Real World Computer Forensics

Jessica Riccio
California Polytechnic State University, San Luis Obispo

June 7, 2012

“Technology now permits millions of important and confidential conversations to occur through a vast system of electronic networks. These advances, however, raise significant privacy concerns.”
-Bartnicki v. Vopper, 2001

Abstract

Computer forensics “is the analysis of information contained within and created with computer systems and computing devices, typically in the interest of figuring out what happened, when it happened, how it happened, and who was involved [22].” For the average citizen a computer forensics investigation might seem daunting and filled with incomprehensible jargon not understood without technical schooling. This paper will provide a better understanding of the processes and steps involved in a computer forensics investigation. Through the explanation and demonstration of prevalent computer forensics software and hardware, the basic procedures of a computer forensics investigation will be explored. Furthermore, two real computer forensics cases are profiled and used to exemplify the real world applications of the procedural events, software, and hardware.

Contents

1 Introduction

In 2012, the majority of the world lives and breathes through computers. Humans are inundated each day with new opportunities offered by computers and new ways of solving our generations' problems through their use. The computer hype is warranted, as, among other things, computer technology helps surgeons through long hours of complicated surgeries in the operating room and increases wheelchair motion accuracy for paraplegics. Despite all the positive aspects that computers have in our daily lives, humans often overlook computers' ability to work as tracking devices, privacy violators, and, ultimately incrimators.

Our computers have the ability to provide many untrustworthy individuals with private information at the drop of a hat. Worms, Trojans, and back-door programs all pride themselves on silently embedding themselves in unsuspecting computers and reaping information until they are found or their task expires. Furthermore, computer users everywhere are faced with the possibility of entrenching themselves in litigation and lawsuit. The ability humans have to penetrate systems, bring down government websites, and hijack crucial national information is enormous. After recent world events like Stuxnet and Anonymous' "barrage of government hacks," this ability is becoming more realized and feared [23] [13]. As concerned as the governments are about digital security, the average person should be twice as concerned. In 2009, it was estimated that 2.6 million code threats existed [11]. With more than 1.7 billion Internet users, the odds are high that average person has been, or will be, the victim of computer crime [11]. However, these citizens lack the general know-how to protect themselves and their machines. Governments have means to identify their weaknesses in networks and security and to remedy them within a reasonable time frame. Governments also have experts in their respective fields constantly trying to prevent the next leak or the next great attack. In contrast, the average person is usually advised to stay away from unfamiliar sites and not to download anything that seems out of the ordinary. While these are good guidelines by which to live, they are not enough. These few rules provide a basis for protection on a minimal level and neglect the real issues such as back-door programs stealing information from the visitation of any website, trusted or not. Additionally, these rules are often over-used and misunderstood because the general public is lacking the key knowledge for their optimal protection.

By demonstrating that computer forensic tools are applicable through real world scenarios, this paper exemplifies the technical aspects of computer forensics to educate the average consumer population. In addition, it seeks to provide examples of real world experiences in computer forensic procedures for "new-comers" to the field. The programs are complex, but the demonstrations and explanations attempt to lay out the topics in plain language.

In summary, this paper will look at two similar cases and demonstrate the application of various computer forensic software and hardware. The software and hardware are used by law enforcement and investigators, but can also be obtained by the general public. Furthermore, the specifics of each of the cases will be looked at and the generalities of the process will be exhibited. By the end of this paper, the reader should be able to understand the follow of a typical computer forensics investigation from start to finish and know how to conduct various aspects of a computer forensics case including forensic hard drive imaging, network analyzing, and port scanning.

2 Case Description and Beginning Steps of Inquiry

By stepping through cases based on concrete, authentic facts, it is possible to gain a greater and deeper understanding of the concepts and procedures present in a typical computer forensics investigation. For this reason, the two cases exhibited in this paper involve similar circumstances and investigative processes. While the cases are based on real cases from Burgess Forensics, the names and places have been changed to respect the privacy of the individuals.

2.1 The Roommate Who Couldn't Be Trusted

All too often, people come to a computer forensics expert's office with victim stories and what they think has happened. While it is easy to automatically assume that they are making more out of their situation that really is, a majority of the time people do know there is something happening to them, even if they do not know exactly what it is that is happening. This sequence of events follows closely to a story of man, Tim Jackson, who thought his roommate, Jason Walsh, was spying on him through Tim's computer.

Both men worked for a wealthy international manufacturing company in Dallas and had recently be involved in some office drama. Tim's supervisor had allegedly "come onto him," and Tim made it apparent to his supervisor that "he wasn't interested" [19]. Soon after the encounter Tim was let go. Feeling like his termination was unwarranted, Tim suspected his objection to his supervisor's advances was the real reason behind the company letting him go. Not completely understanding how they had any grounds to treat him in this way, he began to wonder how they found anything on him. Without skipping a beat, his attention turned to his roommate, Jason. Tim believed Jason to not only be spying on him through his computer but also to be sending incriminating evidence to their employer, contributing to his release.

After making his case, it was determined there was enough evidence to warrant Tim's suspicions and the investigation into whether or not Jason had been spying on him and stealing his documents began [19].

2.2 Too Close For Comfort

One of the most frightening feelings a person can experience is the perception that they are being watched and cannot do anything about it. This scenario was all to real for Mary, a high school teacher in Oregon, who knew she was being watched through her computer, but she didn't know how or why. Recently, in one of her classes, a student had begun repeating words and sentences that the teacher had said in her home. She knew the boy was not in the house when she had spoken these words, and she even went outside to see if, from the outside of the house, he could hear her conversations. She could not figure out how the boy had eavesdropped on her conversations and was beginning to feel more uncomfortable than before.

Before seeking professional help from a private investigator, Mary had enough know-how to determine that, somehow, her computer was the culprit. She began educating herself in computer hacking procedures, hoping to figure how the boy had listened to her conversations. Furthermore, Mary had also begun using computer protection software including Norton Anti-Virus and network monitoring software, Netstat. With Netstat revealing nothing more than average network stats, Norton proved to be slightly more effective. Norton had uncovered a back-door Trojan, the Sasser Worm, but it was not how the boy had listened in on Mary [18].

Finally, having exhausted all of her personal experience, Mary turned to computer forensics in hopes of having her fears calmed and the alleged eavesdropping stopped.

2.3 Beginning Steps of Inquiry

As shown in the two previous cases, before the actual investigation can take place, it needs to be determined if a case even exists with the current information. When someone requests the help of a computer forensics expert, usually the attorney of the victim, will contact the expert and explain what has happened. While the attorney is explaining the facts of the story thus far, it is imperative to take notes about what is being said. Afterwards, the computer forensics expert will usually ask clarifying questions that will help him or her decide how to proceed next. These questions can include whether the computer involved is a laptop or a desktop computer, age of the computer, hard drive specifications, file system and architecture , and the operating system.

The next step is for the computer forensics expert to estimate the amount of time the discovery process will take. From here, the expert can send a quote for the work to the attorney. The attorney can then accept the bid or they can counter the bid and return it to the expert. If the expert and the attorney can come to an agreement on the time frame and price, both parties will sign a detailed contract and the expert will either request the hard drive be sent to the office or arrangements will be made for the expert to go to the site of the computer and acquisition the data there. This concludes the preliminary process of the entire case. The next step is to perform the discovery with various tools.

3 Tools

Both software and hardware tools assist the computer forensics expert in the investigation. Without the software, a great deal of time would be spent manually sifting, searching, and aggregating information together, causing the entire process to take a great deal longer to complete. Therefore, software programs are an essential part of the process. Hardware tools, such as enclosures and write blockers, assist in making the investigation easier. When used in combination, both tools are invaluable in computer forensics.

3.1 Programs

Often, computer forensic experts will use programs that have already been created for these purposes, as opposed to writing their own programs. The programs listed below are used today in the computer forensics industry. While there is a great deal of overlap with the functionality of these programs, more often than not, a computer forensics expert will pick a favorite program for one task and another program for a different task, even though both programs could accomplish nearly all of the same tasks. The key to using these programs is to find the program best suited for the investigator and the task at hand.

3.1.1 Media Tools Professional

Media Tools Professional is a computer software that is used by industry professionals as well as government agencies in order to make identical copies of a hard drive. It is vitally important that during an investigation the expert never compromise the integrity of the data and information contained on the hard drive. If the hard drive is somehow altered or modified by the expert, it could jeopardize the entire investigation. For this reason, some investigators prefer using a hardware copier is preferable, because it is a physical reassurance that the data is not compromised. However, software-based copying is more than reliable enough for making a forensically-sound copy.

