# Issues in Computer Forensics

Sonia Bui
Michelle Enyeart
Jenghuei Luong

COEN 150
Dr. Holliday
May 22, 2003

## Abstract

Computer forensics is a new and fast growing field that involves carefully collecting and examining electronic evidence that not only assesses the damage to a computer as a result of an electronic attack, but also to recover lost information from such a system to prosecute a criminal. With the growing importance of computer security today and the seriousness of cyber crime, it is important for computer professionals to understand the technology that is used in computer forensics.

This paper seeks to provide basic information regarding the fundamental technologies used in computer forensics. Topics covered include the recovery of deleted data, basic response to an intruder on a system, technology of key logging software and devices, and the legal and ethical aspects of computer forensics.

This paper does not seek to replace the extensive resources available on these subjects but serves as a survey of the area and an introduction into the vast and complicated area known as computer forensics.


## Introduction

Computer forensics involves the preservation, identification, extraction, documentation and interpretation of computer data.[1]

The three main steps in any computer forensic investigation are acquiring, authenticating, and analyzing of the data. Acquiring the data mainly involves creating a bit-by-bit copy of the hard drive. Authentication is the ensuring that the copy used to perform the investigation is an exact replica of the contents of the original hard drive by comparing the checksums of the copy and the original. Analysis of the data is the most

important part of the investigation since this is where incriminating evidence may be found.

Part of the analysis process is spent in the recovery of deleted files. The job of the investigator is to know where to find the remnants of these files and interpret the results. Any file data and file attributes found may yield valuable clues. Investigation of Windows and Unix systems are similar in some ways, but the forensic analyst can tailor the investigation to one or the other since each operating system is different in unique ways. If deleted data could not be recovered through the use of common forensic tools, more sensitive instruments can be used to extract the data, but this is rarely done because of the high cost of the instruments.

Data recovery is only one aspect of the forensics investigation. Tracking the hacking activities within a compromised system is also important. With any system that is connected to the Internet, hacker attacks are as certain as death and taxes. Although it is impossible to completely defend against all attacks, as soon as a hacker successfully breaks into a computer system the hacker begins to leave a trail of clues and evidence that can be used to piece together what has been done and sometimes can even be used to follow a hacker home. Computer forensics can be employed on a compromised system to find out exactly how a hacker got into the system, which parts of the system were damaged or modified. However, system administrators must first be educated in the procedures and methods of forensic investigation if a system is to be recovered and protected. With the help of computer forensics, administrators are able to learn about mistakes made in the past and help prevent incidents from occurring in the future.

Each time any kind of input is fed into the computer, whether it is a key pressed on your keyboard, or a click on the mouse, a signal is generated and sent to the appropriate computer application and they can be intercepted in your computer via a software program that is running in the background or physically from some external device. [2] Keystroke loggers are made specifically for this purpose and can be employed by a network administrator to ensure employees are not misusing the company resources; or they can be used by hackers to steal passwords, social security numbers, and any other sensitive information entered by an unsuspecting person.

Because of the wealth of information that can be gained from a computer forensics investigation, ethical considerations should be examined. Computer forensics is essentially a means for gathering electronic evidence during an investigation. In order to use this information to prosecute a criminal act and to avoid suppression during trial, evidence must be collected carefully and legally. It is particularly important to be aware of the privacy rights of suspects, victims and uninvolved third parties. An investigator needs to have knowledge of several laws and statutes that govern electronic evidence collection including the fourth amendment of the constitution, 18 U.S.C. §2510-22, also known as the wiretap statute, the Electronic Communications Privacy Act (ECPA), and the USA PATRIOT Act. Each of these items affects the legality of electronic evidence and the appropriate procedures to acquire that evidence.

## General Steps in a Forensic Investigation

The three main steps to a forensic investigation are the acquisition of the evidence, the authentication of the recovered evidence, and the analysis of the evidence.[3]

Although each forensic investigator may add their own steps in the forensics process, these three steps (acquisition, authentication, and analysis) are essential to any forensic investigation.

Acquiring evidence in a computer forensics investigation primarily involves gaining the contents of the suspect's hard drive. But other aspects may be involved in the acquisition of evidence. Photographs of the computer screen and the entire computer system in its installed configuration may yield useful information to the investigator. In addition, some forensic investigators believe in gathering evidence before shutting down the suspect's computer; this is a source of arguments within the forensics community - whether to shutdown the computer immediately and preserve the exact state that it was found, or to gather evidence before shutting down in order to gain any volatile data that might be destroyed on shutdown (like the running processes on the computer).[4]

Ideally, the forensic analysis is not done directly on the suspect's computer but on a copy instead. This is done to prevent tampering and alteration of the suspect's data on the hard drive. The contents of the hard drive are copied on one or more hard drives that the investigator will use to conduct the investigation. These copies, or images, are obtained by coping bit by bit from the suspect's hard drive to another hard drive or disk. The hard drive containing the image of the suspect's hard drive obtained in this manner is called a bit-stream backup. The reason why hard drives must be copied bit by bit is because doing so ensures that all the contents of the hard drive will be copied to the other. Otherwise, unallocated data (such as deleted files), swap space, "bad" sectors, and slack space will not be copied. A goldmine of evidence may be potentially held in these unusual spaces on the hard drive.[5] Of course, the investigator must make sure that the

hard drive or disk used to hold the copy is completely free of any data so that the evidence will not be tainted. The commonly used forensics tools for the imaging of hard drives are Safeback and Encase, which also performs many other forensics functions. There are also disk-wiping tools to clean the image hard drive.

