Chapter 4

DIGITAL FORENSICS: MEETING THE CHALLENGES OF SCIENTIFIC EVIDENCE

Matthew Meyers and Marcus Rogers

Abstract This paper explores three admissibility considerations for scientific evidence currently engaged in U.S. courts: reliability, peer review and acceptance within the relevant community. Any tool used in a computer forensic investigation may be compared against these considerations, and if found wanting, evidence derived using the tool may be restricted. The ability to demonstrate the reliability and validity of computer forensic tools based on scientific theory is an important requirement for digital evidence to be admissible. A trusted third party certification model is discussed as an approach for addressing this issue.

Keywords: Computer forensic tools, evidence, admissibility

1. Introduction

It should come as no surprise that there is a dramatic increase in digital evidence being brought before courts in the United States and elsewhere in the world. As a result, courts are becoming concerned about the admissibility and probative value of digital evidence. Meanwhile, the discipline of computer forensics appears to be struggling over methods and practices that will meet the courts' "standards" for scientific evidence. For the purpose of this discussion, the term "computer forensics" is defined as the use of an expert to preserve, analyze and produce data from volatile and non-volatile storage media.

The admissibility of evidence in U.S. federal courts and many state courts is based on the Federal Rules of Evidence (F.R.E.) [17] and upon various Supreme Court opinions that interpret its constitutional and legal application. F.R.E. Rule 702 specifically addresses the testi-

Table 1. Daubert and F.R.E. 702 criteria.

Daubert	F.R.E. 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

mony of experts concerning scientific evidence and is applicable to computer forensics. Several opinions guide the application of F.R.E. 702, among them are the Daubert [18] and Kumho Tire [19] decisions. In the Daubert decision, the court specifically held that Frye [13] was superseded by F.R.E. and several judicial considerations were identified. This paper focuses on the application of Daubert to F.R.E. 702, and its potential impact on the field of computer forensics.

The Daubert decision defines the role of the judge as a gatekeeper tasked with filtering out "junk science." However, in practice, this filtering usually involves attorneys raising Daubert challenges – contesting the qualifications of an expert, the scientific nature of their evidence, and the validity and reliability of the methods and hardware/software tools (e.g., write blockers and software suites) employed. If a tool is successfully challenged, derivative evidence from the tool may not be admissible or, at the very least, is given less weight in deliberations by the judge and/or jury.

The Daubert ruling recognizes that judges, when determining the scientific validity of the method or reasoning in question, are faced with many considerations. This paper examines the considerations of reliability, peer review and acceptance as outlined in Daubert, as well as the applicable sections of F.R.E. (see Table 1) to determine if computer forensics tools meet the consideration for acceptance as scientific evidence. The paper concludes by proposing a solution that meets at least some of the considerations.

2. Reliability and Validity

To demonstrate reliability and validity under Daubert, a number of factors must be taken into consideration: known or potential error rates, testing, and commonly agreed upon methods. Unfortunately, computer forensic tools and techniques fall short of meeting these considerations. Currently, there is a strong reliance by practitioners on proprietary software whose error rates are unknown. Vendors, protective of their market share, have not published information concerning error rates or even the exact reasons for minor and major version changes. Furthermore, the forensic community may be prevented from conducting in depth tests by terms imposed by software licenses and legislation such as the Digital Millennium Copyright Act [16]. While there is some limited testing for error rates and reliability of certain products by third parties, e.g., by the U.S. National Institute of Standards and Technology (NIST) [7], these bodies do not assume liability for the results and do not certify or accredit specific tools. Published results pertaining to these tests take several months to become available and are usually based on technologies, tools or applications that have been superseded by newer releases.

Given the lack of information and the restrictions on full error testing and reporting, indirect approaches are used to demonstrate the validity, integrity and reliability of digital evidence. For example, an investigator typically computes a digital signature or hash value for the original evidence (e.g., media, partition, drive) and for the bit-stream image of the original source; the two values can be compared at any time to demonstrate that they match. The algorithms used to compute signatures and hash values provide mathematical assurances that if the values match, the image has not been corrupted or contaminated, and has a high degree of fidelity relative to the original source (a true copy), and can be considered as best evidence [8, 14]. While this approach can determine if an error occurred, it provides no information about the error source or about the actual or potential error rates.

3. Peer Review

One of the Daubert considerations is whether an expert's methods, processes and underlying reasoning have been peer reviewed and/or published. The rationale behind this consideration is that if the implementation of a theory is flawed, the results will be flawed and, by peer review or publication, others in the scientific community will have the opportunity to discover flaws and supply recommendations or resolve errors prior to the implementation or acceptance of the theory. The corollary is that tools used to derive the results should also be peer reviewed. Computer

forensic tools automate the basic manual processes of evidence acquisition, examination and analysis, and in some cases, reporting. Indeed, in computer forensics there tends to be a heavy reliance on tools and, as some have suggested, on blind faith. This has lead to an industry myth that certain tools have been accepted by the courts. However, the courts have ruled that an inanimate object (e.g., a software package) cannot be considered an expert [20]. This does not necessarily imply that the tool or the results obtained using the tool cannot be included in scientific testimony. What it does mean is that the individual who used the tool may have to testify about the procedures used and about the reliability of the tool prior to the results being admitted as evidence.

