Computer Forensics: The Need for Standardization and Certification

Matthew Meyers and Marc Rogers
CERIAS
Purdue University

Abstract

This paper is a call for standardization and certification for the computer forensics field. It presents an overview of some of the more serious issues in the maturing discipline of computer forensics and explores three areas within the legal system where computer forensics is most likely to be questioned: search and seizure, expert qualifications, and analysis and preservation. One problem area identified that needs to be addressed sooner, as opposed to later, is the lack of standards and certification. The paper examines the need for standardization and certification by analyzing federal and state court cases (criminal and civil) and concludes with suggestions for dealing with some of the issues raised.

Introduction

The spread of crime using computers was inevitable; the question is how much damage computer crime has caused and still may. The domain of computers, for the purposes of this paper, is confined to media that is intended for a computer to read or be used as a peripheral. For example, a digital telephone answering machine is not within the scope, but the use of a compact disc containing data or written by a computer would qualify. For this paper, computer forensics is defined[1] as "the use of an expert to preserve, analyze, and produce data"[2] from volatile and non-volatile media storage.

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

[1] Computer forensics is defined throughout the paper as: the use of an expert to preserve, analyze, and produce data from volatile and non-volatile media storage. This is used to encompass computer and related media that may be used in conjunction with a computer.
[2] Mack, Mary. Electronic Discovery vs. Computer Forensics. New Jersey Law Journal. October, 20 2003. Page 1. A portion of her definition was used; however, the entire definition was not used due to 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 …"

- admissibility of evidence,
- standards and certifications,
- analysis and preservation.

Historically, a significant portion of court cases has been settled before the trial.[3] In other instances, computer forensics evidence was never contested. Conversely, when computer forensics evidence has been contested, it has provided the foundation for evaluating what, why, and how those issues should be considered when creating computer forensic standards and certifications for the U.S. federal and state court systems.

Search and Seizure

Search and seizure of digital evidence is the first process that is often disputed.[4] If it can be shown that this step was not completed properly, the defense or prosecution's evidence may not be admitted. An illegal search and seizure or improper methodology employed during search and seizure can negatively affect the admissibility of the evidence. Traditional, non-digital instances of search and seizure contentions have been evaluated by courts from precedents.[5] In contrast, the digital cases are still emerging as the technology is created, resulting in few precedents to apply. As such, the methods law enforcement entities use with computer crime investigations becomes the issue. Currently, there are no rigid standards, and the guidelines and recommendations differ between law enforcement sources. [6]

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 (e.g., open view resulting in a search and seizure). For instance, when a computer has the power turned off, the data in volatile media storage, for technical purposes, is virtually 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 no 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.[7] Aaron Caffrey, the defendant, was arrested under the suspicion of

[3] http://www.cybercrime.gov. This site contains a list of current and past select cases by the US DOJ on computer crimes. It is important to note the amount of cases where the indicted person pled guilty.
[4] Mandia, Prosise, Pepe. Incident Response & Computer Forensics Second Edition. McGraw-Hill 2003
[5] Miranda v. Arizona 384 U.S. 436 1966
Katz v. U.S. 389 U.S. 347, 362 1967
Illinois v. Andreas 463 U.S. 765, 771 1983
[6] US Department of Justice Computer Crime and Intellectual Property Section, Criminal Division. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. July 2002
NIJ Electronic Crime Scene Investigation – A Guide for First Responders 2001.
NHTCU Good Practice Guide for Computer Based Electronic Evidence 2003
[7] Leyden, John. Caffrey acquittal a setback for cybercrime prosecution. October 17, 2003. The Register – U.K. Press 3. A description of the court case is given regarding the Trojan defense used by Caffrey that led

launching a denial of service attack against the Port of Houston's systems on September 20th, 2001.[8] The defense argued that a Trojan[9] was installed on the defendant's computer by others who wanted to frame him for the attack.[10] 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 storage media (random access memory).[11] The jury unanimously decided that the defendant was not guilty.[12]

Though courts may grant a search and seizure warrant, law enforcement may ask individuals for verbal or written consent to search and seize items.[13] However, the voluntary nature of consent may vary. In Williford v. Texas,[14] 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.[15] The judge dismissed the claim. In U.S. v. Habershaw,[16] the issue was whether the officers involved had the right to search and seize the computer, and if the defendant was capable of giving consent. The defendant argued that the warrant went "overboard."[17] 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.[18] The defendant contended that the

---

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.

[8] BBC News Inc. Teenager critical of computer police http://news.bbc.co.uk/1/hi/england/hampshire/dorset/3181652.stm October 17, 2003 Page 1

[9] Webopedia. "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."

[10] Leyden, John Page 1

[11] Id. Pages 1-2

[12] Id. Pages 1-2

[13] Id.