The authentication of the evidence is the process of ensuring that the evidence has not been altered during the acquisition process. In other words, authentication shows that the no changes to the evidence occurred during the course of the investigation. Any changes to the evidence will render the evidence inadmissible in a court. Investigators authenticate the hard drive evidence by generating a checksum of the contents of the hard drive. This checksum is like an electronic fingerprint in that it is almost impossible for two hard drives with different data to have the same checksum. By showing that the checksums of the seized hard drive and the image are identical, the investigators can show that they analyzed an unaltered copy of the original hard drive. The algorithms most commonly used to generate these checksums are MD5 and SHA. Some tools to generate checksums use a combination of algorithms such as CRC (cyclic redundancy check) with MD5 in order to ensure a higher quality of authentication.[6]

The last and most time-consuming step in a forensics investigation is the analysis of the evidence. It is in the analysis phase that evidence of wrongdoing is uncovered the investigator. Because of the differences between Windows-based operating systems and UNIX, I will discuss the analysis of the data on these two systems in separate sections. In general, forensic investigators rely on special forensics tools to analyze the huge amounts of data on the hard drive (the size of hard drives continues to get larger and

larger). These range from a hex editor (a text editor that views the data in hexadecimal format) to full-blown forensic toolkits like Encase.

It is important that the chain of custody is maintained throughout the investigation. The chain documents everything that happens to the evidence: who handled it, where and how it was handled, and how it was stored. It preserves the integrity of the evidence. Even if the suspect was guilty, if the chain is not maintained, a lawyer can argue that the chain of custody was not properly established, casting doubt on the damning evidence acquired during the analysis phase.

## Forensic Analysis on Windows systems

Despite the unreliability and propensity to crash, Windows remains the most widely used operating system in people's computers. Investigators must be familiar with how Windows work and the idiosyncrasies associated with Windows in order to conduct a thorough and fruitful investigation.

An intimate knowledge of file allocation and deletion in Windows file systems is needed to recover deleted files. For this paper, I will be focusing on NTFS, the file system used in Windows NT and Windows 2000 and above. But many of the techniques mentioned in this section could be used in earlier versions of Windows with few, if any, modifications.

NTFS stores attributes of files and folders in a system file called the Master File Table or MFT. The attributes in the MFT of most interest to the forensic analyst are the filename, MAC times (the date and time of a file's last modification, last access, and creation), and the data (if the file is small enough) or the location of the data on the disk.

With folders, additional attributes of interest are the index entries in the MFT of the files for that folder or, if the MFT cannot hold the entire folder's entries, the location of these entries in an index buffer (an allocated space outside the MFT to hold these index entries).[7]

NTFS writes data to the disk in whole chunks called clusters. The size of the cluster varies depending on the size of the disk partition and the Windows version. NTFS uses another system file $BITMAP to keep track of what clusters have been allocated on the disk. In the $BITMAP file, a single bit is used to indicate to if the cluster has been allocated or not.

So when a file is allocated the bit for the assigned cluster of that file must be set in the $BITFILE file, a record must created in the MFT, an index entry must be created in the folder's MFT record or index buffer, and addresses of any clusters used to hold file information must be added to the MFT record.

When a file is deleted the bit of the clusters of that file is set to zero in the $BITMAP file, the MFT record is marked for deletion and the index entry is deleted (by moving up the entries below it and thus, overwriting it). However, if the index entry is the last one for that folder, the entry remains visible and thus the attributes are recoverable; useful evidence like file access times can be found. NTFS overwrites the MFT records marked for deletion when creating a new record in the MFT. If no new records have been created in the MFT, the records marked for deletion are not overwritten and useful file attributes and possibly data (if it fit in the record) can be recovered as well.[8]

But it is possible to recover deleted files even after its record is overwritten in the MFT and index entry of its parent folder. If the file data was large enough, the data would have resided in some clusters on the disk instead of the MFT itself. Clusters holding data of deleted files compose part of the unallocated space on the disk, so a simple listing of the file directory's contents will not show the deleted files. Because the forensic analyst has all the contents of the suspect's hard drive, the analyst could search for a deleted file's contents on the disk using a hex editor or other forensic tools. Unallocated space is a huge source of information for analysts because deleted file data residing there may not have been overwritten yet. Unallocated space also contains contents of the index buffers of deleted folder entries.

Moving and renaming a file creates entries in the MFT that have the same MAC times, starting clusters and file sizes. Forensic analysts can examine the record allocated renamed file in the MFT with the deleted file in the unallocated space to compare if they are indeed the same. If they are the same, this can establish proof that a suspect had knowledge of the file's existence since the suspect moved it (if only the suspect had access to the computer). MAC times also can help prove the suspect's knowledge of a file and its contents as they show the time it was created, last modified, and last accessed. For example, if the file was last accessed at a time much later than the creation time, the investigator could show that the suspect knowingly used the file, as shown in a court case involving child pornography in which the defendant had claimed he simply downloaded files of unknown content and forwarded them to others without viewing them. The forensic investigator had evidence of the MAC times of the files in question and that

many of the files had access times far later than the creation times. The defendant pled guilty as a result.[9]

Analysts can also inspect the contents of the Recycle Bin that holds files that are deleted by the user. When a file is deleted it is moved to the Recycle Bin where a record is created in a system file of the Recycle Bin (named INFO) for that particular file. The entry contains useful information for the analyst such as the file's location before it was deleted, the file's original name and path, and the date of the deletion. These pieces of information can show that the suspect did create and knew the location of a file and knowingly deleted it. When the user empties the Recycle Bin, Windows deletes the entries in the INFO file. If it is not completely overwritten, the deleted INFO file entry can still be examined.[10]

As stated before, deleted file data and attributes may reside in the unallocated space. Another area of the disk that may hold deleted file attributes is the file slack. File slack refers to the space between the end of a file and the cluster it resides in. It is often the case that a file does not fit into an exact multiple of clusters. So the space remaining is called file slack and it may contain data from previously deleted files.[11] For the forensic analyst, a bigger cluster means more file slack to examine, and thus are of more value. In addition data may be found in the swap space. If the RAM is full, the OS writes some of the data to a special place on the disk called the swap space. This is the concept behind virtual memory. The swap space may contain the remnants of these deleted files if they were deleted very recently.

