

Evidentiary Implications of Potential Security Weaknesses in Forensic Software

Chris K. Ridder - <[cridder/at/stanford/dot/edu](mailto:cridder@stanford.edu)>¹

Center for Internet and Society
Stanford Law School
559 Nathan Abbott Way
Stanford, CA 94305-8610
<http://cyberlaw.stanford.edu>

August 2, 2007

Abstract

Computer forensic software is used by lawyers and law enforcement to collect and preserve data in a “forensic image” so that it can be analyzed without changing the original media, and to preserve the chain of custody of the evidence. To the extent there are vulnerabilities in this software, an attacker may be able to hide or alter the data available to a forensic analyst, causing courts to render judgments based on inaccurate or incomplete evidence. There are a number of legal doctrines designed to ensure that evidence presented to courts is authentic, accurate and reliable, but thus far courts have not applied them with the possibility of security weaknesses in forensic software in mind. This paper examines how courts may react to such claims, and recommends strategies that attorneys and courts can use to ensure that electronic evidence presented in court is both admissible and fair to litigants.

I. Introduction

Forensic software is frequently used for evidence collection in both civil and criminal matters, because it mitigates risks that can arise with examining media in its native environment,² and because it provides powerful tools for reviewing data that has been collected. In addition, many forensic tools provide features such as MD5 hashing and assignment of CRC values to data, to ensure that the evidence to be introduced at trial remains in the same state as when it was collected.³ The legal and law enforcement communities therefore depend heavily on forensic software to analyze and preserve critical evidence.⁴

¹ Residential Fellow, Stanford Law School Center for Internet and Society. The author thanks Jennifer Granick, Kurt Opsahl, Alex Stamos, Jesse Burns and Tim Newsham for their very helpful comments, and Johnny Lam for his research support.

² These risks include alteration of critical metadata such as time and date stamps when files are accessed and deleted files being overwritten during analysis.

³ *See, e.g.*, “EnCase Forensic Corporate Version 5, The Standard in Computer Forensics,” *available at* http://www.guidancesoftware.com/downloads/95-00-01029_EnCase_Forensic_Corp_and_Dlx_V505.pdf.

⁴ In addition to being a common practice among attorneys for prudential reasons, courts have suggested, and in some cases required, exact binary duplicates (“image copies”) to be made of hard drives, particularly when deleted files are in issue. *See* Gates Rubber Co. v. Bando Chem. Indus. Ltd., 167 F.R.D. 90, 112 (D. Colo. 1996) (criticizing Plaintiff for failing to make an “image backup” of the hard drive and failing to properly preserve undeleted files, where there was evidence that certain files may have been deleted, and holding that a party should “utilize the method which would yield the most complete and accurate results.”); *Simon Prop. Group L.P. v. mySimon, Inc.*,

There are approximately 150 different automated tools used by law enforcement organizations in the investigation of computer crime,⁵ many of which are likely also used in the civil litigation context. The National Institute of Standards and Technology has a program to test that this software does what it claims, but some have argued that not enough work is being done to identify and correct security vulnerabilities.⁶

Forensic software marketing materials promise a high degree of accuracy and reliability. EnCase, one of the industry-standard tools, claims that it produces “an exact binary duplicate of the original drive or media.”⁷ However, some forensic software in certain situations may be vulnerable to deliberate attempts to hide data from the software, or to cause the software to crash.⁸ In addition, to the extent code execution vulnerabilities are present or impersonation attacks are possible, an attacker may be able to change data on the forensic image, or to change the way such data appears to a forensic analyst.⁹

The possibility that an attacker may seek to hide data from forensics software is a serious concern for those trying to collect evidence, but because hidden data by its nature is not likely to

194 F.R.D. 639, 641 (S.D. Ind. 2000) (requiring plaintiff to make a “mirror image” of hard drives, citing the problems with overwriting of deleted files in Gates Rubber); *Playboy Enters., Inc. v. Welles*, 60 F.Supp.2d 1050, 1055 (S.D. Cal. 1999) (ordering a court-appointed forensic computing expert to make a ‘mirror image’ of Defendant’s hard drive where emails had been deleted during litigation); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003) (suggesting that creation of mirror-image copies of computer systems is one way to preserve documents in the state they existed at the time of collection).

