CERIAS Tech Report 2005-28

COMPUTER FORENSICS: TOWARDS CREATING A CERTIFICATION FRAMEWORK

by Matthew Meyers

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

COMPUTER FORENSICS: TOWARDS CREATING A CERTIFICATION FRAMEWORK

A Thesis

Submitted to the Faculty

of

Purdue University

by

Matthew L. Meyers

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

May 2005

ACKNOWLEDGEMENTS

I wish to thank several people who have supported me with my thesis. First, thank you to my committee: Marc Rogers, Toby Arquette, and Eugene Spafford. I particularly wish to thank Marc Rogers, my major professor, for his guidance, support, and time, he has helped me greatly throughout the last year; I appreciate all you have done for me Marc, thank you. Lastly, thank you to my friends and immediate family who have supported me.

PREFACE

The proliferation of computers in daily activities has been correlated with an increase in computer crime. To pursue criminal and civil prosecution for computer crimes, the field of computer forensics emerged. Computer forensics is in its infancy and measures need to be implemented to ensure the field's maturity.

This thesis explores legal aspects of the computer forensics field and how it has and may be contested in the Federal and State Court Systems. From the legal aspects the thesis delves into steps toward the creation of a framework for the computer forensic investigative process. Chapter 1 presents an overview of the computer forensics field. Chapter 2 looks into the legal analysis in respect to the computer forensics field exploring search and seizure, analysis of evidence for court, preservation of evidence, and court room procedures relating to expert testimony. Chapter 3 explores practices revolving around trust and certification in relation to the information technology field and how those practices have matured from their infancy to gain credibility and reliability. The thesis concludes with Chapter 4 and 5 proposing a framework for certification for the computer forensics field based on legal issues.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Meyers, Matthew L. M.S., Purdue University, May, 2005. Computer Forensics: Towards Creating a Certification Framework. Major Professors: Marcus K. Rogers & Toby J. Arquette.

Given the dramatic increase in evidence of a digital or electronic nature in cases brought before the U.S. Court System, there is a growing concern over its admissibility. The question becomes whether the tools used and actors involved to extract and analyze the digital evidence meet the requirements for scientific evidence. This thesis explores how it may be possible to meet the scientific evidence requirements in the U.S. Court Systems by analyzing the legal issues and how other relevant communities such as accounting, auditing, Internet transaction security, and Underwriters Laboratories. The thesis concludes with a proposed certification and standardization system for testing of tools and actors involved in the computer forensics investigation process to mitigate the risks to the computer forensics community. The goal of this process is to bring credibility and reliability to the computer forensics field while at the same time meeting the requirements of the U.S. Court Systems for scientific evidence.

CHAPTER 1: INTRODUCTION TO COMPUTER FORENSICS & THE INVESTIGATION PROCESS

1.1. Introduction

At an apartment in a blue collar neighborhood of South-East London, a police officer saw a plethora of luxury automobiles. Because of the neighborhood the police officer thought there might be illegal activity occurring at the apartment. The officer called in his suspicions and later raided the apartment resulting in the arrest of numerous members of the "iPod crew". From December 2001 to October 2002 the iPod crew stole approximately 70 luxury automobiles (Carter, 2004). The iPod crew purchased the automobiles from dealers using fraudulent documentation. During the investigation police seized an iPod™ and discovered numerous documents used for fraudulent transactions and bank notes to resell the automobiles to unsuspecting individuals. The bank notes acted as proof to the buyer that there were no obligations on the automobile leading the buyer to believe the automobile had a clear title (Howe, 2004).

Crimes perpetrated using technology such as the iPod Crew is becoming more common as a result of the advent of the Internet and rapid growth in technology. Because of the use of computers as an accessory or sole means to commit a crime, computer forensics emerged. The usage of computer forensics has not come without challenges in court regarding the reliability and validity of

the practice. With the current contentions surrounding computer forensics, steps toward sound solutions need to be considered to aid in the field's development. The fact is computer forensics will continue to expand correlating to the growth of the Internet and the quantity of legal cases involving computers. As shown in figure 1.1 the number of reported incidents to CERT®[1] has continuously increased each year.

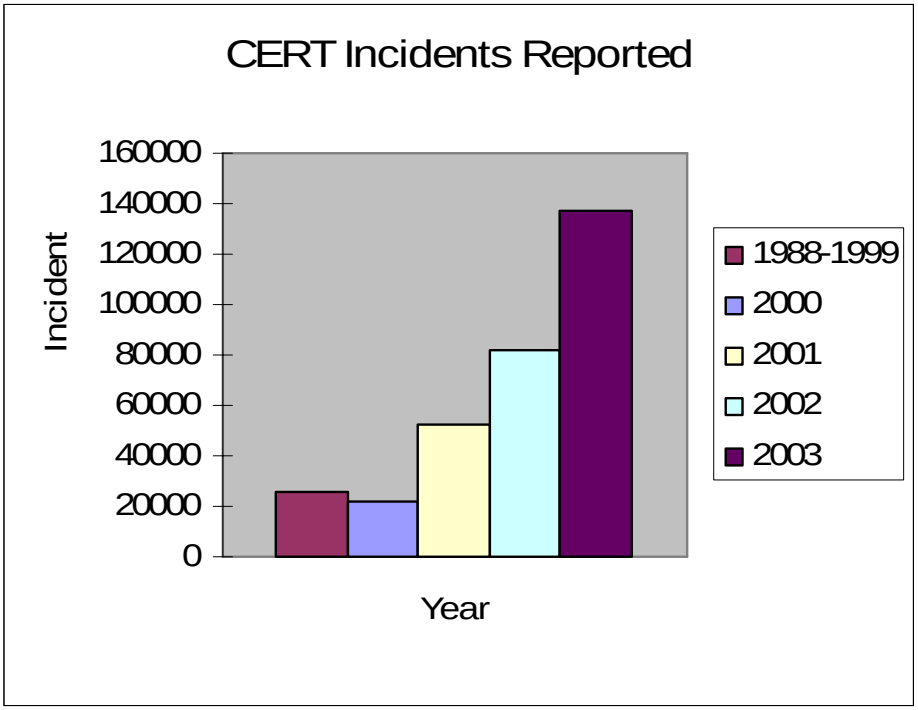

Figure 1.1 CERT® Incidents Reported (CERT/CC, 2004)

[1] CERT/CC® is based at Carnegie Mellon University. The purpose of CERT/CC is to strengthen Internet security by having entities report incidents so CERT/CC can issue reports and responses to mitigate risks. CERT/CC also provides training and assistance in incident response.

1.2. What is Computer Forensics

To obtain information from the iPod used by the iPod Crew for use in a court of law, the police utilized computer forensics. Computer forensics is a sub-discipline of Digital Forensics. Digital forensics is "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources..." (Palmer, 2001). Digital forensics includes other forensics specializations such as network and media forensics. Computer forensics is the "use of an expert to preserve, analyze, and produce data"[2] from volatile and non-volatile media storage (Mack, 2003). Computer forensics encompasses computing devices and related media that may be used in conjunction with a computer such as an iPod, or a multimedia player. The domain of computer forensics is vast. To limit the domain, this paper will focus on legal issues that have and may occur in the computer forensics investigation process (i.e., Fourth and Fifth amendments, and state law are beyond the scope of this paper; however, the author does recognize the inherent legal issues regarding the aforementioned amendments).

1.2.1. What Computer Forensics Involves

When police officers in London confiscated the iPod from the iPod crew the computer forensics process started. In an ideal situation the police officers

[2]A portion of her definition was used; however, the entire definition was not used because of the limited scope presented as she used only single hard drive examination as computer forensics. "Computer forensics is the use of an expert to preserve, analyze, and produce data …"

would have performed (in a high level overview) the following procedures. Upon identifying the iPod as potential evidence, the police officers should take photographs of the scene and what is displayed on the iPod. In most cases the best thing for a police officer to do is request an expert, but for cases when that is not an option, it is recommended that the officer does not power on a device if found off, find the power source if on (e.g. laptop power adapter), or power off the device by removing the power source, to prevent spoliation/contamination even though potential evidence in volatile memory may be lost; in this case removing the battery for the iPod.

The next step is for the officers to “bag and tag” the iPod for transportation while keeping detailed notes of all materials seized and procedures performed. For transportation of the device the officers should keep the evidence, (i.e., the iPod), in a static free bag away from electronic disturbances, such as magnets and radio transceivers. When the officer arrives at the storage facility proper documentation and tagging (chain of custody) should occur for the transfer of the evidence. The investigator should inform the examiner and/or expert about the case and any pertinent information. During the entire forensic process the examiner and/or expert should document each time evidence is checked in and out (chain of custody) from storage and what procedures are being used for extraction, analysis, and preservation of the evidence. During the analysis phase the expert should make an exact copy of the original data using a variety of methods ensuring that the copy is identical to the original. To help ensure that the original is never altered the identical copy will be used for analysis. To

extract information from the iPod the expert should use software and hardware (tools) to sift through the data. At the conclusion of the investigation the expert should preserve the evidence and present the findings in a court of law if required.

1.2.2. Who Uses Computer Forensics

Computer forensics usage is vast and growing rapidly. Computer forensics has been and continues to be used for criminal and civil litigation, educational studies and research in academia, and in the corporate world. In academia, computer forensics is taught and researched to improve the emerging field. The ability to educate and improve upon the emerging field is critical and academia is a crucial component in establishing computer forensics as a recognized and respected scientific field of study. The corporate world primarily uses computer forensics for civil litigation (i.e., trying to discover how employees have been using corporate systems). For example, a case that will be presented in more detail in chapter 2 is between the Four Seasons and Consorcio. Through computer forensics, Four Seasons was able to prove that Consorcio was attempting to circumvent their network security and providing fraudulent data to the courts.

The last primary user of computer forensics is the government. For the purpose of this paper government includes law enforcement and not military and intelligence branches. The usage ranges from trying to discover what a terrorist

may have on his/her computer to child pornography. The most numerous cases are child pornography with intellectual property and identity theft increasing rapidly. The focus of the paper will be on the law enforcement usage and related actors and roles as those are dominant in the field.