Shortcut files in Windows provide analysts with another source of information about files. Shortcut files contain MAC time of the files that they refer to and the full

paths to the referred files.[12] Remnants of deleted shortcut files, like other files, can be searched in the unallocated space, slack space, and swap space of the disk.

Investigators can also examine the Internet files that are cached by Internet Explorer. These files are named Index.DAT and they contain the URL, date last modified by the server and the date last accessed by the user.[13] These caches may be deleted by the user but again, like deleted files and shortcuts, these deleted cached files may be recovered in the spaces of the disk mentioned above.

When a file is printed, temporary files containing the data to be printed are created by the system. These temporary files are used to spool print jobs in order for the application program to continue to be interactive with the user. The temporary files include the data itself and the full path, potentially useful to the forensic examiner. When the printing job is finished, these temporary files are deleted and may be recovered in unallocated space or the swap file.[14]

The forensic analyst may look at Windows registry to find information about hardware and software used. The registry contains the configuration information for the hardware and software and may also contain information about recently used programs and files.[15] Proof that a suspect had installed a program or application may be found in the registry.

Another source to recover files and find evidence is the NTFS $LOGFILE. The $LOGFILE records all transactions done on the NTFS. The $LOGFILE is used to restore the NTFS if (or more appropriately, when) the system crashes. The NTFS is then able to undo or redo transactions. The $LOGFILE may contain index entries for folders, a copy of a MFT record (including MAC times), index buffers, and other potentially useful

information that the examiner can use. For example, evidence of a filename may only exist in the $LOGFILE and nowhere else (if it had been overwritten).[16]

Windows systems give the forensic analyst plenty of sources of useful information. The places mentioned in this paper are just some of the areas that the investigator can search for evidence against the suspect.

## Forensic Analysis on Unix systems

Conducting an investigation on Unix systems is very similar to conducting one on Windows systems. The forensic analyst must understand how Unix allocates and deletes files in order to know where to look for the contents and attributes of files that exist (and potentially hidden) and are deleted. But the idiosyncrasies of Unix provide the investigator with different approaches to analyzing the data on Unix systems versus Windows systems.

Unix and Windows view files very differently. Unix uses the concept of inodes (index nodes) to represent files. Each inode contains the pointers to the actual data on the disk as well as file attributes useful to the investigator; these include the owner ID, access permissions (read, write, execute), the number of links (number of directories referencing the file), the MAC times which are the last modification, access, and change of status (change of owner, permission or number of links), and file size. Note that the filename is not included with the inode. Instead the file name is stored as an entry in the directory structure along with the location of the actual inode. [17]

Like the NTFS on a Windows system, the Unix file system allocates data in fixed-sized pieces called blocks. This is analogous to the clusters used by the NTFS.

Therefore, file slack, the space between the end of a file and the end of the cluster, is also found on Unix systems as well as Windows systems because not all files fit exactly into the blocks on the disk. Forensic analysts can examine the file slack for remnants of deleted files and attributes.

File deletion in Unix involves marking the directory entry for that file name to marked as unused, resulting in the disconnection of the file name with the actual file data and attributes. The inode of the file is marked as unused and some but not all of attribute information is lost. The file data blocks are marked as unused. According to the creators of the Unix forensics toolkit, The Coroners Toolkit (TCT), the deleted file data and attributes remain for long periods of time such as hundreds of days for heavily used systems because Unix has good file system locality – files tend to be clustered together instead of randomly space apart. Unix file systems avoid fragmentation as much as possible to achieve this locality, allowing deleted files and attributes to remain much longer on the disk since chances are slim that the new files to be written to the disk are the same size as these deleted files.[18]

So, deleted files may be easier to recover on Unix systems than on Windows. The Coroner's Toolkit is widely used to examine Unix systems and contains many useful utilities for forensic analysts. One such tool is the unrm, a tool that "undeletes" files. Deleted file attributes can be recovered using the ils tool in the TCT. Remember that file attributes are very important to investigators, especially the MAC times. Even TCT includes a tool called mactime that neatly displays the MAC times of a file.[19]

Everything in Unix is a file. So any transactions done within Unix will leave evidence of that the transaction occurred because the MAC times for the associated files

will be altered. Analysts can examine the MAC times of files in Unix like the MAC times of files in Windows to show that the suspect had knowledge of the existence and contents of a file. However, skilled hackers can alter the MAC times to hide their tracks within the file system since inode information is stored in the file system. So investigators should not completely trust the MAC times of files.

Unix tools can be used to examine the contents of the hard drive. Commonly used commands include find, grep, and strings. Analysts can use these tools to form keywords to search for a specific piece of data like an email or pornography. The TCT includes a tool called lazarus that attempts to classify the blocks of data as text files or binaries. With text files, lazarus checks for the keywords that the analyst has requested in the form of regular expressions.[20]

Places on the hard drive that the analyst could look for remnants of files are nearly the same as those on Windows systems. In addition to the file slack mentioned earlier, investigators can search through the Unix swap file (similar to the Windows swap file), and of course, the unallocated space occupied by unused and deleted files. In addition, for each user in Unix there is a directory named /tmp that holds temporary application files. This is similar to the situation in Windows with temporary application files being created; the contents of these temporary files may still exist in the /tmp directory at the time of the investigation and may be used as evidence against the suspect.[21]

Unix gives the users the ability to repeat commands used in previous sessions. In order to do this, the commands are saved in a shell history file. Thus the shell history file can be examined to trace the steps of a hacker or to show that the suspect knowingly

created, modified, accessed, and/or deleted a specific file. However, a user (or hacker) can clean out the shell history file to cover his tracks.[22] So, the shell history file can be useful only some of the time, especially if no attempt has been made at modifying it.