⁵ See National Institute of Standards and Technology Computer Forensics Tool Testing Program, CFTT Project Overview, available at http://www.cftt.nist.gov/project_overview.htm.

⁶ See, e.g., Newsham, Palmer and Stamos, “Breaking Forensics Software: Weaknesses in Critical Evidence Collection” (2007) at 2, 11-12 (arguing that there is very little data on two popular forensic packages, EnCase and TSK, in the Common Vulnerabilities and Exposures database, and that vendors do not take advantage of the protections for native code that platforms provide); Ryan Harris, “Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem,” 3 DIGITAL INVESTIGATION Supplement 1, September 2006, at 44-49, available at

<http://cyberforensics.purdue.edu/DNN/LinkClick.aspx?fileticket=QIM9nq5fI3Y%3d&tabid=54&mid=444> (arguing that forensic software needs to be hardened against a wide range of potential attack vectors, and that “it would seem that perpetrators are working harder to subvert the system than academia is working to strengthen forensics.”); the Grugq, “The Art of Defiling: Defeating Forensic Analysis” at 45, available at <http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-grugq.pdf> (stating that computer forensics are “[a]s vulnerable as other technologies,” yet “[l]ess scrutinized than other technologies.”).

⁷ “EnCase Forensic Corporate Version 5, The Standard in Computer Forensics,” available at http://www.guidancesoftware.com/downloads/95-00-01029_EnCase_Forensic_Corp_and_Dlx_V505.pdf.

⁸ See, e.g., “Breaking Forensics Software,” *supra* note 6; the Grugq, *supra* note 6 (describing a range of anti-forensics tactics); “Anti-Forensic Tools,” <http://www.networkintrusion.co.uk/foranti.htm> (containing links to a variety of anti-forensic software tools). Guidance Software has disputed the discussion regarding its EnCase Forensic product in “Breaking Forensics Software,” see, e.g., “Guidance Software response to iSEC report on EnCase,” July 26, 2007, available at <http://www.securityfocus.com/archive/1/474727>, as well as the discussion regarding EnCase Enterprise. This paper does not take a position on the accuracy of any particular research regarding forensic software security, but rather simply seeks to analyze what the legal implications are of research that points to potential weaknesses. “Breaking Forensics Software” and other research on forensic software security are discussed only by way of example.

⁹ See *id.*

cause significant evidentiary concerns unless it is found,¹⁰ I will focus in this paper on vulnerabilities that could permit an attacker to add or change data without being detected. In “Breaking Forensics Software,” Newsham et. al discuss a potential risk of code execution vulnerabilities, which could allow an attacker (such as the person being subjected to forensic analysis, an interested third party, or the forensic examiner herself) to execute arbitrary code on the forensic workstation.¹¹ Although they did not demonstrate such an attack, if one were found in the future it could be possible for an attacker to alter the data on the forensic image.¹² Another potential attack vector they discuss is the possibility of an “impersonation attack” against forensic software that is designed to image a live network. If not properly secured, such software could allow an attacker to masquerade as the person the software believes it is collecting from. Combined with a network “man in the middle,” or MITM, attack, such a vulnerability might be used by an attacker to feed the forensic software arbitrary data, for example by presenting a virtual machine containing data of the attacker’s choice to the forensic software instead of the media intended to be collected.

To the extent such attacks are possible, they may also be able to avoid detection. When forensic software captures an individual piece of media, it creates an MD5 hash of the media and the image to confirm they match. If the drive has been seized, as it frequently is in criminal cases, later comparisons will be able to confirm that the forensic image matches the original media. However, if the drive is not seized and remains in use after imaging, the hash value of the original will change as soon as data on the media changes (for example, through normal use) and there will no longer be an opportunity to compare it with the forensic image’s hash value.¹³

Additionally, if an attack against the forensic workstation has occurred,¹⁴ the hash values alone may not be sufficient to guarantee that what a forensic examiner sees is an accurate representation of what is on the original media. Without strong integrity checks of the operating

¹⁰ Attorneys in both the civil and criminal contexts have obligations to conduct a reasonably diligent search for data that may be useful to their opponents, but it is unlikely that this obligation would extend to a search for data that has been hidden so thoroughly as to be undiscoverable by forensic software. Because potentially hidden data may prove critical (and in the criminal context, may be exculpatory), all parties should have an opportunity to conduct their own forensic analysis of the original media and the forensic workstation used by the proponent of the evidence, if they are concerned about potential security weaknesses in the software.