1.3. Actors & Roles in the Computer Forensic Investigation Process

When the police officers arrived in South-East London (discovering the headquarters of the iPod crew) the officers did not know what they were going to find. The officers who where first on the scene had to collect and preserve the integrity of evidence. The officer in this instance is classified as a first responder. A first responder is the first person on the scene (i.e. police officer) responsible for preserving evidence in the condition it was found. With such a task, the first responder needs to have a working knowledge of how the computer forensics process works, to prevent contamination of potential evidence. Several guides have been released to assist first responders identify and learn how to secure and maintain the integrity of potential evidence (e.g., Electronic Crime Scene Investigation – A Guide for First Responders by the National Institute of Justice).

After the initial discovery an investigator will be assigned to find further evidence in the case if applicable. The investigator will interact with the first responder(s) and the examiner(s) and/or expert(s) to collect evidence to reconstruct the crime scene(s) and the events that occurred. As a result of the

infancy of computer forensics, the investigator may also play the role of the examiner and/or expert.

When computer forensics has been contested, the expert is the actor most crucial for court proceedings. The role of the examiner is to extract and preserve the evidence while the expert analyzes, interprets, and presents results. The examiner will normally be called upon by the court for expert testimony. During this process the expert must qualify his or her credentials, procedures used for examination, and the end results. Chapter 2 discusses the court process and the need for a creation of a framework.

CHAPTER 2: LEGAL CHALLENGES TO COMPUTER FORENSICS

2.1. Introduction

Computer forensics is in the early stages of development and as a result, problems are emerging that bring into question its validity in the United States (U.S.) federal and state court systems. For practical purposes, the legal issues relevant to computer forensics are:

- admissibility of evidence;
- acceptability; and
- analysis and preservation

Historically, a significant portion of court cases were settled before the trial.[3] In many other instances, computer forensics evidence was never contested. However, when computer forensics evidence is contested, this builds the foundation to evaluate what, why, and how those issues should be considered when creating computer forensic standards and certifications to meet the requirements for the U.S. federal and state court systems (i.e. legal precedent).

[3] The U.S. Department of Justice maintains a site listing current and past select cases on cyber/computer crimes available at http://www.cybercrime.gov. The important aspect is to notice the amount of cases where the indicted person plead guilty.

2.2. Search and Seizure

Search and seizure of digital evidence is the first process that is often disputed (Mandia et al, 2003). If this step was not completed properly (i.e., illegal search and seizure or improper methodology), the defense or prosecution's evidence may not be admitted. Traditional non-digital instances of search and seizure contentions have been evaluated by courts using precedents (*Miranda* v. *Arizona*, 1966; *Katz* v. *U.S.*, 1967; *Illinois* v. *Andreas*, 1983). In contrast, digital cases are still emerging as the technology is new, resulting in few precedents to apply. As such, the methods law enforcement entities use with computer crime investigations become an issue. Currently, there are no rigid standards or methodologies.

A unique issue with computer forensics search and seizure, centers on the source of the item(s) in the warrant or in verbal/written affirmation when a warrant is not needed (i.e., open view resulting in a search and seizure). For instance, when a computer has the power turned off, the data in volatile memory is impossible to reconstruct. In pre-digital crimes, electricity was not a major factor in the ability to execute a proper search and seizure. Although there are not any documented U.S. federal or state court cases that have addressed this issue, it is a possibility in the future. In the United Kingdom, one defendant questioned the validity of improperly seized volatile media storage (Leyden, 2003).[4] Aaron Caffrey, the defendant, was arrested under the suspicion of launching a denial of

[4] The Caffrey court case regarding the trojan defense led to his acquittal in the denial of service attacks on the Port of Houston. The prosecution and expert in the case fear that the courts decision will lead to a new defense tactic – the trojan defense. This is an important case in the possible need to change current guidelines on how to deal with a 'live' computer.

service attack against the Port of Houston's systems on September 20th, 2001 (BBC News, 2003). The defense argued that a trojan[5] was installed on the defendant's computer by others who wanted to frame him for the attack (Leyden, 2003). The trojan, the defense contended, launched the attack from the defendant's computer but the defendant was not aware of the attack. The forensics examination showed that there was no sign of a trojan, only attack tools on the computer, but could not rule out that a trojan may have been in volatile memory (random access memory) (Leyden, 2003). The jury unanimously decided that the defendant was not guilty (Leyden, 2003).

Though courts may grant a search and seizure warrant, law enforcement may ask individuals for verbal or written consent to search and seize items without a warrant; however, the voluntary nature of consent may vary. In *Williford* v. *Texas*,[6] the appellant complained that the search and seizure of his computer was illegal. The appellant contended that his consent to the search and seizure was tainted, and as there was no warrant, there was no probable cause. The judge dismissed the claim. In *U.S.* v. *Habershaw*, the issue was whether the officers involved had the right to search and seize the computer, and

[5] "A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer" (Webopedia, 2004).

[6] Appellant took his computer to BCI for repairs where a technician discovered what he believed to be child pornography. BCI gave the appellant the choice to call police or they would to report the matter – appellant complied and had called the police. The detective on scene, Owings, read appellant his Miranda rights, appellant signed a waiver. Owings requested appellant if he could search and seize the computer, appellant complied. Court cited *Texas* v. *Brown* and *Waugh* v. *Texas* "the facts available to the officer would warrant a man of reasonable caution in the belief that certain items may be in contraband or stolen property or useful as evidence of a crime" Detective Owings had met the requirements – the court dismissed the voluntaries of appellant's consent to search.

if the defendant was capable of giving consent. The defendant argued that the warrant went "overboard" (*U.S.* v. *Habershaw*, 2002). The defendant gave verbal permission for the officers to operate his computer after the defendant stated the possible location of contraband child pornography images on the computer.[7] The defendant contended that the officers did not have probable cause, even though the contraband was in plain view.[8] The defendant also argued that he was incapable of giving verbal consent.[9] The court found against the defendant in respect to the aforementioned objections. Furthermore, Habershaw, argued against the warrant issued, by stating it was in violation of Federal Rules of Criminal Procedures (FRCP) Rule 41.[10] Habershaw contended that the hard drive was searched too extensively; exceeding the search warrant because it was conducted using a sector-by-sector[11] search (*U.S.* v. *Habershaw*, 2002). The defendant complained that technology is available to do searches by keywords that would not exceed the scope of the search warrant (*U.S.* v. *Habershaw*, 2002). Additionally, the defendant disputed the length of time the

---

[7] "The court upheld searching in which an officer asked defendant to open computer files showing on screen, and defended consented. *U.S.* v. *Lemmons, 282 F.3d 920,926 7th Circ. 2002* – upholding search of computer, where defendant assented to officer's request to her the officer operate the computer" (*U.S.* v. *Laine*, 2001).

[8] "Where the initial intrusion that brings the police within view of such an article is supported, not by a warrant, but by one of the recognized exceptions to the warrant requirement, the seizure is also legitimate" (*Coolidge* v. *New Hampshire,* 2002).
"Police have legal access to property and contraband they come across while acting pursuant to an exception to the Warrant Clause" (*Texas* v. *Brown*, 1983).

[9] The court entertained Dr. Schwartz who diagnosed Habershaw with impulse control disorder and gender Identity disorder. Neither of which gave persuasive evidence to Habershaw not being able to give voluntary consent.

[10] Federal Rules of Criminal Procedure Rule 41 outlines the process of search and seizure in respect to how officers define the warrant to the court (LII, 2004).

[11] "Sectors are the smallest physical storage units of a disk – Each sector stores 512 bytes of data" (Rogers, 2004).

search took as FRCP Rule 41 has a ten-day limit. The court denied both complaints by the defendant stating:

> This execution of the warrant, namely the seizure of the electronic information on the hard drive, took place well within ten days allowed. Further forensic analysis of the seized hard drive image does not constitute a second execution of the warrant or a failure to "depart the premises" as the defendant claims, anymore than would a review of a file cabinet's worth of seized documents (*Coolidge* v. *New Hampshire*, 2002).

Coolidge v. *New Hampshire* lays the foundation for the ability to analyze computer evidence in the ruling it was stated that the forensic analysis process did not constitute a second search and seizure, therefore not violating the ten-day limit in FRCP Rule 41. The judge ruled that using a bit-streamed image does not constitute a second execution of a warrant.

2.3. Admissibility of Tools

There are three primary methods to satisfy the U.S. federal and state court systems requirements for scientific evidence, *Frye*, Federal Rules of Evidence (FRE) 702, and *Daubert*. This section will focus on the two primary standards commonly used today, *Daubert* and FRE 702. To

properly cover admissibility of scientific evidence (admissibility of computer forensic tools), the rulings from the Supreme Court in *Kumho Tire Company* v. *Carmichael* will be considered rather than the FRE 702 interpretation because of the differences between the Supreme Court ruling and interpretation. It is important to keep in mind that *Daubert* is based on the principle that the judge acts as a gatekeeper – filtering out the "junk science." However, this principle normally relies on the attorneys contending the qualifications of an expert, the scientific nature of their evidence, and the validity and reliability of the methods and tools employed. If the tools do not meet the requirements as set out in the guidelines, the findings from these tools may not be admissible or given less importance.

When experts analyze evidence they utilize tools. Tools may include imaging hardware and software write blockers and software suites such as EnCase™ and Forensics Tool Kit™ (FTK™) used in the computer forensics investigation.

This section examines *Daubert* and applicable sections of FRE to determine if computer forensics tools meet the standards for acceptance as scientific evidence; the primary focus is on analyzing the reliability of the tools, peer review status, and acceptability (see Table 1).

2.3.1. Reliability & Validity

To determine reliability and validity under *Daubert* and FRE 702, several factors are required: known or potential error rates, testing, and commonly

agreed upon methods. Here again the computer forensic field has fallen short. With the (computer forensics field's) reliance on proprietary software (e.g., EnCase and FTK), the issue of error rates is an unknown. The vendors have not published information relating to error rates or even the exact reasons for minor and major version changes. Furthermore, the community is prevented from conducting in depth tests by the licensing contracts and legislation such as the Digital Millennium Copyright Act (DMCA) (U.S. Copyright Office, 1998).