Forensic analysis of a Unix system shares some characteristics with that of a Windows system. The search for deleted data involves looking in the same kinds of spaces like the unallocated space, file slack, and swap space. But investigation of Unix systems can involve the use of Unix tools that help in the search for certain patterns among the contents of the disk. In addition, Unix forensics toolkits such as The Coroner's Toolkit enormously aid in the examination of Unix systems.

## Obtaining Magnetic Residue Data

Data overwritten on the hard disk may seem to be unrecoverable. Using the forensic techniques outlined above will not enable the investigator to retrieve data from deleted files that have been overwritten.

However, the hard disk is a physical device. It consists of a stack of disks covered in magnetic material that stores the pattern of 1's and 0's that make up the data. A read/write head hovers above it to read or write data to a track, one of the concentric rings on the disk.

But when a track is overwritten with new data, traces of the old data remain underneath. This is due to the "inability of the writing device to write in the exactly the same location each time, and partially due to the variations in [magnetic] media sensitivity and filed strength over time and among devices." [23]

Specialized equipment is needed to recover some of the overwritten layers through the use of magnetic force microscopy (MFM). MFM creates patterns of the magnetic data on the disk. Thus, any traces of old data will appear on the image of the patterns. The number of layers that can be read depends on the sensitivity of the instrument used to perform the MFM. But it is generally known that these machines can read the first two layers quite easily.[24]

This kind of data recovery at the physical level is rarely done. The machines are very expensive to manufacture and only certain government agencies actually possess them.

## Dealing with an Intrusion

Once a system has been compromised, actions must be taken immediately to ensure that a record of the state of the system is accurately recorded before it is accidentally modified. The first thing is to create an exact copy of the system's entire file contents. Many administrators respond to an intrusion by restarting the compromised system and rebooting the system and restoring from backups. However, this is not the ideal course of action; not only do they neglect the fact that the attack can happen again, but they lose valuable evidence that can be used to trace the attacker. To ensure that the evidence is preserved, a copy of the file system must be made immediately and without rebooting the system (as restarting the computer may change and overwrite files, inadvertently destroy some evidence). This is usually done using a binary disk imaging software that records not only existent files on the hard drive but also every single bit that is left on the system, which in effect records deleted files as well.

It is recommended that first one copy be made from the original drive and then the original should be sealed away and handled as little as possible. It is important to record exactly to whom the original drive has been entrusted to at each step, so that a future prosecution would be more successful. This first copy will now become the "original" from which other copies can be made and examined. This is done to ensure as little handling with the true original as possible. Once the original is copied and safely secured, the investigation can begin.

## Looking into the Logs

The most useful piece of evidence that can help piece together the events are the system's logs. Both UNIX and Windows are capable of logging important events and their details as they occur and they should always be turned on long before an intrusion occurs. The more logs that there are available, the clearer the picture of events will be.

One very useful kind of log is a login log, or connection log. These logs tell precisely every connection attempt that is made by recording the precise date, time, the network IP address of the computer that is attempting to log in, and the result of each login. These logs usually show the very first signs of unusual behavior, for example when an unknown address is attempting to connect to an unusual port number or when multiple unsuccessful attempts are made to login to a specific account.

If an intruder has successfully logged into the system with an account, the system can also keep a shell command history, which can show exactly what each user typed into the shell at what time. This is very useful in trying to figure out what the hacker was trying to do with the system (e.g. which files he/she accessed or modified), but

unfortunately, shell command histories cannot record individual commands executed within a script.

Process accounting logs are very useful for revealing the activities of the intruder by showing exactly which files were executed, when, by whom and for how long. These logs are quite detailed and sometimes very useful. However, reading these logs are difficult because they are sorted in order of when the processes were terminated, so processes that ran longer than others may go unnoticed and those are still running will not be listed.

A hacker may have left a process running and it can be analyzed by first halting the process without killing it, as terminating the process may discard important information as to the plans of the attacker. The process' symbol table and core stack can then be extracted and examined with a debugger.

With these system logs, in addition to any IDS or Firewall logs, a system administrator can piece together a fairly good picture of what the hacker did and is intending to do with the system in the future. From there, an administrator can start repairing the damage and attempt to plug up the holes that allowed the intruder to invade the system.

## Repairing the System

In addition to leaving lots of evidence, hackers often leave numerous amounts of programs and data on the victim's system, usually as a branching off point to attack other systems. These files are generally called "remnant files"[25] and can include anything from

exploit scripts to key logging programs to Trojan horses meant for further damage after a clean-up.

Hackers often replace common executable files on systems such as *ls*, *telnet*, and *find* with their own modified versions that have harmful side-effects, so it is important that system administrators backup their systems often and regularly perform cryptographic checksums such as Message Digest 5 (MD5) or Secure Hash Algorithm -1 (SHA-1) on the file systems. In the event of an incident, files can be compared against the checksums to determine whether or not they have been tampered with.[26] Checksums should also be performed on all system configuration files as modifying those are also part of the hacker's Modus Operandi.

