University of Louisville

ThinkIR: The University of Louisville's Institutional Repository

Electronic Theses and Dissertations

8-2006

Computer forensics methodology and praxis.

Robin Cincinnatis Morrison 1975-
University of Louisville

Recommended Citation

Morrison, Robin Cincinnatis 1975-, "Computer forensics methodology and praxis." (2006). *Electronic Theses and Dissertations.* Paper 1011.
https://doi.org/10.18297/etd/1011

COMPUTER FORENSICS METHODOLOGY AND PRAXIS

By

Robin Cincinnatis Morrison
B.S., University of Louisville, 1999

A Thesis
Submitted to the Faculty of the
University of Louisville
Speed School of Engineering
in Partial Fulfillment of the Requirements
for the Professional Degree of

MASTER OF ENGINEERING

Department of Computer Engineering and Computer Science
Speed School of Engineering
University of Louisville
Louisville, KY

August 2006

COMPUTER FORENSICS METHODOLOGY AND PRAXIS

By

Robin Cincinnatis Morrison
B.S., University of Louisville, 1999

A Thesis Approved On:

28 July 2006

by the following Thesis Committee:

____
Adel Elmaghraby, Ph.D., Thesis Director

____
Ibrahim Imam, Ph.D.

____
Michael Losavio, J.D.

____
Julius Wong, Ph.D.

ACKNOWLEDGMENTS

I would like to say thank you to my distinguished committee members, especially Dr. Elmaghraby. This man has the limitless patience to be able to put up with me for the past thirteen years and for this I am grateful.

I would also like to thank my family for pushing me over the years to finish what I started. I am sorry for all the times that I may have been moody and not want to interact with you. I hope you now understand why.

I want to thank Elizabeth West for all the time she has put in to this project by proofreading, editing, and correcting my grammar. You are not only an unbelievable teacher, wife, and mother, but you are a wonderful human being. There is no way I could have completed this thesis without your help.

I want to thank Dr. Perry Johnson for his pushing me to finish by instilling a sense of urgency and competitiveness in me.

And for those of you I promised a mention, here it is: Clifford Kinniard, Jeremy Smith, Jeff Sosebee, Jey Thomas, Greg Crowe, Larry Smith, and Sean McCreary. Ha! I did it!

ABSTRACT

COMPUTER FORENSICS METHODOLOGY AND PRAXIS

Robin C. Morrison

28 July 2006

This thesis lays the groundwork for creation of a graduate-level computer forensics course. It begins with an introduction explaining how computing has invaded modern life and explains what computer forensics is and its necessity. The thesis then argues why universities need to be at the forefront of educating students in the science of computer forensics as opposed to proprietary education courses and the benefits to law enforcement agencies of having a computer scientist perform forensic analyses. It continues to detail what computer forensics is and is not. The thesis then addresses legal issues and the motivation for the topic. Following this section is a review of current literature pertaining to the topic. The last half of the thesis lays a groundwork for design of a computer forensics course at the graduate level by detailing a methodology to implement which contains associated laboratory praxis for the students to follow.

TABLE OF CONTENTS

PAGE

CHAPTER I

INTRODUCTION AND BACKGROUND

Computing in Modern Life

Computers have permeated almost every aspect of modern life. Their benefits are innumerable. Computers have automated manufacturing processes, sped delivery of goods, enhanced shopping options, made cross-planetary communications virtually instant, and even saved lives through online sharing of medical information. Information is much more easily accessible than in the not-so-distant past and has reduced research time and travel immensely. However, with the rise in the benefits of computing has come the rise of the darker side of computing. In Taoist philosophy, this would be represented by the yin-yang symbol.

Unfortunately, criminals have benefited from technological advancements in computing. Computers have made it much easier to steal trade secrets from companies and have even caused grave threats to national security. Since global communications are controlled by computers, they can also be disrupted by computers. Law Enforcement has a much more difficult time catching illegal bookmakers because in the past, the bookmakers would have volumes of paper with clients and bets, but now this information can easily be stored and hidden on removable media. Organized crime does not have to keep large accounting registries of their activities. They merely need an electronic spreadsheet and relational databases. In fact, one of the fastest growing crimes, identity theft, was not nearly as common before the advent of the Internet boom of the mid-1990s. For as long as there will be computers, there will be people and organizations that use them in criminal activities.

Computers can also be used in civil disputes. A woman divorcing her husband for his infidelities may have proof of his relationships from their home computer. A company being sued for wrongful termination by a former employee may base their defense on the employee's misuse of their computer systems. A person being sued by the Recording Industry Association of America (R.I.A.A.) may be able to verify his or her claims of innocence by the information stored on their computer.

There is a common thread binding these scenarios together: the ability to extract digital information from computer media and the ability to present it in a useful form in a court of law. This method of investigation is known as computer forensics.

Why Computer Forensics?

Is computer forensics a necessary field in the Information Age? Although not a focal point of the overall reporting, several high profile news stories this decade have shown computer forensics to have played a major part in investigations. A woman by the name of Chondra Levy, who was an intern for California Congressman Gary Condit, disappeared seemingly without a trace. In the year 2000, the police forensically examined the information stored on her computer. From the information gained, they were led to search a local park near her home where they found her remains.

In 2001, the Enron scandal broke. By forensically analyzing computers owned by the corporation, federal investigators were able to assess the large scope of the crimes committed by the leaders of the company and secure many convictions. In conjunction with the criminal investigation of the activities at Enron, many civil lawsuits against the corporation have begun.

In December 2004, a Kansas woman brutally murdered a Missouri woman, cutting her unborn baby out of her body and taking the living child with her. Law Enforcement forensically analyzed the computers of both victim and perpetrator and concluded that they had known each other and that this escalated from a case of a random act of violence into a case of premeditated murder. Without a doubt, computer forensics has proven itself to be a vital discipline in these cases. In addition to these very dramatic examples, there are many more lower profile cases on a daily basis that warrant the use of computer forensics in their investigations.

Why Lab-Based Instruction in Computer Forensics?

Why is there a need for lab-based computer forensics training? I have spent the last six years of my life teaching various aspects of computing at a proprietary technical college. I have learned from experience, and many studies support my claim, that the best way to learn a computing skill is hands-on training in a laboratory environment. Unfortunately, most major colleges and universities do not actively support this model. The traditional classroom teaching found there, in my opinion, only gives students a theoretical, surface knowledge of the information being conveyed. It is then up to the students themselves, if interested, to conduct experiments relating to the topics from the classroom. Unfortunately, without adequate methodologies, supervision, and equipment these experiments could lead students to form false assumptions and conclusions.

In my experience as an instructor, I have experimented with many different teaching methodologies. By mixing and matching different techniques, I have settled on a methodology that seems to benefit the most types of students, addressing a variety of learning styles. It heavily involves laboratory-based curricula. Over 80% of the teaching and learning is done in a laboratory environment. The other 20% of learning is done in traditional theory sessions alternating between Microsoft Power-Point style slide shows, video presentations, and the traditional writing board.

In the laboratory environment, approximately 60% of the learning is accomplished through instructor-led, hands-on learning and experimentation. Approximately 20% of the learning is done with guided experiments showing the students step-by-step how to accomplish the learning objectives set before them. The final 20% is experimentation in which the student is required to apply the skills already learned with minimal guidance from the instructor.

Since computer forensics is an extremely hands-on and intensive discipline, I believe the most effective method of learning will be the aforementioned method. I am a staunch proponent of learning-by-doing. A student cannot master a skill by only theoretically learning about the topic. They must be able to apply this knowledge, be able to apply it correctly, and base effective conclusions on their solid methodology.

Why Graduate Level University Instruction?

Training in computer forensics usually occurs in two areas: Law Enforcement and proprietary training. Law Enforcement personnel can receive their training at low or no cost through the National White Collar Crime Commission (NW3C). Training for Law Enforcement can also be received from New Technologies International (NTI) for a fee. For the average civilian, the training can be provided, for a large fee, by companies that focus on computer forensics. Digital Intelligence, Guidance Software, Paraben, Forensic-Computers, and NTI are some of the companies that provide such training.

Unfortunately, the average college student who has decided to focus his or her graduate studies on Information Security cannot afford these expensive training courses. Therefore, training needs to be given at the graduate level in a non-proprietary format to equip students with the necessary investigative skills to ensure competence in the field upon graduation. It should allow for easy transition into the corporate world with possibly a junior position in a consulting firm or maybe an entry-level learning position in a major company with its own forensics department.

The university would be an ideal place to train students in the art and science of computer forensics. Unlike proprietary courses, which generally last only three to five days, usually eight hours per day, the courses at the university can last up to fifteen weeks with up to three hours of classroom learning spread over two or three days per week. There is less of a time crunch for students to learn at the university and more time for experimentation. Also, the university can provide much more lab time outside of the classroom for students to learn, whereas proprietary training usually does not allow for out of class learning at their facilities. I have personally attended a proprietary training course and although it was very good, I could have learned more in-depth if I had been allowed to experiment and learn from hands-on practice outside of normal training hours. This is an area in which university training could excel with more attention paid to this matter.

I believe computer forensics training should be reserved for the graduate level only. During undergraduate studies, students are supposed to experience an abundance of Computer Science or Information Technology fields. This is to allow the students to determine if they want to continue their studies in graduate school with focus on one field of specialty. I believe computer forensics to be too narrow of a field to be offered in the vast array of baccalaureate courses. This discipline is highly specialized and would be valid in an overall Information Security focus in graduate studies. I prefer an undergraduate level course in Information/Computer Security that may briefly expose students to computer forensics, but not a specialized course at that level.

My major reason for championing university training is to put more computer forensic analysts in the field with backgrounds in computing. In my discussions with high-ranking employees of firms providing the proprietary training, I have been informed that most of the people attending these training courses are from backgrounds in law enforcement or are currently law enforcement officers. In the course I attended, I was the only student not currently serving in a law enforcement capacity.

The problem I see with this is that most of the forensic analysis of computers is not being done by those who have intimate knowledge of computing systems. Unless these people have studied computer science, I do not believe their knowledge is complete enough to perform thorough forensic analysis. Simple anomalies in a system under analysis that may go undetected by the law enforcement officer could possibly be easily detected by the Computer Science trained investigator. Do not mistake my words. I fully believe most computer forensic analysts in law enforcement do an excellent job. But, I am of the opinion that someone whose background is in Computer Science or Information Technology would make a better analyst. I believe that taking someone whose background is in computing and teaching them the principles of investigation from a law enforcement perspective is easier and more beneficial than taking someone whose background is law enforcement and teaching them computing sciences.

CHAPTER II

EXPLANATION OF TOPIC

What is Computer Forensics?

The term "computer forensics" was coined in 1991 in the first training session held by the International Association of Computer Specialists (IACIS) in Portland, Oregon [Marcella et al., 317]. Computer forensics is the science of acquiring, retrieving, preserving, and presenting data that has been processed electronically and stored on computer media [Schweitzer, 2]. It is "about evidence from computers that is sufficiently reliable to stand up in court and be convincing" [Vacca, 3].

History of Computer Forensics - Historical Computer Crime

To examine the history of computer forensics, we must first examine the history of computer crime. The art of "phreaking", that is exploring the international telephone systems and stealing service, is said to have originated at the University of California at Berkeley in the early 1970s. John T. Draper earned the moniker "Captain Crunch" when he found out that a toy whistle given away in a box of the cereal produced a 2600 Hertz tone. This is the exact same tone that AT&T mechanical telephone switching systems used at that time. He had previously learned that by producing that tone into a phone receiver, he could fool the mechanical computers controlling the lines into believing the request for service was valid, thus allowing him to receive free, albeit stolen, long distance service. This led to creation of "blue boxes" which reproduced the 2600 Hertz tone allowing the user to steal long distance service from AT&T. To defeat these devices, phone companies improved their computer systems. But, the improvement of telephone computer systems has led to new phreaking techniques and tools, such as green boxes, agua boxes, and mauve boxes. Although a phreaker does not directly access the telephone companies' computers, their actions fall under the categories of telecommunications and computer crimes.

One of the first publicized cases of computer crime also did not directly involve computers. In 1978, Stanley Mark Rifkin defrauded Security Pacific National Bank of US$10,200,000 by using a common technique known as social engineering. The funds were computer transferred to a Swiss bank account, thus creating one of the earliest cases of computer fraud. His caper eventually made it into the pages of the *Guinness Book of World Records* in the category of "biggest computer fraud" [Mitnick & Simon, 6].

Probably the first major event that would show the world the potential of direct computer crimes occurred in 1986. Marjie T. Britz describes what happened in her book *Computer Forensics and Cyber Crime: An Introduction.*

> ...an accounting error of less than one dollar was investigated by a dedicated employee at the University of California at Berkeley. This internal investigation revealed that a German hacker in the employ of the KGB had tapped into a military database and obtained sensitive (but not classified) information. Using only a personal computer and a basic modem, this individual was able to connect to Berkeley computers via an independent data carrier (i.e., Tymnet). Once connected, the hacker was able to move about the MILNET system with remarkable ease and relative impunity. The fact that such vulnerability existed within data systems was especially disconcerting to administrators because of its almost accidental discovery...his findings resulted in the recognition of information risks associated with open systems [Britz, 34].

The entire account of this story has been written by the man directly involved in this game of cloak and dagger. Clifford Stoll's book “The Cuckoo's Egg” is a recommended book on the reading list for those wishing to pursue the International Information Systems Forensics Association's Certified Information Forensics Investigator (IISFA CIFI) certification.

In 1988, Robert Morris, a graduate student at Cornell University, rocked the computing world by releasing the first Internet worm. By making use of a vulnerability in UNIX, his worm successfully staged a buffer overflow attack to crash computers world-wide. The dubbed "Morris worm" "crippled over 6,000 computers and caused between $5 and $100 million in damages" [Britz, 35]. Six thousand does not sound like many computers. But in 1988, this was approximately ten percent of all computers on the Internet. When viewed in this context, one can see the impact that the "Morris worm" had. For his crimes, Morris was convicted of violating the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. Although he did not serve prison time, Morris was sentenced to probation and community service, and he had to pay hefty fines.

Law Enforcement Strikes Back

In the mid- to late-1980s, Law Enforcement and military agencies decided that computer and computer-based crime was beginning to exert a negative influence upon computing and aspects of business and finance. These agencies wanted to be able to pool their resources to be able to combat these new crimes that were becoming more commonplace. They needed to merge investigative skills honed over centuries with rapidly emerging and changing technology.

One of the first groups formed to combat computer crime was the High Technology Crime Investigation Association. In 1984, several members of the Santa Clara County Industrial Security Manager's Group, including John O'Loughlin (now retired but security manager at Intel at that time and later Sun Microsystems) and Pete Kostner, security manager at AMD, approached Santa Clara County District Attorney Leo Himmelsbach to discuss the need for having law enforcement officers trained in the field of high technology crime. Leo Himmelsbach then applied to the State of California and received a grant from the Office of Criminal Justice Planning Project approved by the Calif State Assembly, State Assembly Bill 1078 passed into law August 31, 1984, Penal Code Section 13970 called " SANTA CLARA COUNTY DISTRICT ATTORNEY'S HIGH TECHNOLOGY CRIME PREVENTION PROGRAM" [Smith]. Today it has grown into an international organization of law enforcement agencies, attorneys, and management level and senior staff security professionals (read CIO or CISO) that "is designed to encourage, promote, aid and effect the voluntary interchange of data, information, experience, ideas and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership” [HTCIA].

It was around this time (1984) that the FBI was beginning to sit up and take notice of computer crimes. To properly address the growing demands of investigators and prosecutors in a structured and programmatic manner, the FBI established the Computer Analysis and Response Team (CART) and charged it with the responsibility for computer analysis [FBI].

In 1990, the International Association of Computer Investigative Specialists was “formed to provide training to law enforcement personnel regarding computer forensics and high technology crime” [IACIS]. This organization is committed to promoting training and sharing of techniques and information between law enforcement agencies.

In 1993, the first International Conference on Computer Evidence was hosted by the FBI in which many law enforcement agencies worldwide attended. It was such a success that it eventually led to the 1995 formation of the International Organization on Computer Evidence. The IOCE was tasked with creating a uniform standard to be followed worldwide concerning digital evidence in 1998. The reasoning behind this was to ensure that evidence would be gathered in a like manner internationally and that it would be acceptable in courts regardless of their jurisdiction. The first findings were released for review in 2000 and are being reevaluated and updated as necessary on a regular basis.

Although law enforcement agencies are banding together and attempting to stay ahead of the curve when dealing with modern computer crime, they need the help of civilian computer experts trained in computer forensics. Rapidly changing and modern forms of computer crime is one major reason why.

Modern Computer Forensics - Modern Computer Crime

Modern computer crime can usually be divided into two categories: computer crime and computer-based crime. Computer crimes are crimes committed against computer systems. Computer-based crimes are crimes in which a computer was involved in the commission of the crime.

Computer crimes have drastically evolved from their reported 1986 origins. Worms, viruses, and Trojan horses have become more sophisticated as the computer systems on which they are launched have evolved. Melissa, I Love You, Code Red, Nimda, Blaster, and other malware caused ripples of concern in the major computing circles and widespread panic in the home-based PC market. Propagation of Trojan horses such as SubSeven and BackOrifice have compromised many systems such as those of the Apache Foundation, creator of the most widely-used httpd server. With the rise of the popularity of the World Wide Web has come the hacking and defacing of web sites. One of the more notable incidents was the defacing of the website of the New York Times by the gray-hat hacker Adrian Lamo. Finally, theft of computer components can fall into this category. Many times in the last decade the Los Alamos National Laboratory has fallen prey to theft of computer hard drives containing nuclear secrets.

Computer-based crime is likely more widespread than reported. Most of these crimes are traditional crimes that have been modernized by computers. Identity theft is a major part of this category. Before modern computing, identity theft was difficult and time consuming. To steal one's identity, the criminal had to start by stealing a valued possession, such as a wallet or purse. From there, one could glean information such as Social Security Number, date of birth, address, and credit card numbers. One could take this information and have a new Social Security card and birth certificate issued, subsequently using those documents to procure government-issued identity documents. These allowed the criminal to open lines of credit with retailers in the victim's name and fleece both retailer and credit company. Modern identity theft is much easier. Most victims willingly give their information through social engineering and phishing techniques. It is now possible to steal the identities of many people rapidly with little or no effort.

Another ancient crime that has become much easier to perpetrate with the increase of Internet presence into everyday life is the propagation of scams. One of the most common scams found on the Internet is the Nigerian 419 scam, named after the section of the Nigerian criminal code that this type of crime falls under. A con artist no longer needs to meet their victims face-to-face or try to create a working relationship with them to part them from their money. All that is necessary is sending an email to the intended victim asking them to participate in a get-rich-quick scheme, usually the transfer of large sums of money from Nigeria into their local bank account. The intended victim gets to keep a percentage of the money, usually in the millions of U.S. dollars, for helping get the money out of Africa. All that is necessary is sending your personal bank account information to the person who contacted you. Unfortunately, too many people, mainly senior citizens, have fallen prey to this type of scam.

Yet another major neo-traditional crime that has become much easier with modern computers and the Internet is child pornography. No longer is it necessary for child pornographers to peddle their disgusting wares through seedy fly-by-night mail order companies or in legitimate adult bookstores in which knowing a special code phrase or secret handshake will get pedophiles the filth they want. The Internet has made the delivery of child pornography rapidly available to those who seek it. In fact, the North American Man/Boy Love Association (NAMBLA) has a web site that encourages the legalization of child pornography and sex between adults and children. What was once an underground movement has <u>almost</u> become mainstream and legitimized because of the Internet.