The first step in the process is to access the BIOS for the computer from which you will do the copying and change the primary start up from the hard drive to the CD drive. In addition, the hard drive that will be copied should be put into an external enclosure and plugged into the computer through a USB port. Next, insert the Media Pro Tools disc into the CD drive, and restart the computer. When it restarts, it will load what is on the disc in the CD drive, instead of the operating system on the hard drive. The Media Tools Pro disc will prompt for various options when copying the hard drive. What is unique about the program is that it gives the user the ability to stop the copying process when a block of damaged data is trying to be copied. This stopping is important because, if the damaged part of a hard drive is repeatedly trying to be copied, it will offset the bit count, which can change the hard drive. Media Tools Pro will continue to copy the original hard drive to the hard drive in the computer, bit-by-bit. This bit-by-bit copy ensures that no data will be lost along the way.

3.1.2 EnCase Forensic

EnCase has all of the tools needed for any person, investigator or typical computer user, to find out nearly any the information they may need from a computer. Created by Guidance software, it is designed to "conduct efficient, forensically sound data collection and investigations using a repeatable and defensible process" [15]. EnCase provides the user with different tools including forensic imagining, file indexing, recreation of readable file formats, and file reconstruction. Each of these tasks can be used by the investigator to further understand the data present on the computer. Furthermore, they can assist in the reconstruction of previously deleted or damaged files and determine if someone has attempted to conceal the presence of the file on the system, which would indicate the perpetrator might have something to hide. This program has even earned public recognition in a fairly recent New York Times article. EnCase was used by investigators in both the BTK Killer and Scott Peterson case to convict the defendants [25]. With a strong presence, this program is been used by many investigators and is reputible.

3.1.3 Wireshark

Wireshark is a program created by Gerald Combs that has been named eWeek's "Most Important Open-Source Apps of All Time [3]." This program is designed for analyzing networks and the connections made to and from that network. When Wireshark is running, the user can monitor network "traffic," an action commonly referred to in the computer industry as "sniffing" [5]. Once downloaded and installed, the user can connect to a network and log the packets being received from the Internet. Later, the log can be used to learn more information about a persons' Internet activity including recent search engine queries, websites visited, and files download. In addition, Wireshark can run on multiple operating systems, adding versatility to its list of advantages. Because it is used widely in both industry and educational settings, it is worthwhile program for computer forensics experts and, with a little guidance, general computer users as well [3].

3.1.4 Netcat

Netcat, a very common rootkit detection tool used in the field of computers, is just as common and useful in computer forensics. This program, typically ran from the command line, handles nearly all activities associated with TCP and UDP connections. When "nc" is typed at the command line, sometimes including few to many parameters, the computer running the program can perform various actions such as "read[ing] and writ[ing] data across network connections" [6]. In addition, Netcat is frequently used for port scanning. Port scanning is defined as "the act of systematically scanning a computer's ports [and] identifies open doors to a computer" [17]. This scanning can be a useful way of monitoring networks that the have been previously compromised and are now part of the investigation. Netcat also has many other features including data transfer, "talking" to servers, and sending packets. Depending on the case, these features may or may not be applicable in the discovery process [16].

3.2 Hardware

In addition to software programs, hardware components are important in the investigation. Similar to the severity of a compromised hard drive due to an expert misusing the copying software, the investigation could be compromised without some key tools, such as a write blocker. Furthermore, it is important for investigators to be familiar with the types of hardware that are used in computers today because of the inevitability of having to perform an investigation on typical consumer computers. Thankfully, the majority of computers today have SATA hard drives; however, as the presence of solid-state hard drives continues to increase, it is unclear as to what the steps will be in those types of investigations.

3.2.1 Write Blocker

Write blockers serve a very important purpose in computer forensics cases. Once the investigator or law enforcement team has made the decision to pursue a case, the first step is the acquisition. The acquisition is when forensics software is used to create an identical, forensic copy of the hard drive in question. To ensure that no data or hard drive is compromised, write blockers are often used. Though the hardware of a write blocker is detailed and specific, the concept behind it is easily comprehensible.

A write blocker literally blocks the computer, and person performing the acquisition, from writing to the hard drive in question. The device allows write commands from the hard drive in question to the computer but not from the computer to the hard drive. These write commands are system calls sent out by the kernel, which handles the interaction between the computer and code written on the computer. For instance, if an investigator is using the computer for multiple purposes while making a forensic image of a hard drive, and he accidentally tries to save a document on the hard drive in question, the computer will send a write command to the hard drive. The write blocker will intercept this command, and it will not occur.

Hardware write blockers are used because of their operating system versatility. Write blockers are software independent and therefore can be used with any operating system [14]. In addition, hardware write blockers are designed to work with multiple drive interfaces, such as IDE and SATA. A Native write blocker will write and read from the same interface type, while a Tailgate write blocker has the option of writing to one type of interface and reading from another[14]. Because computer forensics experts deal with different operating systems and hard drive types each day, having a write blocker that can be used with any operating system or hard drive interface is useful. Instead of purchasing many different write blockers, experts are able to purchase one versatile write blocker and conduct many investigations that include varying hardware and software components.

Figure 1 demonstrates what a typical write blocker set up would look like. The hard drive being investigated (right) is connected to the write blocker (left) through a two chords. The multicolored chord connecting the hard drive and the write blocker is a power supply for the hard drive. In this instance, the hard drive being investigated is a SATA hard drive and therefore needs a SATA connector chord. Without power to the hard drive, data could not be extracted from it. Next, the red chord connected to the hard drive and write blocker is the chord which handles the transfer of data from the hard drive to the expert's computer. The black chord (left) will be plugged into the expert's computer through a USB port (not shown). Once connected, the expert can begin any number of tasks on the hard drive without fear of compromising the hard drive in the investigation.

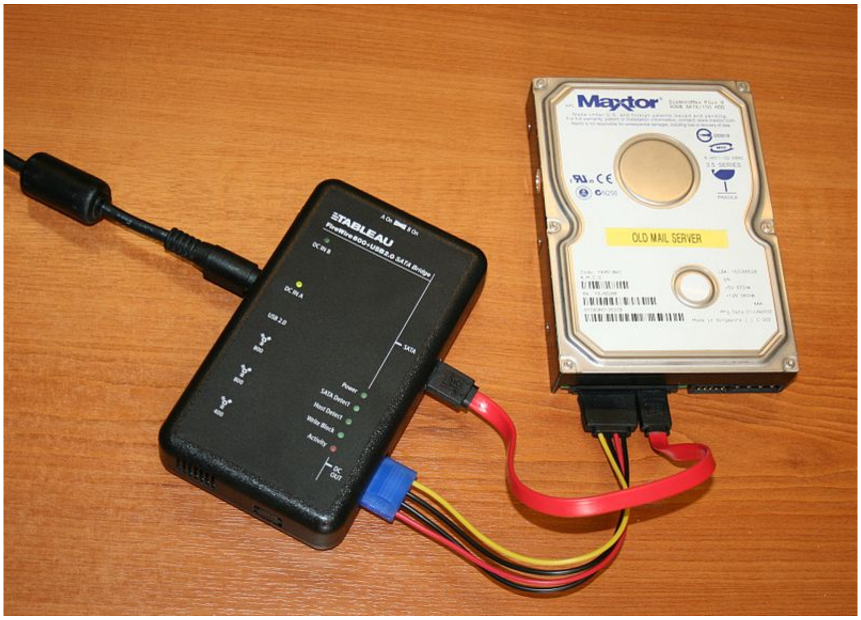


Figure 1: Write Blocker Set Up [21]

3.2.2 Hard drives

Approximately ninety-nine percent of computers today contain a SATA hard drive, the successor to the IDE hard drives [10]. While there are some advantages to having a SATA hard drive, such as faster performance and making a more cost effective system, at the hardware level, the architecture of all hard drives is nearly identical [10].

Upon opening a hard drive, rendering it unusable, the technician would find platters. As picture in Figure 2, platters are “[vertical] stacks of discs...covered with magnetic material [7].” Within the platters are tracks that are more commonly referred to as cylinders. These cylinders, “sets of parallel tracks on each of the platters,” are then divided into sectors. On each sector, the computer stores data and code for applications it runs. When a hard drive is copied during an investigation, each sector is copied over, bit-by-bit, and when a “bad” sector is encountered, it is best to just skip the damaged part and continue on in the copying process.