¹¹ This finding is probably not unique to forensic software; many software programs written in C that accept untrusted input have a potential risk of code execution vulnerabilities.

¹² If an attacker were able to execute arbitrary code on the forensic workstation, it could be used for a wide variety of operations that could jeopardize an investigation or alter evidence. For example, an attacker might be able to change the way the forensic software displays data to the examiner, alter the behavior of the function that reports the hash value of the image to display an arbitrary hash value, or embed a rootkit that waits for the forensic examiner to connect the workstation to a public network (for example, to apply the latest Windows patches) and then gives the attacker an opportunity to change the way the forensic software interprets certain data or review evidence on the forensic workstation.

¹³ This problem would also be present when forensic software images a live system or network, which may include imaging hard drives, network traffic, and even data in RAM that can change rapidly. In the case of an impersonation attack, the hash value would match the attacker’s data set, rather than the media intended to be collected; this may not be verifiable against the original media if the original media’s hash had changed.

¹⁴ It is unlikely that a forensic examiner would want to run forensic software on the system being collected from, because running the operating system during collection could change data during the normal course of its operation. In addition, there is likely to be a greater risk that the operating system on the target machine (vs. the operating system on the forensic workstation) has been compromised.

system running on the forensic workstation in addition to the forensic software itself,¹⁵ an attacker may be able to compromise the routines that display the hash, causing a false hash value to be displayed. An attacker may also be able to change the way the forensic software displays the data on the image, such that even if the examiner were looking at a perfect bit-for-bit copy of the original, the documents would appear as the attacker had specified, rather than as they are on the original media.

The potential vulnerability of forensic software to attack, combined with the potential for such an attack to go undetected, has implications not only for admissibility of evidence, but for the administration of justice generally. After all, the stakes are extremely high: people go to jail and fortunes are paid depending on what the forensic software says. It is absolutely critical that it be secure. In this paper, I review three evidentiary doctrines that could cause forensic software with demonstrated security vulnerabilities to be excluded from evidence: authenticity, the best evidence rule, and reliability.

II. Authenticity of forensic evidence

Evidence may only be used in court if it is authentic. The authentication of a document is “satisfied by evidence sufficient to support a finding that the matter in question is what the proponent claims.”¹⁶ Once this standard is met by the proponent of the evidence, the jury then considers the relevance and weight of the evidence in the context of the case.¹⁷ Forensic images will be vulnerable to findings that they are not authentic in proportion to the attack surface of the tools, and the likelihood that they have been compromised.

Generally, when a party in litigation seeks to offer evidence, it must show “that the exhibits offered into evidence were the same as those taken, and their contents were in the same condition when analyzed and introduced as when taken.”¹⁸ This is usually shown by demonstrating that the continuous custody of the evidence was such as to render it improbable that anyone tampered with the original item or substituted a different item.¹⁹ A more stringent showing on chain of custody may be required when the evidence is of a type more susceptible to alteration or substitution.²⁰ Forensic software should be hardened as much as possible against tampering and impersonation attacks, to strengthen claims that a forensic image can be reliably traced back to the intended source.

A proponent must offer more than a reliable chain of custody in demonstrating that the evidence is what the proponent claims. For example, a witness with knowledge of the document may testify that it is authentic,²¹ it may be compared with similar evidence that has already been

¹⁵ In addition to integrity checks, the risk that a workstation has been compromised during a prior investigation can be mitigated by running a clean installation of both the operating system and forensic software for each new case.

¹⁶ Fed. R. Evid. 901(a).

¹⁷ See *United States v. Goichman*, 547 F.2d 778, 784 (1976). Note that even if a court admits evidence that has potentially been tampered with, the jury may find arguments about the accuracy of the software to be persuasive enough to disregard it.