Other traditional crimes that have become modernized due to computers are illegal bookmaking, racketeering, counterfeiting, forgery, insider trading, and embezzlement (such as the salami slicing technique that was first introduced to most people in the movies *Superman III* and *Office Space*). New types of crimes have sprung up directly related to computing. Cybersquatting is the practice of buying Internet domain names belonging to companies or famous people and then trying to sell them to said organizations for an unbelievable mark-up in price or just not allowing ownership of them by those who should legitimately have ownership rights. This has been outlawed by Congressional legislation. Cyberstalking and cyberharassment have moved the traditional crime of stalking or harassing someone into a virtual realm. The cyberstalker can harass their victim almost anonymously to the point in which the victim no longer wants to use a computer. Online pharmacies are supposedly selling prescription drugs to people who want them by having a phony doctor write them an online prescription without a physical consultation and having them filled and shipped to their home illegally. Finally, the most common computer-based crime, as it was recently outlawed, is the dissemination of spam. Spam is unwanted email, usually in large volumes. Everyone who has an email address has fallen victim to spammers.

Forensically Combating Modern Computer Crime

The problem with committing crimes of any nature, especially computer crimes, is the fact that evidence of the crime is always left behind. No matter how great the cover-up of a computer crime, with enough determination and with the appropriate tools virtually all computer crimes can be solved. Does this necessarily mean that a perpetrator will be convicted or if someone will even be captured? No. But the evidence found should point to the fact that some sort of crime was committed.

How can we combat modern computer crime using computer forensics? Computer forensics is an after the fact (ex post facto in legal terms) process. If the process is performed after the fact, how can it be used to fight crime? First, computer forensics can be used to secure digital evidence that a crime has committed and can be entered into court proceedings as circumstantial evidence. As far as I know, no one has ever been convicted on computer evidence alone. However, many criminals have been convicted by the computer evidence in conjunction with volumes of other evidence. Second, computer forensics can be used to validate the source of a crime being committed, whether it be human or machine. Third, computer forensics can be used to promote awareness of the power of information and how it can used and misused by average people. Finally, computer forensics can be used to learn about new forms of Internet-based attacks before they are common knowledge. By implementing computer systems such as honeypots and analyzing them frequently, we are able to identify new attacks and create fixes or patches for them so that when they become commonplace, they will be easily defeated or eradicated.

Computer Forensics vs. Computers in Forensics

Computer forensics, as stated previously, is the art and science of examining computer media for digital evidence to be useful in a court of law. There is a difference between computer forensics and computers in forensics. One way computers can be used in forensics is through software forensics. The purpose of software forensics is not to look for general digital evidence for court proceedings. Software forensics is mostly concerned with examining malware. By analyzing a piece of malware, the software forensics analyst is attempting to determine certain aspects concerning the software. Discovering information such as how the code was written, how it behaves, how it propagates, and ideally identifying the person(s) who created it are the major goals of software forensics. Although computers must be used in this area of forensics, it is not computer forensics.

Next, an example of computers in forensics is the Echelon system. The Echelon system is the computer system used by the United States and allies to listen to wireless (and some say wired) phone conversations and computer traffic around the world. It roughly works this way: the National Security Agency (NSA) created an algorithm known as *Semantic Forests*. It was then licensed to Raytheon

Company. Raytheon uses this algorithm as a basis for its commercial product, SilentRunner. Raytheon then leased SilentRunner back to the NSA. SilentRunner is then implemented on Echelon's computer systems. All phone conversations intercepted by Echelon are recorded and computer transcribed into text documents. SilentRunner has been programmed to "understand" the meaning of the message as opposed to just keyword searching a document. "...they (the NSA) wanted the computer to be able to "think," and be able to interpret the contextual meaning of a document, just as a human brain would interpret the nuances of a written communication" [Anastasi, 217]. Therefore, the computer forensically analyzes the conversation and determines its meaning. Many terrorist coded messages have been intercepted and cracked using this method. Although this is a good example of computers in forensics, it is not computer forensics.

Finally, computers can be used in forensic examinations conducted by investigative laboratories. Popularized by television programs such as *CSI*, viewers can see how computers are beneficial to forensic investigations. One recent episode showed how a computer could create a mirror image of a photograph and combine that image with the original to form a new image. Although an example of computers in forensics, it is definitely not computer forensics.

CHAPTER III

LEGAL ISSUES IN COMPUTER FORENSICS

Disclaimer: I am not an attorney and am not offering legal advice on any matters in this section of the thesis. Do not accept my opinions as legitimate legal opinions. By reading this section you agree not to hold the author nor the University of Louisville responsible for any actions taken by the reader in accordance with the information listed in Chapter III.

U.S. Constitution Fourth Amendment Rights

Many people are worried today that their individual rights and right-to-privacy are being eroded by the state. Although this is the opinion of some, there are still many protections available to citizens. The first line of protection from government intrusion is the Fourth Amendment to the Constitution: 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 [Archives]. Obviously the Founding Fathers of our nation had no concept of computers when they wrote the Bill of Rights in the late 18th century. Yet, these general protections do apply to our computers and information in the 21st century. In a rough summary, a warrant is necessary to be sworn out to seize and search a computer by an agent acting on the behalf of the government with some exceptions:

- Consent: If the owner of the computer agrees to allow the seizing and/or searching of the machine, then no warrant is necessary.
- Third-Party Consent: If the computer is routinely used by a group of individuals, then any of the regular users may give consent. If the computer is also used by a spouse or domestic partner, that person may give consent. If the computer is owned by a minor, the minor's parents may give consent. If the computer belongs to a private network (e.g. in the workplace), a system administrator may give consent.
- Implied Consent: If the owner of a computer has voluntarily given up parts of their 4th Amendment rights (such as in terms of employment) then the consent to search and seizure may be implied.
- Exigent Circumstances: Exigent circumstances apply when it is necessary to search and seize if an agent of the government believes that it must be done to prevent the imminent destruction of data. This is usually difficult to prove ex post facto; therefore it is advantageous to get a warrant in this situation.

- Plain View: If a crime is committed with a computer in plain view of an agent of the government, a warrant is not necessary to seize the computer on which the crime was committed nor one needed for the subsequent searching of data. The plain view doctrine does not authorize agents to open and view the contents of a computer file that they are not otherwise authorized to open and review [S&S].
- Search Incident to a Lawful Arrest: If you are in possession of an electronic device (such as a pager or PDA) at the time of your arrest, a government agent may be able to seize the device and search it without a warrant.
- Border Searches: If someone is attempting to import an electronic device such as a computer into the U.S. from a foreign country, the government has the right to search and seize these devices without warrant.

(Each bulleted topic comes directly from [S&S]. The summations are my own except where annotated.)

The preeminent question concerning the Fourth Amendment is this: How does it directly apply to computer forensics? Whether we are directly an agent of the government (such as a law enforcement officer) or an acting agent of the government (such as a private contractor to a law enforcement agency), we must abide by the restrictions placed upon us by the Fourth Amendment. We must abide by the terms of the warrant that specify exactly what we are allowed to seize and search pertaining to computer systems. If no warrant was executed, then we must make sure we are within the narrow bounds of the warrant-less exceptions. We should do this by receiving a written legal opinion from the appropriate government agent stating that the search met the warrant-less criteria and that our forensic analysis does not violate the Fourth Amendment rights of the computer's owner.

Non-Government Agent Searches

Unfortunately, your rights under the Fourth Amendment do not apply when search and seizure is performed by a non-government agent. A non-government agent is one that is not directly an agent of government (e.g. law enforcement) or acting upon the behalf of a government agency. Generally, searches in this section pertain to matters of tort law, also known as civil law or civil matters. In these arenas, subpoenas are usually issued as a method of forcing someone to turn over a computer for searching. The forensics examiner must make sure that any subpoenaed computers are examined as if there was a search warrant issued and take care to follow the proper guidelines.

When involving matters of the workplace, the seizure and searching of computers can be a tricky matter. Usually consent for an investigation is given by the owner (most times the company) of the computers. In accordance with most corporate end-user agreements, an employee waives their right of privacy pertaining to usage of the company's computer systems. There is a thin line, though, concerning what information can be seized and used in civil matters. There is debate in the courts and the legal community about personal information stored on these computers and the gray area of violating one's privacy. What information is considered personal and what is considered company property? Even if a voice mail system is company property, the contents of the voice mails themselves may not be. It depends on the jurisdiction as to how they interpret these quandaries. For the forensic examiner, it is best to produce all possible information and allow the attorneys to sort out the legal issues. Nevertheless, since the analyst will probably be called to testify, it is best to at least have some knowledge of how the local court system views these issues.

U.S.A. Patriot Act of 2001

As it pertains to cybercrime, the U.S.A. Patriot Act of 2001 has redefined many provisions in current statutory law of the U.S. Code that either pertain directly or indirectly to our forensics investigations. In summary:

> Section 814 makes a number of changes to improve 18 U.S.C. § 1030, the Computer Fraud and Abuse Act. This section increases penalties for hackers who damage protected computers (from a maximum of 10 years to a maximum of 20 years); clarifies the *mens rea* required for such offenses to make explicit that a hacker need only intend damage, not a particular *type* of damage; adds a new offense for damaging computers used for national security or criminal justice; expands the coverage of the statute to include computers in foreign countries so long as there is an effect on U.S. interstate or foreign commerce; counts state convictions as "prior offenses" for purpose of recidivist sentencing enhancements; and allows losses to several computers from a hacker's course of conduct to be aggregated for purposes of meeting the $5,000 jurisdictional threshold. [USAPA2001]

These changes indirectly affect our forensic investigations. Specifically, if in the course of our analysis we determine that someone has illegally gained access to the system *with the intent to damage* the computer, a whole host of penalties may be enacted upon that person. Thus, it is no longer necessary to prove that specific damage was done to a computer (e.g. data destruction or theft of intellectual property) but that the intruder's intent was to damage the computer. This affects the scope of the investigation because now the forensic examiner must now only determine that an intrusion was made with the idea of damaging the computer instead of actually proving that damage was done. This technically releases a lot of investigative burden from the examiner.

As a side note, I am personally mortified by how broadly this concept has been written into the law and how even more broadly the law can be interpreted. How is it possible to know a person's exact motive in relation to accessing a computer? Some signs of intent can be evident such as unauthorized creation of user accounts and log file editing to remove traces of sessions. But where does the interpretation of the law end? I foresee the possibility of using this provision of the Patriot Act to levy penalties upon what we generally would refer to as "innocent mistakes." For example, someone mistakenly logs into a system without authorization (I have heard of it happening many times before with some systems using auto-login utilities) and when realizing their mistake end the session. This unauthorized entry can easily be misconstrued as an attempt to damage a system by hypersensitive network administrators and criminal charges can be filed against the perpetrator. Also frightening is the classification of specific computers as being used for national security or criminal justice. In combination with the intent to damage, further penalties can be levied against someone making an "innocent mistake" if the computer has been labeled as "used for national security or criminal justice." Since there is not really a definite standard for labeling a computer in this manner, anyone can arbitrarily determine that a computer is to be labeled in this manner. When you happen to access most computer systems, they usually do not identify their purpose to the user. Therefore, a prosecuting attorney could, at a later time, label a computer in such a manner as to levy more penalties upon a defendant.

There are some positive aspects to the Patriot Act. Section 816 requires the Attorney General to establish such regional computer forensic laboratories as he considers appropriate, and to provide support for existing computer forensic laboratories, to enable them to provide certain forensic and training capabilities. The provision also authorizes the spending of money to support those laboratories [USAPA2001]. This is gainful as the University of Louisville is a direct beneficiary of this provision.

Other U.S. Statutes Pertaining to Computer Crimes

There are a few other federal statutes that computer forensics examiners must be aware of since the information that is gathered may fall directly under the jurisdiction of the following laws:

- 18 USC § 1030 Fraud and Related Activity in Connection with Computers: This law pertains to the unauthorized access of computers used by the U.S. government or financial institutions.
- 18 USC § 2701 Unlawful Access to Stored Communications: This law pertains to the unauthorized access of email communications that reside in a storage medium. In other words, if you steal or access emails that are stored on a hard drive, CD/DVD ROM disc, floppy disk, etc., and destroy or alter them, you are in violation of this statute.

How these laws affect a forensics analyst is by placing the burden of finding proof on us. If someone is charged under either one of these statutes, the examiner must produce the proof if any exists.

There are other statutes that pertain to computer crimes but would not fall directly into the scope of this thesis. Pertaining to the U.S.A. Patriot Act of 2001 and the above sections of the U.S. Code, it should be evident that more technology-savvy people are needed to help craft future laws concerning computers.

State and Local Regulations Concerning Computer Crime and Individual Rights

The Commonwealth of Kentucky has a multitude of laws in its Kentucky Revised Statutes that pertain to computer crimes:

- KRS 434.845 Unlawful Access to a Computer in the First Degree.
- KRS 434.850 Unlawful Access to a Computer in the Second Degree.
- KRS 434.851 Unlawful Access to a Computer in the Third Degree.
- KRS 434.853 Unlawful Access to a Computer in the Fourth Degree.
- KRS 434.855 Misuse of Computer Information
- KRS 510.155 Unlawful Use of Electronic Means to Induce a Minor to Engage in Sexual or Other Prohibited Activities -- Prohibition of Multiple Convictions Arising From Single Course of Conduct.

These statutes place the burden on the examiner to produce evidence, if any. For KRS 434.845, .850, .851, and .853 the analyst must determine if unlawful access was obtained and what damage was done. It is then up to the Commonwealth's attorney to decide under which statute to pursue charges. For KRS 434.855, .845 must first be violated and the information is either stolen or received. KRS 510.155 pertains to chatting up a minor on the Internet for purposes of sexual acts being committed by or on said minor. This provision also covers state government agents posing as minors on the Internet. Since chat logs can be stored on a hard drive (and most are), the forensics examiner must produce any evidence relating to violation of this statute.

From what I can gather from the web pages of the Louisville Metro government (http://www.louisvilleky.gov/MetroCouncil/default.htm), it apparently defaults to KRS law concerning computer crimes as I could not find any ordinances pertaining to them.

What is evident is that anyone who wishes to be employed as a computer forensics analyst must be well-versed in the applicable laws surrounding search and seizure. Not only must one have assurance that what actions one performs are legal, but one must be prepared to justify what actions one took and why.

CHAPTER IV

MOTIVATION FOR TOPIC

Why are Forensic Analysts Necessary?

The need for forensic analysts is four-fold. First, with the advent of inexpensive personal computers it has become easy to own one. Personal computers are no longer only in the possession of the wealthy or universities. Many households have at least one, if not many, computers. Internet access is also becoming cheaper. Gone are the days of Internet access being limited to those who could afford the per-minute charges of dial-up access. It is now cheaper to have a 6 Mb/s Internet connection than basic cable television. The combination of cheaper and faster personal computers coupled with cheaper and faster Internet access has created an environment in which computer-related crime has become rampant.

Next, the number of companies who have become computer-oriented has dramatically risen in the last decade. Most companies today that do not have an Internet presence cannot compete with those who do. Internally, companies have also replaced archaic manual work practices with modern computer-based practices. The popularity of relational database management systems (RDBMS) by vendors such as Oracle, IBM, and Microsoft are an example of this trend. These RDBMS systems have simplified the storage and retrieval of massive amounts of data by almost entirely eliminating the need for filing cabinets full of irreplaceable combustible paper materials. Drafting and architectural design has almost completely migrated to Computer Aided Drafting (CAD) tools. Due to these advancements, companies have become greatly computer-based. Combine this with having an Internet presence and you have created an environment in which computer-related crime and theft of trade secrets can thrive.

Thirdly, with computer-related crime rising, Law Enforcement is having a much greater time combating this non-traditional criminal field. Most local police departments, save for ones in major metropolitan areas, have neither the manpower nor the time or budget to investigate computer-related crimes. Law Enforcement agencies are generally understaffed and underfunded for investigating traditional crimes and would rather allocate their meager resources to destroying methamphetamine labs, arresting burglary and murder suspects, and policing neighborhoods than tracking down hackers and disgruntled employees. Therefore, no training is given to recruits in tracking computer crimes at most police academies. Most departments who maintain computer crime divisions must spend large sums of money to train seasoned officers to cope with the dynamics of changing digital crimes.

Finally, the reluctance of Law Enforcement to intercede in civil matters is well-known. Information valuable to civil litigation can be stored on computers. The activities of a cheating spouse can possibly be found on a personal computer. Information pertaining to misuse of computer systems by an employee can be beneficial to a company that is the defendant of a wrongful termination lawsuit. By viewing the contents of a computer, a defendant accused of pirating software, movies, or music can prove their innocence or ensure their guilt.

These four situations prove a singular point: computer forensic analysts are necessary. Criminal activity can be buried in computer media. Civil lawsuits can hinge entirely on computer-based information. The only sure-fire method of producing the necessary information for criminal and civil proceedings is through computer forensics. Only a well-trained computer forensics analyst can procure and produce this data and make it stand up in a court of law.

Why is Computer Forensics Training Necessary?

The necessity of computer forensics training is very evident. As a law enforcement tool, it can be invaluable in tying together the activities or associations of suspects or groups. It can also be used by attorneys to establish the fault or prove the innocence of a defendant. Many large companies are now keeping computer forensic analysts on staff to augment their Information Security teams. Some corporations, such as Deloitte & Touche, LLC, even have large, multi-location computer forensics departments that can image and analyze massive volumes of information at many locations given little notice.

Currently, Law Enforcement in general is unable to handle the case load presented by computer crime in addition to traditional criminal activities. The possible steps for the law enforcement community to rectify this situation are to either train their own members to perform computer forensics work, thus removing much needed manpower from traditional sectors, or hire civilians. Although the Federal Government is stepping forward to help Law Enforcement by creating regional forensics centers in major metropolitan areas, eventually this may not be enough. Training civilians willing to work for Law Enforcement in the area of computer forensics must be the solution. In fact, some of the regional forensics centers, initially only staffed by law enforcement officers trained in computer forensics, have had to hire civilians to cope with the overwhelming amount of casework with which they have been presented.

In the civil arena, attorneys will need to hire private, impartial firms to perform computer forensics as necessary. This is usually essential in cases of wrongful termination due to computer misuse. Even if the defendant company has its own internal computer forensic analysis team, a good plaintiff's attorney would be able to raise reasonable doubt concerning the information captured and analyzed by a non-neutral party. Therefore, an ably trained computer forensic analyst who is impartial is crucial.

It is my goal to ensure that computer forensics training is available to not only Law Enforcement but to any competent and educated civilian willing to pursue the field as their career. They must be as passionate about computer forensics as I am and not just consider it a hobby or means to make money. They must be willing to further explore the art and science of it and commit to further research so that the discipline does not become stagnant.

Definition of Thesis Scope

Although the field of computer forensics is wide-ranging, covering topics such as live network capture, raid array analysis, etc., the scope of this thesis is rather narrow. This thesis will focus exclusively on hard drive analysis from machines that are not running when information capture takes place. This is the most common form of computer forensics analysis today. Incorporating a wider field of the types of analysis would only serve to distract from the main focus.

We can further refine our scope by identifying the specific major tasks of our methodology and praxis. In the acquisition phase, we will concentrate on sanitizing media, acquiring data, and chain of custody. In the analysis phase, we will concentrate on finding obvious information, keyword searching, auditing log files, malware detection, file header rectification, NTFS alternate data streams, image processing, and data carving. Finally, in the post-analysis phase, we will concentrate on documentation lifecycle and report writing.

By rather narrowly defining our scope, we should be able to incorporate most necessary tasks used in a forensics analysis and guard against scope creep by staying within the defined guidelines.