Given the restrictions on full error testing and reporting, one method to establish some validity is to prove the reliability of the imaged or extracted data. If a forensic examiner makes a bit-stream image of the original source, the examiner can then compare the hash of the file structure of the original to the forensic copy by utilizing tools (checksum[12] algorithms) such as MD5[13] or SHA1.[14] These tools provide reasonable reliability that the image or the data written to a drive(s) is identical to the original and thus can be considered best evidence (*Ohio* v. *Cook*, 2002; *Four Seasons* v. *Consorcio*, 2003).

---

[12] "A simple error-detection scheme in which each transmitted message is accompanied by a numerical value based on the number of set bits in the message. The receiving station then applies the same formula to the message and checks to make sure the accompanying numerical value is the same. If not, the receiver can assume that the message has been garbled" (Webopedia, 2004).

13 "MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits. When using a one-way hash function, one can compare a calculated message digest against the message digest that is decrypted with a public key to verify that the message hasn't been tampered with. This comparison is called a "hashcheck"" (Webopedia, 2004).

[14]"The Secure Hash Algorithm takes a message of less than 2^{64} bits in length and produces a 160-bit message digest that is designed so that it should be computationally expensive to find a text, which matches a given hash. I.e. if you have a hash for document A, H(A), it is difficult to find a document B that has the same hash, and even more difficult to arrange that document B says what you want it to say" (DesAutels, 1997).

Table 1 *Daubert*, *Frye*, and FRE 702 Criteria

Daubert	FRE 702 *Kumho Tire* Version
"(1) such testimony was admissible only if relevant and reliable	"(1) can be and has been tested
(2) the Federal Rules of Evidence (FRE) assigned to the trial judge the task of insuring that an expert's testimony rested on a reliable foundation and was relevant to the task at hand	(2) has been subjected to peer review or publication
(3) some or all of certain specific factors—such as testing, peer review, error rates, and acceptability in the relevant scientific community might possibly prove helpful in determining the reliability of a particular scientific theory or technique" (*Kumho Tire*, 1999).	(3) has (a) high known or potential rate of error, relevant to the scientific community – where such factors are reasonable measures of the testimony's reliability; the trial judge may ask questions of this sort not only where an expert relies on the application of scientific principles, but also where an expert relies on skill or experience-based observation" (*Kumho Tire*, 1999).
Frye	FRE 702
"The rule is that the opinions of experts or skilled witnesses are admissible in evidence in those cases in which the matter of inquiry is such that inexperienced persons are unlikely to prove capable of forming a correct judgment upon it, for the reason that the subject-matter so far partakes of a science, art, or trade as to require a previous habit or experience or study in it, in order to acquire a knowledge of it. When the question involved does not lie within the range of common experience or common knowledge, but requires special experience or special knowledge, then the opinions of witnesses skilled in that particular science, art, or trade to which the question relates are admissible in evidence" (*Frye* v. U.S.., 1923).	"If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if
	(1) the testimony is based upon sufficient facts or data,
	(2) the testimony is the product of reliable principles and methods, and
	(3) the witness has applied the principles and methods reliably to the facts of the case" (LII, 2004).

While this approach can determine if an error occurred, it provides no information related to actual or potential error rates. Granted, there is testing for anomalies and reliability of some tools by third parties such as the National Institute of Standards and Technology[15] (NIST). However, NIST does not assume liability for the results and does not certify or accredit any specific tool.

One approach that many individuals have participated in and favor, is open source as the end all solution to tool anomalies. In the 1960's to 1970's the open source community emerged based on the principle of sharing information – the code for software and hardware. One reason for open source is to have the ability to know the program code. In an effort to show that open source is superior to closed source there have been arguments raised that the use of open source tools may increase the reliability of digital evidence derived from these tools (Kenneally, 2001). Proponents of the open source movement have stated that because end users can examine the source code, it is more secure and thus more reliable. However, the ability to view the source code does not necessarily translate to better security or to meeting the requirements of reliability, testing, and peer review (Poulson, 2001). The openness means that the source code is often the work of several authors who may or may not be trustworthy, who may or may not follow any software engineering method, and the code can be altered at anytime including after formal testing for error rates. With the ability for the tool and the code to be altered after testing and be continuously altered, the

[15] NIST. Computer Forensic Tool Testing Project. available from: http://www.ojp.usdoj.gov/nij/sciencetech/cftt.htm. This site presents results based on tests conducted at NIST on specified tools with the testing conditions so others may reproduce those results.

courts may find that the tool does not meet the requirements. Simply put, open source does not mean that it is peer reviewed. Questions remain as to who are the 'peers,' where was the source code published (e.g., journals, conferences), and does the potential to be reviewed mean that it has been reviewed?

2.3.2. Peer Review

According to *Daubert* and FRE 702, the expert's methods and processes must be consistent with methods that have been peer reviewed and/or published. The rationale being that, if the implementation of a theory is flawed, the results will be flawed; by requiring peer reviewing or publication, others in the relevant scientific community have the opportunity to discover flaws and supply recommendations or resolve errors prior to implementation. Hence, the tools used to derive the results must also be peer reviewed. A tool for computer forensics translates the basic manual processes into an application or device (e.g., storage preservation, recovery, and analysis). While there tends to be a heavy reliance on tools, the courts have found that an inanimate object (e.g. a software package, a tool) cannot be considered an expert (*State of Washington* v. *Leavell*, 2000).[16] This does not necessarily mean that the tool or results from that tool cannot be included in scientific testimony; the individual using the tool will often have to attest to the procedures used for it to be deemed admissible.

[16] The defense contended that an inanimate object, EnCase, cannot testify because it could not be cross-examined and does not meet the *Frye* test (new standard is *Daubert*). The court found it was not possible for such cross-examination to occur but that the expert who utilized the software package may testify on its behalf on the scientific and procedures.

Currently there are only limited publications for computer forensics methods and processes. At the time of writing there are two peer-reviewed journals specifically dedicated to computer forensics, the International Journal of Digital Evidence[17] and the Journal of Digital Investigations.[18] It is uncertain whether the criteria for peer review requires publication in journals focusing in a particular field, but based on the precedent set by other forensic sciences (e.g., forensic psychology, DNA analysis), the lack of such journals and conferences does not help the effort.

2.3.4. Acceptability

In *Daubert*, section three requires that the applied scientific principle be accepted in the relevant scientific community. This assumes two factors: that there is a relevant scientific community and that community has accepted the principles. This is problematic, as computer forensics being a relatively new field may not have an established scientific community per se. Currently the default has been to fall back on the use of established vendor tools as being industry standard and therefore accepted. However, in some instances the expert's choice of a tool is based solely on the ratings available on web sites, with little or no direct testing being conducted by that expert (*Williford* v. *Texas*, 2004).

The immaturity of computer forensics has further ramifications. The American Academy of Forensic Sciences (AAFS) has not fully recognized

[17] International Journal of Digital Evidence. available from: http://www.ijde.org
[18] Journal of Digital Investigations. available from: http://www.sciencedirect.com/science/journal/17422876

computer forensics as a scientific sub-discipline. To date the U.S. Court System has not commented on this fact, possibly because of the lack of technological depth. However, with the defense bar becoming more technically sophisticated, it is foreseeable that the recognition of the field and its underlying theory by the AAFS or a similar body will be a requirement for meeting the standards for scientific evidence. This requirement has been enforced with other pseudo forensic disciplines such as handwriting analysis/forensics where expert testimony has been nullified based on the fact that the application of the theory did not satisfy *Daubert* and FRE 702 requirements.[19]

2.4. The Expert

When conducting an analysis in computer forensics, the expert utilizes tools to examine and extract information pertaining to the crime. However, an area of concern is if one can be considered an expert solely based on his or her ability to use a tool, without the ability to clearly define how the tool works or knowing the program code. The majority of the tools used in computer forensics

---

[19] Federal Rules of Evidence Rule 901 discusses the admissibility of evidence by the requirement of authentication and identification; particularly through illustrations. "The court is merely holding that the Government has failed to meet its burden of establishing that the proffered expert testimony in this case is admissible under Rule 702. Second, even if the court were to hold that handwriting analysis is not a field of expertise under the rules, that would not render Rule 901(b)(3) meaningless. Rule 901(b)(3) does not deal exclusively with handwriting comparison, despite the fact that the Advisory Committee Notes for the rule discuss handwriting comparison testimony. Other types of comparison testimony are encompassed within the rule. Last, and most important, Rule 702 and Rule 901 must be read together. Rule 901(b)(3) contemplates testimony by an expert--but before an expert's testimony can be admitted, it must past through the gates of Rule 702. In this case, Mr. Cawley's testimony did not make it through the Rule 702 gate and, therefore, Rule 901 is irrelevant to the question of whether his testimony is admissible" (*United States* v. *Saelee*, 2001).

are proprietary and copyrighted, thus negating the ability to access the source code.[20] Currently, this inability of the expert to test the code and understand exactly what the tool is performing, has not hindered the admissibility of expert's testimony. In *Williford* v. *Texas*, the court found that an expert does not need to know the code of the software package (tool) nor the background processes. However, this does not mean that the object or results from that object cannot be used for scientific testimony; although in some circumstances, the individual using the tool will have to attest to the procedures used. A possible argument to be made in court regarding the third criteria of *Daubert* is that the computer forensic community has accepted certain industry standard tools such as EnCase. However, with a field in its infancy, is it justified to say that the relevant scientific community has accepted certain tools? The current experts have to qualify their educational background, which includes courses taken by corporate (*California* v. *Rodriguez*, 2001) or federal agencies on how to operate software packages and conduct search and seizures. In some cases, the qualifications are that the "expert" is the computer expert for a local police force.