Hackers also tend to hide files on a victimize system by deleting them, by placing them in obscure locations, or by giving them unusual names that are not easily found. A hacker's deleted files can be found and recovered using appropriate utilities that are available on the Internet. Sometimes hackers prefix hidden filenames with two or more periods so that the *ls* command does not list them normally. They can hide fragments of data of unused blocks left from internal fragmentation of files scattered throughout the file system. They can also sometimes insert data inside code or data segments of regular executable files and are undetected because those blocks are never accessed by the executables. A clever hacker can even hide information inside comments of executables and images on UNIX systems.[27] All of these hiding methods can be handled with the correct tools and the correct techniques.

## Tracking the Hacker

After examining the logs and a reasonable interpretation of the hacker's activities has been reached, a next possible step is to trace down the hacker himself. Unfortunately, this is rarely an easy task. The system logs are the only key to find out who is responsible for the attack. When an attacker invades a system, they often modify or delete logs that can be used to trace him, so it is good practice to set up your system so that logs are written to an offline file system as to prevent the hacker from accessing them. A similar practice should be adopted for the cryptographic checksums of system executables and system configurations. This will ensure that the system can be recovered successfully and perhaps even catch the person responsible.

Network router logs can also be useful in finding a hacker as they record information about packets that pass through. If a general time frame for the attack can be determined, then it will be much easier to find relevant information on network logs. Once an IP address is determined to be the source of the attacks, a simple *traceroute* can find the system.

However, this system is likely to be simply another victimized system that the hacker has used, so this entire process must be repeated for that system and any other systems along the way until the hacker is ultimately found. Unfortunately, this is difficult because there are many barriers that prevent us from finding the perpetrator. If any compromised system along the way did not keep adequate logs, then the trail grows cold very fast. If the ISP of the hacker is uncooperative then tracing becomes difficult as well. Most difficult of all, if one of the compromised systems lies across international borders then things get a lot more complicated.

It is because of these and other complications that can bring the hunt to a screeching halt. The best that can be done is to do the best we can to restore the services, learn from past mistakes, consistently update system security patches and to stay vigilant.

## Keystroke Loggers

Keystroke loggers run primarily in the background of a computer and many run in "stealth" mode, meaning they are not listed in process lists and hide the registry modifications it makes to system settings. Once each key is intercepted, the information may be stored somewhere on the computer (or a remote computer) to be accessed later or streamed, in real-time, over the network to the person who started the logging program.

Keystroke loggers have become more advanced and now are capable of features such as notification for the logger's initiator when specific behavior or content is encountered and can even record screenshots of anything that is displayed on the monitor at any particular event or at regular time intervals, allowing key loggers to become even more intrusive.

A key logger normally consists of two parts: a Dynamic-Link Library (DLL) file that performs the logging, and an executable (EXE) file that loads the DLL and sets the hook onto the keyboard[28]. A hook is defined as any mechanism that uses a function to intercept events before they can reach an application. The function can then change, manipulate, or discard (keyboard) events in any way before allowing them through to the destination application. Hooks come in two flavors: system-wide and thread-specific; key loggers use system-wide hooks. DLLs are files that contain functions (as well as other information) that can be linked to any application at run-time. When this is done, the

functions in a DLL are attached to processes themselves and are mapped into the process's address space, allowing them to be called from the process. DLLs are used for keyboard hooks because any application can then call the keystroke logging function in the DLL and enables recording of all keystrokes from all applications[29].

## Finding the Spy

Keystroke logging programs can be installed either in person who has physical access to the target computer, or remotely, either by a "Trojan horse" application or by a hacker who has gained root access to a system. Once loaded, the keystroke logging software is virtually undetectable by the user. Key loggers normally use little memory and do not affect a computer's performance, making it more difficult to detect. However, there are anti-snooping products available that claim to be able to find such key loggers by probing the resident memory and recognize the programs that exhibit devious behavior. Products, like one called KeyPatrol[30], use behavior-detecting and pattern-matching algorithms. Once a particular application has "hooked" the keyboard, the application can be easily found by detecting a procedure call to the keystroke logging function. Products also can search through resident memory and match applications against numerous known key logging programs; much like anti-virus software searches a computer for programs matching known viruses.

## A Physical Alternative

Another way that keystrokes can be monitored is by a physical device that is connected directly to the keyboard. The most well-known of such devices is the

KeyGhost[31] key logger which is a small device that is placed on the end of the keyboard cable and is plugged into the back of the computer.

This device has many advantages over its software counterparts. It is easy to install, works with any operating system, and cannot be detected by anti-snooping software. Installing the device requires no expertise whatsoever of computers and can be done regardless of whether the computer is on or off. This device is OS independent and cannot be detected by software because it does not require any software or drivers; it simply reads the keystrokes as it is inputted into the keyboard, records the information on a flash memory embedded in the device and allows each key to pass through to the computer unchanged. The software then can record keystrokes even before the OS is loaded and stores BIOS passwords as well. The device requires no external power and causes no slow down due to use of system resources. The data that is recorded is kept in 128-bit encryption to prevent unauthorized extraction of data.

To access its stored information, a specific series of keys must be pressed on the keyboard that are highly unlikely to be pressed accidentally (much like a password). Once the correct combination is detected, the device will output a menu by sending a series of keystrokes to the computer and can be viewed with any text editor. From there, the information can be downloaded, erased, and the device's options can be changed.

They drawback of this device is that it has a finite amount of memory and can only store so many characters; depending on how much a person is willing to spend on the device, the KeyGhost device can store anywhere between 128,000 keystrokes and 2,000,000+ keystrokes. Once all the memory is filled before it is downloaded, the device will begin overwriting the oldest recorded data.

The device itself closely resembles an ordinary keyboard cable extension but anyone who checks the back of their computer will be able to notice it. This particular vendor also offers keyboards that have the KeyGhost device built into it that behave as any keyboard would, except for its logging capability, giving added secrecy to the device.