It has been suggested that the use of open source tools satisfies the peer review consideration and may increase the reliability of digital evidence derived from the use of these tools [4]. Proponents of the open source movement have stated that because end users can examine (peer review) the source code, it is more secure and, therefore, more reliable. However, the mere ability to view the source code does not translate to better security or to meeting the requirements of reliability, testing and peer review [9]. Furthermore, open source code is often the work of several authors who may or may not be trustworthy and who may or may not follow state-of-the-art software engineering methodologies. Also, the code can be altered at any time, including after formal testing for error rates. Thus, the courts may find that open source tools do not meet the scientific considerations. Simply put, open source does not in and of itself mean that it is peer reviewed: Who are the peers? Where was the source code published (e.g., journals, conferences)? The potential for the source code to be reviewed does not equate to it actually being peer reviewed.

The exact nature of peer reviewing and vetting by way of publication is problematic in general, and not just for open source tools. Few publications directly address computer forensic methods and processes. At the time of writing this paper, there were only two quasi peer-reviewed journals dedicated to computer forensics: *International Journal of Digital Evidence* and *Journal of Digital Investigation.* In reviewing the Daubert considerations, it is unclear whether peer review requires publication in journals or presentation at conferences focusing on the particular field in question. Given the precedent set by other forensic sciences, e.g., forensic psychology and DNA analysis, the lack of such journals and conferences at the very least does not support the inference of peer vetting, and the reliability and validity of scientific methods and reasoning.

4. General Acceptance

Yet another important consideration mentioned by the U.S. Supreme Court in Daubert is whether a tool, technique or principle has "attracted widespread acceptance within a relevant scientific community." This presumes two elements: (i) there is a relevant scientific community, and (ii) the community has a generally accepted set of principles or processes. Since computer forensics is a relatively new field, it may not have an established scientific community *per se*. While the American Society of Crime Laboratory Directors – Laboratory Accreditation Board (ASCLD-LAB) has recognized computer forensics as a scientific subdiscipline, other professional bodies such as the American Academy of Forensic Sciences (AAFS) have not formally done so. To date U.S. courts have not commented on this fact. However, with defense attorneys becoming technically sophisticated, it is possible that the recognition of the field and its underlying theory by the AAFS or a similar body will be included as a consideration for admission as scientific evidence. This rationale has been used in the case of forensic disciplines such as handwriting analysis, and has resulted in expert testimony being nullified based on the lack of a scientific foundation [15].

Demonstrating the requirement of general acceptance is difficult even when concerns about the lack of a relevant scientific community are ignored. This has resulted in the default argument that practitioners use established vendor tools that are "industry standard" and the tools are, therefore, "generally accepted." The criteria governing "industry standard" are ambiguous at best. Often, an expert's choice of a tool is the outcome of an aggressive marketing campaign by a vendor; little or no direct testing or validation of the tool is conducted by the expert [11]. The cost of a tool rather than its scientific validity often impacts its general acceptance, especially since most law enforcement agencies have limited budgets.

5. Proposed Solution

No silver bullet exists for meeting all the F.R.E. 702 and Daubert considerations; therefore, interim approaches must be considered. As discussed above, no entity currently certifies computer forensic tools and no entity is accountable for their testing. Furthermore, no trusted third party currently attests to the reliability and validity of computer forensic tools. This is a logical area to start in developing a solution.

Numerous web sites created for electronic commerce applications implement a technology called secure socket layer (SSL) [3] to encrypt information in transit. Part of SSL revolves around the issuance and

maintenance of third-party certificates. SSL uses a trusted third party to verify information about the certificate holder and to ensure that the certificate provided matches that of the holder; this approach mitigates the risk of malicious access. The SSL model, based on a trusted third party, has gained wide acceptance in the electronic commerce community and has resulted in its ubiquitous use.

The computer forensics field could employ a trusted third party for certification purposes. Several companies and underwriting laboratories certify and accredit products, applications and hardware [12] (also see FIPS 140-2 [6]). Accounting entities have offered to certify the trustworthiness of websites and web transactions (e.g., WebTrust [1]). A logical extension would be for computer forensic tools (open source and proprietary) to be certified by impartial underwriters laboratories. By using this approach, intellectual property concerns of vendors can be alleviated and the blind faith reliance on vendors' assertions that their tools work as advertised can be set aside.

To be of any real value, the trusted organization must make both the results and its testing methodologies open to scrutiny (peer review). The end result of this process is a sort of "Good Housekeeping Seal" for computer forensic tools and an updated, publicly available list of approved tools that the courts could turn to for guidance on general acceptance and reliability.

The main limitation of this approach is liability, which will require the certifying entity to purchase liability insurance. To mitigate the problem of ever increasing malpractice insurance premiums as in the health care industry [2], a trusted third party who evaluates and certifies a computer forensic tool may offset some of the liability to the company that produced the tool. The third party would still have to carry liability insurance, but hopefully with reduced premiums.