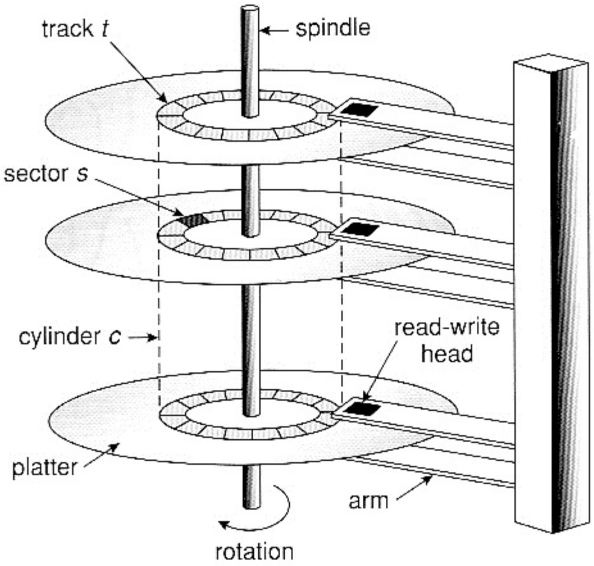


Figure 2: Sector and Platter Design [1]

By viewing the hard drive through a wider lens, often, hard drives are divided into partitions. A partition "allow[s] a single drive to appear to be multiple individual drives [7]." Most people will partition a hard drive to install multiple operating systems or to have partition specific store devices. It is up to the user how many partitions they will want, but one partition must always be designated as the boot partition [7]. The presence of this partition guarantees that the computer will always have a place from which to boot.

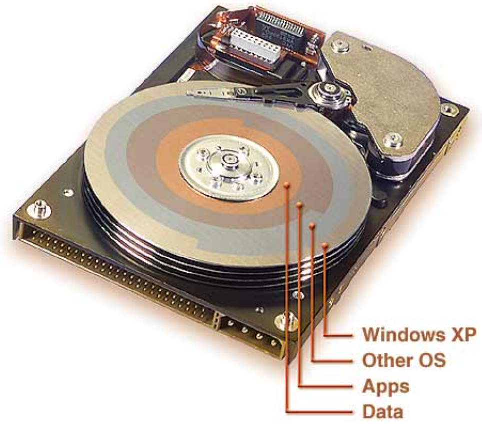


Figure 3: Partitions of a Hard Drive [4]

4 Process

The process of information and data discovery in a computer forensics case is dynamic, needing to be adapted and altered to fit the specifics of each case. The two processes below are specific to the case; however, a general sequence of events and tasks can be extracted and used as a model for other cases.

4.1 The Roommate Who Couldn't Be Trusted

Once the computers had been delivered to the computer forensic expert's office, a blind copy was made with Media Pro Tools. Because of this cases' age, most of the programs that are currently being used today were either not available for Macintosh computers at the time this case took place, or the program was minimal.

Because Tim had accused Jason of spying on him through his computer while Tim was away from the apartment, the first evidence to look for were instances of the roommate's name or variations of his name in any of the files. This part of the process was carried out by the use of FWB Toolkit, a once-more-common Macintosh oriented computer forensic software [19]. In addition to the search of Jason's name, all the files were sorted by their creation and modification date. File Buddy was used to categorize and search through the files and to determine if any of the files had been created of modified while Tim was not present [19]. Data Recovery was also used to see if any files or various logs had been deleted from the hard drive.

Both of the above methods of discovery yielded information. First, when the roommate's name was search for on the hard drive, the address book was shown as a place where his name had been. After looking more closely at the emails sent from this address, it was plausible that some of the words found in the emails were a sign that some sort of spying was occurring. In addition, deleted printer and fax logs were found with dates matching the dates that Tim said he was not in the apartment [19].

4.2 Too Close For Comfort

Thankfully, Mary had done a great deal of back-end work, making it easier to know where to start for the investigator. Because of what had happened, it was obvious that the boy had gained remote access to her computer. When the computer arrived at the computer forensics office, the first step was to look for this remote access. This task was done using three anti-malware programs in conjunction with a rootkit detection program. In addition to these programs, EnCase was used to determine the last time the admin password was changed on the computer. Through a series of menus, it was possible to see all the information regarding the users' password and account login information, including the last time the password was typed, correctly or incorrectly, and when the user had logged on to the computer.

At this point in the discovery process, none of the programs or search had yielded enough results to determine exactly how the boy had listened in on Mary's private conversation. The next step was to look for a mystery account or activity within a "phantom" account. The mystery account, also known as the guest account, is an option that nearly all computers still support today. If the boy had found a guest account on Mary's computer, the same information that was checked for on Mary's account could have been checked to see if this was there he gained access. The "phantom" user, an administrator account that is installed on computers bought at retail stores, could have been the means by which the boy gained access to the computer. (This account has no password protection on it and makes it an easy target for intrusion.) However, after testing, both of these results still ruled that this was not how the boy had listened in on Mary.

After nearly all other tests were exhausted, the final step was to look at the Internet connection. Mary had been using a cable modem, which in regards to security, is equivalent to unprotected WiFi. Though the previous programs had given no indication of a remote access program or the remote control access service being turned on, it could have been that the boy was exceptional at what he did and had removed any signs of him being on the computer. A list of all the known remote access software was compiled and searched for on the computer. Lo and behold, there were five instances of one of the programs hidden in the system restore files. A further examination of the system restore files in EnCase revealed a date and IP address near each instance of the program. It was determined that this must have been how he acquired access to the computer: through the modem with a remote access software program [18].

4.3 General Process

As demonstrated in the experiment section, the process of discovery is often melded to meet the needs of the case at hand. First, the computer expert needs to determine what type of files or data will need to be included in the evidence. From here, choosing which program to use is up to the discretion of the expert. As the process of gathering information proceeds, detailed notes of which programs have been used and what material has been looked through. In some investigations, computer forensics experts will give the general information to the attorney, at which point the attorney will determine what will or will not help their client in the court room. Though more often than not, many of the experts participating in the case will find information, decide if it could be relevant to the case and file it away for the attorney's approval at the end of the discovery process. Once all the tests and programs have been ran and the expert has done all they can do with the information given, they may request addition hardware (if it can be provided and is applicable to the case) or give the information they have to attorney or victim. Finally, the hardware is returned to its respective owner and the case continues.

5 Experiments

This section details the design, procedure, and findings of my experiments. The purpose of each experiment is to work with the computer forensics software that is used in industry today and to apply other computer forensic knowledge. Through the experimentation, a better understanding of technical procedures is gained. Furthermore, the experiments are meant to resemble aspect of a real computer forensics case albeit on a smaller scale. In addition, all of the programs used below are free or open-source and can be obtained by the general public for educational benefit.

5.1 Hard Drive Copy

As stated previously, correctly making a copy of the hard drive in question is crucial to maintaining the integrity of the data. If the computer forensics expert alters the data in question it could compromise the case as a whole. The purpose of this experiment is to demonstrate through the use of two programs how to clear a hard drive and how to make an identical copy of it for further investigative uses.

5.1.1 Tools

The tools used in this experiment included a 320 GB SATA hard drive, a hard drive, Darik's Boot and Nuke (DBAN) 2.2.6, and Norton Ghost 2003.

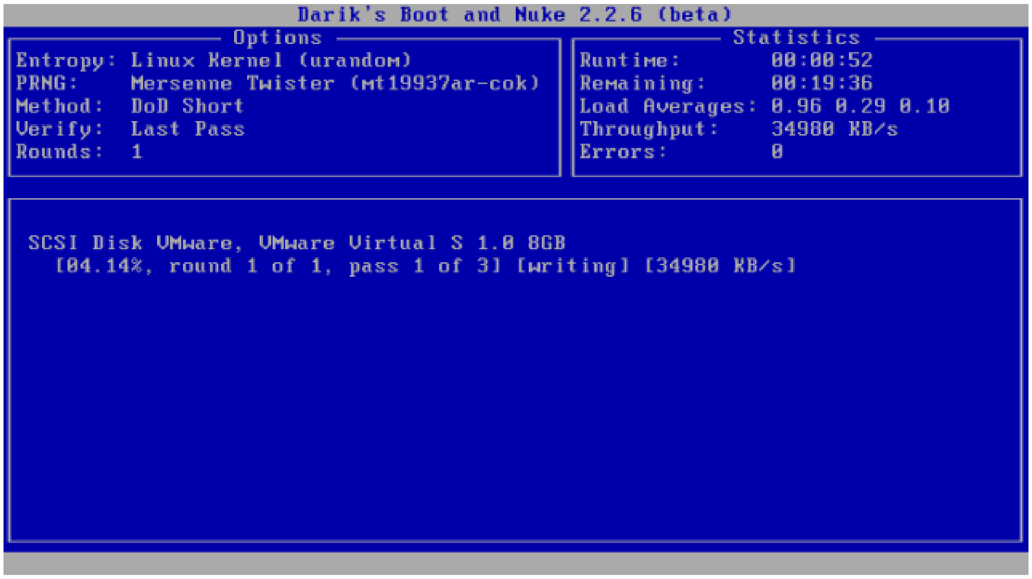
5.1.2 Procedure

Before beginning the experiment, it is imperative to remember which hard drive contains the data needing to be copied and which hard drive is going to be wiped clean. Also, the BIOS need to be changed so the computer will boot from the CD Drive first, not the hard drive.

1. Insert the DBAN disc into the CD Drive of the computer that contains the hard drive you are going to be writing to.

2. The computer will boot from the disc and a menu screen will be displayed. Choose which hard drive you want to wipe clean.