In addition, to have an expert discredited based on credentials, one must show deficient argumentation. In *Broderick* v. *Texas*, the appellant contested that "his counsel was ineffective for failing to object to evidence suggesting that he had been in possession of child pornography." (*Broderick* v. *Texas*, 2000) The prosecution's expert was not able to discover any live files, only deleted files

[20]"Appellant's counsel objected to Detective Owings's testimony regarding the use of EnCase and images copied by it on the ground that Detective Owings was not qualified as an expert to testify about the theory or technique in developing the EnCase software or its reliability" (*Williford* v. *Texas*, 2004).

that they were unable to reconstruct. The files recovered were descriptive in a sexual manner, some with names from the previous case of the contaminated hard drive. Moreover, the expert did not view any of the files (*Broderick* v. *Texas*, 2000). "Broderick argues that his counsel should have objected to this evidence, and was deficient for failing to effectively cross-examine the witness and for failing to obtain his own expert witness to rebut the evidence" (*Broderick* v. *Texas*, 2000). Although the court ruled against the appellant because this was not originally disputed and was part of a post-conviction relief motion, this is an issue of serious concern for future cases. In the U.S., every citizen is guaranteed a fair trial, if one is not achievable because of lack of expertise of legal counsel and experts in an area that could acquit the defendant, then the foundation of the legal justice system has been compromised.

2.5. Analysis and Preservation

If the evidence makes it through the first two processes, it must be proven that the analysis and preservation was conducted properly. A common practice is to make a bit-stream image[21] of the storage media that is to be examined. It is possible to use hashing algorithms such as MD5 or SHA1 to try to validate that the data written on the drive(s) is identical to the original. The courts have indicated that if the values computed for the source and image match, the image is a valid copy and considered to be original (*Ohio* v. *Cook*, 2002; *Four Seasons*

[21] A bit-stream image is one where a hard drive sends bit by bit, live and "dead" data to another hard drive.

v. *Consorcio*, 2003). In *Taylor* v. *Texas*, the testimony by the expert showed that he used a contaminated hard drive from a prior case to make a mirror image of the appellant's drive. Furthermore, the expert formatted[22] Taylor's drive by accident when attempting to prepare the destination drive (*Taylor* v. *Texas*, 2002). Unfortunately, the court did not make a decision on this contention and upheld the trial court's decision. In all likelihood, the appellant was found guilty because of testimony of other witnesses. Nonetheless, the fact that a court would ignore that evidence was clearly contaminated should have more bearing in a case that is based strictly on computer evidence.

Once the computer evidence is in the possession of law enforcement, steps must be taken to ensure that the evidence is not contaminated or destroyed. In *Regina* v. *Caffrey* (Leydon, 2003), the potential evidence was destroyed once the power to the computer was terminated. However, computer evidence may be lost by other means, such as age, electromagnetic force, and dropping of storage media. In *Ohio* v. *Cook*, the defendant disputed several issues on the legitimacy of the data and the circumstantial evidence on whom was the creator of the files. "The state maintains that a forensic computer examiner will rarely, if ever, be able to find evidence actually placing a person at the keyboard committing the crimes" (*Ohio* v. *Anderson*, 2004). The defendant claimed proper steps were not taken to ensure the integrity of the data on the

[22] "To prepare a storage medium, usually a disk, for reading and writing. When you format a disk, the operating system erases all bookkeeping information on the disk, tests the disk to make sure all sectors are reliable, marks bad sectors (that is, those that are scratched), and creates internal address tables that it later uses to locate information. You must format a disk before you can use it. reformatting a disk does not erase the data on the disk, only the address tables" (Webopedia, 2004).

hard drive, such as placing the drive in a static bag (*Ohio* v. *Cook*, 2002). The defendant also contested the date and time of files on the system as the state did not test the CMOS[23] for the current time of the system nor place a battery on the CMOS when put in evidence for integrity of the system clock. The defense's computer forensic expert discovered the system clock was off by roughly five minutes and the defendant was not home during the times of all file creation (*Ohio* v. *Cook*, 2002). However, the court found that it is plausible to remotely access the system and create the files in question (*Ohio* v. *Cook*, 2002). The court also found that such measures as described to ensure integrity are not needed as the mirror image was authenticated to be an exact copy of the original (*Ohio* v. *Cook*, 2002). On the other hand, if the defendant was correct, the hard drive may have lost bits in transit, (*Ohio* v. *Cook*, 2002) possibly occurring if the evidence was placed next to a radio communication device with ample power in the back of a police cruiser causing data to be lost and resulting in bit manipulation (National Institute of Justice, 2001; National High Tech Crime Unit, 2003). Although it is feasible that damage to the drive occurred, the likelihood of the bits being re-arranged to form child pornography is unlikely.

Timelines are as important in pre-digital forensics as in computer forensics. In attempts to reconstruct when events may have occurred, the system clock is not always the most reliable device. In *Ohio* v. *Anderson*, the arguments raised were two pronged; if the time stamps were correct, the

[23] "Personal computers … contain a small amount of battery-powered CMOS memory to hold the date, time, and system setup parameters" (Webopedia, 2004).

defendant claimed he did not own a compact disc recorder at the time, hence, it was difficult to prove that the defendant made the compact discs (CD), and other storage media in question (*Ohio* v. *Anderson*, 2004). The first dispute was that the last creation date for the CD was January 1997, and the appellant did not have a CD copier until August 1999. He also stated that his office computer's multimedia player history file showed that no files were viewed from the CD in question (*Ohio* v. *Anderson*, 2004). The state found that Anderson knowingly possessed the pictures on the compact disc because of Internet chat logs of the defendant. However, Anderson was able to get charges dropped on a similar instance regarding a jaz® disc.[24] As the state could not prove that the defendant had knowledgeable possession of images on the media (*Ohio* v. *Anderson*, 2004), the court upheld its previous decision that it is rare to identify an individual at the computer where the crime took place; but plausible if other evidence supports that the defendant would have knowledge of the evidence such as chat logs or other deliberate actions.

In *Four Seasons* v. *Consorcio*, one controversy dealt with the creation of files on the floppy discs (i.e., timeline inconsistencies). The plaintiff claimed the defendant made fraudulent discs that had been filed as evidence, destroying the originals. "Based upon the examination and breakdown of the serial number, Ashley determined that the floppy disc had been manufactured at the Verbatim® factory in Taiwan on the 154th day of 2002. The fact that these floppy discs were not the original floppy discs from February 2002 was clearly shown…"(*Four*

[24] A jaz disc is a removable media created by iomega®.

Seasons v. *Consorcio*, 2003). It is difficult to have storage media containing evidence manufactured after the creation date of the evidence. While it was not a complicated method to prove legitimacy, it allowed the court, without hesitation, to disregard the defendant's claims. This case also discussed the usage of log files and who was able to create signatures left in the log files. The log files are used to record authorized and unauthorized attempts to access privileged information and devices on the network. In this instance, the overwhelming amount of forged packets coming from Consorcio into Four Seasons was evidence of blatant hacking attempts. This resulted in the expert from Consorcio reversing his previous claims that the logs were legitimate traffic (*Four Seasons* v. *Consorcio*, 2003).

In attempting to manipulate the evidentiary procedures of the court, entities have, as in *Four Seasons* v. *Consorcio*, attempted to create fraudulent information.[25] In *Kucala Enterprises* v. *Auto Wax Company*, the issue dealt with the software package Evidence Eliminator™,[26] installed on the computer for the purpose to destroy evidence. The computer forensic expert was unable to determine the extent to which the aforementioned software was used; only that it had been installed on the computer in question (*Kucala* v. *Auto Wax Company*, 2003). The use of software to cleanly wipe data resulting in a low probability of recovery has been tested and proven. Not out of the ordinary, the court ordered Kucala to pay attorney fees and costs for court proceedings from the time Kucala

[25] Recall from *Four Seasons* v. *Consorcio* the duel over the floppy discs and evidence was claimed to be created prior to the manufacturing of the floppy discs.
[26] Evidence Eliminator is a tool that claims to delete evidence securely so that programs that recover deleted files cannot recover files deleted with Evidence Eliminator.

first ran Evidence Eliminator up to and including the time, the parties appeared before the court for the hearing (*Kucala* v. *Auto Wax Company*, 2003). The fine in this case was much less than what could have been if the evidence existed. The case was dismissed because there was no longer evidence with which to pursue legal action.

CHAPTER 3: LOOKING TOWARDS OTHER PRACTICES FOR CERTIFICATION AND STANDARDIZATION

3.1. Introduction

The U.S. Court Systems are having difficulties in mandating and interpreting standardization and certification for computer forensics. Therefore, it becomes the responsibility of the scientific community to assist in this endeavor. While it may not be feasible to have absolute standards and methodologies because of each case being unique, there are intrinsic characteristics that are found in a majority of cases that can be used in creation of a framework.

Working towards a creation of a framework for a field relies on identifying areas of contention as explored in chapter 2. From the identified areas of contention this section analyzes and borrows from established practices towards a solution. To analyze the issue of tools this section compares and contrasts (high-level overviews) trust and certification architectures: secure socket layer (SSL) certificate issuance and maintenance, WebTrust™, and Underwriters Laboratories® (UL®). To mitigate the risk of expert contentions the second section will explore certification in technical and non-technical fields with high-level overviews of: American Institute of Certified Public Accountants (AICPA), Information Systems Security Certification Consortium ($(ISC)^2$), and Information Systems Audit & Control Association (ISACA).

3.2. Tool Certification

Because of conditions of uncertainty, trust, and legal issues certifications emerged to mitigate the legal liability and risk posed to entities and with the intention of reassuring consumers of a product or service. In the mid 1990's the Internet faced issues of providing assurance to entities of the reliability and validity of the product or service offered. To mitigate this issue entities developed and continue to improve upon implemented solutions that appear to have mitigated legal liability and risk while reassuring entities of the reliability and validity of the product or service offered.

3.2.1. SSL Certificate Issuance

In the early days of public and business usage of the Internet there was immense concern surrounding transaction security. The concern over security resulted in entities hesitating to purchase goods and/or services via the Internet. To mitigate this risk of data interception and improve customer relations, the information technology community turned to cryptography. The community decided that the communication channel between the two parties (computers) needs to be reliable and maintain privacy for transmission of data. To this end, secure socket layer was created, with deployment starting with SSL 2.0 in 1994. SSL has continued to evolve with SSL 3.0 in 1996 and Transport Layer Security (TLS) 1.0 in 1999 (Hickman, 1995; Lorch, 2000; Treese et al, 2005). SSL was created using peer reviewed methods and comments (i.e., review for comment document (RFC)) and cryptographic technologies. In the creation of SSL trust

relationships were critical to ensure integrity and security. In a high level view, SSL is broken down into web browser, certificate issuer, certificate holder, and validity.