[14] Williford v. Texas 127 S.W.3d 309; 2004 Tex. App. 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 called the police. The detective on scene, Owings, read appellant his Miranda rights, appellant signed a waiver. Owings asked 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.

[15] Id.

[16] U.S. v Habershaw Criminal No. 01-10195-PBS, 2002 U.S. Dist. Lexis 8977. The defendant was arrested and found guilty of being in possession of child pornography. The defendant contested his mental ability to give verbal or written consent.

[17] Id. Page 22

[18] Id. Page 16-17 The court citing U.S. v. Laine, 270, F.3d 71, 76 1st Cir. 2001. The court upheld searching in which an officer asked defendant to open computer files showing on screen, and defendant consented.

officers did not have probable cause, even though the contraband was in plain view.[19] The defendant also argued that he was incapable of giving verbal consent.[20] 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 Rule 41.[21] Habershaw contended that the hard drive was searched too extensively, exceeding the search warrant since it was conducted using a sector-by-sector[22] search.[23] The defendant complained that technology is available to do searches by keywords that would not exceed the scope of the search warrant.[24] Additionally, the defendant disputed the length of time the search took as 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.[25]

This court case lays the foundation for the ability to analyze computer evidence in the forensic process past the ten-day limit stated in Rule 41. The judge ruled that using a bit-streamed image does not constitute a second execution of a warrant.

The "Expert"

In order to determine the admissibility of scientific expert testimony, several tests are applied; for computer forensics the focus is on Daubert[26] and Federal Rules of Evidence (FRE) 702 (Rule 702).[27]

U.S. v Lemmons, 282 F.3d 920,926 7th Circ. 2002 – upholding search of computer, where defendant assented to officer's request to allow the officer operate the computer.

[19] Id. Page 17 The court citing Coolidge v. New Hampshire, 403 U.S. 443, 465, 91 S. Ct. 2002, 2037, 29 L. Ed. 2d 564 "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."
The court also cited Texas v. Brown 460 U.S. 730, 738-739 Police have legal access to property and contraband they come across while acting pursuant to an exception to the Warrant Clause.

[20] Id. Pages 18-22 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.

[21] Id. Page 24 Federal Rules of Criminal Procedure 41. Rule 41 outlines the process of search and seizure in respect to how officers define the warrant to the court.

[22] "Sectors are the smallest physical storage units of a disk – Each sector stores 512 bytes of data". Marc Rogers Disk Structures and The Boot Process February 4, 2004

[23] U.S. v. Habershaw Page 22

[24] Id. Page 22-26

[25] Id. Page 17 The Court citing Coolidge v. New Hampshire

When conducting an analysis in computer forensics, the "expert" utilizes tools to examine and extract information pertaining to the crime. However, an area of contention is whether one can be considered an expert solely based on his ability to use a tool or software package, without the ability to clearly define how the tool works or reviewing the source code. The majority of the tools and software used in computer forensics is proprietary and copyrighted, thus negating the ability to access the source code.[28] Currently, this inability of the expert to test the code and understand exactly what is happening under the hood, so to speak, 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 nor the background processes.

The question arises concerning if an expert who cannot attest to area three of Daubert qualifies as an expert. The third criteria of Daubert states specific factors such as peer review, error rates, and acceptability in the relevant scientific community are important elements to consider when determining the reliability of the scientific tests.[29] Currently it is difficult to meet the third criteria due to a lack of error rates for most of the tools and methods. Additionally, there are no standards in the field or peer reviews of methods.

The courts have found that an inanimate object (e.g. a software package) cannot be considered an expert.[30] This does not mean that the object or results from that object cannot be used for scientific testimony, however in some circumstances, the individual using the software package will have to attest to the

---

[26] Kumho Tire Company v. Carmichael 526 U.S. 137; 1999. Page 137 The Court cites Daubert v. Merrell Dow Pharmaceuticals, Inc. 509 US 579, 1993. In a case involving the admissibility of scientific expert testimony, the U.S. Supreme Court held that (1) such testimony was admissible only if relevant and reliable; (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; and (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.

[27] Id. Page 139 In determining the admissibility of an expert's testimony, including the testimony of an engineering expert, under Rule 702 of the FRE, a federal trial judge may properly consider one or more of some specific factors – whether the theory or technique (1) can be and has been tested, (2) has been subjected to peer review or publication, (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.

[28] Williford v. Texas Page 312. "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."

[29] Kumho Tire Company v. Carmichael. Court citing Daubert v. Merrell Dow Pharmaceuticals Page 137

[30] State of Washington v. Leavell Cause No 00-1-0026-8 October 20, 2000. The defense contended that an inanimate object, EnCase™, cannot testify since it could not be cross-examined and does not meet the Fry 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.