3. When the correct hard drive is chosen, choose "wipe." While it is wiping the hard drive, the screen will look as it does in Figure 4.



```
                       Darik's Boot and Nuke 2.2.6 (beta)
--------------------- Options -------------------- ----------- Statistics ----------
Entropy: Linux Kernel (urandom)                     Runtime:        00:00:52
PRNG:    Mersenne Twister (mt19937ar-cok)           Remaining:      00:19:36
Method:  DoD Short                                  Load Averages:  0.96 0.29 0.10
Verify:  Last Pass                                  Throughput:     34980 KB/s
Rounds:  1                                          Errors:         0

 SCSI Disk VMware, VMware Virtual S 1.0 8GB
   [04.14%, round 1 of 1, pass 1 of 3] [writing] [34980 KB/s]
```

Figure 4: Screen Shot of DBAN [2]

4. When DBAN reaches 100 percent, remove the DBAN disk and insert Norton Ghost 2003 into the CD drive.

5. After Norton Ghost has been inserted, shut down the computer.

6. Once the computer has shutdown double check to make sure that both hard drives that will be used are plugged into the power supply and mother board.

7. Turn on the computer and boot from Norton Ghost.

8. When a list of options are presented on the screen, choose "Option 2: Load CD drives (IDE and SCSI). This is equivelant of mounting a drive in Linux.

9. When this finishes, look for a command prompt "A:\" and the line preceding it. The preceding line is the drive letter for the "mounted" CD ROM. Input "[drive letter]:\support \ghost" on the command prompt "A: \"

10. Norton Ghost will now ask which drives are usable in Ghost. Click “OK.”

11. On Menu, click “Options.”

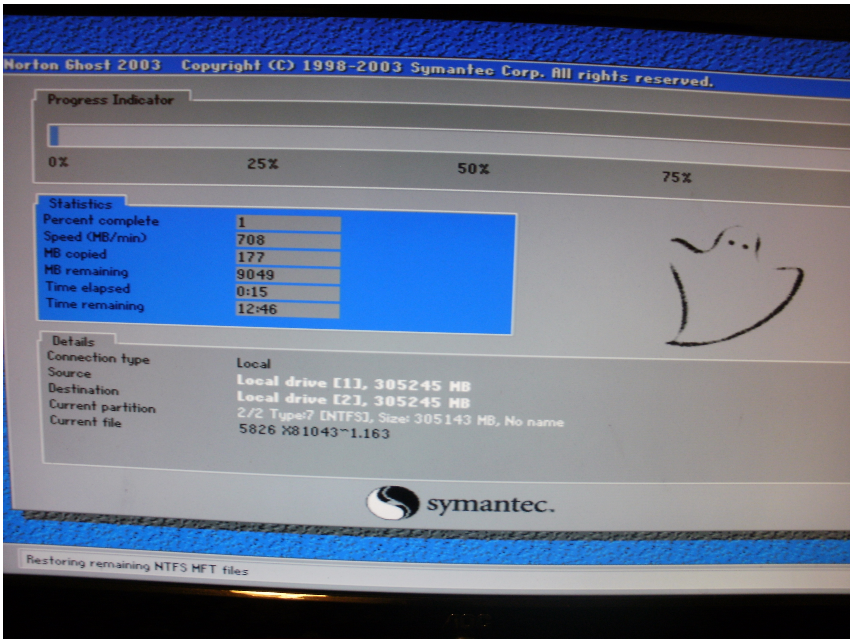
12. Click on “Misc.” tab and check “Force Cloning” and ”Accept.”

13. From the home screen here, locate the “Local” button. Hovering over it will list all the options for the hard drive you are copying from.

14. Hover over the “Disk” button. Just as with the “Local button”, it will list all the options for the hard drive you wish to copy to; Click “To Disk.”

15. Norton Ghost will now highlight which drives are the source drives and destination drives. Click“OK” when the correct drives are selected.

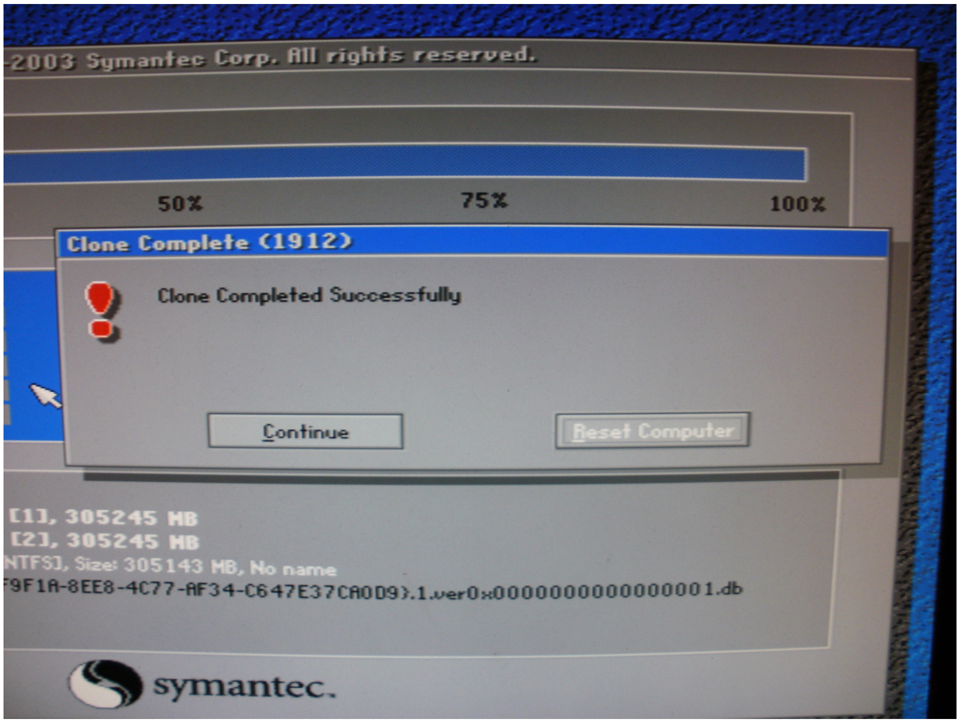
16. Norton Ghost will begin copying data from the “investigative” hard drive, sector by sector, to the “expert’s” hard drive. [8]



```
Norton Ghost 2003   Copyright (C) 1998-2003 Symantec Corp. All rights reserved.

Statistics
Percent complete     1
Speed (MB/min)       708
MB copied            177
MB remaining         9049
Time elapsed         0:15
Time remaining       12:46

Details
Connection type      Local
Source               Local drive [1], 305245 MB
Destination          Local drive [2], 305245 MB
Current partition    2/2 Type:7 [NTFS], Size: 305143 MB, No name
Current file         5826 X81043~1.163

Restoring remaining NTFS MFT files
```

Figure 5: Screen Shot of Norton Ghost Copying

17. When the copying process is finished, a window will appear with two options: "Continue" or "Reset Computer." Click "Continue."



```
-2003 Symantec Corp. All rights reserved.
```

Clone Completed Successfully

```
[1], 305245 MB
[2], 305245 MB
NTFS], Size: 305143 MB, No name
F9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000001.db
```

Figure 5: Screen Shot of Norton Ghost Completion Window

18. This will take you back to the main menu and your computer can now be shutdown.

This concludes the process of "wiping" a hard drive and making an identical copy of the hard drive in question.

5.2 Wireshark

Monitoring a network for malicious activity is not only an important part of computer forensics but of the computer world in general. Typically, networks and connections are monitored because of previous suspicious activity with a certain individual. This activity often includes but is not limited to child pornography. The individual's actions are logged with a program such as Wireshark and then delivered to a computer forensics expert to be looked over and sorted through.

5.2.1 Tools

The tools used in this experiment included a computer, a wireless connection to a network, and Wireshark.

5.2.2 Procedure

To capture the packets and information needed for the investigation:

1. Download Wireshark from http://www.wireshark.org/download.html. Make sure to download the version compatible with the computer's operating system and architecture (i.e. Mac, Windows, etc.).

2. Following the on-screen instructions, install Wireshark on the machine that will be monitoring the connection.

3. Once installed, open the program and determine which connection you will be monitoring. For Ethernet connection, chose the option that begins with \Device... The information after \is dynamic and will be different each time the program is loaded and therefore, is not pertinent. If the connection is wireless, simply choose the second option.

