CERIAS Tech Report 2005-18

COMPUTER FORENSICS: MEETING THE CHALLENGES OF SCIENTIFIC EVIDENCE

by Matthew Meyers, Marc Rogers

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

Computer Forensics:

Meeting the Challenges of Scientific Evidence

Matthew Meyers and Marc Rogers

{mlmeyers, mkr}@cerias.purdue.edu

CERIAS

Purdue University

Recitation Building, 656 Oval Drive

West Lafayette, IN 47907

December 08, 2004

Abstract

This paper explores the three main criteria for admissibility of scientific evidence in the U.S. Court Systems (Federal and State): reliability, peer review, and acceptability.[1] The current tools used in the field of computer forensics are compared against these criteria. If the tools do not meet the requirements, the expert may be restricted from presenting materials from those tools and casting doubt on the scientific credibility of computer forensics. The ability to determine the reliability and validity of the tools derived from scientific theory are posited as possible first steps to increase the likelihood of digital evidence being admissible in the U.S. Court System. A trusted third party certification model is discussed as one possible approach to addressing some of the issues raised regarding the current state of computer forensic tools.

Keywords: Computer Forensics, Daubert, Frye, FRE 702, Cyber law, Forensic tools

Introduction

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 and true value. The field of computer[2] forensics[3] appears to be

[1] The authors recommend reading the paper Computer Forensics: The Need for Standardization and Certification by Matthew Meyers and Marc Rogers for additional background information on the necessity to address legal issues for computer forensics.

[2] For the purposes of this paper, the domain of computers 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 in the scope of this paper, but the use of a compact disc containing data or written by a computer would qualify

struggling over methods and practices that will meet the courts' standards for scientific evidence.

There are three primary methods to satisfy the U.S. federal and state court systems requirements for scientific evidence, Frye, Federal Rules of Evidence 702 (FRE 702), and Daubert. This paper will focus on the two primary standards commonly used today, Daubert and Federal Rules of Evidence (FRE) 702. To properly cover admissibility of scientific evidence (computer forensic tools admissibility), the rulings from the Supreme Court in *Kumho Tire Company v. Carmichael*[4] will be considered. 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 usually relies on the attorneys contending the qualifications of an expert, the scientific nature of their evidence, and the validity

---

[3] Computer forensics is used throughout the paper and is defined 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.

[4] Kumho Tire Company v. Carmichael, (97-1709) 526 U.S. 137 (1999) 131 F.3d 1433, reversed: Engineering testimony rests upon scientific foundations, the reliability of which will be at issue in some cases. See, e.g., Brief for Stephen Bobo et al. as Amici Curiae 23 (stressing the scientific bases of engineering disciplines). In other cases, the relevant reliability concerns may focus upon personal knowledge or experience. As the Solicitor General points out, there are many different kinds of experts, and many different kinds of expertise. See Brief for United States as Amicus Curiae 18—19, and n. 5 (citing cases involving experts in drug terms, handwriting analysis, criminal modus operandi, land valuation, agricultural practices, railroad procedures, attorney's fee valuation, and others). Our emphasis on the word "may" thus reflects Daubert's description of the Rule 702 inquiry as "a flexible one." 509 U.S., at 594. Daubert makes clear that the factors it mentions do not constitute a "definitive checklist or test." Id., at 593. And Daubert adds that the gatekeeping inquiry must be " 'tied to the facts' " of a particular "case." Id., at 591 (quoting United States v. Downing, 753 F.2d 1224, 1242 (CA3 1985)). We agree with the Solicitor General that "[t]he factors identified in Daubert may or may not be pertinent in assessing reliability, depending on the nature of the issue, the expert's particular expertise, and the subject of his testimony." Brief for United States as Amicus Curiae 19. The conclusion, in our view, is that we can neither rule out, nor rule in, for all cases and for all time the applicability of the factors mentioned in Daubert, nor can we now do so for subsets of cases categorized by category of expert or by kind of evidence. Too much depends upon the particular circumstances of the particular case at issue.

and reliability of the methods and tools[5] 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 at the very least given less importance.

This paper examines Daubert and applicable sections of FRE (see table 1) 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. In exploration of the above, the paper ties the loose ends together to derive a possible solution for computer forensics tools to meet some of the requirements of Daubert and FRE.

Table 1 Daubert and FRE 702 Criteria (*Kumho Tire Company v. Carmichael)*

Daubert	**FRE 702**
(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	(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

[5] For the purposes of this paper the term tools encompasses hardware and software. For example, tools may include imaging hardware and software, block writers hardware and software, and software suites such as EnCase and Forensics Tool Kit

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).[6]

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[7] algorithms) such as MD5[8] or SHA1.[9] 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.[10] While this approach can determine if an error

---

[6] U.S. Copyright Office. Digital Millennium Copyright Act. Washington D.C. 1998. available from: www.copyright.gov/legislation

[7] 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.

8 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 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."

[9] 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.

[10]Ohio v. Brian Cook, 149 Ohio App. 3d 422; 2002 Page 429

occurred, it provides no information related to actual or potential error rates. Granted, there is testing for (error rates and reliability of) some products by third parties such as the National Institute of Standards and Technology[11] (NIST). However, NIST does not assume liability for the results and does not certify or accredit any specific tool.

There have been arguments raised that the use of open source tools may increase the reliability of digital evidence derived from these tools.[12] 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[13] or to meeting the requirements of reliability, testing, and peer review. The openness means that the source code is often the work of several authors who may or may not be trust worthy, 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 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), does the potential to be reviewed mean that it has been reviewed?

Peer Review

Four Seasons v. Consorcio Page 70

[11] 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.

[12] Kenneally, Erin. "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.