¹⁸ *State v. Perry*, 69 N.W.2d 412, 417 (Iowa 2003).

¹⁹ See *State v. Gibb*, 303 N.W. 2d 673 (1981); *State v. Bakker*, 262 N.W.2d 538, 542-43 (1978).

²⁰ See *Bakker*, 262 N.W.2d at 543.

²¹ Fed. R. Evid. 901(b)(1).

authenticated,²² or it may have distinctive characteristics that, in light of the circumstances make it likely to be authentic.²³

To the extent there are insufficient “external” sources of authenticity,²⁴ a proponent of forensic evidence will need to demonstrate the accuracy of the forensic software itself. Federal Rule of Evidence 901(b)(9) provides that evidence may be authenticated by “describing a process or system used to produce a result and showing that the process or system produces an accurate result.”²⁵ Although it appears that no courts have considered the potential for security weaknesses in forensic software, the prevailing view is that data obtained from forensic images satisfies the authenticity requirement.²⁶ However, should the tools be shown to produce inaccurate results, they may become vulnerable to challenge.²⁷

Some courts have expressed skepticism with regard to electronic evidence that is capable of being altered. In *St. Clair v. Johnny’s Oyster & Shrimp, Inc.*,²⁸ the court held that Plaintiff’s evidence of boat ownership taken from an online Coast Guard vessel database was insufficient to withstand a motion to dismiss, because the Internet is “inherently untrustworthy,” “[a]nyone can put anything on the Internet,” and “hackers can adulterate the content on any web-site from any location at any time”). In *United States v. Jackson*,²⁹ the court found that web site postings lacked authenticity, reasoning that the defendant could not show that “web postings in which the white supremacist groups took responsibility for . . . racist mailings actually were posted by the

²² Fed. R. Evid. 901(b)(3).

²³ Fed. R. Evid. 901(b)(4). For example, if a document contains information that only the person in possession is likely to possess, it will be held to be authentic. See, e.g., *United States v. Reilly*, 33 F.3d 1396 (3d Cir. 1994); *United States v. Console*, 13 F.3d 641 (3d Cir. 1993).

²⁴ In addition to evidence such as child pornography, where only the possessor is likely to know whether the image is authentic, this will occur with logs and other metadata, where it would be very unlikely for a person to know whether a particular log entry has been altered.

²⁵ See, e.g., *United States v. Taylor*, 530 F.2d 639, 641-42 (5th Cir. 1976) (video of a bank robbery was authentic even though the tellers were locked in the vault and unable to testify as to what happened, because they were able to testify how the film was loaded into the camera, how the camera was activated, and that the film was removed from the camera immediately after the robbery and developed). See also, *United States v. Alicea-Cardoza*, 132 F.3d 1, 4 (pen register data admitted upon showing that as the message comes in, the pen register stores exactly what comes out of the beeper); *State v. Sensing*, 843 S.W.2d 412, 416 (1992) (holding that the machines at issue were subjected to “exhaustive testings,” undergo “constant monitoring” and are “nearly infallible”).

²⁶ See, e.g., *State v. Cook*, 777 N.E.2d 882, 886-892 (Ohio Ct. App. 2002) (holding that under Rule 901(b)(9), Guidance Encase was a process or system that produces an accurate result and there was “no doubt that the mirror image was an authentic copy of what was present on the computer’s hard drive,” where defendant’s own expert was satisfied with the way the forensic image was collected); *Bone v. State*, 771 N.E.2d 710, 716-17 (Ind. App. 2002) (finding deleted picture files from forensic images authentic where defendant didn’t challenge procedures employed, and police detective testified that he made a forensic image of the hard drive, described the software used to retrieve the deleted files, and testified that he printed the deleted pictures exactly as he found them on the defendant’s computer); *State v. Schroeder*, 613 N.W.2d 911, 918 (Wis. Ct. App. 2000) (upholding lower court’s decision not to allow a demonstration that the forensic investigator had modified data on the computer, where the demonstration would not have shown anything related to the nineteen child pornography pictures at issue).