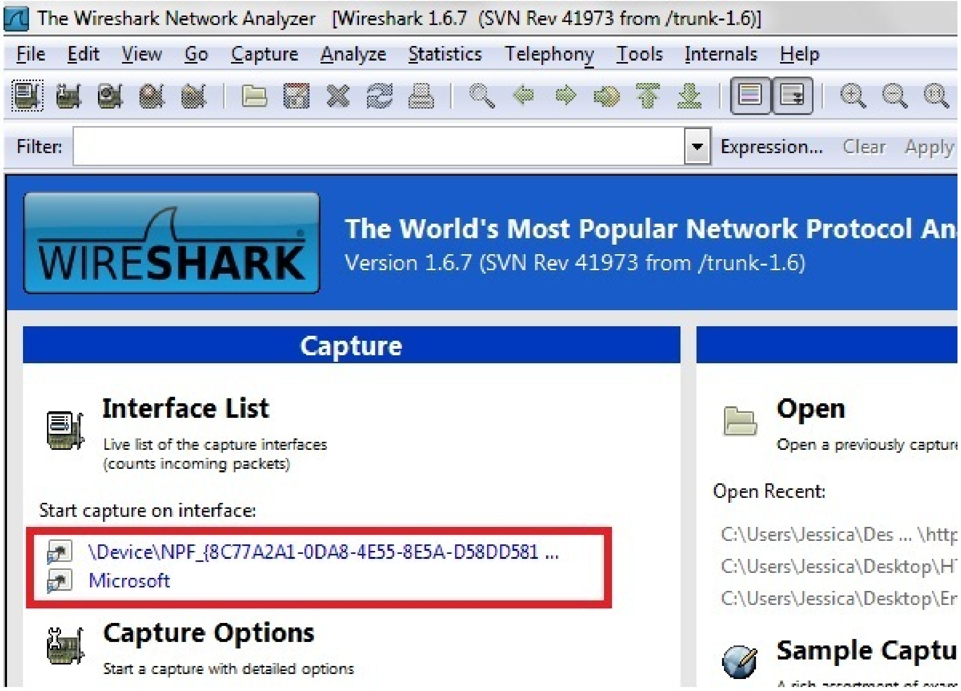
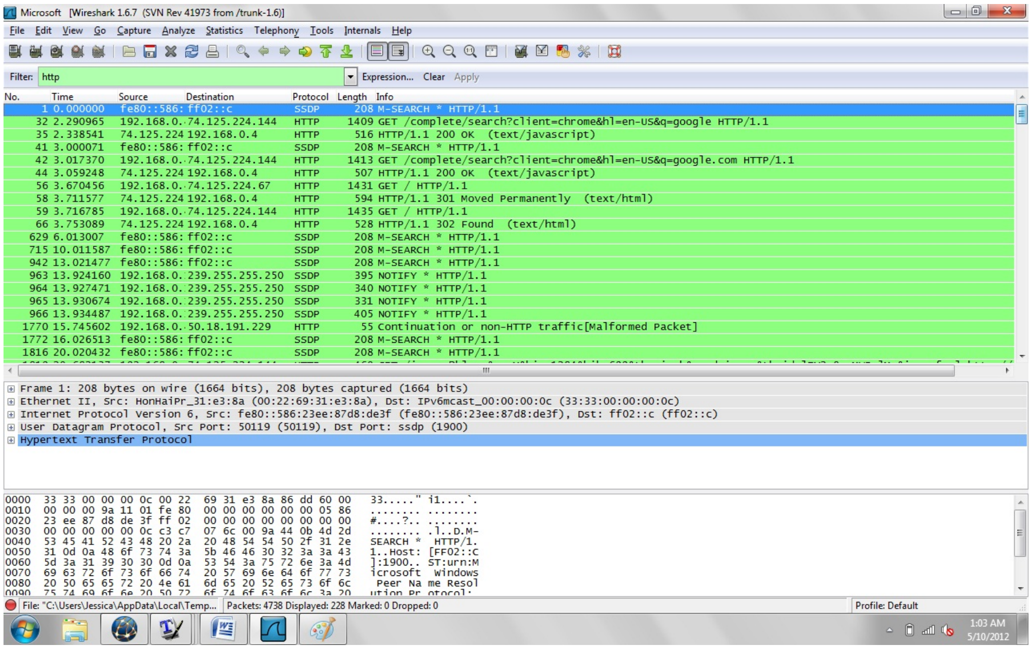

The Wireshark Network Analyzer [Wireshark 1.6.7 (SVN Rev 41973 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply
WIRESHARK
The World's Most Popular Network Protocol An
Version 1.6.7 (SVN Rev 41973 from /trunk-1.6)
Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start capture on interface:
\Device\NPF_{8C77A2A1-0DA8-4E55-8E5A-D58DD581 ...
Microsoft
Capture Options
Start a capture with detailed options
Open
Open a previously captur
Open Recent:
C:\Users\Jessica\Des ... \http
C:\Users\Jessica\Desktop\H
C:\Users\Jessica\Desktop\Er
Sample Captu

Figure 6: Screen Shot of Connection Options in Wireshark.

4. Once the connection type has been determined and chosen, the monitoring process will begin.

5. While the connection is open, one can view the packets being sent and received over the network by both the computer doing the monitoring and all other computers connected to the network.


Microsoft [Wireshark 1.6.7 (SVN Rev 41973 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply

```
No.   Time       Source          Destination       Protocol Length Info
    1 0.000000   fe80::586: ff02::c           SSDP      208 M-SEARCH * HTTP/1.1
   32 2.290965   192.168.0.·74.125.224.144    HTTP     1409 GET /complete/search?client=chrome&hl=en-US&q=google HTTP/1.1
   35 2.338541   74.125.224 192.168.0.4       HTTP      516 HTTP/1.1 200 OK  (text/javascript)
   41 3.000071   fe80::586: ff02::c           SSDP      208 M-SEARCH * HTTP/1.1
   42 3.017370   192.168.0.·74.125.224.144    HTTP     1413 GET /complete/search?client=chrome&hl=en-US&q=google.com HTTP/1.1
   44 3.059248   74.125.224 192.168.0.4       HTTP      507 HTTP/1.1 200 OK  (text/javascript)
   56 3.670456   192.168.0.·74.125.224.67     HTTP     1431 GET / HTTP/1.1
   58 3.711577   74.125.224 192.168.0.4       HTTP      594 HTTP/1.1 301 Moved Permanently  (text/html)
   59 3.716785   192.168.0.·74.125.224.144    HTTP     1435 GET / HTTP/1.1
   66 3.753089   74.125.224 192.168.0.4       HTTP      528 HTTP/1.1 302 Found  (text/html)
  629 6.013007   fe80::586: ff02::c           SSDP      208 M-SEARCH * HTTP/1.1
  715 10.011587  fe80::586: ff02::c           SSDP      208 M-SEARCH * HTTP/1.1
  942 13.021477  fe80::586: ff02::c           SSDP      208 M-SEARCH * HTTP/1.1
  963 13.924160  192.168.0.:239.255.255.250   SSDP      395 NOTIFY * HTTP/1.1
  964 13.927471  192.168.0.:239.255.255.250   SSDP      340 NOTIFY * HTTP/1.1
  965 13.930674  192.168.0.:239.255.255.250   SSDP      331 NOTIFY * HTTP/1.1
  966 13.934487  192.168.0.:239.255.255.250   SSDP      405 NOTIFY * HTTP/1.1
 1770 15.745602  192.168.0.·50.18.191.229     HTTP       55 Continuation or non-HTTP traffic[Malformed Packet]
 1772 16.026513  fe80::586: ff02::c           SSDP      208 M-SEARCH * HTTP/1.1
 1816 20.020432  fe80::586: ff02::c           SSDP      208 M-SEARCH * HTTP/1.1
```

```
⊞ Frame 1: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits)
⊞ Ethernet II, Src: HonHaiPr_31:e3:8a (00:22:69:31:e3:8a), Dst: IPv6mcast_00:00:00:0c (33:33:00:00:00:0c)
⊞ Internet Protocol Version 6, Src: fe80::586:23ee:87d8:de3f (fe80::586:23ee:87d8:de3f), Dst: ff02::c (ff02::c)
⊞ User Datagram Protocol, Src Port: 50119 (50119), Dst Port: ssdp (1900)
⊞ Hypertext Transfer Protocol
```

```
0000  33 33 00 00 00 0c 00 22  69 31 e3 8a 86 dd 60 00   33....." i1....`.
0010  00 00 00 9a 11 01 fe 80  00 00 00 00 00 00 05 86   ........ ........
0020  23 ee 87 d8 de 3f ff 02  00 00 00 00 00 00 00 00   #....?.. ........
0030  00 00 00 00 00 0c c3 c7  07 6c 00 9a 44 0b 4d 2d   ........ .l..D.M-
0040  53 45 41 52 43 48 20 2a  20 48 54 54 50 2f 31 2e   SEARCH *  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  5b 46 46 30 32 3a 3a 43   1..Host: [FF02::C
0060  5d 3a 31 39 30 30 0d 0a  53 54 3a 75 72 6e 3a 4d   ]:1900.. ST:urn:M
0070  69 63 72 6f 73 6f 66 74  20 57 69 6e 64 6f 77 73   icrosoft  Windows
0080  20 50 65 65 72 20 4e 61  6d 65 20 52 65 73 6f 6c    Peer Na me Resol
0090  75 74 69 6f 6e 20 50 72  6f 74 6f 63 6f 6c 3a 20   ution Pr otocol:
```

File: "C:\Users\Jessica\AppData\Local\Temp...
Packets: 4738 Displayed: 228 Marked: 0 Dropped: 0
Profile: Default
1:03 AM
5/10/2012

Figure 7: Screen Shot of Packets in Wireshark.

6. To stop the capture, click on the “Capture” button and the top of the page and select “Stop” from the drop-down menu.

7. To save the captured information, click “File” and select “Save” from the drop-down.

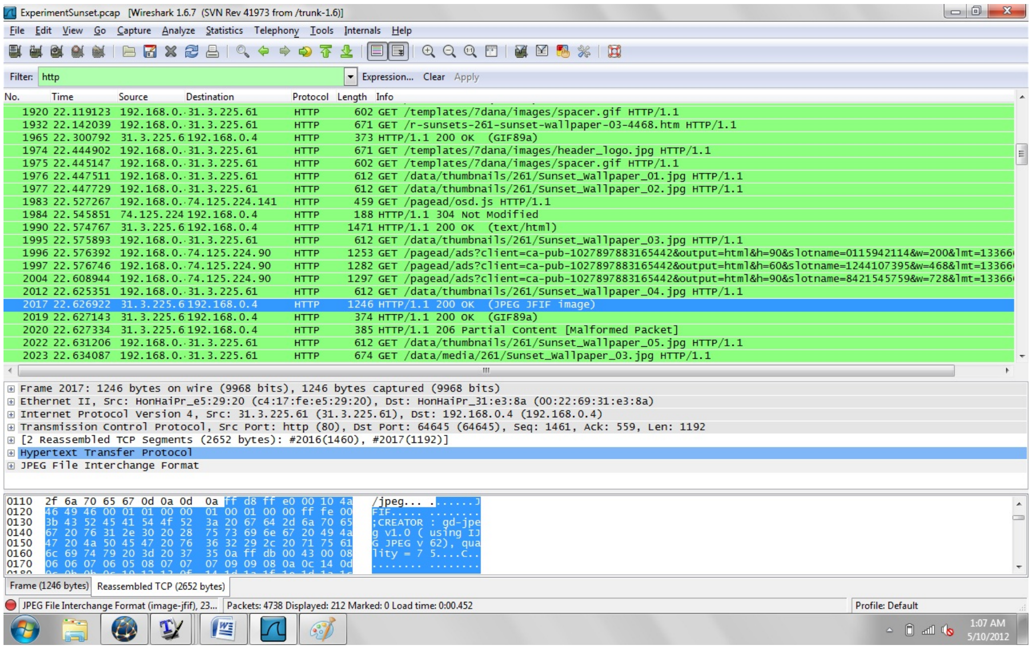
To investigate the capture log and extract a JPEG image:

1. With Wireshark open, click “File” at the top of the screen and select “Open” from the drop-down menu to open the saved capture log.

2. Because are looking for a JPEG file being looked at or downloaded from the Internet, type “http” into the filter field at the top of the screen.

3. Looking through the packets, a JPEG image will have “HTTP/1.1 200 OK (JPEG JFIF image)” listed in the information field.

4. Highlight the desired packet by clicking it once.


ExperimentSunset.pcap [Wireshark 1.6.7 (SVN Rev 41973 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply

```
No.  Time      Source          Destination      Protocol Length Info
1920 22.119123 192.168.0. 31.3.225.61     HTTP      602 GET /templates/7dana/images/spacer.gif HTTP/1.1
1932 22.142039 192.168.0. 31.3.225.61     HTTP      671 GET /r-sunsets-261-sunset-wallpaper-03-4468.htm HTTP/1.1
1965 22.300792 31.3.225.6 192.168.0.4     HTTP      373 HTTP/1.1 200 OK  (GIF89a)
1974 22.444902 192.168.0. 31.3.225.61     HTTP      671 GET /templates/7dana/images/header_logo.jpg HTTP/1.1
1975 22.445147 192.168.0. 31.3.225.61     HTTP      602 GET /templates/7dana/images/spacer.gif HTTP/1.1
1976 22.447511 192.168.0. 31.3.225.61     HTTP      612 GET /data/thumbnails/261/Sunset_Wallpaper_01.jpg HTTP/1.1
1977 22.447729 192.168.0. 31.3.225.61     HTTP      612 GET /data/thumbnails/261/Sunset_Wallpaper_02.jpg HTTP/1.1
1983 22.527267 192.168.0. 74.125.224.141  HTTP      459 GET /pagead/osd.js HTTP/1.1
1984 22.545851 74.125.224 192.168.0.4     HTTP      188 HTTP/1.1 304 Not Modified
1990 22.574767 31.3.225.6 192.168.0.4     HTTP     1471 HTTP/1.1 200 OK  (text/html)
1995 22.575893 192.168.0. 31.3.225.61     HTTP      612 GET /data/thumbnails/261/Sunset_Wallpaper_03.jpg HTTP/1.1
1996 22.576392 192.168.0. 74.125.224.90   HTTP     1253 GET /pagead/ads?client=ca-pub-1027897883165442&output=html&h=90&slotname=0115942114&w=200&lmt=13366
1997 22.576746 192.168.0. 74.125.224.90   HTTP     1282 GET /pagead/ads?client=ca-pub-1027897883165442&output=html&h=60&slotname=1244107395&w=468&lmt=13366
2004 22.608944 192.168.0. 74.125.224.90   HTTP     1297 GET /pagead/ads?client=ca-pub-1027897883165442&output=html&h=90&slotname=8421545759&w=728&lmt=13366
2012 22.625351 192.168.0. 31.3.225.61     HTTP      612 GET /data/thumbnails/261/Sunset_Wallpaper_04.jpg HTTP/1.1
2017 22.626922 31.3.225.6 192.168.0.4     HTTP     1246 HTTP/1.1 200 OK  (JPEG JFIF image)
2019 22.627143 31.3.225.6 192.168.0.4     HTTP      374 HTTP/1.1 200 OK  (GIF89a)
2020 22.627334 31.3.225.6 192.168.0.4     HTTP      385 HTTP/1.1 206 Partial Content [Malformed Packet]
2022 22.631206 192.168.0. 31.3.225.61     HTTP      612 GET /data/thumbnails/261/Sunset_Wallpaper_05.jpg HTTP/1.1
2023 22.634087 192.168.0. 31.3.225.61     HTTP      674 GET /data/media/261/Sunset_Wallpaper_03.jpg HTTP/1.1
```

```
⊞ Frame 2017: 1246 bytes on wire (9968 bits), 1246 bytes captured (9968 bits)
⊞ Ethernet II, Src: HonHaiPr_e5:29:20 (c4:17:fe:e5:29:20), Dst: HonHaiPr_31:e3:8a (00:22:69:31:e3:8a)
⊞ Internet Protocol Version 4, Src: 31.3.225.61 (31.3.225.61), Dst: 192.168.0.4 (192.168.0.4)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 64645 (64645), Seq: 1461, Ack: 559, Len: 1192
⊞ [2 Reassembled TCP Segments (2652 bytes): #2016(1460), #2017(1192)]
⊞ Hypertext Transfer Protocol
⊞ JPEG File Interchange Format
```

```
0110  2f 6a 70 65 67 0d 0a 0d  0a ff d8 ff e0 00 10 4a   /jpeg... .......J
0120  46 49 46 00 01 01 00 00  01 00 01 00 00 ff fe 00   FIF..... ........
0130  3b 43 52 45 41 54 4f 52  3a 20 67 64 2d 6a 70 65   ;CREATOR : gd-jpe
0140  67 20 76 31 2e 30 20 28  75 73 69 6e 67 20 49 4a   g v1.0 ( using IJ
0150  47 20 4a 50 45 47 20 76  36 32 29 2c 20 71 75 61   G JPEG v 62), qua
0160  6c 69 74 79 20 3d 20 37  35 0a ff db 00 43 00 08   lity = 7 5....C..
0170  06 06 07 06 05 08 07 07  07 09 09 08 0a 0c 14 0d   ........ ........
```

Frame (1246 bytes)
Reassembled TCP (2652 bytes)
JPEG File Interchange Format (image-jfif), 23...
Packets: 4738 Displayed: 212 Marked: 0 Load time: 0:00.452
Profile: Default
1:07 AM
5/10/2012

Figure 8: Screen Shot of Highlighted JPEG Packet in Wireshark.

5. Click on the “JPEG File Interchange Format” option below the packet field.

6. Right click the same option and select “Export Selected Packet Bytes.”

7. A window will appear asking for save options. The format Wireshark uses to save these types of images is a .raw extension, allowing virtually any program to open them for viewing.