[13] Poulson, Kevin. "Microsoft: Closed Source is More Secure." April 2001. available from: http://www.securityfocus.com/news/191.

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. It follows then that 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 where storage preservation, recovery, and analysis occur. 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.[14] 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 in order to for it to be deemed admissible.

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[15] and the Journal of Digital Investigation.[16] 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.

---

[14] 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 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.
[15] International Journal of Digital Evidence. available from: http://www.ijde.org
[16] Journal of Digital Evidence. available from: http://www.sciencedirect.com/science/journal/17422876

Acceptability

Section three of Daubert 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 extremely 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. Often 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.[17]

The immaturity of computer forensics has further ramifications. The American Academy of Forensic Sciences (AAFS) has not fully recognized computer forensics as a scientific sub-discipline. To date the U.S. Court Systems has not commented on this fact, possibly due to 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 satisfying Daubert and FRE 702 requirements.[18]

---

[17] Williford v. Texas 127 S.W.3d 309; 2004 Tex. Pages 312-313

[18] United States v. Saelee 162 F. Supp. 2d 1097; 2001. "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

One Possible Solution

While there is no silver bullet for meeting all criteria of the Daubert and FRE 702, interim stopgap approaches should be considered. As previously discussed, there is no entity that certifies or accredits computer forensics tools, nor assumes accountability for their testing. Further, there is no trusted third party attesting to the reliability and validity of the tools. With E-Commerce, numerous web sites implement secure socket layer (SSL) for encryption of information. Part of SSL revolves around the certificate, issuance, and maintenance.[19] This method uses a trusted third party to state information about the certificate that can be verified to ensure that the certificate provided matches the information to mitigate the risk of malicious access. This model is based on a trusted third party and has resulted in the near ubiquitous use of SSL in the business and consumer market place.

The computer forensics field may employ the concept of the trusted third party. There are currently companies and underwriting labs that perform evaluations resulting in certified and accredited products, applications, and hardware (e.g., FIPS 142 certification[20]). For example, accounting firms have offered certifications of trust for websites for several years (e.g., WebTrust[21]). It is only logical that the testing of computer forensic tools (both open source and proprietary) move to this impartial

---

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."

[19] Freier, Karlton, Kocher. *SSL 3.0 Specification.* available from: http://wp.netscape.com/eng/ssl3/. November, 1996.

[20] Federal Information Processing Standards Publications FIPS 142 Washington D.C. November 2003. available from: http://www.itl.nist.gov/fipspubs/geninfo.htm

[21] American Institute of Certified Public Accountants. WebTrust available from: http://www.cpawebtrust.org/

underwriters lab[22] approach. By using this approach the intellectual property concerns of the vendors can be alleviated (i.e., non-disclosure agreements) and the blind faith reliance on the vendors that their tools actually work as advertised can be set aside.

In order to be of any real use, these trusted organizations must make the results and their testing methodology open to community (peer reviewed). The end result may be some sort of 'Good House Keeping' forensic seal of approval, and a master list of approved computer forensics tools that the judiciary could turn to for guidance on acceptability and admissibility.

Obviously, there are limitations to the approach. The leading issue will be liability concerns. Liability by some is considered an unavoidable evil in our society, and one that is exploited. For instance, one issue with the health care industry in the United States is the liability of doctors and difficulties of providing affordable care due to insurance companies acquiring malpractice liability.[23] The trusted third party who evaluated and issued a level of trust for the tool (certified it), may offset the liability of the company that produced the tool. Thus, third parties would have to carry some sort of insurance to mitigate their liability. This has financial implications and if abused, poses issues similar to medical malpractice insurance.

Another limitation is the rate of change of the tools (e.g. patches, version upgrades, new technology). Several of the current computer forensic tool vendors release minor version changes at a rate of one every two to three months. This would require a continuous retesting and certification process, thus resulting in a delay for the new

[22] Underwriters Laboratories. available from: http://www.ul.com/
[23] The Foundation for Taxpayers & Consumer Rights. available from: http://www.consumerwatchdog.org/healthcare/medmal.php

version being accepted and sold to the community. This has obvious economic ramifications to the vendor community.

The last issue to be considered for now is whether the third party should be a government agency or private sector organization. This is a contentious issue as the potential for a niche market/monopoly is very high, yet what trust is there in monopolies? The companies would have to be at arms length from the vendors and makers of the tools and be seen as completely neutral and impartial. The notion of neutrality is support for a government or quasi-government entity that receives funding independent of the market place and private sector. Regardless of the private/public sector debate, in the long run, trust is the key to the model's success.

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.[24] As the defense bar becomes more knowledgeable regarding digital evidence and computer forensics, there will be an

[24] Kerr, O. (2004). "Computer crime and the coming revolution in criminal procedure." Conference Proceedings, Cybercrime and Digital Law Enforcement Conference, Yale Law School, March 2004.

increase in Daubert and FRE challenges, and more judicial scrutiny on the point of what constitutes valid scientific evidence computer forensics.[25]

Simply stated, the computer forensics field is not meeting the U.S. Court Systems required criteria for acceptable scientific evidence. Therefore, the computer forensics field needs to implement solutions to meet the required criteria or have them forced upon the field by the U.S. Court Systems. Rather than attempting to reinvent the wheel, the computer forensics field needs to look to the other forensics sciences for direction, and as suggested in this paper, adopt models and approaches from other industries and business areas.

There is a very real risk that if computer forensics does not act decisively, and in a timely manner, it will suffer a fate similar to other fields (e.g., handwriting forensics, polygraph) and be relegated to the role of a pseudo science or worse, a junk science.

[25] 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.

ERROR: undefined
OFFENDING COMMAND:

STACK: