framework for Computer Forensics Investigations Involving Microsoft Vista". 2008. Systems, Applications and Technology Conference, 2008 IEEE Long Island.
- \*[17] Allen, William H. "Computer Forensics". 2005. Security & Privacy, IEEE. Volume 3, Issue 4.
- [18] Access Data. "Forensic Toolkit". (Online) Retrieved April 13th, 2009, from <http://www.accessdata.com/forensictoolkit.html>
- [19] Sleuthkit.orf. "The Sleuth Kit". (Online) Retrieved April 13th, 2009, [from http://www.sleuthkit.org/sleuthkit/desc.php](http://www.sleuthkit.org/sleuthkit/desc.php)
- [20] Get Data Software. "Recover My Files". (Online) Retrieved April 13th, 2009, <http://www.recovermyfiles.com/>
- [21] New Technologies, Inc. "Computer Evidence Processing Steps". (Online) Retrieved April 13th, 2009, <http://www.forensics-intl.com/evidguid.html>