8. Once saved, the image can be opened and viewed.

When compared with the picture originally viewed on the Internet, we can see that, in fact, the saved JPEG extracted from the saved log is the same image.

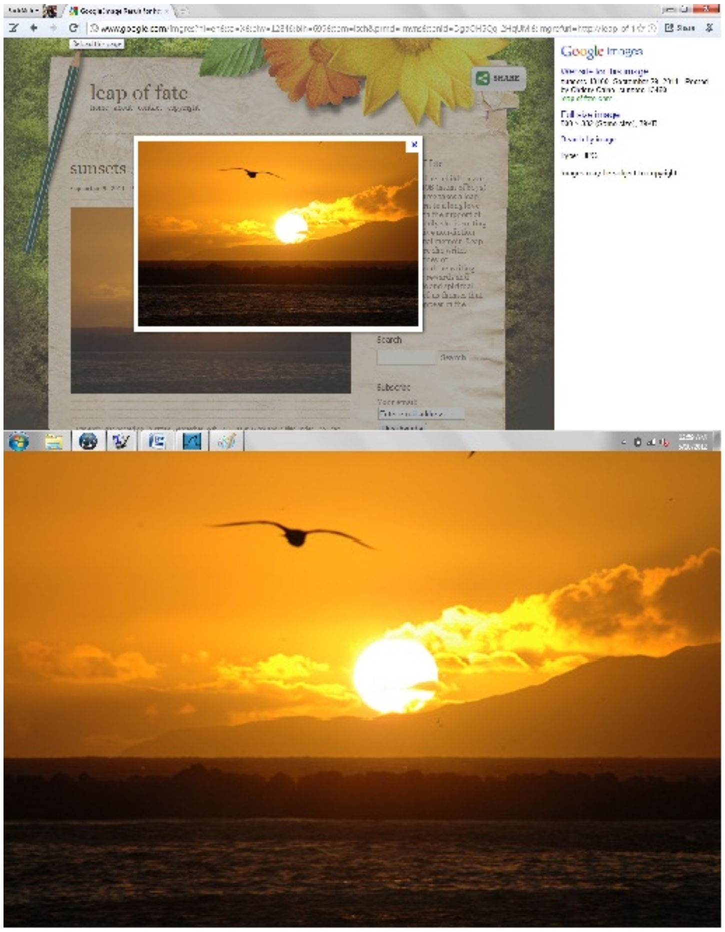


Figure 9: Comparison of Searched and Extracted Image.

5.3 Netcat

Netcat is a powerful tool in computer forensics. In this experiment, Netcat is used to demonstrate how ports are “listened” to and how to send files to another computer through port connections.

5.3.1 Tools

The tools used in this experiment include a desktop computer running a JoliOS operating system and a laptop running Windows 7 Ultimate.

5.3.2 Procedure

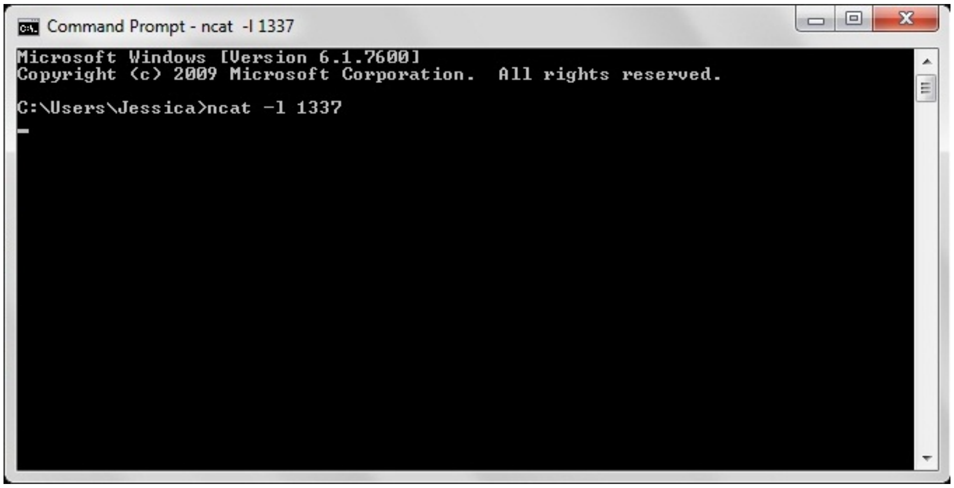
Before beginning the process of transferring a file through port connection, it is necessary to download and install Netcat on both computers. Depending on the operating system, different installations may need to be downloaded; however, all installations can be downloaded from http://nmap.org/ncat/. In addition, the commands used in this experiment are representative of the operating systems they are associated with. Please make sure that when replicating this experiment the commands for Netcat match the operating system to which they pertain.

1. Once Netcat is installed on both computers, open a command terminal on each computer.

2. Designate one computer as the "instigating" computer and the other computer as the "listening" computer.

3. On the "instigating" computer, create a file, via the terminal, that has some desired text. *Note: It is best to not include a file extension type in the naming of your file.*

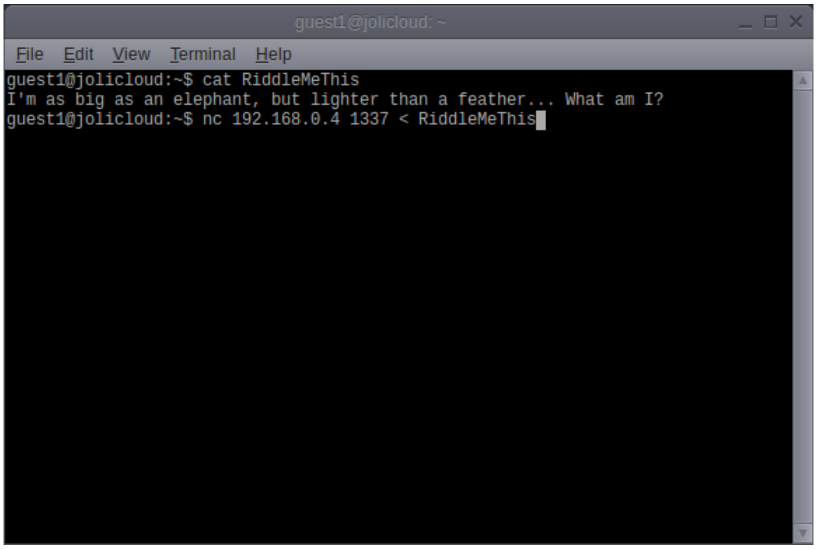
4. On the "listening" computer, type "ncat -l 1337" in the terminal. This action connects the computer to port 1337 and is now "listening" to the port.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Jessica>ncat -l 1337
_
```

Figure 10: “Innocent” Computer Terminal

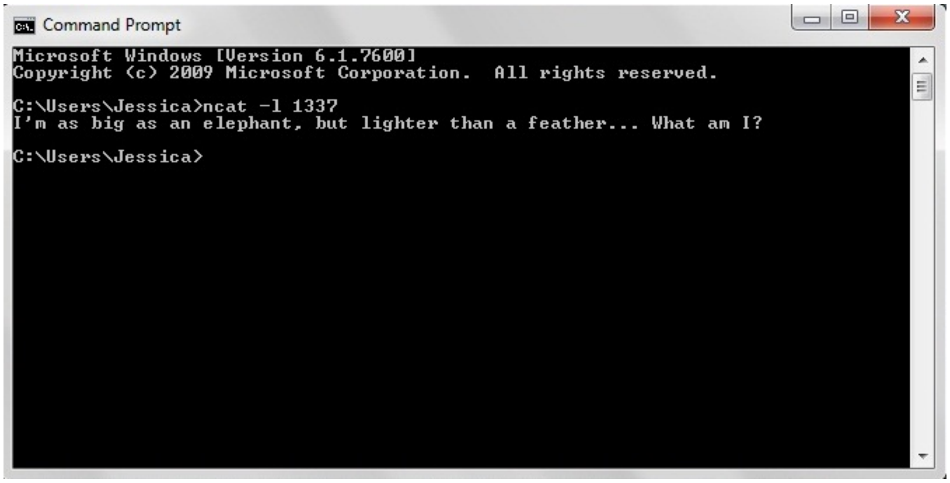
5. On the “instigating” computer, type “nc [IP Address of the “listening” computer] <[name of the file created in step 1].” This will send contents of the file over the connection of port 1337.