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 tool,s such as EnCase™. However, with a field in its infancy, is it justified to say that the relevant scientific community has accepted certain software packages? The current experts have to qualify their educational background, which includes courses taken by corporate[31] 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 and purchased a software package based on a web-based report on the rating.[32]

In addition, in order to have an expert discredited based on credentials, one must show deficient expostulation. In Broderick v. Texas,[33] the appellant contested that "his counsel was ineffective for failing to object to evidence suggesting that he had been in possession of child pornography."[34] The prosecution's expert was not able to discover any live files, only deleted files 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.[35] "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."[36] Although the court ruled against the appellant, since this was not originally disputed and was part of a post-conviction relief motion, it is of serious concern for future cases. In the U.S., every citizen is guaranteed a fair trial; if one is not achievable due to lack of expertise of legal counsel and investigators in an area that could acquit the defendant, then the very foundation of the legal justice system has been compromised.

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[37] of the storage media that is to be examined. It is possible to use checksum[38] algorithms such as MD5[39] or SHA1[40] to try to

---

[31] California v. Rodriguez No. SCR-28424 CSR No. 7062 January 9-11, 2001 Testimony Regina v J.M.H Ontario Superior Court O.J. No 5513; 2003 ON,C Lexis 4742

[32] Williford v. Texas Pages 312-313

[33] Broderick v. Texas 35 S.W.3d 67; 2000 page 72, 78

[34] Id. page 72

[35] Id. Page 78

[36] Id. Page 78

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

[38] Webopedia 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.

39 Id. 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

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.[41] In Taylor v. Texas,[42] 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[43] Taylor's drive by accident when attempting to prepare the destination drive.[44] 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 due to testimony of other witnesses. Nonetheless, the fact that a court accepted evidence that was clearly contaminated should have more bearing in a case that is strictly computer evidence based.

Once law enforcement has possession of the computer evidence, steps must be taken to ensure that it is not contaminated or destroyed. In Regina v. Caffrey,[45] the potential evidence was destroyed when 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,[46] the defendant disputed several issues on the legitimacy of the data and the circumstantial evidence on who the creator of the files was. "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."[47] The defendant claimed proper steps were not taken to ensure the integrity of the data on the hard drive, such as placing the drive in a static bag.[48] The defendant also contested the date and time of files on the system as the state did not test the CMOS[49] for the current time of the system nor place a battery on the CMOS

---

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."

[40] W3.org/PICS/DSig/SHA1_1_0.html The Secure Hash Algorithm takes a message of less than 264 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.

[41] Ohio v. Brian Cook, 149 Ohio App. 3d 422; 2002 Page 429
Four Seasons v. Consorcio Page 70

[42] Taylor v. Texas 93 S.W.3d 487;2002 Pages 499-502

[43] Webopedia. 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.

[44] Taylor v. Texas Pages 499-500

[45] Leydon, John repeat 2

[46] Ohio v. Cook Page 430

[47] Ohio v. Anderson Case No. 03CA3 3-02-04 Page 15

[48] Ohio v. Cook Page 428

[49] Webopedia. Short for ***c****omplementary* ***m****etal* ***o****xide* ***s****emiconductor*. Pronounced ***see****-moss*, CMOS is a widely used type of semiconductor. CMOS semiconductors use both NMOS (negative polarity) and PMOS (positive polarity) circuits. Since only one of the circuit types is on at any given time, CMOS chips require less power than chips using just one type of transistor. This makes them particularly attractive for use in

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.[50] However, the court found that it is plausible to remotely access the system and create the files in question.[51] 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.[52] On the other hand, if the defendant was correct, the hard drive may have lost bits in transit.[53] If the evidence was placed in the back of a police cruiser next to a radio communication device with ample power, data could be lost and bit manipulation could occur.[54] 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 just 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 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, and other storage media in question.[55] 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.[56] 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 (a form of media storage). The state could not prove that the defendant had knowledgeable possession of images on the media.[57] 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[58] one controversy dealt with the creation of files on the floppy discs. The plaintiff claimed the defendant made fraudulent discs filed as evidence, destroying the originals. "Based upon the examination and

---

battery-powered devices, such as portable computers. Personal computers also contain a small amount of battery-powered CMOS memory to hold the date, time, and system setup parameters.

[50] Ohio v. Cook Page 429

[51] Id. Page 430

[52] Id. Page 429. The court cited Ohio Evid. R. 901(B)(9) and Rigby v. Lake Count 1991, 58 Ohio St.3d 269, 271

[53] Id. Page 428

[54] NIJ Pages 35-36 HTCUS Page 13

[55] Ohio v. Anderson Page 14

[56] Id. Page 14

[57] Id. Page 20

[58] Four Seasons v. Consorcio Page 86

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…"[59] 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 use 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[60] that the logs were legitimate traffic.