²⁷ *But see*, *People v. Lugashi*, 205 Cal.App.3d 632 (1988) (holding that a proponent of computer evidence need not introduce testimony on the acceptability and reliability of the hardware and software as a prerequisite to admissibility); *United States v. Catabaran*, 836 F.2d 453, 458 (9th Cir. 1988) (questions “as to the accuracy of [computer] printouts, whether resulting from incorrect data entry or the operation of the computer program, as with inaccuracies in any other type of business records, [affect] only the weight of the printouts, not their admissibility”).

²⁸ 76 F.Supp.2d 773, 774-75 (S.D. Tex. 1999).

²⁹ 208 F.3d 633, 638 (7th Cir. 2000).

groups, as opposed to being slipped onto the groups' web sites by Jackson herself, who was a skilled computer user.” These cases are not representative,³⁰ and courts are likely to find forensic images authentic absent a showing that they are fairly susceptible to tampering. However, they demonstrate that some courts will consider security vulnerabilities in electronic systems an issue in determining authenticity.

Courts have expressed a great deal of confidence in a hash value's ability to authenticate a forensic image.³¹ However, hash values could be at risk of being undermined where code execution vulnerabilities or impersonation attacks are present, or where the original drive was not retained by the investigators and is not verifiable against the original media. Where the original media is available, courts have a number of options to reduce the risk that compromised forensic evidence is admitted: they can admit the original media into evidence, provide an opportunity for both parties to examine the original, or provide both parties an opportunity to conduct their own forensic analyses.³²

In cases where the original media has changed such that there is no way to verify that the forensic image has not been tampered with, there is a stronger argument that the system used to produce the image does not produce an accurate result. However, given courts' willingness to admit forensic images, there would probably need to be a suggestion that tampering was likely in a given case in order for evidence to be excluded. This creates a difficult situation for litigants who are not able to make such a showing if they believe tampering has occurred; and an opportunity for those who would seek to frame them.

IV. The Best Evidence Rule

The Best Evidence Rule provides that “[t]o prove the content of a writing, recording or photograph, the original writing, recording or photograph is required. . .”³³ There are a number of exceptions to this general rule. For example, Federal Rule of Evidence 1001(3) provides that if “data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an ‘original.’” Some documents obtained from a forensic

³⁰ See, e.g., *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F.Supp.2d 1146, 1153-54 (2002) (finding printouts of web pages authentic); *United States v. Tank*, 200 F.3d 627, 630 (9th Cir. 2000) (finding authentic printouts of chat room logs, where the person recording the logs has deleted nonsexual conversation and time and date stamps).

³¹ See, e.g., *Sanders v. State of Texas*, 191 S.W.3d 272 (Tex. App. 2006) (holding EnCase Forensic software accurate and reliable over defendant's unsupported assertion that it was inaccurate and unreliable, based in part on expert testimony that MD5 hash used to validate the image ensured no possibility of error).

³² Thus far, courts do not appear to have taken this route, and instead have denied parties an opportunity to look at the original media, apparently in reliance on the authenticity of the forensic imaging process. See *Positive Software v. New Century Mortgage*, 259 F.Supp.2d 561 (N.D. Tex. 2003) (holding that defendant had made only unspecified allegations regarding the accuracy and quality of EnCase imaging); *State v. Butler*, 2005 WL 735080 (Tenn. Crim. App. Mar. 30, 2005) (noting that trial court required government to produce forensic images, but refusing to order the original hard drive because it could be altered during analysis, despite defendant's argument that “computer programs in existence did not create true mirror images”), *abrogated on other grounds*, *State v. Pickett*, 211 S.W.3d 696 (Tenn. 2007). Other courts have required production of forensic image files, apparently in the absence of a request for the original media. See, e.g., *United States v. Hill*, 322 F.Supp.2d 1081 (C.D. Cal. 2004).