CHAPTER V

SURVEY OF LITERATURE

Search and Seizure of Information

A *search* was legally defined by the courts in *State vs Woodall* as “an examination of a man’s house or other buildings or premises, or of his person, or of his vehicle, aircraft, etc., with a view to the discovery of contraband or illicit or stolen property, or some evidence of guilt to be used in the prosecution of a criminal action for some crime or offense with which he is charged” (according to *Black’s Law Dictionary*). A *seizure* was defined in *Molina vs State* as “the act of taking possession of property, e.g., for a violation of law or by virtue of an execution” [of a warrant] [Shinder & Tittel, 588]. These terms define are generally accepted when pertaining to physical items. But how can these terms apply to the concept of information which is an intangible quantity? In other words, how can we search for and seize something that doesn't physically exist? In Chapter III of this thesis, I detailed my interpretation of the rights of search and seizure as provided by various laws such as the Fourth Amendment to the Constitution, the U.S.A. Patriot Act of 2001, and various Kentucky Revised Statutes. In this section, we will explore the ideas and recommendations concerning search and seizure techniques as they relate to computer forensics from readily available technical books.

In his book, John Vacca breaks down the searching and seizing of information in four easy to remember steps:

1. Preparation
2. Snapshot
3. Transport
4. Examination

In the preparation phase, Vacca emphasizes preparation before proceeding to the search and seizure location. Tips are to make sure all media have been sanitized and documented as such (Vacca, 136). He also recommends that if you are not the person to perform the analysis, you need to make sure you the person you have chosen to perform the examination. The person needs to be highly skilled and be able to competently testify in court concerning the methods used to perform the analysis and what information was found in the search (Vacca, 136-7).

In the snapshot phase, Vacca recommends literally taking snapshots of the scene of the seizure. He wants photos of the entire physical area surrounding the machine to be seized. After that, photographs of the actual computer the seizing is performed on is to be photographed in detail. Make sure to document every component and type of connection whether internal or external. Vacca then goes on to explain labeling everything in accordance with your predetermined methodology. The evidence custodian at the scene (if you have one) is to then go through and validate everything that has been done in the investigation thus far. What sets Vacca apart from other works I have read is his insistence on videotaping the entrance upon the scene of all personnel involved, all actions of the searching and seizing, the exiting the scene, and the transportation and storage of the seized materials. He recommends this so no defense attorney can claim that evidence was planted by the person or team performing the search and seizure (Vacca, 137-8).

In the transport phase, Vacca first assumes that the forensic investigators have the authority to transport the seized items to an off-site location. After making recommendations for packing and transporting, he once again is adamant about videotaping (or photographing in this step) the evidence leaving the scene and its journey to the transport vehicle. He also strongly recommends videotaping/photographing and documenting the moving of the evidence from the transport vehicle into the storage or examination facility (Vacca, 138).

In the final phase, examination, Vacca explains documenting the preparation of the seized information. Unpacking and visually inspecting the evidence is first. He then recommends making duplicates of the hard drive if this was not done on-scene. When finished, it is now time to inspect the BIOS of the seized machine and check for time discrepancies. Both of these previous steps must be documented. When finished duplicating the original drive, you are then to seal it in an anti-static bag and store it in a proper storage facility (Vacca, 138-9).

Chain of Custody

Chain of custody is primarily a list of persons and their respective time and places in which they have come into contact with or possession of a piece of evidence. Douglas Schweitzer states that "the chain-of-custody process is used to maintain and document the chronological history of the evidence" [Schweitzer, 149]. He recommends having two forensic investigators assigned to each case so that each can observe and document the steps of the other. He highly recommends over-documenting because of the importance of chain of custody to computer forensics. He maintains that one of the most well-known tactics used in a courtroom is the claim of mishandling evidence (see the notorious O.J. Simpson trial). By documenting everything possible, you minimize this possibility (Schweitzer, 149). Schweitzer includes a checklist of items to note as you are working on the case:

- The current date and time (include appropriate time zone)
- Broken hardware or any significant problems
- Note on the evidence found, which will go into your final report in more detail. These would essentially be notes that anyone could pick up and, at a glance, know exactly where you left off in your assessment of the seized computer and media.
- Special techniques (for example, sniffers, password crackers, and so on.) used above and beyond normal processes.
- Outside sources used (for example, third-party companies or products that helped to provide assistance and information)
- The names of all personnel involved in the investigation including a list of administrators responsible for the routine maintenance of systems
- A record of all applications running on the suspect's computer
- A list of who had access to the collected evidence including date and time of access, as well as date and time of any actions taken by those with access. In addition, the clock of the affected system must be compared with the actual current time and any discrepancies must be noted with the system clock left unchanged. Adjustment of the clock may subsequently be considered data tampering, leaving the resultant evidence inadmissible.
- Details of the initial assessment leading to the formal investigation
- Circumstances surrounding the suspected incident including who initially reported the suspected incident along with date and time
- A complete list of all computer systems included in the investigation along with system specifications
- A printed copy of any organizational policies and logon banners that relate to accessing and using

computer systems

- A comprehensive list of steps used to collect and analyze evidence (All points [Schweitzer, 149-50])

While making these notes, Schweitzer recommends you do so in a notebook in which pages cannot be removed. This should prevent a legal defense team from claiming that information beneficial to their client was removed from the notebook.

I chose to profile the Schweitzer book in this section because it presents the most comprehensive information relating to chain of custody and its importance to a forensics investigation. I believe this is so because his book focuses more on incident response, which is the first phase of an investigation, than the actual computer forensics analysis process. Mandia, Prosise, & Pepe's *Incident Response & Computer Forensics* placed more emphasis upon the physical handling of evidence as opposed to the chain of custody documentation (Mandia et al., Chapter 9). Nelson et al.'s *Computer Forensics and Investigations* barely even mentions chain of custody (Nelson et al., 28) but does provide a sample chain of custody form for a corporate investigation. The list what the differing fields of the form are, but no explanation of what should be recorded or in what manner (Nelson et al., 34-6).

Data Acquisition

There is a bit of debate in the computer forensics community about whether to create a bit-stream duplicate of a suspect hard drive or just to make an image of it. Creating a bit-stream duplicate involves transferring all information bit-by-bit from one hard drive to another without changing the information on the source drive. In other words, a bit-stream duplicate is an exact clone of its parent. An image is similar to a bit-stream duplicate in that it copies all bits from the source drive but differs in how it stores this information. The imaging process creates a file (or multiple files) containing this information as opposed cloning a hard drive. These files can be compressed for easier storage and transportation or can remain uncompressed. The advantage of imaging is that the information can be stored on CD or DVD media and transported easier than a duplicated hard drive. The advantage of a bit-stream duplicate is the ability to actually use (or reuse) the hard drive as it was in the suspect machine. Whichever route is taken, the information must be verified using MD5 or SHA checksums on both the source and target drives.

Most of my sources I explored for this section recommend creation of a bit-stream duplicate ((Carrier, 47-

9), (Kruse & Heiser, 15), (Mandia et al., Chapter 7), (Nelson, et al., 47-9), (NTI, Section 4), (Schweitzer, 49-51), (Vacca, 35-37)) as their preferred method of copying the information from a suspect hard drive. The lone holdout is Shinder & Tittel's *Scene of the Cybercrime: Computer Forensics Handbook.* This book never actually mentions bit-stream duplication and concentrates solely on imaging (Shinder & Tittel, 560). Schweitzer refers to bit-stream duplication as "imaging" (Schweitzer, 49) and Nelson, et al. gives definitions and explanations of the differences between both (Nelson, et al., 47).

As for recommendations of what tools to use to perform a bit-stream duplication, **dd** is the most common tool mentioned for a software-based copy , although NTI's SafeBack software ((Mandia et al., 164-8), (Nelson et al., 293), (NTI, Section 4), (Vacca, 35-37)) is the one mentioned most after **dd**. For hardware-based copies, the ICS ImageMASSter Solo is the hardware device recommended most ((Kruse & Heiser, 14-5), (Mandia et al., 154), (Nelson, et al., 205-6)).

All sources highly emphasize the need to verify that the information on the source and target drives are exact via MD5 or SHA sums. The need to ensure that the data on the suspect drive was not disturbed prior to duplication is also impressed upon the reader.

Examination Guidelines

Even though the sources used for this thesis are in relative agreement in the previous section concerning forensic duplication, they will diverge greatly come the examination guidelines section. Each source has and should have their own opinions concerning the steps of examination. What I did not expect was the great diversity of these opinions. All are valid. However, I can believe it may lead to confusion amongst those who choose to learn forensic examination procedures from only one source. Therefore, this section will detail a cross-examination of the recommendations provided by the various authors.

Beginning with Marcella et al.'s *Cyber Forensics – A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, the editors decide to break down the examination guidelines into two sections, non-liturgical (Marcella et al., Chapter 2) and liturgical (Marcella et al., Chapter 3) forensic examinations. A non-liturgical examination is one that is not expected to involve a trial or legal action of some sort. A liturgical examination is one in which a trial or legal action is expected. I do not think this is wise as it impresses upon the reader that one can approach an investigation from either point of view and this can affect the outcome of the information found. I can understand why they would perform differing investigations, but I still feel leery about it. How I differ in my approach is to treat all investigations as liturgical because you never know if your examination will become a component of a trial. Your investigation may cause someone to be fired and in turn they sue their former employer for wrongful termination. The examination you performed must be thorough enough to withstand the scrutiny of a well-prepared defense attorney. Therefore, unless I had in writing the requirement to perform a non-liturgical analysis with the stipulation that I would be held without fault if the case were to ever proceed to trial, I would perform a liturgical analysis. This would be done to protect me from being incorrectly sued by a client who believes that my non-liturgical examination harmed them.

The non-liturgical examination process recommended by Marcella et al. is rather non-invasive. Its first step is to isolate the equipment (Marcella et al., 27-8). Making sure you are investigating and duplicating the correct machine is of utmost priority in this step. Once seized, an examination of cookies (Marcella et al., 29-31), bookmarks (Marcella et al., 31-2), history buffer (Marcella et al., 32-4), cache (Marcella et al., 34), temporary

Internet files (Marcella et al., 35), tracking of logon duration and times (Marcella et al., 35-6), recent document list (Marcella et al., 36), tracking of illicit software installation and use (Marcella et al., 37-8), reviewing the system (Marcella et al., 38-41), a manual review (Marcella et al., 41-2), and hidden files (Marcella et al., 42-3) is performed. As this is a highly non-invasive procedure, I believe the only conclusions that can be drawn from this type of investigation is whether or not an employee violated the company's AUP (acceptable use policy for the computer systems). Not much more information can be gathered using the steps prescribed by Marcella et al.

There can be many comparisons drawn between the different sources pertaining to a liturgical examination. By default, the other sources imply performing a liturgical examination by the more invasive methodologies they recommend ((Kruse & Heiser, 16-9), (Mandia et al., Chapter 11), (Nelson, et al., Chapter 10)). Kruse & Heiser recommend beginning with a cursory examination of the master boot record and boot sector of a drive using either a hex editor or a forensic examination program (Kruse & Heiser, 16). Next, they recommend using whatever search tools you have available, whether your hex editor or forensic program, to perform a keyword search on the system

(Kruse & Heiser, 16). Mandia et al. and Nelson et al. unfortunately spend most of their time not explaining techniques as much as seemingly pitching forensic examination software products and giving an overview of the techniques using these products ((Mandia et al., 244-59), (Nelson et al., 322-35)). Two of the sources then agreed upon the next step: retrieving deleted files ((Kruse & Heiser, 17), (Mandia et al., 260-75)). Finally, Kruse & Heiser and Mandia et al. recommend examining slack space and unallocated clusters for fragments or entire pieces of files ((Kruse & Heiser, 17), (Mandia et al., 275-8)).

Interesting to note is the importance that Nelson et al. places on finding hidden data. Even though the book virtually ignored the general concept of retrieving deleted files, it does produce a fine section concerning common data hiding techniques (Nelson et al., 335-44). The techniques explored are hiding partitions (Nelson et al., 335-7), marking bad clusters (Nelson et al., 337-8), bit-shifting (Nelson et al., 338-42), steganography (Nelson et al., 342-3), file encryption (Nelson et al., 343), and recovering passwords (Nelson et al., 344).

As for Marcella et al., I was disappointed by their chapter concerning liturgical examinations (Marcella et al., Chapter 3). This chapter was a rehash of the previous non-liturgical examination guidelines, focusing exclusively on Microsoft Windows operating systems, with some additions. The additions were few and not really invasive techniques. The addition of searching the hard drive temporary files (Marcella et al., 55), such as swap space, and the registry (Marcella et al., 57-64) did not truly offset the need for more invasive procedures that a liturgical examination should include.

As for Vacca's book, he really did not cover the techniques used to perform a forensics investigation. His book focused more on the steps up to and including the data seizure, constructing a timeline based upon the seized information, and information warfare. It seems his book prefers to focus on the acts committed as they are being committed as opposed to finding the evidence of the acts ex post facto.

Are these sources poor in nature? By no means. Most of these sources choose to be more specific in their chapters that deal with each popular operating system individually. Unlike Marcella et al.'s exclusive focus on performing forensic examinations on Microsoft Windows-based machines, the other three major sources have chapters or sections of chapters pertaining to UNIX/Linux forensics ((Kruse & Heiser, Chapter 11), (Mandia et al., Chapter 13), (Nelson et al., sections of Chapters 4 & 10)). They also have chapters or sections of chapters dealing with Windows forensics ((Kruse & Heiser, Chapter 8), (Mandia et al., Chapter 12), (Nelson et al., Chapter 3 and parts of Chapter 10)). Since these specifics are beyond the scope of this thesis, they will not be investigated.

Basic Report Structure

The best source I have read concerning the topic of report writing is the National Institute of Justice's *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. Although the other sources gave their opinions upon what should be included in a report ((Mandia et al., Chapter 17), (Nelson, et al., Chapter 13)), I believe it is best to trust the ones who run the courts, the United States Government. The reason why I am focusing primarily on this source is that the likelihood that your investigative case winds up in court is fairly high. If the government publishes a resource in which it outlines what needs to be in a report, then we can safely assume this is what is minimally expected to be entered as evidence in a courtroom. Does this mean that only these items are to appear in the report? No, but it does give us a skeleton on which to craft our report around and add additional items as necessary (specifically if the prosecutor wanted certain findings highlighted).

The following list contains what, at a minimum, must be in the examiner's report:

- Identity of the reporting agency.
- Case identifier or submission number.
- Case investigator.
- Identity of the submitter.
- Date of receipt.
- Date of report.
- Descriptive list of items submitted for examination, including serial number, make, and model.
- Identity and signature of the examiner.
- Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files.
- Results/conclusions. (All points [NIJ, 20])

The NIJ also states that it would be beneficial to include the following even though it is not mandatory:

- Summary of findings
- Details of findings
  This section should describe in greater detail the results of the examinations and may include:
  - Specific files related to the request.
  - Other files, including deleted files, that support the findings.
  - String searches, keyword searches, and text string searches.
  - Internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity.
  - Graphic image analysis.
  - Indicators of ownership, which could include program registration data.
  - Data analysis.
  - Description of relevant programs on the examined items.
  - Techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and *file name anomalies*.
- Supporting materials
- Glossary (All points [NIJ, 20-1])

In Appendix A of the NIJ source, the government has compiled a list of sample cases with their sample concluding reports that is an excellent source of information for those concerned about how to format their reports (NIJ, 23-38).

In general, even though the sources used may differ in their approaches, one can create a basic methodology from the summation of the information provided.

CHAPTER VI

METHODOLOGY OF INSTRUCTION

Introduction to Methodology

The methodology I am proposing here is one that is easily teachable in a classroom and laboratory setting. By no means is it complete as it remains in the scope of this thesis. This methodology may be comparable to what one would receive if they attended a basic computer forensics course provided by a proprietary company. This methodology is my informed opinion on what should be taught to students in a graduate-level computer forensics course. It has been influenced by outside sources listed in the references. The laboratory curricula of Appendix A of this thesis is to be applied in the laboratory section of a computer forensics course following this methodology. Although it does not cover all sections of the methodology, it does complement its major topics.

Introduction to Standard PC Hardware

Students need to know the geometry of hard drives so they will understand how an operating system physically stores information on disk. This is done so they will know how easy it is to hide information that is not evident to the naked eye. Topics that should be addressed are:

- Hard drive components and materials
- Platters
- Tracks
- Cylinders
- Sectors
- Physical Sector Structure
- Heads
- Calculating hard drive capacity from CHS method
- Multiple Zone Recording
- Accessing the Drives
    - Interrupt 13 Access
    - 16-Bit ATA Addressing Access
    - Bit Shift Translation
    - Logical Block Addressing (LBA)
    - Extended Interrupt 13 Access
    - 48-Bit ATA/ATAPI Addressing Access
- Host Protected Areas

Differing Media Standards

Students must be able to understand and differentiate among the three major hard drive interfaces, their respective generations, and various implementations of the technologies. This allows the student to be prepared when he or she encounters a computer with a less than usual hard drive interface or implementation scheme. Topics that should be addressed are:

- IDE/ATA Interface (PATA)
    - Historical IDE Standards
    - Current ATA/ATAPI-6 Standard
    - Transfer Speeds (MB/s)
    - 40-pin, 80-pin, and Notebook Connectors
- Serial-ATA Interface (SATA)
    - SATA/150 Standard (aka SATA/1.5Gb Standard)
    - SATA/3Gb Standard (aka SATA/300 Standard)

    - Transfer Speeds (MB/s)
    - Connectors (Data and Power), Notebook Connectors
    - eSATA
- SCSI Interface
    - Historical SCSI Standards
    - Current Ultra320 Standard
    - New Serial Attached SCSI Standard
    - Transfer Speeds (MB/s)
    - Various 50-pin Connectors, Current 68-pin and 80-pin Connectors
    - SCSI Termination and Device IDs
- RAID
    - What is RAID?
    - Common RAID Levels and Where Commonly Found
        - RAID 0
        - RAID 1
        - RAID 5
        - RAID 0+1
        - RAID 1+0
        - JBOD RAID
    - Software RAID Array vs. Hardware Implementation

System Documentation

Students need to learn the utmost importance of documentation of all processes used and all evidence found. It cannot be stressed enough by the instructor that a court case may collapse solely upon the fact that the documentation was shoddy, incomplete, or worse yet, nonexistent. The students must learn that even if the steps they take seem inconsequential, they need to document. Topics that need to be addressed are:

- Creating and continuing chain of custody forms
- Documenting procedures
    - Tools used and purpose of tool
    - Search strings
    - Data carves
    - File rectification
    - Log examination

    - Image viewing and processing
    - Etc.
- Maintaining and storing documentation
- Making sure documentation is easily readable

Data Capture and Verification

The first crucial step in computer forensics is the accurate capture and verification of all information from a suspect hard drive. If this step is performed incorrectly, it is virtually a waste of time to perform a forensic analysis as the information captured is most likely "dirty", meaning the information probably changed moving from the source drive to the target drive. In this section, an emphasis must be placed upon using all precautions when capturing data and verifying that the information has not been altered. Topics that need to be addressed are:

- Target Media
    - New Hard Drives
    - Reusing Hard Drives
        - Forensic Sanitizing
        - DOD Standard for Forensic Sanitizing
    - New vs. Used Debate
- Capture Situation: Seizure of Entire Computer System vs. Hard Drive Seizure
- Capture Situation: Live Capture vs. Lab Capture
- The Great Debate: To Pull the Plug or Not? Shutting Down Running Systems.
- To Dump or Not to Dump? (Memory of a Running System)
- Documenting a System with Photographs
    - Photographing the Screen of a Live System
    - Photographing (from all angles) an Entire Computer System Being Seized
- Common Methods of Capture
    - Portable Duplication Devices

  - Duplicating or Imaging Using Lab-Based Equipment
  - Crossover Cable Capture
- Forensic Bit-Stream Duplication
  - What Bit-Stream Duplication Is
  - Advantages Over Imaging
  - Logistics of Bit-Stream Duplication
    - Cost
    - Storage of Duplicates
  - Advantages of Having More Than One Duplicate
  - Devices for Duplication
  - Hashing the Source Hard Drive
    - MD5 Sums
    - SHA Sums
    - Limitations and Attacks of MD5 Sums
    - Limitations and Attacks of SHA Sums
  - Verification of Original (MD5 and/or SHA)
  - Verification of Duplicate (MD5 and/or SHA)
- Forensic Imaging
  - What Forensic Imaging Is
  - Advantages Over Bit-Stream Duplication
  - Logistics of Forensic Imaging
    - Cost
    - Storage of Images
  - Hardware Write-Blockers
    - Why They are Necessary
    - Functions
    - Various Types, Interfaces, and Manufacturers
  - Imaging Software
  - Verification of Original (MD5 and/or SHA)
  - Verification of Duplicate (MD5 and/or SHA)
- Storage and Transportation of Suspect Hard Drives and Duplicates/Images
  - Equipment Necessary for Short-Term Storage and Transportation
    - Lockable Container(s) (Preferably Padded)
    - Anti-static Bubble Wrap and Bags
  - Equipment Necessary for Storage During Cases
    - Heavy-Duty Personal Fire-Proof Safes
    - Bank Vault Safe Deposit Boxes
    - Company Vault
  - Equipment Necessary for Long-Term Storage
    - Likelihood of Needing Long-Term Storage
    - Dynamic Media (Hard Drives) vs. Static Media (Tapes, DVD-ROM, etc.)
    - Storage Conditions

Chain of Custody

Of next most vital importance is chain of custody. Chain of custody is the process of documenting when the suspect and duplicate/image hard drives are in someone's possession, who that person is, where and when it is being stored when not in someone's possession, and what actions are being performed on those drives. Concepts that need to be presented to the students are:

- Chain of Custody Forms
  - What Should Be Included on a Chain of Custody Form
  - Sample Chain of Custody Forms
  - How to Fill Out a Chain of Custody Form
  - How to Create a Custom Chain of Custody Form
  - Short- and Long-Term Storage of Forms

System Investigation, Non-Forensic Environment

PREFACE

The reasoning behind why there is even a discussion of performing part of a system investigation in a non-forensic environment is the additional benefits that come about using these techniques. I am a firm believer in making multiple bit-stream duplicates or a single bit-stream duplicate and multiple forensic images. The multiple copies will allow for a forensic and a non-forensic viewing.