The web browser may have support for SSL 2.0 and 3.0. With a browser that supports the SSL protocol the browser contains information on trusted certificate issuers that the browser manufacturer includes and if applicable, those that are manually added. The browser also includes a mechanism to update the certificate issuer list with the public key and the revocation list (Freier et al.1996).

The certificate issuer is a trusted third party that has a public and private key. The certificate issuer keeps the private key and releases the public key so consumers may validate the certificate for the website. All appropriate data is transferred using public/private key cryptography. If the certificate is not valid the consumer's browser typically warns that information transmitted may not be secure. Additionally, if a certificate is compromised the issuer or holder may revoke the certificate to alert the consumer that the certificate is not valid and information transmitted may be insecure or un-trusted. The key concept here is that there is a trusted third-party that validates that the site is what it represents itself to be and that the data transmitted is computationally secure giving consumers and entities assurance of the data transmitted.

3.2.2. WebTrust

Though SSL made improvements to online transactions, consumers are/were concerned about online transactions. In 1998, AICPA conducted a

survey and discovered that 85 percent of consumers would not use their credit cards online because of security concerns (Grant Thornton, 1998). To increase consumer confidence the AICPA and the Canadian Institute of Chartered Accountants (CICA) created WebTrust. WebTrust is an auditing procedure for online websites to provide trust between the consumer and entities. To accomplish this WebTrust is composed of areas such as: privacy, trust, security, and policy.

WebTrust is based on the same principles as auditing requirements for publicly traded companies (i.e., an independent third-party validation process). The independence requires that the entity performing the audit and the employees for that entity not have any interest in the entity they are auditing. To become WebTrust certified an auditor who is a member of either AICPA or CICA must pass the in the United States the Certified Professional Accountant Examination (CPA) and in Canada the Chartered Accountant Exam to be eligible to take the WebTrust exam to conduct WebTrust audits. At the end of the audit for WebTrust the auditor will issue his or her findings. The process for the entity to gain the WebTrust seal is similar to SSL certificate issuance and maintenance (AICPA/CICA. 2000).

Through the WebTrust process there is a common theme of trust and security. For consumers and entities the process and later certification relies on the trust and security of the WebTrust branding. The main principle to obtain from WebTrust is using an independent third-party to issue a level of trust (i.e., certificate) that demonstrates to consumers the site is trusted.

3.2.3. Underwriters Laboratories

As in WebTrust and SSL the goal is to build an online trust between the consumer and entity. Another approach is the trust between consumers and entities for the products purchased. In 1894 the Underwriters Laboratories (UL) were established as an independent not-for-profit organization to give assurance to consumers on safety products. Since inception, UL has expanded worldwide and tested millions of products (UL, 2005). UL has also expanded into other areas of validation to give assurance and trust to companies. For instance, there is most likely a sticker affixed to the back of a television or underneath a laptop with the UL logo and the certificate number indicated it has passed their product evaluation.

To maintain the level of trust with the consumers and government UL must remain independent. Furthermore, UL publishes all standards and certifications for products for review. UL goes further by allowing consumers to read all standards and certification and who UL has certified. The process that the UL undergoes for testing of hardware is different in each case, but the main principle is that the UL tests and then issues a certification that a product meets a standard if appropriate (UL, 2005).

3.3. Actor Certification

To show credibility of knowledge for individuals in a professional community, accreditation and certification bodies were established. The principle behind this is to have an individual in the community demonstrate knowledge that

is required to perform that job function. The certifications explored in this section have strengthened their communities and other communities such as legal and financial.

3.3.1. Certified Professional Accountant Exam

For the financial sector in the United States, the CPA exam is the gold standard for demonstrating knowledge to certify financial statements. For instance, if you are not a CPA and audit the financial statements of Purdue University, a CPA must sign off and issue the report. The CPA is administered by the AICPA. To become a CPA the candidate must meet requirements. The requirements to take the examination vary by jurisdiction; some may require educational and/or work experience. Because of the jurisdictional issues if a CPA moves between states they may be required to recertify for that state, similar to the bar examination. Furthermore, to retain your status you must be a member of AICPA, recertify, have enough continued educational credits, and abide by AICPA regulations and procedures. The goal behind the exam is to demonstrate the examinees' practical and theoretical knowledge in four areas: auditing and attestation, financial accounting and reporting, regulation, and business environment and concepts. This exam is 14 hours, where the examinee performs real-world scenarios of auditing and financial reporting and completes written essays and multiple choice questions for all categories (AICPA, 2005). With the difficulties in the accounting industry the CPA exam has been modified and has a portion for hypothetical situations if new regulations are

imposed. Further, the test is peer-reviewed by a committee (the committee is comprised of AICPA members who have successfully passed the CPA exam), thus the framework for the CPA exam allows modification for future growth and changes in the industry. Additionally, the AICPA offers additional certifications for CPAs in specialized areas, such as WebTrust.

3.3.2. ISACA

The accounting community has had to adapt to technology by auditing the systems where financial information is processed and stored. This gave birth to the information technology auditor. The primary organization for information technology auditors is ISACA (Information Systems Audit & Control Association). ISACA offers two certifications, the Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM).

The CISA has been around since 1978, and has been constantly updated and peer reviewed by the CISA review board. Every five years the test is compared to the industry to ensure it is meeting requirements and retrofitted if needed. Eligibility for the test is one of the most demanding, with five years work experience in the field during a 10-year period. There are substitutions for requirements with education or work in a related field but a maximum of two years exemption. The examinee must adhere to the ISACA Professional Code of Ethics and demonstrate educational growth and work experience in the field on an annual basis to maintain the certification. The examination is modular and uses real-world scenarios for testing the knowledge of the examinee in the

following seven categories: 1. management, planning, and organizations of information systems, 2. technical infrastructure and operational practices, 3. protection of information assets, 4. disaster recovery and business continuity, 5. business application system development, acquisition, implementation, and maintenance, 6. business process evaluation and risk management, and 7. the information system audit process (ISACA, 2004; ISACA, 2005).

3.3.3. $(ISC)^2$

The $(ISC)^2$ offers the Certified Information Systems Security Professional Certification (CISSP). The basis was to band several groups together with a common goal of information systems security and certify individuals for this profession based on the common body of knowledge for information security. The board updates and peer-reviews the test regularly. The examinees must have four years full-time work experience in one of the ten areas in the common body of knowledge (CBK). A candidate may substitute one year of work experience for a college degree in a related area and one additional year for a Masters in Information Security from a national center of excellence. Furthermore, all candidates must adhere to the code of ethics by $(ISC)^2$. The exam is six hours focusing on the ten domains of the CBK: 1. access control systems and methodology, 2. applications and systems development security, 3. business continuity planning and disaster recovery planning, 4. cryptography, 5. law, investigation and ethics, 6. operations security, 7. physical security, 8. security architecture and models, 9. security management practices, 10.

telecommunications and network security ((ISC)^2, 2005). Upon certification professionals are required to pay annual membership dues, continue professional education by completing 120 units in a three-year time period ((ISC)^2, 2005).

CHAPTER 4: CREATING A FRAMEWORK FOR COMPUTER FORENSICS

To assist the courts and the scientific community this chapter explores the creation of a framework for computer forensics to address the concerns presented in chapter 2. The framework is in two separate areas, tools and actors. To try to satisfy the applicable court requirements the framework is based on the areas of contention discussed in chapter 2 and FRE 702, *Daubert*, and *Frye*.

4.1. Proposal for Tools: One Possible Solution

While shopping on the Internet and finalizing the transaction do you question what is occurring behind the information presented on your screen? Most people do not have a complete picture of what is occurring behind the scenes but trust the process to some extent. The certifications (e.g., WebTrust) and auditing standards (e.g., Statement on Auditing Standards No. 70) provide an additional level of trust. In traditional products such as televisions, computers, light bulbs, and millions of other electronic products Underwriters Laboratories (UL) certifies to assure consumers and may be used in legal proceedings.

Unlike Internet or traditional products there is no method to provide an additional level of trust. This problem will most likely grow as experts using

computer forensics tools without knowing nor able to discover what occurs in the process(es) (i.e., the program code). With computer forensics tools there are two options, an open or closed source. For purposes of this section neither open nor closed source tools have inherit benefits over the other.

If the method to derive evidence does not meet the requirements for scientific evidence in the U.S. Courts, then what follows may not be admissible. In creating a framework for tools to possibly be accepted by the courts as scientific evidence features will be used from the previously discussed established certifications in information technology, accounting, and engineering practices. A trusted independent third-party (TITP) should be established for testing and certification of computer forensic tools or utilize an existing entity (i.e., Underwriters Laboratories). The TITP must be not-for-profit and may not outsource its testing to minimize potential independence issues. The processes that the TITP utilizes must be peer-reviewed, published, and made publicly available along with results for each tool. The TITP should assume partial liability for only what they have performed and certify how the tool functions under their testing conditions. Testing will vary for each tool (e.g. write blocker v. EnCase); however, testing must ensure that the tool performs accurately under random testing in a controlled environment to prevent vendor testing manipulation. The end result would be a list of approved tools that the judiciary could utilize if a *Daubert* contention arose.

4.1.1. Do We Need A Framework For Tools?

To partially satisfy reliability and validity criteria of FRE 702 and *Daubert* testing must occur. If there has not been any testing of the tool, then the court may not grant admissibility of the evidence. Though the framework does solve for testing, there is still an inherit problem that comes with information technology products, namely the issue of protecting intellectual property. Most information technology companies that sell a product such as EnCase or FTK rely on their intellectual property to remain in business. Assume the role of a director for Guidance Software™, the manufacturer of EnCase. Why would Guidance Software want to spend additional funds to validate their intellectual property? The software, tool has been contested and so far stood its ground, so why spend the funds and how much if any intellectual property must Guidance concede to the community?