³³ Fed. R. Evid. 1002.

image are likely to fall within this rule,³⁴ but the forensic images themselves and perhaps some other data on them are arguably not “readable by sight.” Federal Rule of Evidence 1003 provides a basis for admitting these into evidence as duplicates: “[a] duplicate is admissible to the same extent as an original, unless . . . in the circumstances it would be unfair to admit the duplicate in lieu of the original.”³⁵

Whether to admit forensic data under the Best Evidence Rule will therefore come down to a question of whether the image or the data “accurately reflects” the original, or whether it is fair to admit the evidence. The analysis will be similar to the one discussed above with regard to authenticity.

III. Reliability of forensic tools

Federal Rule of Evidence 702 provides that an expert (by knowledge, skill, experience, training, or education) may testify about scientific, technical, or other specialized knowledge 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.” Courts have an obligation to act as a “gatekeeper” to ensure that such testimony is reliable.³⁶

In *Daubert v. Merrell Dow Pharmaceuticals, Inc.*³⁷, the U.S. Supreme Court held that in order to be reliable, expert testimony must be “derived by the scientific method” and “supported by appropriate validation.”³⁸ The Court noted several non-exclusive factors that courts may consider in evaluating the reliability of scientific, technical and other evidence supported by expert testimony:

- whether the theories and techniques employed by the scientific expert have been tested;
- whether they have been subjected to peer review and publication;
- whether the techniques employed by the expert have a known error rate;
- whether they are subject to standards governing their application; and
- whether the theories and techniques employed by the expert enjoy widespread acceptance.³⁹

³⁴ See Graham, Handbook on Federal Evidence, Sixth Edition at 827, n. 4 (2006) (suggesting that if an item offered as evidence has been through several digital incarnations and is subsequently printed out, then that printout is an original pursuant to Rule 1001(3)).

³⁵ See, e.g., *State v. Morris*, 2005 WL 356801 (Ohio App. Feb. 16, 2005) (holding that where police inadvertently destroyed original hard drive that forensic image was based on, EnCase image file was admissible as a duplicate (not an original) because the hash value matched the original drive at the time of collection.)

³⁶ See *Kumho Tire Co., Ltd. v. Carmichael*, 526 U.S. 137 (1999) (holding that with regard to scientific, technical or other specialized knowledge, where the “factual basis, data, principles, methods, or their application are called sufficiently into question . . . the trial judge must determine whether the testimony has ‘a reliable basis in the knowledge and experience of [the relevant] discipline.’”). Note that the rule requires judges to be gatekeepers of testimony, not the evidence itself. However, as a practical matter an expert will be needed to lay the foundation for technical evidence and to rebut claims of unreliability.

³⁷ 509 U.S. 579 (1993).

³⁸ *Daubert*, 509 U.S. at 590.

³⁹ *Id.* Note that in the *Daubert* analysis, whether the forensic image was actually compromised or not is irrelevant; a court will look only to whether the software that created the image used reliable techniques.

The extent to which particular forensic software tools used by an analyst have been tested or subject to peer review will vary considerably with regard to which tools are at issue, and practitioners would do well to select well-tested (and testable) tools.⁴⁰ Many tool manufacturers test their software in a range of conditions, although this work is not always made public.⁴¹ The NIST Computer Forensics Tools Testing Project⁴² is also a valuable source of testing information, but it does not appear to be strongly focused on finding security vulnerabilities in the software. Rather, most testing seems to have been focused on showing that the software does what it purports to do on datasets that have not been deliberately created to confuse the software. Although security testing of forensic software may not have been as robust as some would desire,⁴³ this gap in testing standing alone probably will not result in the exclusion of evidence. Nevertheless, a more rigorous approach to testing for vulnerabilities would create greater assurance in the legal community that the software is reliable.

To the extent security vulnerabilities are present, they introduce a risk of error in that an attacker could alter the data on the forensic image (or the way the data appears to an examiner). Further, as discussed above, hash values may not be a reliable means to eliminate error entirely, because they themselves may be subject to attack or circumvention. The risk of an attacker compromising the forensic software through a security exploit is difficult to quantify, but the higher the risk of error, the more susceptible the evidence will be to exclusion under *Daubert*.⁴⁴

There are recognized industry practices governing the use of forensics software, and many manufacturers offer certification programs,⁴⁵ but there is no formal certification for forensic analysts and techniques vary widely.⁴⁶ Yet even the strictest certification standards would not address the impact of vulnerabilities in the software, which if present and successfully exploited might be impossible to detect. Therefore, courts must also look to whether there are strong security standards governing the forensic tools themselves. To the extent more work is done to define strict, industry-wide security standards for forensic software, the software will be more likely to be found reliable.⁴⁷

⁴⁰ Open source tools may provide an advantage with regard to the “testability” factor.