I am of the opinion that much is lost in a forensics investigation if you cannot view the system "in context."

In other words, if you cannot get the look-and-feel of a system and be able to search for obvious pieces of evidence, you may not be getting the entire story being presented by the suspect system. This is why I prefer to be able to seize an entire computer system so I can use one of the bit-stream duplicates (definitely not the original hard drive) to manually search a system. Even without the original computer system, the duplicate should work in another computer system, usually with a tweaking of the drivers. This "in-context" look can help fill in the gaps of the overall picture. I can easily see what software is installed on the system, what programs run upon system startup, if malware is on the system, if hacktools or other nefarious items exist, and other things that are more complicated in a forensic environment. Therefore, I believe a full forensics analysis should not be done without a non-forensic environment component.

Malware Detection Phase I

The first action that should be taken when starting the system is to search for initial signs of malware. There are many types of malware, but we are specifically searching for booby-traps. These are programs that are created to destroy the contents of a hard drive if the operating system is booted in a way that is unexpected.

For example, if the system boots without the user pressing a specific key combination, the software may be activated to destroy the contents of the drive. To circumvent this, we should boot the system from a protected floppy disk and physically search the hard drive for known booby-traps. If we are satisfied that none are present, then we should reboot the system without the floppy in place. If we detect one, we should determine what is the sequence of events to perform to allow for normal system booting or we can attempt to destroy the booby-trap by physically removing it from the system.

Understanding the Target Environment

Once we boot the system, we need to understand the target environment. The students should be taught the following concepts in relation to this:

- Determining if a login ID and password is necessary
  - Using tools to crack or change system passwords
- Determining the Operating System
  - Forcing Microsoft systems to identify themselves
  - Forcing UNIX/Linux systems to identify themselves
- Looking for customized PATH variables
- Viewing user lists and group lists
- Determining what processes are running
- Listing open ports and services with the system idle (this can be a great help in determining if any malware or rogue processes exist)

Looking for Obvious Information

This is the section in which we search for obvious pieces of evidence. In a forensic environment, it can be easy to overlook things because you are seeing them in an abstract manner and not in context. Therefore, we will begin searching for many things that may not appear obvious in a forensic environment but should stand out in a non-forensic environment. Things such as:

- Start with the Desktop
    - Look at what files are on the Desktop.
    - Is there a custom background?
    - Is there a custom screen saver?
    - Is there a custom theme?
    - Is there a custom mouse pointer?
    - Do the shortcuts go to their intended programs or files?
    - Are there mislabeled things on the Desktop?
    - In Windows, what are the recently viewed documents and what are listed as favorites?
    - What are the programs that can be run from the task bar/start menu?
- Search the Documents area
    - Is there anything that obviously appears to be evidence?
    - Is there anything that looks abnormal or out of place?
- Search for Email
    - Tracing email headers to determine true source
- Search for installed software
    - Determine what programs are on the system
    - Look for software packages buried in non-default locations. This could mean that someone is trying to hide something.
    - Determine if anti-virus and/or anti-spyware software is installed and if the definitions are up-to-date.

The following sections do not necessarily need to be performed in the order listed.

Log File Audit and Interpretation

- Read the security log to determine who logged onto the system and when.

- Read the event viewer log (for Windows) to determine what programs have run (if enabled).
- Read the history of commands run (for UNIX/Linux) to determine what commands were issued.
- If the system has a software firewall, determine its settings and read the log for connections to and from other machines.
- Traverse any other logs the system may be keeping.

Malware Detection Phase II

In this section, we need to be on the lookout for any forms of malware in the system. Viruses, worms, Trojan horses, spyware, adware, keyloggers, and nefarious cookies can cause major problems to a computer. I have been told stories third-hand about how someone accused of being in possession of child pornography was exonerated when a forensics analyst determined that a Trojan horse or spyware was surreptitiously downloading images to their system. I would even categorize programs that allow a user to destroy data as malware. We should sweep the system for malware but **not** destroy it. This sweeping should give us a listing of what is plaguing the system. We then should be able to correlate with the logs the communications the machine performed via the malware. If the system contains anti-virus or anti-spyware tools, we may also want to sweep the system as a whole through a write-blocker (after booting through a safe floppy disk or through another machine). This may determine for us whether these tools had been disabled by the malware (this is very possible). I would also recommend sweeping with multiple tools as not all tools will find all things.

Improper User/Privilege Detection

This is also a fairly easy technique to perform and you will find this primarily in servers but it is known to appear in PCs that have been hacked. Most people who create new user accounts on a system as a way to return to a compromised computer for further exploration/damage, storage of files, or to use as a base for launching attacks on other systems. Most lesser-skilled hackers are not going to create account names that match the naming scheme used by legitimate accounts. This makes it rather easy to spot the phony account. For the accounts that seem to meet the naming criteria but seem out of place (doesn't seem to be in the correct user group, etc.), rectification with the logs of when and from where the account was created is necessary. Non-default group names may also be a sign of an intrusion. If students are aware of the default user groups in Windows and UNIX/Linux, it should make these aberrations stand out.

System Investigation, Forensic Environment

PREFACE

In this section, there are some assumptions that need to be made. We are going to assume that the students have available to them multiple forensics analysis tools including at least one major analysis program (such as EnCase, FTK, etc.) and multiple minor programs (data carving tools, password crackers, file viewers, forensic boot floppy, etc.). We will also assume that the students will be shown how to properly set up their equipment and how to properly use these tools.

Please note that these steps do not necessarily need to be performed in any particular order.

Alternate Data Stream Detection (NTFS Only)

One of the easiest tasks that can be performed in a forensics environment is detecting NTFS Alternate Data Streams. ADS allows someone to implant information, whether maliciously or not, into a file that cannot be detected by normal means. These additions do not alter the properties of the file that is acting as the "carrier" of these streams. Neither the size nor the display of the file is modified. The information concerning the stream is stored in the $MFT and its mirror which cannot be read while the computer is up and running. Students should be instructed in the following areas:

- Determining that a hard drive has been formatted using NTFS.
- Selection of readily available tools for detecting ADS

    - CrucialADS
    - LADS
- What to do if an ADS is found
    - Viewing and documenting the contents of the ADS

File Header/Signature Rectification

A technique commonly used to hide a file's true file type or contents in Windows is to change a file's extension. Windows unfortunately reads a file's three character extension to determine which program to use to view/edit the file. Simply changing this extension is enough to confuse the operating system. Students should learn:

- How to manually search file headers/signatures
    - Using hex editors
    - Comparing a file's header with a known good list of file headers
    - Using the Linux command **file**
- Automated signature rectification using main analysis tool

File Recovery/Data Carving

Most people are under the mistaken impression that when they delete a file that it is removed physically from the disk. These same people also believe that when a hard drive or floppy disk is reformatted that all the prior information is also gone. In this section, the students need to be trained in the knowledge that this simply is not true and deleted files can be recovered in most cases. Concepts for the students to learn:

- What is data carving?
- How data carving is useful in our investigations.
- In which situations a file would not be recoverable
    - Overwriting with new files
    - Data destruction via tools created for that purpose
    - Physical disk destruction
- Recovery via Electron Microscope (and how that is beyond the scope of the course)
- Areas to look for files to recover
    - Unallocated Space
    - File Slack
    - RAM Slack
    - Host Protected Area
    - Unused Disk Space
- How to extract the contents of these areas
- How to carve files
    - What tools are available
    - Updating file signatures
    - How the tools work
- Recovering, Restoring, and Renaming carved files

Image Processing

With image processing, the students need to learn that all images are not what they seem. They need to learn about methodically performing a visual inspection of files and what steganography is. Topics to cover include:

- Viewing and cataloging images
- Determining the content of images
- Steganography
    - What is steganography?
    - How is it used?
    - How steganography differs from cryptography
    - Commonly available steganography tools
- Using tools to determine if files contain steganography
    - Using the tools that create stego files
    - Stegdetect tool
    - Stegbreak tool
- Extracting steganographic information
- Even though steganography is commonly associated with image files, explain how other files can contain

steganography. Give examples.

Keyword Searching

A fairly easy way to find information rather quickly is to perform a keyword search. When contracting out to a client, the client may provide a list of keywords to search for in the filesystem. If not, you can easily create a personal list of keywords on a case-by-case situation. By interacting with the client, you can usually determine what information to search for. Students should learn:

- The purpose of keyword searching
- How to create a keyword list if not provided one
  - Exact words or phrases
  - Wildcard usage
- Using wildcards to search for email
- What tools to use to keyword search
- How to interpret results

Report Writing

Upon completion of the forensics analysis, a report must be written detailing the findings of the examination. Emphasis upon good grammar, clean formatting, and clear presentation of facts and conclusions must be imparted to the students. They need to learn:

- What should be included in the final report.
- What should NOT be included in the final report.
- Report formatting (all from [NIJ, 29-30])
  - Identity of the reporting agency.
  - Case identifier or submission number.
  - Case investigator.
  - Identity of the submitter.
  - Date of receipt.
  - Date of report.

- Descriptive list of items submitted for examination, including serial number, make, and model.
- Identity and signature of the examiner.
- Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files.
- Results/conclusions.
- Summary of findings
- Details of findings
  - Specific files related to the request.
  - Other files, including deleted files, that support the findings.
  - String searches, keyword searches, and text string searches.
  - Internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity.
  - Graphic image analysis.
  - Indicators of ownership, which could include program registration data.
  - Data analysis.
  - Description of relevant programs on the examined items.
  - Techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and file name anomalies.
- Supporting materials
  - List supporting materials that are included with the report, such as printouts of particular items of evidence, digital copies of evidence, and chain of custody documentation.
- Glossary

This methodology should serve the students well. It should be equivalent to a private forensics training course. The labs in the appendices should amply complement the above methodology.

CHAPTER VII

CONCLUSIONS AND DISCUSSION

Computer Forensics is a field of Information Security that will be necessary to study and improve for many years to come. Universities will need to train and prepare graduate-level students with the necessary skills to be a competent forensics analyst upon achievement of his or her degree. The most effective methods of teaching computer forensics have been laid out in this thesis. If universities choose to implement the laboratory curricula presented, it will greatly benefit students who wish to learn computer forensics and wish to become a successful computer forensics analyst.

In this section of the thesis, we will discuss two major topics: the major shortcomings of this thesis and how this work could eventually be expanded. Actually, these two topics complement each other as the major shortcomings of this thesis would be the proper avenues to explore to expand this work.

The scope of this thesis is the greatest limitation placed upon its writing. When I first began researching this topic, I was full of ideas that I wanted to include in my writings. Compiling the list of the topics I wanted to touch on would have created an outline suitable for a mass publication literary work. Unfortunately, I had neither the time nor the patience to write a tome of that magnitude. With the help of Dr. Elmaghraby, I was able to pare down my thoughts and ideas into a form actually smaller that what is listed in my outline. This trimming and rearranging helped focus me onto hard drive and similar media forensics. It was at this point that I realized that there was a glaring omission. I had neglected to include a section specifically dedicated to the methodology I was to prescribe. I originally believed it would be enough to have a literature review and a laboratory section alone. After much pondering, I decided a methodology section was in order to explain why I chose to create the lab portion as I did. As this is the seventh instance of my thesis, the methodology did not appear until the fifth writing. Thus, we can begin determining how this work can be expanded by first revisiting the thesis scope.

In shortened form, this thesis is to cover techniques directly concerning performing a computer forensics analysis of a hard drive or other related media. This is where expansion upon this topic can begin. The first place where expansion can be beneficial is to focus on the forensic examinations of specific operating systems. Since this thesis is for the most part operating system neutral, the first action I would take is created three sections dedicated solely to the three major operating systems: the Microsoft Windows family, the UNIX/Linux family, and the Apple OS families (even though Apple OS X could conceivably be placed in the UNIX/Linux family). I would then further break down the sections into subparts. In the Microsoft Windows section, I would rend it into the Windows 9x family and the Windows NT family. For Apple OS, it would be split into pre-OS X and OS X families. For UNIX/Linux, it would be tricky. I would have a section with generalizations of each the commonalities between the different distributions and another section with the portions that pertain to the specifics of the distributions. I would want to at least cover AIX, HPUX, IRIX, SCO, Solaris, BSD and the Linux distributions Red Hat, SuSE, Debian, and Slackware.

The next avenue to explore in further expanding this thesis is live analysis. Since this thesis focuses exclusively on performing forensic analyses of systems that are no longer running, branching into live analysis is logical. A live analysis is one in which the suspect computer system is currently in operating mode with processes running. A live analysis is rather tricky to perform as data is changing in real time and crucial information may be destroyed. There are programs available on the market to perform a live analysis, such as Guidance Software's EnCase Enterprise Edition, but these require installation, activation, and processes running long before a live analysis is performed.

A third avenue to explore is network forensics. Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents [SearchSecurity]. The requirements for storage of this information is astronomical given the speed and volume of data that flows through the Internet or common networks. Some of this may be accomplished by creating a honeypot for attack, but usually not enough information is gathered from one machine. Therefore, the time and effort involved can outweigh the benefits. But, this is still a viable topic to be examined.

Finally, the field of software forensics is another avenue in which to explore expanding this thesis. Although a distinct tangent from the scope of the thesis, it still merits mentioning here. The goal of software forensics is not to examine a system to determine if crimes have been committed or gather information for a legal brief; it is to examine a piece of malware and determine who wrote the software in an attempt to capture them. You can learn how the malware was written, how it works, its purpose, and hopefully the author by using established software forensics methods.

I believe these topics are good starting points for expansion upon this thesis.

REFERENCES

Parenthetical entries are how each source is referenced in the body of the thesis. In the body of the thesis, parenthetical entries represent sources used and/or explored but not quoted. Bracketed entries are direct quotes.

Anastasi, Joe. (2003). *The New Forensics: Investigating Corporate Fraud and the Theft of Intellectual Property*. Hoboken, NJ: John Wiley & Sons, Inc. ISBN 0-471-26994-8. (Anastasi)

Britz, Marjie T. (2004). *Computer Forensics and Cyber Crime: An Introduction*. Upper Saddle River, NJ: Pearson Prentice-Hall. ISBN 0-13-090758-8. (Britz)

Carrier, Brian. (2005). *Files System Forensic Analysis*. Upper Saddle River, NJ: Addison-Wesley. ISBN 0-321-26817-2. (Carrier)

Federal Bureau of Investigation. *Forensic Science Communications*. Volume 2, Number 4, October 2000. http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm (FBI)

International Association of Computer Investigative Specialists. http://www.iacis.info/iacisv2/pages/thepresident.php. (IACIS)

International High Technology Crime Investigation Association. http://www.htcia.org/index.shtml. (HTCIA)

Kruse, Warren G. II and Jay G. Heiser. (2002). *Computer Forensics: Incident Response Essentials*. Boston, MA: Addison-Wesley. ISBN 0-201-70719-5. (Kruse & Heiser)

Mandia, Kevin, Chris Prosise and Matt Pepe. (2003). *Incident Response & Computer Forensics, 2nd Edition*. Emeryville, CA: McGraw-Hill/Osbourne. ISBN 0-07-222696-X. (Mandia et al.)

Marcella, Albert J., Ph.D. and Robert S. Greenfield,(Eds.). (2002). *Cyber Forensics – A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*. Boca Raton, FL: Auerbach Publications/CRC Press LLC. ISBN 0-8493-0955-7. (Marcella et al.)

Mitnick, Kevin and William L. Simon. (2002). *The Art of Deception*. Indianapolis, IN: Wiley Publishing, Inc. ISBN 0-471-23712-4. (Mitnick & Simon)

Nelson, Bill, Amelia Phillips, Frank Enfinger and Chris Steuart. (2004). *Computer Forensics and Investigations*. Boston, MA: Thomson Course Technology. ISBN 1-59200-382-6. (Nelson et al.)

New Technologies, Inc. *Computer Evidence Processing Steps*. http://www.forensics-intl.com/evidguid.html (NTI)

Schweitzer, Douglas. (2003). *Incident Response: Computer Forensics Toolkit*. Indianapolis, IN: Wiley Publishing, Inc. ISBN 0-7645-2636-7. (Schweitzer)

SearchSecurity.com. *SearchSecurity.com Definitions*. http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci859579,00.html. (SearchSecurity)

Shinder, Debra Littlejohn and Ed Tittel. (2002). *Scene of the Cybercrime: Computer Forensics Handbook*. Rockland, MA: Syngress Publishing, Inc. ISBN 1-931836-65-5. (Shinder & Tittel)

Smith, John C. *History of HTCIA*. http://www.jcsmithinv.com/HTCIAhistory.htm. 2001.(Smith)

U.S. Drug Enforcement Administration. *Microgram Bulletin*. Vol. XXXVIII, NO. 10, Computer Corner #199. October 2005. http://www.usdoj.gov/dea/programs/forensicsci/microgram/mg1005/mg1005.html (USDEA)

U.S.A. Patriot Act of 2001. http://www.cybercrime.gov/PatriotAct.htm (USAPA2001)

United States Constitution. http://www.archives.gov/national-archives-experience/charters/bill_of_rights_transcript.html (Archives)

United States Department of Justice. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* http://www.cybercrime.gov/s&smanual2002.htm (S&S)

United States Department of Justice National Institute of Justice. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. http://www.ncjrs.gov/pdffiles1/nij/199408.pdf. April 2004. (NIJ)

Vacca, John R. (2002). *Computer Forensics: Computer Crime Scene Investigation*. Hingham, MA: Charles River Media, Inc. ISBN 1-58450-018-2. (Vacca)

Wikipedia. *Wikipedia, the Free Encyclopedia*. http://en.wikipedia.org (Wiki)

Zadjmool, Ray. *Hidden Threat: Alternate Data Streams*. http://www.windowsecurity.com/articles/Alternate_Data_Streams.html (Zadjmool)

These are sources that were read and have influenced the writing of this thesis but were not directly quoted or expounded upon in the thesis.

Davis, Chris, Aaron Philipp and David Cowen. (2005). *Hacking Exposed: Computer Forensics Secrets & Solutions*. Emeryville, CA: McGraw-Hill/Osbourne. ISBN 0-07-225675-3.

Digital Intelligence, Inc. *Training Manual: Computer Forensic Essentials*.

Draper, John T. *Cap'n Crunch in Cyberspace*. http://www.webcrunchers.com/crunch/

Genco, Elizabeth A. *Learning by Doing*. http://infosecuritymag.techtarget.com/2002/apr/learningbydoing.shtml

Guidance Software. *EnCase Forensic Edition Version 4 User Manual*. Guidance Software, Pasadena, CA. 2004.
International Organization on Computer Evidence. *G8 Proposed Principles For The Procedures Relating To Digital Evidence*. http://www.ioce.org/ G8_proposed_principles_for_forensic_evidence.html

Lunn, Dorothy A. *Computer Forensics - An Overview*. http://www.giac.org/practical/gsec/ Dorothy_Lunn_GSEC.pdf

Nelson, Bill, Amelia Phillips, Frank Enfinger and Chris Steuart. (2004). *Guide to Computer Forensics and Investigations*. Boston, MA: Thomson Course Technology. ISBN 0-619-13120-9.

Pollitt, Mark M. *A Brief History of Computer Forensics*. http://ncfs.org/documents/swgde2000/historyofCF.pdf

Scientific Working Group on Digital Evidence. *Best Practices for Computer Forensics v2.0*. http://ncfs.org/swgde/documents/swgde2006/ Best_Practices_for_Computer_Forensics%20V2.0.pdf.

Stanley, Aaron and Evan McGoff. *Choosing Hardware for a Computer Forensic Lab*. The ISSA Journal, March 2006. pp. 11-13.

Stoll, Cliff. (2000). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Pocket Books. ISBN 0743411463.

StorageReview.com. *Reference Guide – Hard Disk Drives*. http://www.storagereview.com/map/lm.cgi/platters

APPENDIX A: LABORATORY PRAXIS

PREFACE: Laboratory Equipment Requirements

When creating a laboratory to perform a forensic analysis of a computer, two major factors come into play. The first factor is the money involved to purchase the needed equipment and software; the second is the actual computer and software needed to be purchased. This section will focus on creating a small forensics lab on a minimal budget that will allow one to complete the following lab exercises and be a good entry-level setup if the student decides to continue into a career as an independent consultant.

The money factor will greatly influence the choice of equipment purchased but should not affect the choice of software purchased. Since we should attempt to have standardized software, it will be assumed that we will need at least one primary forensics software package to perform standard analysis functions and one to perform the task of data carving. For those on a very tight budget, I recommend purchasing Access Data's Forensic Toolkit® (US$1095 at time of writing) to perform the standard analysis functions and the DataLifter® File Extractor Pro (US$155 at time of writing) to perform data carving functions. FEPro is much more robust and allows for creation of custom signatures to carve with than the built-in data carving tool of Forensic Toolkit®. For those with a larger budget, I recommend purchasing Guidance Software's EnCase® Forensic Edition (Price unknown at the time due to the company not publishing prices anymore. Assumed to be in the US$2500-$3000 range per personal license.) along with the DataLifter® Forensicware Solutions™ (US$335 at time of writing) and Paraben's P2 Power Pack (US$1495 at time of writing) which contains a whole host of tools that makes an investigation easier such as encryption cracking tools and chat analyzers.

As for the hardware required for a forensics analysis, a powerful PC is necessary that has the capability to interface with the three major types of hard drives (SATA, SCSI, and IDE) with write-blocking capability. Also necessary is the ability to read DVD/CD discs, floppy disks, and various flash media and thumb drives. The necessity to read these media types in a read-only manner cannot be stated enough. Therefore, the options are limited to either purchasing a computer forensics specific machine or purpose-building one yourself. For off-theshelf machines, there are at least three manufacturers building forensics-specific machines. One is Forensic Computer (http://www.forensic-computers.com) of Glen Lyn, VA. Their baseline product, the Original Forensic Tower II (US$4990 base price at time of writing) is available as a beginner's forensic computer. Another company is Digital Intelligence (http://www.digitalintelligence.com) of Waukesha, WI. Their baseline product, F.R.E.D. (US$5999 base price at time of writing) is also a good starter computer. Finally, ForensicPC (http://www.forensicpc.com) which is a subsidiary of Axis Microsystems, Inc. of Medford, MA offers the entry-level ForensicPC Pentium D Tower (US$3495 base price at time of writing).

I am of the opinion that a computer that is purpose-built may actually be more powerful than what is commercially available for an equivalent price. My personal recommendations of minimum requirements would be:

- AMD Opteron Dual-Core Processors (at least one, preferably two)
- 2GB RAM (more is better, but Windows XP cannot address more than 4GB)
- At least 200GB internal SATA storage (for OS and tools)
- Removable drive bays to house forensic copies of evidentiary hard drives for examination purposes (writable for cloning, read-only for investigation)
- Hardware write-blockers capable of interfacing with SATA, SCSI, and IDE
- DVD/RW drive for saving information
- DVD-ROM drive for accessing information on DVD/CD discs
- Floppy Drive

- PCMCIA/Media Card reader (read-only)
- Plenty of USB 2.0 and Firewire ports
- Sound card
- Windows-based Operating System (Linux as an additive option)

I recommend the AMD processors versus the Intel processors by personal choice. It is my opinion that the AMD processors are better on the whole. I shall attempt to clarify my opinion with the following analogy from the automotive world: the Intel processors have more horsepower whereas the AMD processors have more torque. It's great to go fast (horsepower) but fast is not a big help when severe number-crunching is necessary (torque) and your forensics machine needs all available power when performing an analysis. Therefore, I would choose AMD products over Intel.

Everything written in this section prior has been mostly my personal opinion. The following laboratory exercises have been written to make use of the equipment already available to the student at the university. The University of Louisville is in possession of an older-model F.R.E.D. unit from Digital Intelligence. This unit is equipped with Guidance Software's EnCase® Forensic Edition, Digital Intelligence's DriveSpy, Image, PDWipe, PDBlock, and PART, and DataLifter® Forensicware Solutions™. Another important tool included with FRED is

FTK Imager. It will be very necessary in the first section of labs. Other software that may be used will be outlined in the labs with locations on the Internet where students may download them as necessary.

Forensic Imaging Lab

Forensic Sanitizing of Target Media

Purpose:
To acquaint students with the rudimentary forensic task of wiping media.

Objectives:
By the end of the lab, the students should be able to:

- Forensically sanitize media
- Familiarize themselves with F.R.E.D.

Key Concepts:

- Forensic Sanitizing

Materials Students Need to Supply:

- Floppy Disk (DSHD) or blank CD-ROM

Introduction:

Our first task before ever entertaining the thought of creating a forensically sound image is to ensure the media onto which we place an image or perform a bit-stream duplication has been made forensically clean. I prefer using new media every time, but for our purposes and for training purposes we need to learn how to sanitize target media. To do so, we need to make our hard drives conform to the U.S. Department of Defense Standard 5220.22-M/NISPOM 8-306. To roughly paraphrase this standard, all target media must have all addressable locations overwritten with a character (usually 0x01), its complement (usually 0x10), and then a random character. This overwrite result must then be verified. EnCase makes this very easy for us.

However, I want us to have the capability to use non-GUI, non-Guidance Software tools. After some research, I have found what seems to be a decent tool called Darik's Boot and Nuke (DBAN) at http://dban.sourceforge.net. Although it claims to be able to wipe in accordance with the DOD specifications, it cannot wipe the Host Protected Area (HPA) of a disk. But, it seems to be a good tool and I have read many good reviews of it. Therefore, we will use it in this lab.

Methodology:

Instructions for wiping HDD to DOD specifications using EnCase:

1. When the power to F.R.E.D. is turned OFF, replace the HDD drive tray marked "Secondary IDE" with another drive tray containing your target hard drive (THD) which you wish to wipe.
2. Power up F.R.E.D. and login to Windows XP.
3. Start EnCase by double-clicking the EnCase icon on the desktop. Please make sure the red key-fob is still plugged into a USB port at the rear of the machine. It will be lit-up if so. EnCase will not work properly without the key-fob.
4. Click on Tools -> Wipe Drive
5. Click in the box next to #1 Local Drives (which places a check mark in it). This will instruct EnCase to only search local devices and not any you may have connected to through a crossover cable or other network device. Click Next. It will then search F.R.E.D. for his local devices.
6. In the Choose Devices window, you will find many choices of drives and/or devices to choose. EnCase has icons for partitions and icons for entire physical disks. The icons for partitions are represented by a "clip art" representation of a hard drive. THIS IS NOT WHAT WE WANT. We do not want to destroy the contents of a partition; we want to wipe an entire physical medium. The icon for a physical device could possibly be described as a yellow disk platter with a read/write head attached. The one we are looking for is usually #11 in the list. It should show the hard disk's label, number of sectors, and size. We want to make sure we do not choose incorrectly, so please make sure you are choosing the correct one. Know in advance the size of the drive you are wiping. This helps a lot and can keep you from wiping a device you

did not intend to. When you have made the decision of which device to wipe, click on the box next to the device (which places a check mark in it) and click Next.

7. The choice of Verify Wiped Sectors is already chosen for us. Please do not uncheck it. EnCase then asks you to enter a hex character for it to write to the disk. 0x00 is the default. Change the value to 0x01. Click Finish.
8. At this point, a new window will pop up and ask (roughly) if you are sure you wish to wipe this disk. You are then required to type the word "Yes" in the provided box. Do so now and click OK.
9. Depending on the rotational speed of the THD, this process will take anywhere from 5-15 minutes per gigabyte of hard drive space you are wiping and verifying. Since this is a labor intensive process, you may want to go do something else at this point.
10. Success! When finished, you should be presented with a window showing results and verification. If you were doing this for a case, you would click in the box to note the information for the case.
11. Now, repeat steps 4-10 but substitute a value of 0x10 for 0x01 in step seven.
12. Now, repeat steps 4-10 again but substitute a random hex value in step seven.
13. When Step 12 is completed, you have successfully completed three of the seven passes required to make a medium security-level wipe in accordance with DOD specifications. I will not torture you by requiring you to do seven passes. You have successfully completed Task #1 when you verify the disk is empty.

<u>Instructions for wiping HDD to DOD specifications using DBAN</u>:

To use DBAN, you do not need to use F.R.E.D. I recommend just using one of the three available machines in the lab with the drive trays in them.

1. Install THD in one of the removable drive trays of the available machines. I have left a screwdriver set in the lab for this purpose. You do not need to screw the THD into place, but you may need to remove a hard drive from the tray that is screwed in place.
2. Place THD tray into top slot and power on machine. As the machine is booting, insert floppy or CD-R

containing DBAN-1.0.6 to allow the computer to boot from disk. If you boot from CD, you will need a formatted floppy in the drive to store the verification file it will output when finished.

3. When the initial DBAN boot screen appears, just press the Enter key and allow it to commence booting.
4. Once booting has completed, you will be presented with the DBAN screen (which is white text on a blue background if you get something else for some unknown reason). Here is where you will make your choices for wiping the drive.
5. Type the **M** key to choose the method of wiping. You will be presented the possibilities. Use the arrow keys or the **J** and **K** keys to move the arrow next to DoD 5220-22.M and press the Enter key. This chooses our DoD standard.
6. Type the **V** key to choose the method of verification. The default choice should be Verify Last Pass. This is the choice we want as it will determine if the disk is clean only after the seventh pass, not after each pass. Press the Enter key.
7. Press the **Space Bar.** This selects which disk we choose to wipe. If you have multiple disks showing on the screen, use the arrow keys or the **J** and **K** keys to move the arrow next to the disk you choose to wipe and then press the space bar.
8. Press the **F10** key. This begins the process of wiping the drive (without delay or verification as EnCase does.
9. Depending on the rotational speed and seek time of the THD, this process can last up to many hours (It took me slightly over two hours to wipe a 3GB HDD that I believe to be only 4200RPM). As with the EnCase instructions, you may want to find something else to do during this time.
10. Success! You will be presented with a finishing screen (white text on black background) asking you to insert a floppy disk to record log files and verification information. You will need a blank, DOS formatted disk for this. The files will be in .tgz format (compressed tarball). In Windows, you can use a program like WinRAR to unpack these files. In Linux, you can just use the built-in command **tar -zxvf** with the package name.

You will need to turn in a print out of the verification logs from DBAN for part of your lab grade.

WARNING: There is a small but forgivable problem with DBAN. After writing the log files, it goes into a continuous loop to rewrite them. Just hit the reset button on the computer or just power off.

Hashing Images and Drives
Creating Bit-Stream Duplicates (The Quick and Dirty Method)
Creating Forensic Images

Purpose:
To acquaint students with the rudimentary forensic tasks of hashing and imaging.

Objectives:
By the end of the lab, the students should be able to:

- Compute MD5 and/or SHA-1 sums of images
- Create a forensic boot floppy
- Create duplicates using Symantec Ghost
- Create images using FTK Imager
- Create images using Paraben Forensic Replicator

Key Concepts:
- Hashing Images and Drives
- Creating Duplicates
- Creating Images

Materials Students Need to Supply:
- Floppy Disk (DSHD)

Introduction:
Acquiring forensically sound images or duplicates of a hard drive is one of the most crucial tasks an forensic analyst must complete. If the information on the Source Hard Drive (henceforth known as SHD) gets changed by one bit, it can throw an entire investigation into jeopardy. This is sometimes known as having "dirty information" or "dirty data" and a good defense attorney will have this evidence excluded from any legal action. Therefore, you must make sure the information you are about to copy has

not been tampered with since it became a possession of the authorities. Chain of Custody documentation is of utmost importance in this matter.

The question remains, how can we make a forensic image or duplicate of a SHD? Many methods exist but there are generally two major categories: Hardware-based imaging/duplicating and Software-based imaging/duplicating. Hardware-based imaging/duplication is performed by products such as the ICS Solo-3 family of products, Logicube Forensic MD5, and Digital Intelligence HardCopy. These products can create duplicates rather rapidly and will print out (you usually provide the portable printer) hash values and other information about the SHD and the Target Hard Drive (henceforth known as THD). These products make the process very easy and efficient, but they usually cost $1000 or more. Most startup forensic analysts cannot afford this luxury so they rely on the other category, Software-based imaging/duplication. This is the category we will focus on in this lab. In this lab, we will practice hashing SHDs with commercially available products. We will also do a quick and dirty software-based duplication onto forensically clean THDs. Finally, we will create forensic images using commercially available products.

<u>NOTICE</u>: Make sure you have forensically wiped the THD you plan on using for Section C of this lab. Refer to part (i) for methodology. Also make sure the THD is the same size or larger than the SHD.

<u>Methodology</u>:

A. <u>How to Hash a Hard Drive Using EnCase</u>:

1. With F.R.E.D. powered off, place the SHD into an empty drive tray, replace the cover, and insert into SCSIBlock tray. Please make sure the SHD jumper is set to Cable Select or Master.
2. Power on F.R.E.D.
3. Allow Windows XP to boot and login by providing the CECS 694 account password.
4. Double-click on the EnCase icon on the desktop to start the program.
5. Click the NEW button below the File menu. EnCase requires you to create a new case to acquire a drive. We really don't need to do this at this point, but we must. So when information concerning Case Number, Examiner Name, etc. appear, just press Enter or click

FINISH. I have some defaults listed that will meet our purposes.

6. Click File --> Add Device. This allows us to choose which hard drive we want to hash.
7. In the Add Device window, click in the checkbox next to Local Drives (checkbox #1) and click NEXT. This process takes a few minutes as EnCase searches for all devices attached to F.R.E.D.
8. In the Choose Devices window, click in the checkbox next to the Physical Drive representing our SHD (usually Physical Drive #3; usually checkbox #16). Click NEXT.
9. In the Preview Devices window, we are to double check that this truly is the drive we want to acquire. If so, click FINISH or press Enter. It is now acquiring the drive.
10. We are now back to our original EnCase screen. You will now see that our SHD is now listed below Case 1 in the left hand window. Click in the box next to our SHD in this window. DO NOT click in the pentagon next to the box. It has a different meaning. We do not want this.
11. Notice how the screen has changed a bit. This is just a text dump of the SHD contents. Now click Edit --> Hash. It will ask for start and end sectors. The default is the entire drive. This is what we want. Click OK or press Enter. This begins the hashing process. It should take less than ten minutes for this process to finish.
12. SUCCESS! You now have an output of the hashing in a conclusion window. Copy and paste all this information into some sort of text file and save it into the folder you have created for your team on the Q: drive and name it EnCaseHash.

B. <u>How to Hash a Hard Drive Using Paraben Forensic Replicator</u>:

1. Download and install Paraben Forensic Replicator demo version (http://www.paraben-forensics.com/programs/replicatordemo.exe) if not already installed.
2. With F.R.E.D. powered off, place the SHD into an empty drive tray, replace the cover, and insert into SCSIBlock tray. Please make sure the SHD jumper is set to Cable Select or Master.
3. Power on F.R.E.D.

4. Allow Windows XP to boot and login by providing the CECS 694 account password.
5. Double-click on the Forensic Replicator icon on the desktop to start the program.
6. Click File --> Calculate Checksum of Physical Drive.
7. You are presented with a new window which is the introductory window for checksum calculation. Click NEXT.
8. We are now shown a scroll pane listing all physical drives the software finds (it is much quicker than EnCase). Choose the disk representing the SHD (usually Disk #3). Ensure that both checkboxes remain checked. Click NEXT.
9. In the next window, we are asked if we wish to calculate a hash on the entire physical drive or just a few sectors. The default choice is Process the full physical drive. This is what we want. Click NEXT.
10. The Report Wizard window is next. We want to choose HTML File as our output and click the first three checkboxes to be placed in out output. Click FINISH.
11. We are now confronted with a SAVE dialog. Name the file PFRHash and save it in the folder you have created for your team on the Q: drive. Click SAVE or press Enter.
12. This begins the hashing process. It should take less than ten minutes to perform.
13. SUCCESS! A dialog box appears on the screen containing the information saved in our HTML file.

C. A Quick and Dirty Method to Create a Forensic Duplicate Using Symantec Ghost:

I call this a Quick and Dirty Method because it is the poor person's imaging with a minimum of programs and money. The longest part is creating the forensic boot floppy. Once done, you can use the Digital Intelligence program Image to create an executable image of the disk for future duplicates. Unfortunately, this imaging method will not stand up in court, but in internal company investigations, it should work. The hash value of the drive will be different of the THD than the SHD unless you have the exact same model THD as SHD with the exact same specifications. This does not really matter in internal investigations. However, you may want to make other images using other programs if the case could generate legal action of some sort.

1. Power on F.R.E.D. At the boot menu screen, use the arrow keys to choose MS-DOS 6.22 and press the Enter key when highlighted.

2. You will be presented with many different loading options and you can just allow the default to load. You will be asked approximately four further loading questions. You can choose to answer No to all of them or allow the defaults to occur when the choices time out.

3. Now you are presented with a C:\> prompt. Insert a DSHD (1.44MB) floppy disk into the A: drive. At the prompt, type **format a:/s**.

4. The operating system will ask you to insert a disk into the A: drive. Press the Enter key. When it is finished formatting, give the disk the volume name of **4N6BOOT.** You do not want to format another.

5. Now the fun begins. Switch to the A: drive by typing **A:** at the C:\> prompt and press Enter.

6. At the A:\> prompt, type **ATTRIB -R -H -S *.*** and press Enter. This removes read-only attributes, hidden attributes, and system attributes from all files. This is necessary for the next step.

7. Type **dir** at the prompt to show the files on the floppy disk. Remove the drvspace.bin file typing **DEL DRVSPACE.BIN.** This file is very bad! It must go and sit in the penalty box where it will feel shame. This file attempts to write to hard drives, so we do not want it.

8. You now need to copy two programs, Symantec Ghost and Digital Intelligence's PDBlock to the floppy. At the A:\> prompt, type **COPY C:\GHOST\GHOST.EXE .** and press Enter (notice the dot after the space after EXE as it is crucial it is there). When that process is finished, type **COPY C:\DIGINTEL\PDBLOCK.EXE .** (again notice the dot). These two commands will copy the files you need onto the disk.

9. You now need to create a file on the floppy called config.sys by typing **EDIT A:\CONFIG.SYS** (yes, I know it's redundant but you can never be too sure) at the A:\> prompt. This will open a nice blue screen for you to type in. Add this singular line: **LASTDRIVE=Z** and save and exit the file. The purpose of this is to not confuse DOS if it finds a lot of devices.

10. Now you need to create another file on the floppy called autoexec.bat by typing at the prompt **EDIT A:\AUTOEXEC.BAT .** This is a file that DOS reads in the booting process to run programs on startup. You need to make two entries. On the first line, type **A:\PDBLOCK.EXE 0 /NOMSG /NOBELL .** This command will activate the PDBlock program which is a software write blocker. The option 0 (zero) will protect only the first drive in the system. The option /nomsg will not pop up a message on the screen every time a write is blocked. The option /nobell will not sound the annoying little tone continuously when a write is blocked. The second entry in autoexec.bat should be **A:\GHOST.EXE -IR .** This automatically starts Ghost for us with the proper switch to make a forensic copy. Save and exit the file.

11. You must now wipe all free space on the floppy to make sure nothing can contaminate your system. To do this, switch back the the C: drive by typing **C:** at the A:\> prompt and press Enter. At the C:\> prompt, type **DRIVESPY** and press enter. DriveSpy is a forensics program from Digital Intelligence that has many purposes including wiping disks.

12. When DriveSpy starts, it will give you a listing of hard drives and their associated information on the screen, as well as a SYS> prompt. This is the first DriveSpy prompt. Type **DA** and press Enter to switch to the floppy drive. You are now presented a listing of the partitions on the A: drive. At the DA> prompt, type **P1** and press Enter. This will allow you to access the information stored on the floppy.

13. You are presented with information concerning what is stored on the disk and a new DAP1:\> prompt (DAP1 stands for Drive A Partition 1). At this prompt type **WIPE /FREE** and press Enter. This will allow you to wipe the unallocated areas of the disk. DriveSpy will ask you if you are positive you want to do this. Type **Y** and the program begins.

14. When it is finished, DriveSpy will return to the DAP1:\> prompt. Type **EXIT** here and press Enter. You have exited DriveSpy and are back to your C:\> prompt.

15. SUCCESS! You have you floppy disk ready to run an image.

16. To create an image, connect the SHD to the IDE0 cable in a computer. Make sure the jumper is set to Master. Connect a FORENSICALLY CLEAN THD to the IDE1 cable in the same machine. Make sure the jumper on the THD is also set to Master.

17. Power on the computer after placing your forensic boot floppy in the drive.

18. Sit back and watch. Wait for Ghost to begin. Press Enter when prompted with OK buttons from Ghost. It is just complaining like most Symantec products do.
19. You should now see the Ghost main screen. Press the right arrow twice (to choose Disk-to-Disk imaging) and press Enter.
20. You should see the SHD listed as Drive 0 and the THD listed as Drive 1. You need to choose the SHD as the drive to image from (it is the default) by pressing Enter.
21. You need to choose the THD as the drive to image to (it is the default) by pressing Enter.
22. A new screen listing the choices you have made is now showing. Press Enter.
23. Ghost will ask you if you are sure you want to do this. Press the left arrow to our affirmation of starting and press Enter. The process begins.
24. When Ghost is finished, it will ask you if you want to reboot or not. We don't want to reboot, so choose not to. Press the down arrow key until Quit is highlighted and press Enter. You are now down. Power off the machine.
25. To prove your imaging worked, place the THD into an empty drive tray and WITH F.R.E.D. POWERED OFF slide the drive into the SCSIBlock drive bay.
26. Power on F.R.E.D. If you see a new drive, SUCCESS! If not, retrace your steps to find what you did incorrectly.

D. How to Create a Forensic Image Using FTK Imager:

1. With F.R.E.D. powered off, place the SHD into an empty drive tray, replace the cover, and insert into SCSIBlock tray. Please make sure the SHD jumper is set to Cable Select or Master.
2. Power on F.R.E.D.
3. Allow Windows XP to boot and login by providing the CECS 694 account password.
4. Click Start --> Programs --> Forensic Tools (Demos) --> Access Data --> Forensic Toolkit --> FTK Imager
5. In FTK Imager, Click File --> Image Drive OR you can press Ctrl+I on the keyboard.
6. In the new pop-up window, click the radio button next to the work Physical. This should change the values in the drop-down list. From the drop-down list, choose Physical Drive 3 and click OK.
7. You are now presented the Export Disk Image window.

From the drop-down list, there are three choices. Raw uncompressed (dd) format is a straight rip using the **dd** tool commonly found in X operating systems. SMART (ew-compressed) is for creating an image for the SMART for Linux forensics tool created by ASR Data (www.asrdata.com/SMART). The .E01 Image type is the native image type of EnCase. This is the selection we wish to make (.E01). Click NEXT.

8. You are next given the E01 Image options window. In the Examiner Name text field, enter both students names. In the Case Number text field, enter CECS 694 Lab 2. In the Notes text field, enter the value "Ripped using FTK Imager." You may leave the Evidence Number and Unique Description text fields blank. Click NEXT.
9. Now, the Image Destination window appears. Change the destination to be the folder you created for your team on the Q: drive and change the filename to be FTK. Make sure the checkbox next to Perform an MD5 hash of the image remains checked. Click NEXT.
10. In the Image Segment Size window, click the radio button next to Custom MB and a slider bar appears. Drag the slider full right until the value under the Segment Info heading is 1.0GB. Click NEXT.
11. If the Summary window values are what you want them to be, click FINISH. If not, click BACK to make changes or click CANCEL to start again.
12. The disk is now being exported. It should not take more than ten minutes.
13. SUCCESS! You should have three files from the FTK Imager in your folder: FTK.E01, FTK.E02, and FTK.txt.

E. <u>How to Create a Forensic Image Using Paraben Forensic Replicator</u>:

1. With F.R.E.D. powered off, place the SHD into an empty drive tray, replace the cover, and insert into SCSIBlock tray. Please make sure the SHD jumper is set to Cable Select or Master.
2. Power on F.R.E.D.
3. Allow Windows XP to boot and login by providing the CECS 694 account password.
4. Double-click on the Forensic Replicator icon on the desktop.
5. In the Paraben Forensic Replicator, click File --> Create Physical drive image...
6. You are now presented with the Creating Physical drive

image wizard which will help walk you through creating an image. Click NEXT.

7. In the Physical drive scroll box, click on the entry for the 4210920 KB - WDC AC14 300R entry (usually Disk 3). Make sure the two checkboxes below our selection remain checked. Click NEXT.
8. You will now be prompted to enter a location and name for your image file. Choose the folder you created for your team on the Q: drive and name the image file PFR. Make sure you check the checkbox for Save in raw format. Click NEXT.
9. The next window is the Report Wizard window. We want our report output to be nice and easy to read, so please click the radio button next to HTML File and check the first three checkboxes below. These checkboxes will place Image Information, Time and Date of Acquisition, and Export Partition Structure information in the report. Click FINISH. You will then need to tell the program where to save your report. Save it in the same directory as the image you are creating.
10. The disk is now being exported. It should not take more than ten minutes.
11. SUCCESS! You will be presented with a pop-up window that lets you know that the image has been created successfully. This window also contains data verification information. Click OK and you are finished. You should have two files in your team directory, PFR.PFR and PFR.html.

Laboratory Assistant's Duties:

- Restore the **dd** image LabAiiImage.1 to a hard drive preferably 4GB in size but you may substitute one that is larger. Please make sure it has been forensically sanitized in advance of restoring the image.

Introductory Investigative Techniques

Finding the Obvious

Purpose:
To acquaint students with the basic skills of forensic analysis and build investigative skills.

Objectives:

By the end of the lab, the students should be able to:

- Pursue a methodical searching of a hard drive
- Find obvious evidence on a hard drive

Key Concepts:

- Basic forensic analysis
- Finding obvious information
- Building investigative skills

Materials Students Need to Supply:

- Floppy Disk (DSHD) from Project A(ii)

Introduction:

One of the great mistakes many novice computer forensics analysts make is to jump right into using forensic analysis tools and miss the overall picture created by the suspect computer's working environment. This is why I propose making at bare minimum two working copies of each suspect media (more specifically, the hard drives). One is for viewing the media out of context in a forensic environment. The other is to view the media in the context of a working environment. Many clues and pieces of evidence can be easily gathered just by booting up a forensic copy of the suspect system. This allows the investigator to see the system as the user would, which can lead to surprising results.

I believe it to be very necessary to view the suspect media in-context before viewing it in a forensic environment. This allows us to determine many things such as if the suspect media is contaminated with malware that could have possibly caused our current investigation (such as spyware that downloads child pornography to a victim's machine), if the perpetrator attempted to destroy evidence, if electronic burglary tools are present and have been used illegally, if pirated software is installed or stored on a system, or if there are any blatant violations of company code of conduct or acceptable use policies in a corporate situation. Many of these may not be easily seen in a forensic environment. Whereas in an out-of-context environment a file or set of files may look suspicious, in context they could be perfectly normal and acceptable.

This project, unlike previous projects, will focus exclusively on viewing a suspect hard drive in a working computer context. **Therefore, neither F.R.E.D. nor any**

forensic tools may be used for this project. This will allow you to build your investigative skills and not have you rely on software that cannot think logically for itself. I trust that you will accomplish this task in a methodical, efficient, and timely manner and you will have a respect for not relying solely on a computer to do your work for you.

NOTICE: Make sure you have forensically wiped the THD you plan on using for this lab. Refer to Lab A(i) for methodology. Also make sure the THD is the same size or larger than the SHD.

Methodology:

In-context Investigation Skills (aka Finding the Obvious):

1. Create a duplicate of the Source Hard Drive (SHD) using the Quick and Dirty Method from the previous project. See Project A(ii) for methodology. The only difference is we want to use the three machines with removable drive bays instead of the tear-down machine. Remove SHD and put it back where it belongs.
2. Place THD in the top bay of one of the computers and boot it. The image was created on this machine so there should be no problems with it working correctly.
3. Complete the scenario below and answer the questions to the fullest extent. You will be graded in accordance of the evidentiary material you find and the completion of the questions.

Project Scenario:

Your consulting firm, Acme Consulting, has been contacted by Thurdsten Industries concerning a problem they are having with an employee of theirs...a Mr. William R. Rubeck. It seems Mr. Rubeck has possibly been violating the company's written policy of acceptable use of its computer systems. Unfortunately, Mr. Rubeck has placed some sort of password protection scheme into the BIOS of his corporate computer that will not allow it to boot without the correct password. This is why your team has been brought in. Your company has been tasked with seizing Mr. Rubeck's hard drive and imaging it for forensic analysis during non-business hours. Thurdsten Industries is so confident of the guilt of Mr. Rubeck that they have not authorized a full forensics analysis. They only want your company to produce any information that is visible in a non-forensic environment so they can justify terminating the suspect's employment.

Assumptions: You are to assume that the seizing and imaging of the suspect drive has been accomplished by other members of the team. You are also to assume that you have been presented with a forensic copy of the suspect hard drive and that all chain-of-custody forms have been appropriately begun and/or completed. You are also to assume the basic components of a corporate acceptable use policy for computers (use your best judgment).

Questions to Answer:

1. Is there sufficient evidence to terminate the employment of Mr. Rubeck? If so, please list all pieces of evidence and their location in the filesystem (path from filesystem root).

2. Is there sufficient evidence to launch a criminal complaint against Mr. Rubeck and have ordered a full forensic examination of his hard drive? If so, please list all pieces of evidence, their location in the filesystem, and why you believe a criminal complaint need be sworn against Mr. Rubeck.

Answers to Questions:

1. Yes. Students are to list the paths and find the following:

- Pornographic images
- Pornographic web sites visited in cache
- Evidence eliminator program
- L0phtcrack
- Hack-tool Gencontrol disguised as Google Earth
- Apache web server
- Steganography tools and someone's Master's Thesis on steganography
- BitTorrent client

Let them know that short-hand is acceptable when referring to My Documents (no need for the full path in that case).

Value of this question: 80 points

2. Yes. In building upon the students learning investigative techniques, they should have discovered not only the steganography tools but a program known as Easy Office. In the mailer program of Easy Office, a sent email

should be found addressed to the organization known as NAMBLA (if the students do not know what this organization is, they may use their own time to look it up). This email lets the webmaster know that the images are up on the suspect's web server. Upon cursory glance, the images appear to be legitimate pictures of soccer players. But using the students' new-found investigatory powers, they should recognize that the combination of steganography tools, seemingly legitimate images, and NAMBLA is not good. The student should then use to steganography tools to attempt to extract other files from the images on the Apache server. The students should be able to extract from each image of a soccer player a file containing child pornography. ***Unacceptable:*** Even though some of the pornographic images found may have titles leading one to believe that the subject is under age, they are not the child pornography files they are supposed to find and no points are to be awarded if they do not find the hidden images. **Value of this question: 20 points**

NOTE: NO ACTUAL PORNOGRAPHIC IMAGES OR CHILD PORNOGRAPY IS USED IN THIS LAB. THEY ARE MERELY IMAGES OF STICK FIGURES WITH THE WORDS "PORNOGRAPHY" OR "KIDDIE PORN".

Laboratory Assistant's Duties:

- Restore the **dd** image LabBImage.1 to a hard drive preferably 4GB in size but you may substitute one that is larger. Please make sure it has been forensically sanitized in advance of restoring the image.
- Grade students submissions and submit grades to professor.

Intermediate Investigative Techniques

File Header/Signature Rectification

Purpose:
To acquaint students with the intermediate technique of file header/signature rectification.

Objectives:
By the end of the lab, the students should be able to:

- Understand what file signatures are and their importance to describing a file.

- Be able to identify a file type by its signature.
- Be able to rectify a file by its signature.

Key Concepts:

- Using hex editors
- Using EnCase to rectify file signatures

Materials Students Need to Supply:

- EnCase University Edition Academic Training CD
- A suitable Windows-based hex editor (UltraEdit32 is recommended)

Introduction:

A common way people try to hide files in any operating system (and especially in Microsoft variants) is to change the extension of a file in the hopes that anyone looking for specific information will overlook it. As most of you should know, Windows is heavily reliant upon a file's three character extension to determine what type of file it is and with what program to access the file. Fortunately for us, this does not actually change what type of file it really is; it only obscures its true identity to the naked eye.

The question we then need to answer is how we go about finding which files have their extensions changed or obfuscated in an attempt to hide the true contents of a file. This is completely different from steganography, which is hiding information or a file inside of another file. This is just an attempt to mask a file of one data type as a file of another data type.

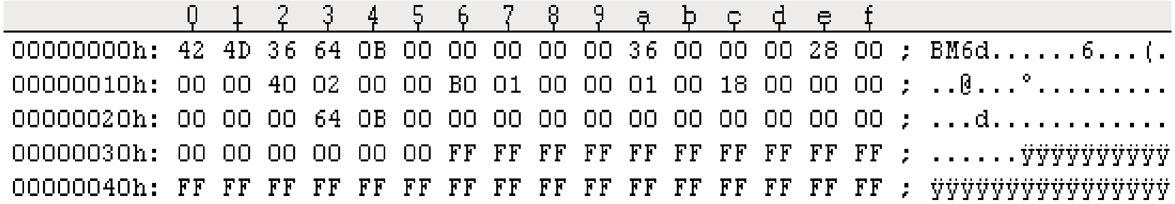
UNIX/Linux has a great utility built in that allows you to very quickly determine what is the data type of a file. This utility is **file**. In X-based operating systems, a file's extension is not necessary for the kernel to determine what type of file it is and what program to use to access it. Therefore, you find many files in these OSes that have no extension. The kernel reads the inodes where a file's information is stored and determines the type of file. The **file** utility is very easy to use: **file <filename>**.

Unfortunately, Windows does not have a utility such as this built-in. We must find another method to determine if a file is legitimate or not. There are two major avenues we can use to approach this. The first method is to manually determine the file type and rectify the extension (in Windows) using a hex editor. The other way is to allow a program such as EnCase to perform an automated rectification of the files using its built in file signature lists. For this lab, we are going to do both. We are first going to examine the contents of a file and specifically look for its signature. We will also learn how easily information can be changed in a file and how Windows can be tricked into believing a file is what it is not. We will also learn how to use EnCase to rectify files based upon their signatures (which should be one of the first steps an examiner should do when using EnCase).

Methodology:
YOU WILL NOT NEED TO USE F.R.E.D. FOR THESE EXERCISES. THEY CAN BE PERFORMED ON ANY MACHINE USING WINDOWS, A COPY OF THE ENCASE UNIVERSITY EDITION ACADEMIC TRAINING CD, AND A HEX EDITOR.