Because intellectual property is the backbone of most of the vendors and/or manufacturers of digital tools the framework needs to justify how testing is useful to the manufacturers/vendors. The intellectual property of these companies does not necessarily need to be disclosed. Under the proposed framework there is no need for the TITP to know the code of the tool to ensure that the tool functions as stated. For example, if XYZ company's tool states it makes bit-stream images that are exact copies of the original, the TITP would test the tool to ensure it meets that functionality. Further, the TITP will certify the tool and assume partial liability for ensuring that the tool performs as stated under the TITP testing procedures. Similar to the National Institute of Standards

and Technology Computer Forensics Tool Testing (NIST CFTT) the TITP would use a controlled environment to test the functionality of the tool. Assume the bit-stream imaging tool used can only bit-stream image hard disk drives, and only integrated drive electronics (IDE) and enhanced integrated drive electronics (EIDE). In this case, the TITP would test several IDE and EIDE hard disk drives with known outcomes to see if the bit-stream image device they are testing performs as expected. This does not require the vendor of the bit-stream imaging tool to reveal their intellectual property (e.g. NIST CFTT).

Another problem with computer forensic tool vendors is the release of patches and new versions; patches are usually implemented to correct errors in the tools. This issue has affected other industries such as automobile manufacturers (e.g., recalls for faulty seat belts), though the patches typically come after scrutiny and after an event occurred to trigger the scrutiny. The area of patching the tools without knowing the exact cause could lead to cases being overturned because the evidence was obtained and extracted using tools that had errors. This may meet the requirements of scientific evidence.

The current framework does not answer this concern directly. However, the testing phase may be able to discover the errors to prevent the need for patches. Furthermore, the framework can provide detailed explanations for patches via the list provided to the judiciary. For instance, if XYZ company discovers that their tool (a software program used to recover deleted files) displays duplicates of all deleted files then the company should release a patch. The patch released would correct this error and in the judiciary list an explanation

would state the extent of the error, how the error may affect results, and the versions affected. Through the testing and certification process, this should satisfy the first requirement of both *Daubert* and FRE 702 and part of the third criteria. Though this may not satisfy the peer review requirements because it is a TITP, it should fulfill the publication requirement (i.e., the publicly available test results, test methodologies, and judiciary list).

4.1.2. Acceptability of the Framework?

In conforming to the rules for scientific evidence, the relevant scientific community must accept the methodologies used for creation (i.e., theories) of the tools. The theories and/or methodologies behind the tools are known in the scientific community, however, the implementation of these is not known. Given that the TITP is testing the implementation of the methodologies for the tools, it is logical that the framework will strengthen the acceptability, reliability, and validity of computer forensic tools as scientific evidence. The availability of the results to the public and the judicial list will allow further review and critiquing of the process. Through this process the results of the TITP should strengthen the acceptability if testing and certification were done properly.

4.2. Proposal for Certification

Currently, the lower courts accept qualifications based on the skills and previous work experience of the experts; while this has been sufficient to date, it

is anticipated that contesting the expertise and qualifications of expert witnesses will become more common in the future. Thus, the need for a national and eventually international recognized certification and standardization for computer forensics is necessary. Although this will not make the expert issue moot, it may help mitigate the exposure of the experts. If there is a national certification, the short-term problems will be individuals going through the qualification process, and dealing with those who have testified as an expert witness in the past failing the examination.

Despite the possible setbacks and side effects to creating a certification, it must be done to strengthen the immature computer forensics scientific discipline to gain credibility, reliability, and validity (Meyers & Rogers, 2005). The certification needs to be implemented by an accreditation organization either created or administered by current organizations such as, American Academy of Forensic Sciences (AAFS) or Information Systems Security Certification Consortium ((ISC)^2). In other fields of study (e.g., accounting and information technology accountability professions) there are methods used to ensure that the practice is credible and reliable, and that the individuals claiming to be professionals have met a certain certification criteria. As previously discussed there are key similarities between the Certified Professional Accountant Examination (CPA), Certified Information Systems Security Professional (CISSP), and Certified Information Systems Auditor (CISA) certifications. All of the examinations test the common body of knowledge, standards and methodologies for the respective profession while not being proprietary. These

key components give credibility to the fields, as it shows an individual is qualified by examination and organizational procedures (i.e., requiring several years of experience prior to qualifying to take the examination). Furthermore, reproducibility of the results is possible by following the same procedures. Currently both of these aspects are missing in the computer forensics field. The question now becomes: is it possible for an approach similar to the above certifications to be applied to computer forensics, and if so, what should be required?

The first problem with creating a certification/standard is the realization that it must have flexibility to allow for revisions; otherwise the standard is worthless because the technology continuously changes. In attempting to deal with the ability to create a standard for computer forensics, each phase of the forensic process needs to be analyzed. For example, in search and seizure, the standard will need to effectively cover all aspects; this would include areas such as the warrant, preservation of evidence, on-scene forensics examination, transportation of evidence, documentation, and 4th and 5th amendments (Kerr, 2004). Accordingly, the certification must be broken down into several qualifying examinations by the role of the actor, as not all persons in the field will participate in all of the investigative phases (e.g., search and seizure, analysis, examination). With this in mind, the construction of a framework is broken down as follows (see Figure 4.1).

Figure 4.1. Pyramid of Actor Roles

4.2.1. First Responder

It is not reasonable to assume that all cases involving electronic evidence and/or requiring computer forensics will be predetermined. As it cannot always be predetermined when electronic evidence may be potential evidence the crime scene may need to be contained by the first responder. A first responder is the first person on the scene (i.e. police officer) responsible for preserving evidence in the condition it was found. The first responder needs to know proper methods to handle potential electronic evidence and when to call in an expert. Additionally, there may be instances when the first responder is required to do preliminary searching of electronic evidence. The first responder will need to demonstrate knowledge in the following areas:

- Ethics;
- Law (applicable state or federal);

- Identification of electronic evidence;
- Seizing and transportation of electronic evidence;
- Documentation;
- Chain of custody; and
- Searching electronic evidence.

The weight for each module will vary. There is also an optional module for first responders, searching electronic evidence. First responders must adhere to all principles of the accreditation organization and be recertified every three years to ensure knowledge, skills, and abilities are maintained and updated (SWGDE, 2004).

4.2.2. Investigator

The investigator's main purpose is to direct in a managerial role the discovery, seizure, transportation, and preservation of evidence. Furthermore, the investigator is also responsible for preparing applicable legal documents to pursue cases (e.g., search warrants). To qualify to be a certified computer forensics investigator the individual must have at least one year work experience as an investigator in a law enforcement unit (i.e., non-digital investigator). Ideally, once the certification process matures the work experience would be one year under a certified computer forensics investigator. The investigator will have required modules of preparation of legal documents and managing an electronic evidence investigation in addition to the same modules as first responder (see

Table 2). The investigator will be required to adhere to all principles of the accreditation organization and go through recertification every three years with continued educational credit requirements to ensure knowledge, skills, and abilities are maintained and updated(SWGDE, 2004).

4.2.3. Examiner

An examiner would normally be found in a large organization where there are experts and either examiners or technicians, depending on terminology used. When a case is brought forth and needs electronic evidence extracted, it may go to an examiner and then to an expert for analysis and interpretation. The examiner is responsible for examination of the electronic evidence. The examiner must demonstrate the theory and applied usage of tools. Additionally, the examiner will be required to take the previous modules of the first responder. The ethics, law, documentation, chain of custody, searching and preservation, and preparation modules will be more in-depth to fit the actor's role accordingly (see Table 2) (SWGDE, 2004). To enhance credibility of the exam there will be a two year work experience requirement in a related field for eligiblability to take the test to be a certified examiner. The examiner will be required to adhere to all principles of the accreditation organization, completed a predetermined amount of continued education credits, and be recertified every two years for quality control and to ensure knowledge, skills, and abilities are maintained and updated.

4.2.4. Expert

The expert is responsible for examination, analysis, interpretation, and presentation of findings in a court of law. The expert will be required to demonstrate knowledge by completing the examiner module requirements; however, the legal module will be more intensive and there will be two additional modules, analysis and presentation modules (see Table 2) (SWGDE, 2004). The expert must hold a bachelor's degree to meet American Society of Crime Laboratory Directors / Laboratory Accreditation Board (ASCLD/LAB) requirements for education (ASCLD-LAB, 2004). To be able to take the test the expert must have two years of experience as an examiner and one additional year under an expert (after maturity of the certification process) for a total of three years of work experience. The expert will be required to adhere to all principles of the accreditation organization; complete a predetermined amount of continued education credits, and go through recertification annually. The certification will entail demonstration of theoretical and practical knowledge of emerging tools and technologies and legal changes. Furthermore, expert court testimony will be reviewed annually for quality control (SWGDE, 2004).

Table 2 Proposed Conceptual Certification Framework Module Requirements

	First Responder	Investigator	Examiner	Expert
Ethics	Yes	Yes	Yes	Yes
Law (Federal and/or State)	Yes	Yes	Yes	Yes
Discovery & Identification	Yes	Yes	Yes	Yes
Seizing & Transportation	Yes	Yes	Yes	Yes
Documentation	Yes	Yes	Yes	Yes
Chain of Custody	Yes	Yes	Yes	Yes
Searching Electronic Evidence	Optional	Optional	Yes	Yes
Preparation	No	Yes	Yes	Yes
Management	No	Yes	No	No
Theory	No	No	Yes	Yes
Practical	No	No	Yes	Yes
Analysis & Interpretation	No	No	No	Yes
Presentation	No	No	No	Yes

Table 3 Proposed Certification Framework vs. SWGDE Proposed Framework (SWGDE, 2004).

	First Responder		Investigator	Command / Supervision	Examiner	Technician	Expert	Examiner / Analyst
Ethics	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Law (Federal and/or State)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Discovery & Identification	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Seizing & Transportation	Yes	Yes	Yes	No	Yes	Yes	Yes	No
Documentation	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Chain of Custody	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Searching Electronic Evidence	Optional	No	Optional	No	Yes	Yes	Yes	Yes
Preparation	No	No	Yes	No	Yes	No	Yes	No
Management	No	No	Yes	Yes	No	No	No	No
Theory	No	No	No	No	Yes	No	Yes	No
Practical	No	No	No	No	Yes	Yes	Yes	Yes
Analysis & Interpretation	No	No	No	No	Yes	No	Yes	No
Presentation	No	No	No	No	Yes	No	Yes	No

Proposed Certification Framework
SWGDE Proposed Framework

4.3. Certification Modules

Elaborating on the previous section, this section presents a conceptual framework of the certification modules. When an accreditation board is established for certification the proposed modules should assist in identifying areas of knowledge, skills, and abilities that the respective actors should posses. This is a conceptual framework only; the accreditation board will need to expand the modules.

4.3.1. Ethics Module

In criminal and civil investigation the goal is to discover the truth no matter what the outcome (i.e., innocent or guilty); this may be difficult in some cases (e.g., the suspect assaults and/or batters an actor). This module will be comprised of ethical based questions that will be appropriate for the actor's role (e.g., discovering, preserving, seizing, analyzing, presenting, and searching of electronic evidence).

4.3.2. Law Module (Federal and State)

The law module will be the most comprehensive module to help mitigate the risk of future incidents during the investigation phases as discussed in chapter 2. This module will need to be customized by state because of different laws and a federal module. The examinees will be tested on their knowledge of what constitutes and requires: consent, a warrant, searching, seizing, and

preservation. The breadth and depth of knowledge required for the areas will vary by actor role.

4.3.3. Discovery & Identification of Electronic Evidence Module

This module tests the examinee's knowledge of discovery and identification of electronic evidence. For example, the first responder should be able to identify potential sources of electronic evidence (e.g., pictures of items such as a computer, printer, fax machine, pager, cellular phone, and digital camera). Although discovery may occur after the first time, (i.e., searching a drive and finding information not in the search warrant thus requiring an additional warrant) this module does not cover searching evidence and discovery of information not pertaining to the case that would require a warrant.

4.3.4. Seizing and Transportation of Electronic Evidence Module

The trojan defense, spoliation of evidence, and manipulation of evidence are only a few examples that need to be addressed in this module. To ensure that safety, reliability, and validity of potential evidence the seizing and transportation is important to all actors. For this module the examinee will need to demonstrate his/her knowledge to properly seize and transport electronic evidence (e.g., demonstrate knowledge of how to assess the scene and when appropriate to contact an expert to prevent contamination of potential evidence). As the expert is not required in all instances, the actor (i.e., first responder) will

need to demonstrate the procedures to properly seize and transport potential electronic evidence. To fully asses the examinee's knowledge this module will be broken down into a hands-on and written portion.

4.3.5. Documentation Module

To provide a timeline for when events occur during the entire investigation and post-investigation documentation is required. The focus during the investigation should be on documenting the crime scene and collection process. To help facilitate in the ability to move documents between actors a standardized, sequential numbering system is needed (e.g., the Bates numbering system) (Lisson, 2005). All examinees will need to know how to use the numbering system to prepare documentation. Furthermore, the examinees will need to demonstrate his/her writing abilities and examiner's and expert's technical writing skills. This module would be comprised of a multiple choice section of mock documents where the examinee will demonstrate how to use the numbering system and a writing section to demonstrate applicable writing skills.

4.3.6. Chain of Custody Module

During the investigation it is important to document who has accessed potential evidence and its current location (chain of custody). In a simplistic overview, the chain of custody is a record of who has accessed evidence and where it is maintained in a log file. The log file typically contains time and date

that evidence is checked in/out, identifier (i.e., badge or employee number), item number, and location. The examinee needs to demonstrate the procedures of chain of custody and what information must be maintained in the log.

4.3.7. Searching Electronic Evidence Advanced Module

Although not all actors should be conducting searching of electronic evidence there may be situations where it is necessary. Therefore, this module is optional for first responders and investigators and required by examiners and experts. Occasions may occur when electronic evidence was not expected at the crime scene; however, it is required to search the evidence that moment to pursue the case (e.g., *U.S.* v. *Habershaw* the first responders did not know that they would be conducting a search of electronic evidence). Because these instances occur the first responder should be prepared to do limited searching of electronic evidence. The first responder should use basic tools (e.g., write blocker and a software tool such as File Hound)[27] to search for files and if evidence is discovered proceed with proper procedures (i.e., seizing and transporting and/or calling an expert). The examinee for this module will be required to demonstrate knowledge in searching and limited usage of tools in a hands-on and written portion.

[27] File Hound was developed at Purdue Universities School of Technology CyberForensic Laboratory by Blair Gillam. File Hound was developed for first responders and local law enforcement agencies with minimal funding to identify potential pornographic images prior to seizing or taking further action on the system.

4.3.8. Preparation Module

During an investigation, legal documents may need to be prepared prior to gathering potential evidence (i.e., search and seizing warrant). To obtain permission from the courts to gather potential evidence, the investigator should indicate the location and forms of electronic evidence. This module assesses the knowledge of the investigator on how to properly prepare documentation. The examinee will be given a hypothetical situation and must prepare the proper documentation and obtain permission to proceed with his or her investigation with a mock court approval.

4.3.9. Managing Electronic Evidence Module

Although the primary actor for this module (i.e., the investigator) is assumed to have managerial skills, the examinee must demonstrate his/her ability to apply those skills to electronic evidence (computer forensics). The purpose of this module is to assess the ability of an investigator to coordinate a crime scene and case that has an electronic evidence portion. This module tests the examinee's ability to direct individuals through the phases of the computer forensics investigation. This will be accomplished by the examinee demonstrating his/her knowledge of electronic evidence in a hypothetical scenario with multiple choice questions and written sections.

4.3.10. Theory & Practice of Tools Module

To strengthen credibility the examiner and expert must be able to explain what is occurring at each step of the investigation and examination process and why certain events are occurring (e.g., how data is being recovered and why it is possible to recover data). The SWDGE has identified the following areas of required knowledge and skills for examiners: write protect, media characterization, physical/logical copy, restoration, directory listing, erased file recovery, residue extraction, search by criteria, internet activity, password recovery, verification, identification and/or recovery of hidden information, and identification and/or recovery of encrypted data (Scientific Working Groups on Digital Evidence and Imaging Technology, 2004). The examiner and expert must know how to apply the theories behind the tools to real-world scenarios. This module tests the examinee's knowledge in a practical scenario with a mock examination and a written portion.

4.3.11. Analysis & Interpretation Module

In the analysis and interpretation phase the expert will take the examination results and extract information that is relevant for the case. Essentially, the expert will take the data and make it into information that can be used and understood by the courts. Data not relevant to the case should not be used unless permission is granted by the courts to access that information (i.e., additional search warrants). The examinee will need to demonstrate knowledge

of analyzing, interpreting, and correlating data in a hypothetical scenario with written and hands-on sections.

4.3.12. Presentation Module

The expert may be called upon by a court to testify on evidence presented or possibilities of events occurring. The expert needs to be able to demonstrate credibility of his or her knowledge and skills along with the evidence presented to ensure it meets the applicable state or federal criteria for scientific evidence. Additionally, the expert needs to demonstrate written skills, as much of the work submitted to the court and jurors is documentation. The module will test the examinee in a mock trial where the examinee presents (i.e., prepares visual representations and documentation) the hypothetical scenario from the analysis module and is cross-examined by lawyers and judges.

CHAPTER 5: CONCLUSION

The number of cases involving computer forensics and digital evidence will continue to increase as computers become more intertwined in society. Currently the computer forensics field, and its derived evidence, has difficulty meeting the *Daubert* and FRE 702 criteria. This has serious consequences to the computer forensics field as it can only survive for a finite period if its existence relies solely on the lack of technical and scientific understanding of the courts. The fact that the U.S. Court Systems have given the computer forensics field the rubber stamp for admissibility to this point is no guarantee that it will do so indefinitely (Kerr, 2004). As the defense bar becomes more knowledgeable regarding digital evidence and computer forensics, there will be an increase in *Daubert* and FRE challenges, and more judicial scrutiny on the point of what constitutes valid scientific evidence computer forensics (Smith, Bace, 2003). Simply stated, currently the computer forensics field is not meeting the U.S. Court System's required criteria for acceptable scientific evidence. Therefore, the members of the computer forensics field needs to take decisive actions to implement sound solutions to meet the required criteria for the U.S. Court Systems.

In exploration of the legal challenges and requirements for scientific evidence for the U.S. Court Systems this thesis proposed certification for tools and roles in the computer forensic investigation process. Through legal exploration the framework identified the current and future areas of contention. The proposed framework for certification of tools and actors may fill the void in computer forensics and fulfill the requirements of scientific evidence for the courts. The principles proposed in the framework allow for flexibility and mandate continual peer reviewed updates of requirements for testing of actors and tools.

The proposed conceptual framework for certification of tools is the first step towards bringing reliability, credibility, and validity to the computer forensics field. Through the proposed framework for tool certification a trusted independent third party (TITP) would be established to conduct the testing. All results and reason for patches of certified tools would be made publicly available and a list provided to the judiciary in a “good housekeeping list.” The acceptability of tools is crucial as if the tools do not meet the requirements for scientific evidence then the evidence may not be admissible. Through the proposed framework the criteria of *Frye*, *Daubert*, and FRE 702 may be satisfied because:

1. Establishment or utilization of an established accreditation board, therefore creating a recognized relevant scientific community required by *Daubert* and FRE 702;
2. Testing tools required by *Daubert* and FRE 702;

3. Peer review of tools and actor certification process required by *Daubert* and FRE 702;
4. Potential known error rates through the testing required by *Daubert* and FRE 702 Supreme Court interpretation;
5. Certification of tools (i.e., demonstrating that the tools are sound and based on scientific theory) required by *Daubert* and FRE 702.
6. Certification of actors (i.e., demonstrating special knowledge, skills, and abilities to qualify as an expert) required by *Frye*, *Daubert*, and FRE 702;
7. Expert testimony resting on a reliable foundation required by *Daubert* and FRE 702; and
8. Tools and actors being subjected to peer review and publication of results to assist the U.S. Court Systems and required by *Daubert*;

Although the proposed framework is not the answer to all the problems it is a starting point for the computer forensics and digital forensics communities to use as a foundation based on legal requirements and rulings. Through this foundation the computer forensics community may be able to overcome issues that can be correlated to its infancy. The ability to mitigate the legal risks to the computer forensics community may be accomplished using sound principles similar to other fields (i.e., accounting, Internet transaction trust, Underwriters Laboratories).