Another limitation is the rate of change of computer forensic tools (new patches, versions and technologies). Often, vendors release new versions with minor changes every two to three months. This situation would require continuous re-testing, re-certification and re-publication of the test results, resulting in delays in the new version being released to the computer forensics community. Protracted delays have obvious economic ramifications to vendors and to practitioners, due to the inevitable price increases that would be passed to them by vendors. The certification of open source tools is an issue: Who will pay for certifying open source tools? Open source tools are often popular because they are free. Absent potentially costly certification, will the results obtained using open source tools be deemed inadmissible in court if only proprietary tools are certified?

The issue of whether or not the trusted third party should be a government agency or a private sector organization also must be considered. This is a contentious issue as there is the potential for a niche market or a monopoly by one company. Clearly, the certifying entity should be perceived as being completely impartial. The requirement of neutrality would tend to support the use of a government or quasi-government entity. Notwithstanding the private/public sector debate, trust is the key to the success of this model. If the computer forensic community distrusts the process, the model is flawed and the faith of the courts in the reliability and validity of the certification results will be undermined.

6. Conclusions

The number of court cases involving digital evidence will continue to increase as computers become more intertwined in society. Currently, the discipline of computer forensics and the derived digital evidence have difficulty meeting the F.R.E. 702 and Daubert considerations. This can have serious consequences for the computer forensics discipline as a whole. The discipline cannot survive for long if it relies on the lack of technical and scientific understanding by the courts. While U.S. courts have been willing to admit evidence generated by computer forensic tools based on face value, there is no guarantee that they will do so indefinitely [5]. As defense attorneys become more knowledgeable about computer forensics and digital evidence, there will be an increase in the number F.R.E. and Daubert challenges, more judicial scrutiny over what constitutes admissible digital evidence, more negation of testimony, and possibly increased suppression of evidence [10].

To minimize this potential, the computer forensics community must consider solutions that meet the Daubert considerations or risk the imposition of court-mandated solutions. Rather than attempting to reinvent the wheel, the community needs to look to other forensic sciences for direction and guidance, and, as suggested in this paper, adopt models and approaches that have proven to be effective. There is a real risk that if the computer forensics community does not act quickly and decisively, the discipline may end up being viewed by the courts as a pseudo science, or worse, a junk science.

References

[1] American Institute of Certified Public Accountants, WebTrust (www.cpawebtrust.org).

[2] Foundation for Taxpayers and Consumer Rights (www.consumer watchdog.org/healthcare).

[3] A. Freier, P. Karlton and P. Kocher, *The SSL 3.0 Protocol* (wp.netscape.com/eng/ssl3/draft302.txt), 1996.

[4] E. Kenneally, Gatekeeping out of the box: Open source software as a mechanism to assess reliability for digital evidence, *Virginia Journal of Law and Technology*, vol. 6(13), 2001.

[5] O. Kerr, Computer crime and the coming revolution in criminal procedure, *Proceedings of the Cyber Crime and Digital Law Enforcement Conference*, 2004.

[6] NIST, *Security Requirements for Cryptographic Modules*, FIPS PUB 140-2 (csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf), 2001.

[7] NIST, *National Software Reference Library and Computer Forensics Tool Testing Project* (www.nsrl.nist.gov/Project), 2003.

[8] Ohio Court of Appeals, State of Ohio v. Brian Cook, 777 NE 2d 882, 2002.

[9] K. Poulsen, Microsoft: Closed source is more secure (www.securityfocus.com/news/191), 2001.

[10] F. Smith and R. Bace, *A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony as an Expert Technical Witness*, Addison-Wesley, Boston, Massachusetts, 2003.

[11] Texas Appeals Court, Williford v. State of Texas, No. 11-02-00074-CR, 127 SW 3d 309, 312-313, 2004.

[12] Underwriters Laboratories (www.ul.com).

[13] U.S. Circuit Court of Appeals (DC Circuit), Frye v. United States, 293 F. 1013, 1923.

[14] U.S. Circuit Court of Appeals (11th Circuit), Four Seasons v. Consorcio, 267 F. Supp. 2d, 70, 2004.

[15] U.S. District Court (Alaska District), United States v. Saelee, 162 F. Supp. 2d 1097, 1105, 2001.

[16] U.S. Government, *Digital Millenium Copyright Act*, Pub. L. No. 105-304, 112 Stat. 2860 (www.copyright.gov/legislation/dmca.pdf), 1998.

[17] U.S. Government, *Federal Rules of Evidence* (judiciary.house.gov/media/pdfs/printers/108th/evid2004.pdf), 2004.

[18] U.S. Supreme Court, Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579, no. 92-102, 1993.

[19] U.S. Supreme Court, Kumho Tire Company v. Carmichael, 526 U.S. 137, no. 97-1709, 1999.

[20] Washington Superior Court, State of Washington v. Leavell, Cause No. 00-1-0026-8, 1-17, 2000.