Hex Editor File Examination and Rectification:

1. Make sure you have a hex editor installed. I recommend using UltraEdit32 (http://www.ultraedit.com) if you are using Windows. It is a fine, inexpensive program that does so much more than just hex editing and as of the time of this writing, they have a full-version demo free for 45 days.
2. Open MSPaint and create a file with anything in it.
3. Save this file as its default data type (.bmp) and place it in a location that is easy to reach (such as the Desktop).
4. Change the extension on the file from .bmp to something else (I used .doc for this).
5. Windows will ask you if you really want to do this as it could make the file unstable. Yes, this is what we want.
6. Notice how Windows now changes the icon to the datatype the system now thinks it is. Double-click the file to open it. You should see nothing but junk (or so it seems...).
7. Now you know how Windows relies so heavily on the three character extension of a file. We know the file is actually a bitmap, but Windows doesn't. This is sufficient enough to fool Windows, but not the **file** utility of Unix/Linux. Here's why:
8. Close the file and reopen it using your hex editor. You should see something similar to this:

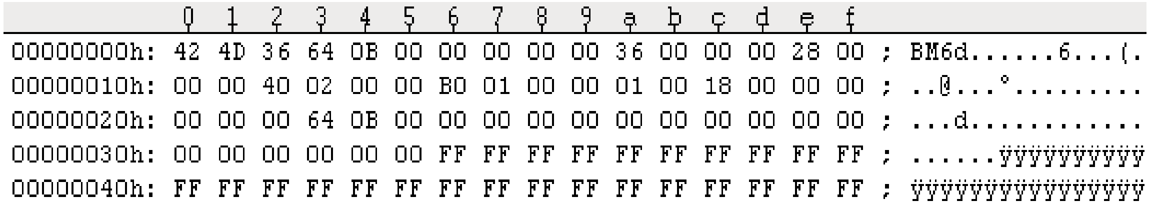


```
             0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: 42 4D 36 64 0B 00 00 00 00 00 36 00 00 00 28 00 ; BM6d......6...(.
00000010h: 00 00 40 02 00 00 B0 01 00 00 01 00 18 00 00 00 ; ..@...°.........
00000020h: 00 00 00 64 0B 00 00 00 00 00 00 00 00 00 00 00 ; ...d............
00000030h: 00 00 00 00 00 00 FF FF FF FF FF FF FF FF FF FF ; ......ÿÿÿÿÿÿÿÿÿÿ
00000040h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ; ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

9. This proves that the file actually is a bitmap. How? Start at offset 0x00. 0x00 is 42 which corresponds to the character B. 0x01 is 4D which corresponds to the character M. This is the telltale sign that the file is a bitmap. This is the file's signature. All files have a file signature, usually within the first few characters of a file. This is sometimes referred to as a file header. Some files even have a file footer as part of its signature. PDF files have an end-of-file (EOF) footer as part of its signature. This is conclusive evidence that Windows reads a file's extension and not its signature to determine the type of file. For a list of some common file signatures, check out http://www.garykessler.net/library/file_sigs.html.
10. Now, let's get a bit crazy. Change this file into a PDF file by not only changing the extension but by changing the signature. Don't forget to add the appropriate footer. In your report, you will need to turn in the hex code (appropriately cropped) of the bitmap file you created and its true conversion to PDF. Also turn in your results of whether or not you got Adobe Acrobat Reader to open your converted bitmap file.

Answers:

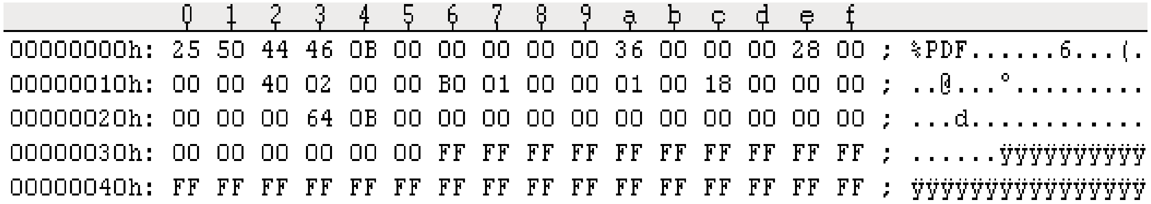
The bitmap file they created should look something like this:



```
             0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: 42 4D 36 64 0B 00 00 00 00 00 36 00 00 00 28 00 ; BM6d......6...(.
00000010h: 00 00 40 02 00 00 B0 01 00 00 01 00 18 00 00 00 ; ..@...°.........
00000020h: 00 00 00 64 0B 00 00 00 00 00 00 00 00 00 00 00 ; ...d............
00000030h: 00 00 00 00 00 00 FF FF FF FF FF FF FF FF FF FF ; ......ÿÿÿÿÿÿÿÿÿÿ
00000040h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ; ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

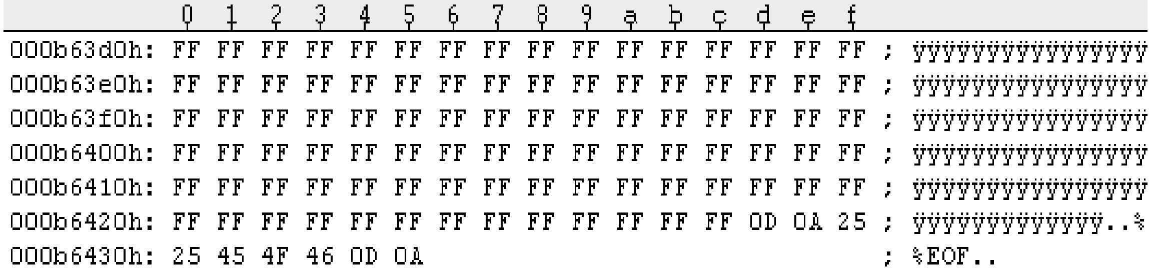
The bitmap modified into a PDF file should look something like this:

Headers



```
            0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: 25 50 44 46 0B 00 00 00 00 00 36 00 00 00 28 00 ; %PDF......6...(.
00000010h: 00 00 40 02 00 00 B0 01 00 00 01 00 18 00 00 00 ; ..@...°.........
00000020h: 00 00 00 64 0B 00 00 00 00 00 00 00 00 00 00 00 ; ...d............
00000030h: 00 00 00 00 00 00 FF FF FF FF FF FF FF FF FF FF ; ......ÿÿÿÿÿÿÿÿÿÿ
00000040h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ; ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

Footers