Privacy

Computer forensics investigations typically involve one of two privacy issues. The first occurs when evidence is retrieved a particular computer or electronic device. In this case, the investigating officers need to be careful to avoid charges of illegal search and seizure. In other words, they need to comply with the Fourth Amendment to the Constitution. The second issue involves evidence pertaining to Internet usage.

The Internet is usually considered an open forum that allows users the anonymity to express themselves without fear of reproach. It is important to provide the opportunity for such anonymity in order to promote free speech. Furthermore, it allows the minority voice to be heard when fear of backlash from the majority might otherwise keep it silent. However, when that anonymity is used to perpetrate a crime, such as accessing bank records or circulation of child pornography, it is no longer a matter of the minority opinion, but of tracking down and prosecuting a criminal. The dilemma lies in allowing most users to remain anonymous and maintain their privacy, while determining the identity of the few involved in illegal activities.

## The Fourth Amendment

Technology has invaded most aspects of our lives, and computers have become ubiquitous. In 2000, more than fifty-one percent of American households had a

computer[32]. Many people have access to computers, including those with criminal intentions. In some cases, computers are simply fancy storage devices for keeping records. When this is the case, examination of the computer (as previously explained) can produce valuable evidence.

In legal cases that involve seizure of a computer or other electronic device, it is important that investigators comply with the Fourth Amendment. 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 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.[33]

The amendment mandates that, in order to search a suspect's personal property, the investigating officer must first obtain a search warrant. This is true for any electronic devices found in the suspect's home, work, or that are considered personal property. Failure to do so will often result in a suppression of the evidence. In other words, evidence illegally obtained cannot be used during prosecution.

A search conducted without a warrant is not illegal if it does not violate a person's reasonable expectation of privacy. With respect to a computer, "the Fourth Amendment generally prohibits law enforcement from accessing and viewing information stored in a computer without a warrant if it would be prohibited from opening a closed container and examining its contents in the same situation."[34] Typically, a computer is protected from such search and seizure when it is under the control of the owner. However, when the device is under the control of another person, the owner has less expectation of privacy if that person is allowed to access the system. For example, the computer is temporarily

placed under the control of another person, and that computer is not password protected, then the owner does not have a reasonable expectation of privacy.

For example, in a 1998 case, a computer repairman in Texas noticed that the computer he was fixing was low on memory. He contacted the owner's wife, and with her permission, attempted to free up some space on the hard drive by removing JPG files that took up a lot of space. However, he first opened the files to make sure he was not deleting personal or important images. During this process, he discovered seventeen files containing child pornography. Without searching further, he contacted his superior who then contacted the police and the FBI. The technician "copied the seventeen images onto a floppy disk, which he gave to [the police detective], who copied them before faxing them to [the FBI agent], who seized the computer after obtaining a search warrant."[35] In this case the FBI agent, acting as a government agent, did obtain a search warrant before actually seizing the computer, thus complying with the Fourth Amendment. However, the defendant "sought to suppress the images, contending that they were seized in violation of the Fourth Amendment. He claims that the store's search went beyond the permission given by his wife, thereby invalidating any evidence that flows from the search." [36]

This case serves to illustrate two exceptions to the warrant requirement. The first is "agents may search a place or object without a warrant or even probable cause if a person with authority has voluntarily consented to the search."[37] For consent to be given by a third person, in Grimes' case, his wife,

that person must have access to the property. Typically, a spouse or significant other is considered to have access to all property in the household.

The second exception involves private searches. "The Fourth Amendment does not apply to searches conducted by private parties who are not acting as agent of the government."[38] When the person performing the search has no original intention of investigating criminal activities leading to prosecution, and that person does not work the government, then that search can be considered a private search. In the above case, the search was performed with the intent to delete files, and the incriminating evidence was accidentally discovered.

Another important exception to the warrant requirement involves information in plain view. In this case "the agent must be in a lawful position to observe and access the evidence, and its incriminating character must be immediately apparent."[39] Included in this exception is information obtained by peering over a suspect's shoulder. Additionally, when an investigator is examining a computer for evidence related to one crime, but finds evidence of another crime, it is unlawful for the detective to switch the focus of his/her search and look primarily for evidence of the second type. For example, in United States v. Carey, a detective searching for drug evidence opened a JPG containing child pornography. The detective then "spent five hours accessing and downloading several hundred 'jpg' files in a search not for evidence of the narcotics trafficking that he was authorized to seek and gather pursuant to the original warrant, but for more child pornography."[40] Only the first file, which came into plain view during another unrelated search, was admissible in court. In a very similar case, United

States v. Walser, the detective was looking for drug related records when he found child pornography. He then ceased searching and applied for a new warrant to search for more child pornography. This appears to be the proper way to deal with incriminating evidence unrelated to the current investigation.

Finally, another important exception involves work-place searches. Typically employers own the computers that the employees use, and therefore, they can search employee computers without warning. Furthermore, searches initiated by a non-government employer are considered private searches and therefore do not violate the Fourth Amendment. Additionally, the employer is considered to have access to the computers and can provide the consent required for warrant-less searches during a criminal investigation. Ideally, the employer should have a published company policy and warning banners that inform computer users of their rights. However, even policy promising user confidentiality may not protect the employee from a search.

## Privacy and the Internet

As educated users, we know that our Internet connection is not as anonymous as we might want. Typically, most users do not hide their IP address, which can usually be traced back to a specific computer, thus revealing the location of the user. Furthermore, Internet Service Providers (ISPs) often keep records that link access accounts and IP addresses to individual users. However, ISPs generally serve the public at large, and it is in their best interest to protect the rights of their customers. An investigator must go through the proper processes in order to attain a user's identity.