The computer forensics practitioners must act as it is necessary for its survival. Time is no longer a luxury; the computer forensics community cannot

rely on AAFS indefinitely as the time frame of digital forensics being accepted as a forensic field may be years away. Computer forensics as a field has experienced events that should never be repeated (e.g., lack of standards, certification, and peer review). For the field of computer forensics to mature, there must be a national system for certifying tools used and actors involved in the investigation process. The continued lack of a certification for the tools used and actors involved in the investigation process may ultimately lead to the same fate as other fields, (e.g., handwriting forensics and polygraph) and result in computer forensics being relegated to the role of pseudo science or worse, a "junk science." The framework is the foundation to fill the void and bring reliability and credibility while possibly preventing an untimely demise for the computer forensics field.

REFERENCES

AICPA. (2005). The Uniform CPA Examination. Retrieved on March 7, 2005 from http://www.cpa-exam.org/.

AICPA/CICA. (2000). WebTrust Program for Certification Authorities. Version 1.0 Retrieved on March 7, 2005 from http://www.aicpa.org.

American Society of Crime Laboratory Directors (ASCLD-LAB). (2004). Legacy: Personnel Qualifications. Retrieved on March 25, 2005 from http://www.ascld-lab.org/legacy/aslablegacypersonnel.html.

BBC News Inc. (2003). Teenager critical of computer police Retrieved on March 7, 2005 from http://news.bbc.co.uk/1/hi/england/hampshire/dorset/3181652.stm.

Broderick v. Texas (2000) 35 S.W.3d 67

California v. Rodriguez (2001) No. SCR-28424 CSR No. 7062 January 9-11, 2001 Testimony

Carter, Helen. (2004). iPod files help to snare car theft gang. The Guardian. Final Edition. London.

CERT/CC. (2004). CERT/CC Statistics 1988-2003. Retrieved on February 4, 2005 from http://www.cert.org/stats/cert_stats.html.

Coolidge v. New Hampshire. (2002). 403 U.S. 443, 465, 91 S. Ct. 2037, 29 L. Ed. 2d 564

DesAutels, Phillip. (1997). SHA1 Secure Hash Algorithm - Version 1.0. Retrieved on March 7, 2005 from http://www.w3.org/PICS/DSig/SHA1_1_0.html.

Four Seasons Hotels & Resorts v. Consorcio Barr. (2003) 267 F. Supp. 2d 1268; U.S. Dist. Lexis 8717; 16 Fla. L. Weekly Fed. D 389

Freier, Karlton, Kocher. (1996). SSL 3.0 Specification. Retrieved on March 7, 2005 from: http://wp.netscape.com/eng/ssl3/.

Fyre v. U.S. (1923) 293 F. 1013 D.C. Cir. Retrieved on March 7, 2005 from http://www.law.harvard.edu/publications/evidenceiii/cases/frye.htm.

Grant Thornton. (1998). CPA WebTrust Seal Erases Consumer Concerns about Electronic Commerce. Tax&Business Advisor. 7

Hickman, Kipp. (1995). The SSL Protocol. Retrieved on March 24, 2005 from http://wp.netscape.com/eng/security/SSL_2.html.

Howe, Melvyn (2004). 'IPOD CREW' KINGPIN BEGINS JAIL SENTENCE. PA News.

Illinois v. Andreas. (1983) 463 U.S. 765, 771

Information Systems Audit & Control Association. (2004). Candidate's Guide to the CISA Exam. Rolling Meadows, IL: ISACA

Information Systems Audit & Control Association. (2005). Requirements for CISA Exam. Retrieved on March 7, 2005 from http://www.isaca.org.

$(ISC)^2$. (2005). $(ISC)^2$ Retrieved on March 7, 2005 from :https://www.isc2.org, https://www.isc2.org/cgi-bin/content.cgi?category=97, https://www.isc2.org/cgi/content.cgi?category=7.

Legal Information Institute. (2004). Federal Rules of Evidence. Retrieved on March 7, 2005 from http://www.law.cornell.edu/rules/fre/rules.htm.

Legal Information Institute. (2004). Federal Rules of Criminal Procedures. Retrieved on March 7, 2005 from http://www.law.cornell.edu/rules/frcrmp/Rule41.htm.

Katz v. U.S. (1967) 389 U.S. 347, 362

Kenneally, Erin. (2001) "Gatekeeping Out of the Box: Open Source Software as a Mechanism to Assess Reliability for Digital Evidence." Virginia Journal of Law and Technology. Fall 2001.

Kerr, Orin. (2004) Computer Crime and the Coming Revolution in Criminal Procedure. Yale Law School

Kucala Enterprises v. Auto Wax Company. (2003) 56 Fed. R. Serv. 3d 487

Kumho Tire Company v. Carmichael. (1999), (97-1709) 526 U.S. 137 131 F.3d 1433

Leyden, John. (2003). Caffrey acquittal a setback for cybercrime prosecution. The Register, Retrieved March 7, 2005 from http://www.theregister.co.uk/2003/10/17/caffrey_acquittal_a_setback/.

Lisson, Jeffery. (2005). Tracking Documents in Litigation For Less Than $30. Lexis Nexis, Retrieved April 4, 2005 from http://www.lexisone.com/legalresearch/onetoone/techno05.html.

Lorch, Markus. (2000). Secure Internet Protocols. Department of Computer Science at Virginia Tech. Retrieved March 24, 2005 from http://web.archive.org/web/20010804222946/http://csgrad.cs.vt.edu/~mlorch/securityprotocols/6.6.html.

Mack, Mary. (2003). Electronic Discovery vs. Computer Forensics. New Jersey Law Journal, 1.

Mandia, Prosise, Pepe. (2003). Incident Response & Computer Forensics (Second Edition). New York, NY: McGraw-Hill

Meyers, Rogers. (2004). Computer Forensics: The Need For Standardization And Certification. International Journal of Digital Evidence. Fall 2004, Volume 3, Issue 2.

Meyers, Rogers. (2005). Computer Forensics: Meeting The Challenges of Scientific Evidence. In Proceedings, International Federation for Information Processing Digital Forensics Working Group 11.9.

Michaely, Womack. (1999). Conflict of Interest and the Credibility of Underwriter Analyst Recommendations. The Review of Financial Studies Special Vol. 12, No. 4, 653-686

Miranda v. Arizona. (1966). 384 U.S. 436

National High Tech Crime Unit. (2003). Good Practice Guide for Computer Based Electronic Evidence.

National Institute of Justice. (2001). Electronic Crime Scene Investigation – A Guide for First Responders. Washington D.C.: National Institute of Justice

Ohio v. Anderson. (2004). Case No. 03CA3 3-02-0415

Ohio v. Brian Cook. (2002). 149 Ohio App. 3d 422; 429

Palmer, Gary. (2001). A Road Map for Digital Forensic Research. Utica, New York. Digital Forensics Research Workshop. Retrieved on March 22, 2005 from http://www.dfrws.org/dfrws-rm-final.pdf.

Poulson, Kevin. (2001). Microsoft: Closed Source is More Secure. Retrieved on March 7, 2005 from http://www.securityfocus.com/news/191.

Regina v. J.M.H. (2003) Ontario Superior Court O.J. No 5513; ON,C Lexis 4742

Rogers, Marc. (2004). Disk Structures and The Boot Process.

Texas v. Brown. (1983). 460 U.S. 730; 738-739

Taylor v. Texas. (2002) 93 S.W.3d 487; 499-502

Tresse, Rescorla, Housley, Harman, Mankin. (2005). Transport Layer Security. Retreived on March 24, 2005 from http://www.ietf.org/html.charters/tls-charter.html.

Scientific Working Group on Digital Evidence. (2004). Recommended Guidelines for Developing a Quality Management System. Retrieved on March 23, 2005 from http://ncfs.org/swgde/SWGDE%20Recommended%20Guidelines%20for%20Developing%20a%20Quality%20Management%20System%20(October%202004).pdf.

Scientific Working Groups on Digital Evidence and Imaging Technology. (2004). SWDGE/SWGIT Proficiency Test Program Guidelines Version 1.0. Retrieved on March 23, 2005 from http://ncfs.org/swgde/documents/swgde2004/SWGDE-SWGIT%20Proficiency%20Test%20Document%20_October%202004_.pdf.

Scientific Working Groups on Digital Evidence and Imaging Technology. (2004). SWDGE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence Version 1.0. Retrieved on March 23, 2005 from http://ncfs.org/swgde/documents/swgde2004/SWGDE-SWGIT%20DE%20Training%20Document%20_October%202004_.pdf.

Smith, F. & Bace, R. (2003). A guide to forensic testimony: The art and practice of presenting testimony as an expert technical witness. Boston, MA: Addison-Wesley.

State of Washington v. Leavell. (2000) Cause No 00-1-0026-8.

Syntegra. (N.D.) Common Criteria An Introduction.

UL, Underwriters Laboratories Retrieved on March 7, 2005 http://www.ul.com.

U.S. v. Habershaw Criminal. (2002). No. 01-10195-PBS, U.S. Dist. Lexis 8977.

United States v. Saelee. (2001). 162 F. Supp. 2d 1097.

U.S. v. Lemmons. (2002). 282 F.3d 920,926 7th Circ.

U.S. v. Laine. (2001). 270, F.3d 71, 76 1st Cir.

United States Department of Justice. Retrieved on March, 5, 2005, from http://www.cybercrime.gov.

U.S. Department of Justice Computer Crime and Intellectual Property Section, Criminal Division. (2002) Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Washington D.C.: United States Department of Justice

U.S. Copyright Office. Digital Millennium Copyright Act. Washington D.C. 1998. Retrieved on February 2, 2005 from: www.copyright.gov/legislation.

Williford v. Texas. (2004). 127 S.W.3d 309; Tex. App.

Webopedia. (2004). Online Computer Dictionary for Computer and Internet Terms and Definitions. Retrieved on March 7, 2005 from http://www.webopedia.com/TERM/c/checksum.html, http://www.webopedia.com/TERM/m/md5.html, http://www.webopedia.com/TERM/T/Trojan_horse.html, http://www.webopedia.com/TERM/f/format.html.