```
guest1@jolicloud:~$ cat RiddleMeThis
I'm as big as an elephant, but lighter than a feather... What am I?
guest1@jolicloud:~$ nc 192.168.0.4 1337 < RiddleMeThis
```

Figure 11: “Instigating” Computer Terminal

6. The text of the file created should appear in the terminal window of the “listening” computer.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Jessica>ncat -l 1337
I'm as big as an elephant, but lighter than a feather... What am I?

C:\Users\Jessica>
```

Figure 11: File Text on “Listening” Computer

7. Once the text has been received, the connection will be closed on the “listening” computer.

8. This concludes the experiment.

While transferring files from one computer to the next might not be of great importance or use, the concept behind the transfer is necessary to understand the interworkings of other, more common events. The concept can be applied to the transferring of a computer virus or malicious code to a computer through an open port without the knowledge of the user.

6 Conclusion

Once the discovery part of a computer investigation has finished, the computer forensics expert is almost finished. Information is gathered and sent of to the appropriate persons involved in the case. Sometimes, undesired or unforeseeable conclusions are reached, which could weigh in heavily in determining the outcome of the case.

6.1 The Roommate Who Couldn't Be Trusted

While some information was found during the investigation, the specificity of the evidence is debatable. Though the deleted printer and fax logs showed that Jason had used Tim's computer while he was away, there was not enough evidence to formally accuse Jason of printing and sending incriminating documents to their employer. The ruling in Tim's case is unknown and irrelevant for the purpose this case serves in this paper. This cases demonstrated how important it is to know what is being looked for and what information is actually important. Just because evidence exists, does not necessarily mean it is the right evidence or that it will benefit a particular side in the case [19].

6.2 Too Close For Comfort

Finally, after wading through countless data entries and files, the answer to Mary's initial question could be answered. It was inferred that in the system restore, the instances of the program showed that once he had gained access, the boy installed a "prepackaged hacking and exploit program, streamed the files back to his computer, ensuring that his presence would be kept his secret [18]." The information was given to the respective authorities and the case took an unexpected turn. Because the IP addresses were dynamic, the company who owned each of them was constantly turning over the numbers and switching the users. Since there was no name directly associated with the IP addresses found on Mary's computer, a subpoena was needed to see if these were in fact the boy's IP address. When law enforcement received the list of names from the company, they went to arrest the owner of the IP address. After arriving at the house, they quickly realized this was not the boy in Mary's class. The boy had used this person's IP address, and worked through it, to accomplish his spying on Mary. Law enforcement ruled that more than likely the boy had gotten into this person's computer and then into Mary's. In the end Mary was able to keep her job and the boy was transfered out of Mary's class [18].

6.3 General Cases

After the discovery process has finished, the hard drive or computer is sent back to the respective person from which it came. It is then determined to what degree the evidence found will support the client's claim. Sometimes the evidence is not conclusive enough and the computer forensics expert must make this known. While the computer forensics expert is working for a client, it is not always a guarantee that the discovery will yield information that is helpful. In fact, some information can actually hurt the client or not be of any legal use at all. At the end of the investigation it is important to remember that it is not the job of the computer forensics expert to convict or acquit the client based on what they have found; there job is to only tell the truth about the data and information collected. From that point, the burden of conviction falls on the jury or judge to decide the outcome of the entire case.

6.4 Possible Applications of Computer Forensics

A recent study conducted by the Pew Research Center found that "48% of all adults who use the Internet...say they usually need someone else to set up a new device for them or show them how to use it" [24]. Based on this statistic, it can be assumed that many adults are therefore unfamiliar with the computer hardware they use each time they are using the Internet. Furthermore, if an individual is using a device they do not have a working understanding of, it would be difficult for the individual to protect themselves.

Computer forensics can be a great way to educate the public and general computer users on good computer security techniques. Both of these cases discussed in this paper happened to real people, and the events that unfolded in each story probably have happened again, and will continue to happen, unless people start taking responsibility for their computer usage. In the future, more criminals will shy away from the in-person attacks and welcome the anonymity of computer attacks. It is only when the public can understand basic computer concepts, coupled with real world scenarios, that we, as a society, will be able to comprehend the necessity and importance of responsible computer usage.

In addition to protection, computer forensics can be used to educate the public on how files work, how systems handle deletion of files, and how computers are only as powerful as they are allowed to be. The public would benefit from the knowledge that computer forensics tools can offer by applying general knowledge of computer forensics to specific cases. Through real world application, general computer users can see how computer forensics is not simply used by law enforcement and private investigators, but a methodology that can educate everyone in computer security, computer hardware, and general computer concepts.

References

[1] http://www.cs.uic.edu/~jbell/CourseNotes/OperatingSystems/images/Chapter12/12_01_DiskMechanism.jpg.

Picture of a hard drive mechanism.

[2] http://blog.wisefaq.com/wp-content/uploads/2010/08/DariksBootandNuke2.2.6Beta.png.

Picture of Darik's Boot and Nuke program.

[3] "About wireshark," http://www.wireshark.org/about.html.

Article providing general facts about Wireshark program.

[4] "Partition hard drive," http://www.howtopartitionaharddrive.net/wp-content/uploads/2011/09/partition-hard-drive.jpg.

Picture of a partitioned hard drive.

[5] "Sniffer," http://www.webopedia.com/TERM/S/sniffer.html.

Webpage providing the definition of a sniffer.

[6] "What is netcat," http://netcat.sourceforge.net/.

Webpage providing the information regarding Netcat

[7] "Computer forensics incident response essentials," 2002.

Book detailing basic computer forensics procedure and background.

[8] "Norton ghost users guide," ftp://ftp.symantec.com/public/english_us_canada/products/ghost/manuals/ghost2003_guide.pdf, 2002.

Norton Ghost User Guide providing more information on Norton Ghost.

[9] "Sasser worm hits uk's coastguard network, sophos reports," http://www.sophos.com/en-us/press-office/press-releases/2004/05/va_sassercoast.aspx, 2004.

Article about Sasser attack on United Kingdom Coastguard.

[10] "Serial ata: Meeting storage needs today and tomorrow," http://www.serialata.org/documents/SATA-Rev-30-Presentation.pdf, 2009.

Presentation describing SATA advantages and statistics.

[11] "Interesting internet statistics and facts video," http://www.techmynd.com/interesting-internet-web-statistics-facts/, 2010.

Webpage and video providing facts about the Internet.

[12] "The essential guide to home computer security," http://proquest.safaribooksonline.com.ezproxy.lib.calpoly.edu/9781906124694/firstchapter?query=(((sasser+worm)))&reader=html&imagepage=#X2ludGVybmFsX0ZsYXNoUmVhZGVyP3htbGlkPTk3ODE5MDYxMjQ2OTQvY2gwNl9zZWMwMV
=, 2011.

Article detailing preliminary knowledge of Sasser Worm.

[13] "Hack attack delayed iran's nuclear work: report," http://www.cbc.ca/news/world/story/2011/01/16/israel-iran-nuclear.html, January 2011.

Article from CBC News detailing Israel's Stuxnet Worm.

[14] "Write blockers," http://www.forensicswiki.org/wiki/Write_Blockers, 2011.

Article providing information about write blockers.

[15] "Encase foresnic v7," http://www.guidancesoftware.com/forensic.htm, 2012.

Article providing information about EnCase Software.

[16] "Openbsd reference manual," http://www.openbsd.org/cgi-bin/man.cgi?query=nc, 2012.

Man page regarding "nc" command, i.e. Netcat

[17] "Port scanning," http://www.webopedia.com/TERM/P/port_scanning.html, 2012.

Article providing the definition of port scanning.

[18] S. Burgess, "The case of the teacher and the trickster," http://burgessforensics.com/CSI9_teacher_trickster.php, 2009.

Article from Burgess Forensics.

[19] ——, "The case of the unappreciated underling," http://burgessforensics.com/CSI14-unappreciated_underling.php, 2010.

Article from Burgess Forensics.

[20] E. Conrad, "Cissp study guide," http://proquest.safaribooksonline.com.ezproxy.lib.calpoly.edu/9781597495639/ch06lev1sec6?query=(((sasser+worm)OR(uk+coastguard)))&reader=html&imagepage=, 2011.

Article detailing preliminary knowledge of Sasser Worm.

[21] Errant, "Portable forensic tableau," http://en.wikipedia.org/wiki/File:Portable_forensic_tableau.JPG, 2010.

Picture of a write blocker setup.

[22] S. Hailey, "What is computer forensics?" http://www.csisite.net/forensics.htm, September 2003.

Article from Cyber Security Institute on general Computer Forensics knowledge.

[23] J. N. Hoover, "Anonymous continues barrage of government hacks," http://www.informationweek.com/news/government/security/232800504, 2012.

Article from Information Week detailing recent computer hacking by Anonymous.

[24] J. B. Horrigan, "When technology fails," http://pewresearch.org/pubs/1036/, 2008.

Article from The Pew Research Center regarding computer literacy.

[25] E. A. Taub, "Deleting may be easy, but your hard drive still tells all," http://www.nytimes.com/2006/04/05/technology/techspecial4/05forensic.html?_r=2&ref=techspecial4, April 2006.

Article from New York Times discussing EnCase and its impact in computer forensics.