```
            0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
000b63d0h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ; ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000b63e0h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ; ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000b63f0h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ; ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000b6400h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ; ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000b6410h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ; ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000b6420h: FF FF FF FF FF FF FF FF FF FF FF FF FF 0D 0A 25 ; ÿÿÿÿÿÿÿÿÿÿÿÿÿ..%
000b6430h: 25 45 4F 46 0D 0A                               ; %EOF..
```

Make sure the %PDF is in the header and some variation of .%%EOF. is in the footer.

Adobe Acrobat Reader correctly recognizes it as a PDF file but cannot read it as the information stored within is but junk to the program. AAR states that the PDF may have been corrupted. If only the program knew...

<u>File Signature Rectification Using EnCase</u>:
Imaging having to look manually at each file on a target system. It would take forever. This is why we have automated tools to do this for us. Luckily, EnCase has this function built in. If you plan on purchasing or using a full version of EnCase, you will need to purchase a subscription to NIST's National Software Reference Library Special Database 28 which contains a quarterly updating of file signatures to import and update the signatures that come with EnCase. You can purchase them (at the time of writing) at http://www.nist.gov/srd/nistsd28.htm.

1. Make sure you have installed the EnCase University Edition Academic Training CD.
2. Unpack the Quantum evidence file to your Desktop or other handy location.
3. Start EnCase by double-clicking its icon on your Desktop.
4. Drag and drop the Quantum.E01 file into EnCase. A

window should pop up asking you to supply the program with case information. Do this and click Finish. Please wait until EnCase finished verifying the image before continuing to the next step.

5. Click the pentagon in the left-hand column next to Quantum and also click in the checkbox next to Quantum. This should show approximately 13,000 items.
6. To do the signature rectification: Near the top of the screen, you should find a button that says Search with a magnifying glass icon. Press this button. It should pop up a Search box.
7. Uncheck everything except Verify File Signatures. Click Start.
8. Within 30 seconds, it should show a completion box and list for you the number of file signature mismatches.

<u>Questions</u>:

1. How many file signature mismatches were found?
2. A file with a .BMP extension was found to have a bad extension. Determine what type of file EnCase found it to be and explain why EnCase believes it to not be a bitmap.
3. A file with a .JPG extension was found to have a bad extension. EnCase has determined that the file is a Multimedia file. Determine what type of file it actually is.

<u>Answers</u>:

1. 151
2. It is a .JPG file. The file header contains JFIF which is the signature for a .JPG file.
3. It is a .WAV file. The file header contains RIFF and WAVEfmt which is the signature for a .WAV file.

To answer #2 and #3, the students should highlight the files once found and click on HEX on the bottom section's viewer instead of the default Picture button. This will allow them to read the file's signature. If they want, they can export the files themselves and use a stand-alone hex editor to view the files.

<u>Laboratory Assistant's Duties</u>:

None really. Just make sure they have copies of what software is needed and that they turn in the answers for this section.

Keyword Searching

Purpose:
To acquaint students with the intermediate skill of keyword searching.

Objectives:
By the end of the lab, the students should be able to:

- Completely search an image for keywords.

Key Concepts:

- Searching for keywords in files and file fragments of evidentiary target media.

Materials Students Need to Supply:

- EnCase University Edition Academic Training CD

Introduction:
Most people would assume that keyword searching is a basic technique. On the surface, it looks like you would just use a text editor or word processor and click Edit --> Find and enter the search string. It's really not THAT easy. First, you couldn't dump the entire contents of a hard drive into a word processor (including the unallocated space). And second, word processor Find capabilities are limited to a single word or phrase at any given time. Neither of these are beneficial to us. We must have the capability to search large volumes for lists of multiple keywords all at once. Fortunately, most forensic examination software have this needed capability.

What, pray tell, are the keywords we are searching for? It changes on a case-by-case situation. The person contracting you to perform an analysis may give you a list of keywords to look for or they may give you the circumstances surrounding the case and require you to come up with a keyword list. Keywords can be names of people, places, slang words, drugs, sports teams, etc. Virtually anything can be a keyword. It's up to your or your client to determine what to look for. This requires you to stay in contact with the stakeholders in the examination as requirements and keywords are susceptible to change.

In this lab, we have the choice of using two different programs that we have readily available. We can use

Digital Intelligence's DriveSpy to perform keyword searches or we can use EnCase. Since DriveSpy will only work on FAT filesystems and is purely CUI-based, we will opt to use EnCase.

Methodology:

1. Start EnCase by double-clicking its icon on your Desktop.
2. Drag and drop the Quantum.E01 file into EnCase. A window should pop up asking you to supply the program with case information. Do this and click Finish. Please wait until EnCase finished verifying the image before continuing to the next step.
3. Click the pentagon in the left-hand column next to Quantum and also click in the checkbox next to Quantum. This should show approximately 13,000 items.
4. Click View --> Keywords. This will show you the default list of keywords. We want to add to this.
5. In the blank area of the top-right column, right-click and select Add Keyword List. A new pop-up window should appear.
6. In the left hand column, add fifteen or so keywords you want to search for concerning the following themes (the longer the list, the longer the search time):
   - Drugs (specifically slang terms for Kentucky's most well-known export and paraphernalia)
   - Bombs and Explosives
   - Cellular Phones
   - Satan Worship
   - Hacking
7. Make sure to check Unicode as one of the choices as NTFS and Unix/Linux systems use Unicode as opposed to ASCII for text. Click OK.
8. After you have clicked OK, you will notice new keywords in the list. Make sure you checkmark the boxes next to each keyword before you search.
9. Near the top of the screen, you should find a button that says Search with a magnifying glass icon. Press this button. It should pop up a Search box.
10. This time, we want to uncheck Verify File Signatures and check Search Each File for Keywords, Search File Slack, and Undelete Files Before Searching. EnCase should tell you that you have 16 or more keywords. This is because we are including searching for email and web addresses. Click Start and wait for the onslaught.

11. To keep track of what you are finding, click View --> Search Hits. You will need to click on Refresh near the top of the screen to update the findings as the search progresses. A running total of how many keyword search hits is in the far lower right-hand corner of the program. It also estimates how much longer the search will take.
12. You will need to turn in a list of the terms you searched for, the total number of search hits and the number of search hits for each keyword searched.

Answers:
The answers vary by the keyword list.

Laboratory Assistant's Duties:
Make sure each student submits approximately 15 or more keywords, the total number of search hits, and the number of search hits for each keyword in the list.

Advanced Investigative Techniques

Data Carving

Purpose:
To acquaint students with the advanced technique of data carving.

Objectives:
By the end of the lab, the students should be able to:

- Understand the concept of data carving
- Successfully data carve a suspect hard drive

Key Concepts:

- Data carving

Materials Students Need to Supply:

- None

Introduction:
Most people are under the impression that when they delete/remove a file from a computer that the file is gone

and no trace of it exists. Most people also believe that when they reformat a computer's hard drive that all information on it has disappeared permanently. Unfortunately, this is not true in either case. When someone deletes a file, the information of the file is still physically left on disk. The change that most operating systems make is to remove the entry from the list of files (FAT or $MFT in Windows, Inode list for X-based operating systems). All this does is remove the pointers to the file's physical location and the OS marks the clusters as free to be used again. The original file on disk is not physically gone until the clusters where it resides is rewritten. This can be done eventually (and automatically) by the operating system when it reallocates the space for other information or a person can use any number of commercially available products to write information onto these clusters in an attempt to destroy the information. From experience, not all of these products do as well as they claim. Many still leave large amounts of information on the disk.

There is good news, though. We can successfully recover most of the deleted information using a technique called data carving. In Lab C, you were introduced to the concept of file signatures. These are the way that operating systems are supposed to be able to identify what a file's data type is and choose the appropriate program to open the file with. You also learned that Microsoft operating systems rarely follow this method and prefer to look at a file's extension to determine what type of file it is. In this lab, file signatures will be used to identify a file that has been deleted and hopefully recover it.

A data carving program is based on a simple concept. When we data carve, we search three primary areas for files: unallocated clusters, volume slack, and unused disk space. We export these areas to disk and allow the carving program to go to work. The carving program will search these areas for file signatures that it knows and “carve” a file out of that area. It will stop carving when it either gets EOF information or until its upper limit of file size to carve is reached. It is an inexact science. Just a random set of characters that match a known file signature can be misconstrued by the program as the start of a file and it will carve out pure junk. This leads to a lot of incomplete carvings and they will have a tendency to fill a hard drive rather quickly. A carve of a 4GB drive's freespace has been known to produce over 100GB of worthless junk before the program crashed. Therefore, when carving, it is advantageous to constantly monitor the incomplete carves for partial information. If no such information is found, it is best to delete the incomplete files before they get out of hand.

The tool we will use to do our data carving is the DataLifter® File Extractor Pro. We will use the previously used EnCase to extract our disk areas to carve.

<u>Methodology</u>:

1. Start EnCase and create a new case as outlined in Lab A(ii).
2. The Lab Assistant has provided you with an EnCase image called LabDi.E01. Drag and drop this image file into your case. Allow EnCase to verify the image before you continue.
3. Click on the pentagon symbol in the left-hand column next to the icon of a hard drive. This expands the drive image to show all files.
4. After you scroll all the way to the bottom, you will notice three file names: Volume Slack, Unallocated Clusters, and Unused Disk Area. These are the three areas we want to carve. Check the boxes next to these three files.
5. Click Edit --> Copy/UnErase.
6. Make sure the choices "All Selected Files" and "Separate Files" have been selected (by their radio buttons) and click Next.
7. In the Copy column, choose "Entire Physical File" and make sure the Character Mask remains "None." Click Next.
8. Choose the location on disk (your group folder F.R.E.D.'s auxiliary drive) where you wish to export these to and set "Split Files Above" to 4000 (it is easier to type this in than to use the arrow buttons). Click Finish. This process takes about one and a half minutes.
9. SUCCESS! You have now exported the files we want to data carve. You will need EnCase to answer the bonus question.
10. Start File Extractor Pro by double-clicking the icon on the desktop.
11. If FEPro throws up an error stating there is no disk in the drive, just continue to click "Continue" until it finally starts the program.
12. We now want to tell FEPro which types of files we want to carve. We start in the left-hand column, "Common Headers." Make sure to choose all image files and

Internet files by clicking the pentagons next to the appropriate datatype headers.

13. In the center section, "Custom Headers", choose the ones that are image and Internet related (roughly 25 more signatures) by checking the boxes next to them. For this lab we are only concerned with images and Internet files.
14. Now click the Start button (blue triangle). It may continue to throw an error at you but just continue clicking "Continue." You should now see the File Selection Wizard.
15. It is easier to carve one file at a time, so select "A Single File" and click Next.
16. In this new screen, we will select the file we wish to carve. Point FEPro to the Unallocated Clusters file on disk that you carved. Click Next.
17. On this new screen, you will need to choose a location to store what you have carved. Point it to a location in your group's folder on F.R.E.D.'s auxiliary drive. HINT: Make sure your location has a trailing backslash (\ ) at the end or FEPro won't put your carved files in the proper location. This is a feature, not a bug ;) . Click Next.
18. FEPro will present you with a warning. Click Continue to start the carving process. Make sure you monitor the output for the incomplete files to get out of hand. Delete all unnecessary files.
19. When finished, it will display a small report and throw more of the same error. This is fine.
20. SUCCESS! You have successfully raised files from the dead. Now, answer the following questions:

Questions:

1. What is the main theme of the user's Internet surfing and image collection?

2. BONUS QUESTION: NO POINTS INVOLVED, JUST BRAGGING RIGHTS. What operating system (exact version) is the image you imported into EnCase?

Answers:

1. Marijuana

2. Windows 2000 (FAT File System + WINNT folder = Win2K FAT + Windows folder = WinXP or Win9x)

Laboratory Assistant's Duties:

- Provide the students with a copy of the LabDiImage.E01 file for their usage.
- Grade students submissions and submit grades to professor.

NTFS Alternate Data Streams

Purpose:

To acquaint students with locating NTFS Alternate Data Streams.

Objectives:

By the end of the lab, the students should be able to:

- Know what Alternate Data Streams are in NTFS
- Detect NTFS Alternate Data Streams

Key Concepts:

- NTFS Alternate Data Stream Detection

Materials Students Need to Supply:

- Floppy Disk (DSHD) from Project A(ii)

Introduction:

A very sneaky way that people can hide information in a Windows system that uses the NTFS file system is by using alternate data streams. ADS allows someone to implant information, whether maliciously or not, into a file that cannot be detected by normal means. These additions do not alter the properties of the file that is acting as the "carrier" of these streams. Neither the size nor the display of the file is modified. The information concerning the stream is stored in the $MFT and its mirror which cannot be read while the computer is up and running.

Why and when did Microsoft allow this ability in NTFS? Ever since NTFS has been available, the feature of ADS has been integrated into the filesystem. Microsoft did this to allow for compatibility between NTFS and the Macintosh Hierarchical File System (HFS) [Zadjmool]. The modern incarnations of Microsoft's NT family products use ADS as a way to legitimately store information concerning files on the system.

How can we protect against malicious usage of ADS? There is not really much of a proactive approach we can take in this manner. Streams can be easily created at a command prompt in Windows. We must be reactive in nature. We can find ADS using two basic methods. The first is much longer. If you copy the entire contents of a NTFS-based hard drive onto another hard drive that has been formatted with a variant of FAT, Microsoft will display a dialog box every time it encounters the copying of a stream. At this point, you can choose to have the stream saved into a separate, visible file for later viewing or you can destroy the stream. The second method is to use a tool specifically designed to look for ADS and identify them. This is the method we will pursue.

Methodology:

General Methodology Prior to Using Tools:

1. Create a duplicate of the Source Hard Drive (SHD) using the Quick and Dirty Method from the previous project. See Project A(ii) for methodology. The only difference is we want to use the three machines with removable drive bays instead of the tear-down machine. Remove SHD and put it back where it belongs.
2. MAKE SURE F.R.E.D. IS POWERED OFF FOR THIS STEP! Insert THD into an empty drive case and insert into SCSI Block drive bay.
3. Power on F.R.E.D.

Directions for Using CrucialADS:

1. Download CrucialADS from http://www.crucialsecurity.com/products/index.html
2. Unpack the downloaded zip file.
3. Find where you unpacked the zip file to and enter that folder.
4. Double-click on the CrucialADS.exe file.
5. Select the drive that is representative of your THD.
6. Press Start.
7. When finished, record all found ADS and place the results in your lab report.
8. SUCCESS!

Directions for Using LADS:

1. Download LADS from http://www.heysoft.de/nt/lads.zip
2. Unpack the downloaded zip file directly to the C:

drive (this makes it much easier).

3. Open a command prompt.
4. Type **cd \** at the prompt to make sure you are in the right location.
5. Type **lads.exe /s /v <THD Drive Letter>** to start lads. If you add **> lads.txt** it will record all the results for you. *Example:* lads.exe /s /v c: > lads.txt
6. When finished, record all found ADS and place the results in your lab report.
7. SUCCESS!

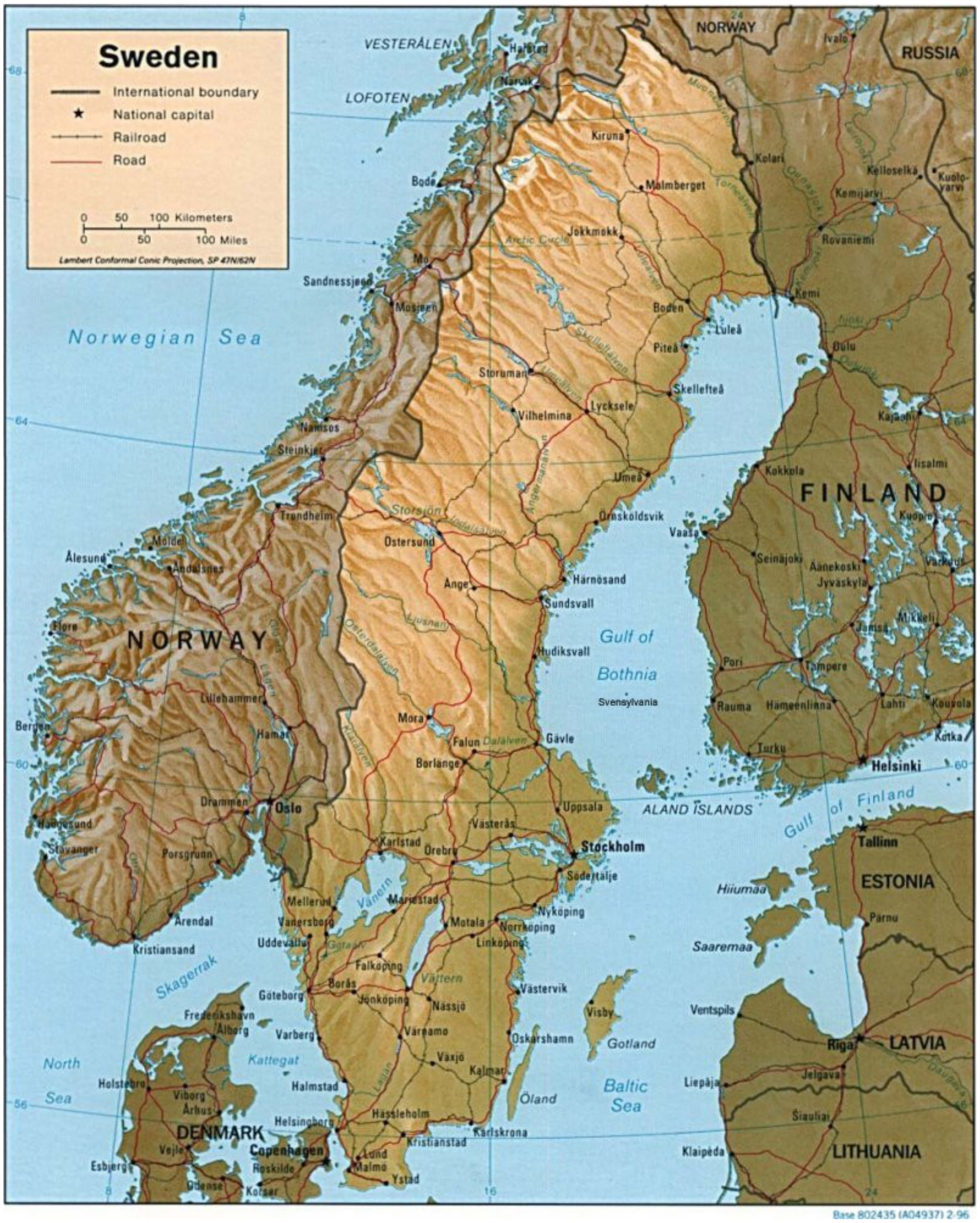
Answers:
The students should find at least two ADS on the target system. I believe the exact number should be three, though.

Laboratory Assistant's Duties:

- Restore the **dd** image LabDImage.1 to a hard drive preferably 4GB in size but you may substitute one that is larger. Please make sure it has been forensically sanitized in advance of restoring the image.
- Grade students submissions and submit grades to professor.

Final Lab Practical

THE SVENSYLVANIA HOOLIGAN BOMBING PLOT



The tiny island nation of Svensylvania is located in the Gulf of Bothnia between Sweden and Finland. After many disputes with the government of King Sven LXXIII, the Svensylvanians declared their independence from Sweden in 1922. It is a peaceful country, except when soccer is involved. The Svensylvanian hooligans are well-known within European football circles as the fiercest, rowdiest, ugliest, and smelliest of them all.

Svensylvania has never been known as a major footballing power. In fact, until qualifying rounds for World Cup 2006, they had won only one international match. They defeated Germany 1-0 in their only prior meeting in 1928. Yet, for this World Cup they assembled the finest team ever seen on their shores. They dispatched the Faroe Islands, Malta, and Liechtenstein in short order. Their only loss was to World Cup 2006 hosts Germany. All Svensylvania needed was a victory over Cyprus by two clear goals and a win by Germany over the Faroe Islands to achieve their hearts' desires. Svensylvania easily defeated Cyprus 3-0 and awaited results from Munich. Alas, the Germans were still bitter from their 1928 defeat to the Svennies and threw their match. They lost shockingly 5-1 to the Faroe Islands in which eight German players collapsed from heat exhaustion in the blazing hot 60 degree temperature. This win by the Faroe Islands allowed them to steal qualification on goal differential from Svensylvania. An utter travesty had occurred.

The results outraged the entire Svensylvanian population. Sven Karlssen of the Svensylvanians of Viking Ancestry Thugs (S.O.V.A.T.), the largest organized hooligan society in the country, released a communique hinting at a “dynamite” half-time show during the final in Berlin.

Interpol has since been granted arrest warrants for all members of S.O.V.A.T. that leave the tiny island nation. After an anonymous tip traced to Canada, the arrest of a suspected leader of S.O.V.A.T. was recently effected in Vilnius, Lithuania. Inside his so-called “safe house”, Interpol seized many of his personal items including his computer.

The computer's hard drive has been entrusted to you, one of the world's foremost computer forensic analysts. You need to determine whether or not the rumors of a World Cup bombing plot are true. If the rumors are false, this man will merely be deported back to Svensylvania. If the rumors are true, Interpol may be able to round up all involved in this heinous plot and save the lives of 80,000 innocent World Cup final spectators.

METHODOLOGIES: The skills learned in the previous labs will now culminate in this project.

TOOLS: All available tools at your disposal may be used.

Solutions to Lab:

Even though there may not appear to be much information on the hard drive, there is in fact much to find. Obvious information found will be pictures of Berlin's Olympic Stadium, a map with Svensylvania on it, and a picture of the Svensylvania flag. This is not incriminating evidence. But, combining this with the alternate data stream containing files explaining how to blow up the stadium, a file listing S.O.V.A.T. members and their worldwide locations, and the following data-carved items:

- Videos and documents relating to explosives
- A video communique' revealing the "dynamite" half-time show

There should be sufficient circumstantial evidence of the plot and Interpol can round up all members of S.O.V.A.T.

Laboratory Assistant's Duties:

- Restore the **dd** image LabEImage.1 to a hard drive preferably 4GB in size but you may substitute one that is larger. Please make sure it has been forensically sanitized in advance of restoring the image.
- Grade students' submissions and submit grades to professor. Students must print contents of both alternate data stream files, list the files concerning the explosives, and correctly identify the name of the hooligan from the communique' video. Partial credit is at the discretion of the grader.

APPENDIX B: Glossary of Terms

adware: Any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used. [Wiki]

alternate data streams: 1. Additional data associated with a file system object that is not readily seen or easily accessed. Commonly found in NTFS. Also known as **forks** in UNIX. 2. Newer area where nefarious users can hide data. Similar to steganography in intention.

bit-stream duplicate: 1. A sequential copying of all of the bits on the media. [USDEA] 2. Transferring all information bit-by-bit from one hard drive to another without changing the information on the source drive. 3. A clone of a hard drive.

black-hat hacker: Someone who breaks into a computer system to deface, destroy, or steal information. May intend to use compromised system to launch attacks on other systems.

blue box: An early phreaking tool, the blue box is an electronic device that simulates a telephone operator's dialing console. It functions by replicating the tones used to switch long-distance calls and using them to route the user's own call, bypassing the normal switching mechanism. [Wiki]

buffer overflow: A programming error which may result in a memory access exception and program termination, or in the event of the user being malicious, a breach of system security. [Wiki]

chain of custody: The order in which a piece of criminal evidence should be handled by persons investigating a case, specif. the unbroken trail of accountability that ensures the physical security of samples, data, and records in a criminal investigation. [Webster's New Millennium™ Dictionary of English]

cyberharassment: In Internet parlance, annoyance above and beyond what is considered tolerable. Usually involves emails harassing a victim.

cybersquatting: The practice of buying Internet domain names belonging to companies or famous people and then trying to sell them to said organizations for an unbelievable mark-up in price or just not allowing ownership of them by whom should have ownership rights.

cyberstalking: The use of the Internet or other electronic means to stalk someone which may be a computer crime or harassment. [Wiki]

computer forensics: The science of acquiring, retrieving, preserving, and presenting data that has been processed electronically and stored on computer media. [Schweitzer, 2]

data carving: A process that uses a set of file headers and footers to search for data that meets the specified search pattern parameters. The term implies that information is "carved" out of the media being searched (implying it is somehow removed). [USDEA]

data destruction: The willful overwriting of data stored in a medium with other data, usually just random values. A technique used by people wishing to cover their tracks after committing computer or computer-based crimes.

file header rectification: The technique of searching a file forensically by its file headers to determine the actual data type of the file. The file is then changed to its appropriate data type in the file system. In Windows, this rectification is done by changing a file's three character extension.

forensic image: An image is similar to a bit-stream duplicate in that it copies all bits from the source drive but differs in how it stores this information. The imaging process creates a file (or multiple files) containing this information as opposed cloning a hard drive.

forensic sanitizing: A process that involves the overwriting of existing data storage locations (containing data) with a new pattern of zeros and ones. Wipe software technology often wipes each storage location multiple times to ensure that none of the original data remains. [USDEA]

gray-hat hacker: A hacker who breaks into systems initially with only the intention to inform the owner of security holes but then crosses the line into black-hat hacking.

honeypot: A trap set to detect, deflect or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data or a network site that appears to be part of a network but which is actually isolated and protected, and which seems to contain information or a resource that would be of value to attackers. [Wiki]

intellectual property: An umbrella term for various legal entitlements which attach to certain types of information, ideas, or other intangibles in their expressed form. The holder of this legal entitlement is generally entitled to exercise various exclusive rights in relation to the subject matter of the IP. The term *intellectual property* reflects the idea that this subject matter is the product of the mind or the intellect, and that IP rights may be protected at law in the same way as any other form of property. [Wiki]

image processing: 1. In computer forensics, determining if an image (e.g. digital photograph) contains steganized information. 2. Determining if an image has been altered from its original.

imaging: The process of creating a forensic image.

keylogger: A diagnostic used in software development that captures the user's keystrokes. It can be useful to determine sources of error in computer systems. Such systems are also highly useful for law enforcement and espionage—for instance, providing a means to obtain passwords or encryption keys and thus bypassing other security measures. [Wiki] Can also be hardware-based.

keyword searching: In a computer forensics examination, creating a list of terms and searching files or target media for these terms.

malware: A generic term encompassing adware, keyloggers, spyware, Trojan horses, viruses, worms, and other nefarious pieces of software.

phishing: A form of criminal activity using social engineering techniques. It is characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. [Wiki]

phreaker (phreak): One who engages in phreaking.

phreaking: A slang term coined to describe the activity of a subculture of people who study, experiment with, or exploit telephones, the telephone company, and systems connected to or composing the Public Switched Telephone Network (PSTN) for the purposes of hobby or utility. [Wiki]

salami slicing technique: The illegal practice of stealing money repeatedly in extremely small quantities, usually by taking advantage of rounding to the nearest cent (or other monetary unit) in financial transactions. [Wiki]

social engineering: The practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick people into revealing sensitive information or getting them to do something that is against typical policies. [Wiki]

spam: Unwanted email, usually in large volumes.

spyware: A broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. [Wiki]

steganography: The art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. [Wiki]

Trojan horse: A malicious program that is disguised as or embedded within legitimate software. The term is derived from the classical myth of the Trojan Horse. They may look useful or interesting (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed. [Wiki]

virus: A self-replicating computer program that spreads by inserting copies of itself into other executable code or documents. [Wiki]

white-hat hacker: A hacker who breaks into systems with only the intention to inform the owner of security holes.

wiping: ***See forensic sanitizing***

worm: A self-replicating computer program similar to a computer virus. A virus attaches itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself. [Wiki]

APPENDIX C: Laboratory Curricula of Less Merit

Microsoft FAT-Based Systems

This lab was originally planned to introduce the students to the FAT filesystem. I initially believed it was important to include it in the main body of the thesis for the students to address during the term of a course. What led to this belief was my many conversations with people who currently work as support technicians for many Internet Service Providers (ISPs). These technicians informed me that many people still use Windows 9x family products and still need help configuring the systems for Internet usage. Because of the number of people still using these products and the people I have met who have upgraded from Windows 9x to Windows 2000/XP, I determined that it would be important to include a teaching/learning section dealing with FAT. Why I chose to remove this lab from the list of labs is that it would be so highly specific (pertaining only to FAT) as to distract from the broader topics that were more important to cover. This lab would be a better fit in an intermediate to advanced level forensics course. Since I was asked by my thesis advisor to only detail labs to be used in a basic forensics course, the development of this lab was put on hold. A rough outline of the lab assignment is as follows:

- Introduction to FAT
- Generations of FAT
    - FAT12
    - FAT16
    - FAT32
- FAT Structure
    - FAT Boot Record
    - Root Directory
    - Data Area
    - Primary and Secondary FAT
    - Cluster Allocation
    - Difference Between FAT16 and FAT32 Allocation
- FAT Exercises
    - What an Empty FAT Looks Like
    - How Files are Saved and Recorded Into the FAT
        - Slack Space and Unallocated Space
    - File Deletion and Fragmentation
    - File Content Changes and How It Affects the FAT
    - How Easy It Is to Alter a FAT Entry

Windows NTFS-Based Systems

This lab was originally planned to introduce the students to the NTFS filesystem. I initially believed it was important to include it in the main body of the thesis for the students to address during the term of a course. Every Microsoft operating system released to the general public since 2000 (with the exception of Windows Me) uses NTFS as its default filesystem with FAT remaining an option. Since Microsoft no longer supports the Windows 9x family of products, if users want to remain relatively secure in their computing by receiving patches and security updates they will need to upgrade to Windows 2000/XP or the forthcoming Windows Vista. Thus, it is important to cover the predominant filesystem used in the computing world. Why I chose to remove this lab from the list of labs is that it would be so highly specific (pertaining only to NTFS) as to distract from the broader topics that were more important to cover. I did realize, though, that the alternate data streams found in NTFS were an important enough topic to merit space in the accepted laboratory praxis section. This lab, as outlined, would be a better fit in an intermediate to advanced level forensics course. Since I was asked by my thesis advisor to only detail labs to be used in a basic forensics course, the development of this lab was put on hold. The structure of the lab would have appeared similar to this:

- Introduction to NTFS
- Generations of NTFS
    - v1.0
    - v1.1
    - v1.2
    - v3.0
    - v3.1
- NTFS Structure
    - NTFS Metadata Files
        - $MFT
        - $MFTMirr
        - $LogFile
        - $Volume
        - $AttrDef
        - . <The Root Directory>

- $Bitmap
- $Boot
- $BadClus
- $Secure
- $UpCase
- $Extend
- Extension File Records
- $ObjID
- $Reparse
- $Quota
- $UsnJrnl

- Similarities Between FAT and NTFS
- NTFS Attributes
  - 0x10 STANDARD_INFORMATION
  - 0x20 ATTRIBUTE_LIST
  - 0x30 FILE_NAME
  - 0x40 $OBJECT_ID
  - 0x50 $SECURITY_DESCRIPTOR
  - 0x60 $VOLUME_NAME
  - 0x70 $VOLUME_INFORMATION
  - 0x80 $DATA
  - 0x90 $INDEX_ROOT
  - 0xA0 $INDEX_ALLOCATION
  - 0xB0 $BITMAP
  - 0xC0 $REPARSE_POINT
  - 0xD0 $EA_INFORMATION
  - 0xE0 $EA
  - 0x100 $LOGGED_UTILITY_STREAM
- DUDS (Default Unnamed Data Streams)
- Alternate Data Streams

- Exercises
  - Virtually Creating NTFS File Entries Into $MFT
  - Virtually Creating NTFS Alternate Data Streams in the $MFT
  - Deleting Files and How It Affects the $MFT

UNIX/Linux Forensics

This lab was originally planned to introduce the students to the UNIX/Linux forensics. I initially believed it was important to include it in the main body of the thesis for the students to address during the term of a course. Linux is a popular alternative to Microsoft Windows and is a free/open-source implementation of the UNIX operating system. UNIX/Linux can be commonly found installed on computers at universities, government research laboratories, and increasingly on home computers. Its popularity extends from its speed and stability benefits over Microsoft products with the ability to create or modify Linux software. It is believed that most web servers worldwide reside on UNIX/Linux systems. The main disadvantage is its complexity in installing, using, and maintenance in comparison to Microsoft products. Why I chose to remove this lab from the list of labs is that the majority of forensic analyses performed will be on computers with a Microsoft operating system. Even though knowledge of UNIX/Linux forensics is very important, it would generally be considered outside the scope of this thesis. Therefore, it has been relegated to Appendix B. This is an outline of what would have been developed:

- History of UNIX
    - 1969 – The Beginning
    - 1974 – The Great Rewrite
    - AT&T and BSD – The Great Split
    - Here Comes the Sun
- History of Linux
    - Richard Stallman and the Free Software Foundation

  - The GNU Hurd
  - 1991 – The Linux Torvalds Kernel
  - The Open Source Revolution
- Common UNIX/Linux Filesystems
  - ext2/ext3
  - FFS
  - JFS
  - ReiserFS
  - UFS/UFS2
  - XFS
  - ZFS
  - Comparing/Contrasting the Filesystems
- Major Filesystem Components
  - Inodes
  - Superblock
  - Datablock
  - Bootblock
  - Journaling
- Common UNIX/Linux Exploits
  - Rootkits
  - Trojanized Binaries
  - Server Attacks
    - Apache
    - BIND
    - Samba
    - sendmail
  - Service Attacks
    - OpenSSH
    - telnet
- Exercises -> Never Developed

CURRICULUM VITAE

NAME: Robin Cincinnatis Morrison

ADDRESS: PO BOX 21761
Louisville, KY 40221-0761

DOB: Louisville, KY – 26 August 1975

EDUCATION
& TRAINING: B.S., Engineering Mathematics &
Computer Science
Speed School of Engineering
University of Louisville
1993-99

Certificate, Computer Forensics Essentials
Digital Intelligence, Inc., Waukesha, WI
January 2005

PROFESSIONAL
SOCIETIES: International Information Systems Security
Association (ISSA)
International Information Systems Forensics
Association (IIFSA)