⁴¹ See Newsham et. al at 12 (noting that according to Carrier, “sufficient public testing tools, results and methodologies either don’t exist or are not public”).

⁴² See *supra*, note 5.

⁴³ See *supra*, note 6.

⁴⁴ The quality of forensic analysis, while not relevant to the impact of vulnerabilities on reliability, will nevertheless be important to a court in deciding whether the forensic evidence as a whole is reliable. In order to gauge the quality of forensic analysis, the opponent of the evidence should have access to the queries the analyst used and be able to reproduce them on a copy of the image. The opponent may also want to conduct their own forensic analysis, preferably on the original media, and preferably with a different set of tools, which could reveal data that may have been hidden from the proponent’s software.

⁴⁵ See, e.g., Guidance EnCE Certification Program, available at http://www.guidancesoftware.com/training/EnCE_certification.aspx.

⁴⁶ See Phil Hearn, “MSU computer forensics course takes aim @ ‘cybercrime,’” available at <http://www.msstate.edu/web/media/detail.php?id=2119> (according to Associate Professor David Dampier, “computer investigative techniques . . . vary widely among local, state and federal law enforcement agencies.”).

⁴⁷ See *supra*, note 5.

Finally, forensic software enjoys widespread acceptance, but this state of affairs is in some measure predicated on the ability of the forensics community to continue demonstrating the reliability of its software.

It does not appear that any courts have considered the implications of security weaknesses in forensic software, but courts that have considered the admissibility of forensic images generally have found forensic tools to be reliable under *Daubert* and related standards.⁴⁸ This state of affairs is not likely to change merely because of a possibility that vulnerabilities in the software can theoretically be exploited. However, if vulnerabilities are demonstrated that are relatively easy to exploit, if security standards in forensic software design are not sufficiently strong, and if public security testing capable of being peer reviewed is lacking, the risk of a *Daubert* exclusion will increase.

VI. Conclusion

As with other forensic techniques, computer forensic tools are not magic; they are complex software tools that like all software may be subject to certain attacks. Yet because these tools play such a critical role in our legal system, it is important that they be as accurate, reliable, and secure against tampering as possible. Vulnerabilities would not only call into question the admissibility of forensic images, but could also create a risk that if undetected tampering occurs, courts may come to the wrong decisions in cases that affect lives and property.

In order to mitigate the risk that a vulnerability may be present in a given forensic software product, courts should routinely allow parties who request it an opportunity to conduct their own forensic analyses of original media. This option may not be available where the original media have changed after the forensic image was created. In these cases, courts should be especially sensitive to the accuracy and reliability of the forensic image, and to the quality of analysis that was undertaken.⁴⁹

The risk of forensic evidence being excluded as inaccurate or unreliable remains low at this time,⁵⁰ because execution of arbitrary code on the forensic workstation has not yet been demonstrated, and because attacks against forensic software outside the security industry do not appear to be occurring frequently. However, stronger security practices on the part of forensic software manufacturers, and sensitivity to these issues by judges, will ensure that forensic images remain admissible and promote fairness by reducing the risk of tampering.

⁴⁸ See, e.g., *Williford v. State of Texas*, 127 S.W.3d 309 (Tex.App. 2004) (finding that police detective qualified as expert on forensic software, and that EnCase was reliable because it is generally accepted in the computer forensic community, is commercially available and can be tested by anyone and in fact has been tested, that SC Magazine had given it five out of five stars in a review, that it has a low potential rate of error, and that EnCase successfully verified the copy of defendant's hard drive).

⁴⁹ Where it is possible for both parties to image such original media at the same time, they should have an opportunity to do so.

⁵⁰ Absent a finding that tampering probably occurred or did occur, which will nearly always result in exclusion.