The problem of determining identity falls under the restrictions of the Electronic Communications Privacy Act (ECPA). The ECPA "governs law enforcement access to the contents of electronic communications stored by third-party service providers."[41] Furthermore, "whenever agents or prosecutors seek stored e-mail, account records, or subscriber information from a network service provider, they must comply with ECPA."[42] Essentially, any email or voicemail communications in storage for less than 180 days can only be accessed with a warrant. However, any communication stored for more than 180 days can be accessed with a subpoena.[43] When a subpoena is used instead of a warrant, the investigator or service provider must provide notice of the intent to view files to the user. It is important to note that the ECPA details restrictions for stored communications and account details only. Any communications that are monitored in real-time are governed by 18 U.S.C. § 2510, also known as the Pen/Trap statute or Title III.

The Pen/Trap statute authorizes devices that monitor the addresses of incoming and outgoing communications. This simple court order allows for such monitoring as tracing a computer intruder's IP address. Conversely, Title III, also known as the wiretap statute, "regulates the collection of actual content of wire and electronic communications."[44] According to Title III, "any person who intentionally intercepts … any wire, oral, or electronic communication … shall be punished" with a fine or imprisonment.[45] However, there are several exceptions to this guideline. For example, the employee of a service provider may access the communications in the normal course of business, if they are provided with a signed court order, when the intercepted message

is from an unwanted computer intruder, or with the consent of either the transmitting or receiving party.

There is some controversy surrounding the current application of the above statues. The government currently uses a tool to "intercept and collect e-mail and other electronic communications."[46] This tool is known as DCS1000, or Carnivore. According to the Deputy Assistant Attorney General in 2000, Kevin DiGregory Carnivore is "a special filtering tool that can gather information authorized by court order, and only that information" and "there are many mechanisms we have in place to prevent against possible misuse."[47]

However, privacy advocates are concerned that Carnivore can be used to do much more. According to an independent review, "incorrectly configured, Carnivore can record any traffic it monitors."[48] Additionally, some fear that it violates the Fourth Amendment: "The 4th Amendment clearly prohibits such sweeping invasions of privacy and property as Carnivore commits."[49] The primary concern here is that a warrant to use Carnivore cannot "particularly describe" the place to search and what exactly to seize as the Fourth Amendment seems to require. However, it appears that this second group of privacy advocates is not taking into consideration the allowances made in Title III and the Pen/Trap statutes. Clearly, as the technology advances, government investigators will have to be careful when collecting evidence to ensure that they are not violating any privacy rights. Future technologies will likely protect individual rights as well as gather information.

## USA PATRIOT Act

Shortly after the terrorist attacks in New York on September 11, 2001, the Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act, also known as the USA PATRIOT Act was signed into law. This act is causing controversy among many privacy advocates because it "includes Internet history … allowing the government to monitor the addresses of incoming and outgoing email as well as any websites or URLs a suspected terrorist visits" which has further impact because "the information sought merely has to be relevant for flushing out terrorists, innocent anonymous users can also be spied upon."[50] These are serious allegations that have dramatic consequences for Internet privacy. However, upon closer inspection of the changes, the act does not seem quite so sinister.

One important change made by the PATRIOT Act to Title III "includes records of session times and durations, as well as any temporarily assigned network address," which includes IP addresses, and "to obtain the means and source of payment" for a particular user. This change will make it easier to trace and identify computer criminals.[51] It is significant that this is one of a few changes that does not terminate on December 31, 2005.

There are several other changes made by the USA PATRIOT Act. For example, investigators can now treat cable companies as they would any other service provider since the cable companies often offer Internet service. Additionally, warrants and subpoenas acquired to investigate a computer crime now apply nationwide, rather than just the district that issued the warrant. This allows investigators to obtain communications sent or received from users across the country.

While it is true that the USA PATRIOT Act does give the government more freedom to invade an individual's privacy, most of those changes are set to "sunset" on December 31, 2005. Additionally, the Act primarily updates the laws to accommodate changes in technology.

Government agents investigating criminal activities are required to stay within the law, particularly the regulations of the United States Constitution and all of its amendments. However, as times change, technology advances, and criminals find new ways to perpetrate crimes, new developments and statutes are required to clarify the boundaries of legal investigation. Computer forensics is at the cutting edge of both technology and the law. Consequently, electronic evidence is a relatively new development in the courtroom, and very little case law has been established to set the precedent for future cases. As the field evolves, new cases and trials will ultimately determine how prosecutors should proceed with criminal investigations that involve electronic data.

## Summary

Many criminal investigations in today's technology rich society will involve some aspect of computer forensics discussed in this paper. Any person undertaking to investigate such a case should be familiar with the basic technologies involved in gathering the information, how to properly gather the data, and how to ensure that the information will be valid as evidence during trial. In particular, it is important to be able to acquire, authenticate and analyze data stored in electronic devices, whether they run Unix or Microsoft operating systems. Furthermore, a competent investigator should

understand the technologies involved in tracing and detecting the actions of a specific computer user. In the above pages, we have given an overview and brief introduction of each of these important aspects of computer forensics. Finally, it is important to avoid becoming a criminal by breaking the law while investigating criminal activities.

Our purpose in compiling this paper was to bring together the different perspectives of computer forensics in one place, but it is not meant to be a complete description of the field. While there is a significant amount of data contained in the previous pages, computer forensics is a vast topic, and the advice of an expert should be sought in any serious investigation. Moreover, computer forensics is a budding field that will continue to grow, especially as the laws governing legal cases evolves and computer technology becomes more ubiquitous.

## References

[1] Warren G. Kruse II and Jay G. Heiser. *Computer Forensics: Incident Response Essentials*. Addison Wesley, Boston 2001, p. 2.