In attempting to manipulate the evidentiary procedures of the court, entities have, as in Four Seasons v. Consorcio, attempted to create fraudulent information.[61] In Kucala Enterprises v. Auto Wax Company,[62] the issue dealt with the software package Evidence Eliminator,[63] installed on the computer for the purpose of destroying evidence. The computer forensic expert was able to determine that the software had been installed on the computer in question, but not the extent to which it was used.[64] The use of software to cleanly wipe data, resulting in a very 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 first ran Evidence Eliminator up to and including the time, the parties appeared before the court for the hearing.[65] The fine in this case was much less than what it could have been if the evidence existed. The case was dismissed because there was no longer evidence with which to pursue legal action.

Conclusion

The inevitable fact that technology is becoming more intertwined in the daily life of the individual will lead to an increase in court cases where computer evidence is a vital component. Because the judicial system is having difficulties in mandating and interpreting standardization for computer forensics, it becomes the responsibility of the scientific community to assist in this endeavor.

---

[59] Id. Page 87
[60] Id. Page 103-105
[61] 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.
[62] Kucala Enterprises v. Auto Wax Company 56 Fed. R. Serv. 3d 487, May 27, 2003
[63] Evidence Eliminator Available online: http://www.evidence-eliminator.com/product.d2w. This product claims to delete evidence securely so that programs that recover deleted files cannot recover files deleted with Evidence Eliminator.
[64] Kucala v. Auto Wax Company Pages 5-7
[65] Id. Pages 24-26

In other fields of study, (e.g., accounting and financial fraud investigation) 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. In the accounting profession, there is the certified professional accountant (CPA) examination, as well as standards and methodologies for the accounting processes. These two key components give credibility to the field, as it shows an individual is qualified by examination (that requires several years of experience prior to qualifying to take the examination) and, that it is possible to follow a procedure to come to the same results. Both of these aspects are missing in the computer forensics field. The question now becomes: is it possible for an approach similar to accounting to be applied to computer forensics, and if so, what should be required?

The first problem with creating a standard is the realization that it must have flexibility in order to allow for revisions. Because the world continuously changes, an inflexible standard is not practical and can become worthless. In attempting to create a standard for computer forensics, each phase of the forensic process must be analyzed to determine the most practical method. In search and seizure, the standard will need to effectively cover all aspects, including the warrant, preservation of evidence, on-scene forensics examination, transportation of evidence, documentation, and 4th and 5th amendments.[66] Accordingly, the certification may need to be broken down into several qualifying examinations, since not all persons in the field will participate in all of the investigative phases (e.g., search and seizure, analysis, examination, etc.).

The second area of concern, the qualifications of expert witnesses, is an issue concerning experts of all fields. The computer forensic field is fairly unique, as it has no credentials or a formal educational process. 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 internationally 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, and those who have testified as experts, failing the examination. If this occurs, it may lead to appeals in cases where evidence was admitted under the qualifications of a computer forensics expert who did not pass the examination.

Regarding the last area discussed, analysis, preservation, and presentation of the evidence, there should be rigorous standards, and requirements coupled with continual updates to the processes. The common methodology used to analyze the evidence currently relies on proprietary software or hardware which does not

[66] Kerr, Orin. Computer Crime and the Coming Revolution in Criminal Procedure. Yale Law School, 2004

allow experts to know exactly what is happening under the proverbial hood. This is a serious issue; the experts must be able to explain what is occurring at each step of the duplication and analysis process and why certain events are occurring (e.g., how data is being recovered and why it is possible to recover data). The expert should know, in detail, the major file systems and theory behind file system structure to adapt those principles to new file systems. Furthermore, in order to determine that the data was properly preserved and analyzed, the computer forensics examiner/expert must know the engineering mechanics behind these devices. Additionally, preservation standards need to be created on how to store original and duplicated evidence to prevent contamination and damage.

Although the problems of computer forensics can be correlated with the field being in its infancy, it is time to take decisive actions. Computer forensics, as a field, has experienced events that should never be repeated (e.g., lack of standards and peer review). In order for the field of computer forensics to mature, there must be a national system for certifying individuals who claim to be professionals. The continued lack of a professional certification, investigative standards, and peer reviewed method, may ultimately result in computer forensics being relegated to a "junk science," as opposed to a recognized scientific discipline.

About the Authors

Matthew Meyers (mlmeyers@cerias.purdue.edu) is a graduate student pursuing his Interdisciplinary Master of Science in Information Assurance and Security at Purdue University.

Marc Rogers Ph.D., CISSP, CCCI, (mkr@cerias.purdue.edu) is an Associate Professor in the Department of Computer Technology at Purdue University. Dr. Rogers is a former police detective, and has extensive experience in computer forensics. His website can be found at http://www.cerias.purdue.edu/homes/mkr/.