[2] HowStuffWorks.com, "Workplace Surveillance." [cited May 21, 2003]. http://computer.howstuffworks.com/workplace-surveillance3.htm.

[3] Kruse and Heiser, op. cit., p. 3.

[4] "Digital Evidence Collecting & Handling," March 20, 2002. [cited May 21, 2003]. http://faculty.ncwc.edu/toconnor/495/495lect06.htm

[5] Kruse and Heiser, op. cit., p. 15.

[6] Ibid., p. 13.

[7] Bob Sheldon. "Forensic Analysis of Windows Systems," from *Handbook of Computer Crime Investigation: Forensic Tools and Technology*, ed. Eoghan Casey. Academic Press, Bath, England 2002, p. 137-139.

[8] Ibid., p. 139-140.

[9] Ibid., p. 134-137.

[10] Ibid., p. 145-152.

[11] Ibid., p. 144.

[12] Ibid., p. 152-157.

[13] Ibid., p. 158.

[14] Ibid., p. 161-163.

[15] Ibid., p. 160 –161.

[16] Ibid., p. 164-165.

[17] Kruse, op. cit., p. 214-215.

[18] Wietse Venema. "File Recovery Techniques." *Dr. Dobb's Journal,* December 2000. [cited May 21, 2003]. http://www.ddj.com/documents/s=878/ddj0012h/0012h.htm.

[19] Ibid.

[20] Dan Farmer. "Bring Out Your Dead," *Dr. Dobb's Journal,* January 2001. [cited May 21, 2003]. http://www.ddj.com/documents/s=871/ddj0101h/0101h.htm.

[21] Kruse, op. cit., p. 301.

[22] Ibid., p. 305-306.

[23] Peter Gutmann. "Secure Deletion of Data from Magnetic and Solid-State Memory", *Sixth USENIX Security Symposium Proceedings*, 1996. available at http://www.cs.quckland.ac.nz/~pgut001/pubs/secure_del.html.

[24] Ibid.

[25] University of Sydney, Australia. Byron S. Collie. Intrusion Investigation and Post-Intrusion Computer Forensic Analysis. September 2000. [cited May 21, 2003]. http://www.usyd.edu.au/su/is/comms/security/intrusion_investigation.html

[26] CERT Coordination Center. Intruder Detection Checklist. July 1999. [cited May 21, 2003]. http://www.cert.org/tech_tips/intruder_detection_checklist.html

[27]Dan Farmer and Wietse Venema. Computer Forensics Analysis Class, August 1999. [cited May 21, 2003]. http://www.porcupine.org/forensics/handouts.html

[28] PestPatrol, Inc. About Key Loggers. [cited May 21, 2003]. http://www.pestpatrol.com/Support/About/About_KeyLoggers.asp.

[29] Gil Dabah & Oren Becker. Keyboard Hook. [cited May 21, 2003]. http://qsoft.ragestorm.net/tutors/windows/kbhook.html.

[30] PestPatrol, Inc. [cited May 21, 2003]. http://research.pestpatrol.com/KeyPatrol/.

[31] Michael A Caloyannides. *Computer Forensics and Privacy*. Artech House, Boston 2001. pgs. 58-64

[32] Eric N. Newburger, "Current Population Reports: Home Computers and Internet Use in the United States: August 2000." U.S. Census Bureau. September 2001, [cited May 21, 2003]; available from www.census.gov/prod/2001pubs/p23-207.pdf23

[33] The Constitution of the United States. (Philadelphia: National Constitution Center, 1997), 22.

[34] Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." July 2002, [cited May 21, 2003], p. 9 available from www.cybercrime.gov/s&smanual2002.htm

[35] FindLaw Cases and Codes. "United States vs. Grimes" March 7, 2001, [cited May 21, 2003], available from http://laws.lp.findlaw.com/getcase/5th/case/0040495cr0&exact=1

[36] Ibid.

[37] Computer Crime, 14.

[38] Ibid, 12.

[39] Ibid, 19.

[40] Ibid, 19.

[41] Ibid, 37.

[42] Ibid, 54.

[43] Electronic Communications Privacy Act of 1986, 18 U.S.C 2703. October 21, 1986. [cited May 21, 2003]; available at www.cpsr.org/cpsr/privacy/wiretap/ecpa86.html

[44] Computer Crime, 70.

[45] Chapter 119 - Wire and Electronic Communications Interception and Interception of Oral Communications. United States Code Annotated, Title 18. Crimes and Criminal Procedure, Part 1 – Crimes. [cited May 21, 2003]; available at www.cybercrime.gov/wiretap2510_2522.htm

[46] David L. Sobel, "Will Carnivore Devour Online Privacy?" *IEEE Computer* V. 34, No. 5 (May 2001), 87-88.

[47] Kevin DiGregory, Statement Before the Subcommittee on the Judiciary on "Carnivore" and the Fourth Amendment. July 24, 2000. [cited May 21, 2003]; available at www.cybercrime.gov/carnivore.htm

[48] Sobel, 87.

[49] "Why Carnivore is bad for you (reason #1)" StopCarnivore.org, 2000 [cited May 21, 2003]; available at http://stopcarnivore.org/whyitsbad/reason1.htm

[50] Carrie Davis, "Kiss Your Privacy Goodbye: Online Anonymity Post-9/11" *The Internet Law Journal*. January 21, 2003. [cited May 21, 2003]; available at www.tilj.com/content/ecomarticle01210302.htm, 4.

[51] Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001. Computer Crime and Intellectual Property Section (CCIPS). November 5, 2001. [cited May 21, 2003]; available at www.cybercrime.gov/PatriotAct.htm, Section 210.