CERIAS Tech Report 2005-17

COMPUTER EVIDENCE V. DAUBERT: THE COMING CONFLICT

by Christopher V Marsico

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

Computer Evidence v. Daubert: The Coming Conflict

Christopher V. Marsico
CERIAS
Purdue University School of Technology
TECH 581G Semester Research Paper in Computer Forensics
March 2004

Table of Contents

Its Elementary

Its elementary dear Watson; e-mail, instant messaging, electronic documents, and databases, no longer does Sherlock Holmes carry only a magnifying glass, his 21st century tool kit includes a write blocker and bit stream backup software. The nature of evidence has changed. Thousands of incriminating documents can be on a memory card the size of a penny. This latent evidence will take the science of computer forensics to discover it. Ask Doctor Watson what the best way to collect electronic evidence is, and he will not know the answer. This one would expect, the problem comes from the fact that neither does Mr. Holmes or today's forensic investigators for that matter. The science of computer forensics has had a brief history, only recently has it moved out of the government and military worlds and in to corporate America (Carrier, 2002). Mr. Holmes may find the evidence and the crook, but will his case and evidence get through the courts?

In the new science of computer forensics, the way he found his "smoking gun," may not meet the requirements of admissible evidence in the United States judicial system. In the past there have not been a significant number of serious legal challenges to computer evidence in court. Cases such as *Gates v. Bando* (1996), where evidence collection methods clearly destroyed evidence, demonstrate that proper tools and methods are necessary for courts to accept evidence (Smith, 2002). Conversely, peer reviewed and documented evidence collection has been accepted in state courts, as in the case of *State v. Cook* (2002) from the appeals court of Ohio. For the most part the courts have been willing to accept the testimony and evidence presented by individuals with a significant understanding of computer systems.

The computer forensic community is constantly changing, new technologies and methods are common and changes are happening at a rapid pace. What is common procedure today may not be common procedure tomorrow. How will a court system put faith in the expertise of individuals and the evidence they collect, when the best practice for this collection changes so rapidly? These issues are discussed in this paper which will present a snapshot of the computer forensic community as it is today, and offer guidance on where the community needs to go to meet the goal of becoming a more mature scientific discipline.

A Brief History of Scientific Evidence

In 1993 the United States Supreme Court made a landmark ruling that would change the way scientific evidence was presented in the court room. The ruling was based on the belief that the rules for presentation of scientific evidence needed to be updated. This ruling was in the case of *Daubert v. Merrell* (1993). Before a decision in this case could have ever been made there had to be a set of events that lead to the ruling. Two key steps in the development of rules for the admissibility of scientific evidence are *Frye* and the Federal Rules of Evidence. An understanding of these is critical to the discussion of computer forensics and the *Daubert* criteria.

Frye

Since 1923 courts in the United States have relied on the "general acceptance" test to determine if evidence was legitimate. This test was based on the ruling in the case of *Frye v. United States* (1923) by the District of Columbia Court of Appeals. This test set the standard that if a scientific practice was generally accepted amongst the scientific

community that it was practiced in, it could be admitted in court. This standard came when the court refused to admit evidence from a device similar to a lie detector test (Bernstein, 2001). The court in its ruling stated that;

> "While courts will go a long way in admitting expert testimony deduced from a well-recognized scientific principle or discovery, the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs."
> (*Frye v. US*, 1923)

"General acceptance" would be used for many years by federal and state courts. Today the test is still used for admission of scientific evidence in several state judicial systems (O'Connor, 2004).

The *Frye* test only applied to true scientific evidence and was used mostly in criminal cases (Bernstein, 2001). *Frye* was a landmark case and the rule showed the court's power to make judgment on what should be evidence. These novel scientific procedures, that are the target of *Frye,* are often referred to as "Junk Science" (NTI, 2004). Evidence from "junk science" is what the "general acceptance" test was designed to remove from court. Bernstein (2001) states that even though *Frye* was not often referenced in cases involving scientific evidence many of the courts were simply using "general acceptance" without citing *Frye*. The author also believes that the *Frye* test was often considered inapplicable in civil cases. The United States with its "general acceptance" test as the guideline for submission of scientific evidence would experience a dramatic change a little more then fifty years later.

FRE

In 1975 the Federal Rules of Evidence (FRE) took effect using standards that had been developed by the United States Supreme Court just a few years earlier. The FRE

now governed the admissibility of evidence into the federal court room. In the discussion of scientific evidence one of the most important rules is #702. This rule, which was recently amended in 2000, states:

> *"If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case."*

It was developed for the determination of a witnesses' ability to be considered an expert. This rule sets a list of key requirements that the witness must meet in order to be considered an expert: sufficient facts, reliable methods, and proper application. One of the complaints with *Frye* was that the ruling was vague (Bernstein, 2002). The FRE countered this ambiguity with specific requirements.

Along came Daubert

In 1993 the United States Supreme Court ruled on a decision involving the case of *William Daubert v. Merrell Dow Pharmaceuticals.* The plaintiff was suing for birth defects allegedly caused by the medicine Benedictine. Daubert had eight different scientific witnesses all testify that the medicine could cause birth defects. The court decided that this evidence was not admissible. The ruling was based on the fact that the court felt these witnesses did not meet the standards set by the Federal Rules of Evidence. They decided that the "general acceptance" test that was outlined in the *Frye* case had now been superceded by the FRE (Bernstein, 2001). The court went on to state; "thus general acceptance is not a necessary precondition to the admissibility of evidence under the FRE" (*Daubert v. Merrell*, 1993). The Supreme Court was saying that lawmakers

purposefully left out information regarding general acceptance so the judge would act as a “gatekeeper” and make a determination on the scientific testimony’s reliability (Bernstein, 2001).

This “gatekeeper” rule extended the powers of the judge in cases with scientific evidence. Now before a trial, a judge may rule on the admissibility of the scientific evidence, not simply the credibility of the witness. The witness’ requirements for credibility are outlined in Rule #702 of the FRE but the guidelines for a judge to rule on the credibility of the actual evidence is not. The judge has the burden of determining if the evidence is both relevant and reliable (Carrier, 2002). This is a shift of power from the *Frye* test, where it was the scientific community that had to show that the science was true based on its acceptability to the community (Rogers, 2003). The “*Daubert Test*” has short comings when there is no scientific community around the science (Carrier, 2002).

With judges empowered to make credibility decisions, a hearing called a “*Daubert Hearing*” may occur before a trail (Smith, 2002). In this hearing each side has the opportunity to present that the science behind the evidence they wish to admit is valid. According to interpretations of the *Daubert* (1993) ruling, the admissibility of scientific evidence should be considered on the following four criteria.

- Has the theory or technique been reliably tested?
- Has the theory or technique been subject to peer review?
- What are the theories or techniques known or potential error rates?
- Has the theory or technique been generally accepted as a standard in its scientific community?

(O’Connor, 2004)

The court later went on to clarify with an opinion in *Joiner* (1997) that these criteria apply to the methodology and principals, not the conclusions drawn from the technique (Benstein, 2001).

The criteria were not specifically outlined to only cover scientific evidence. The case *Kumho Tire v. Carmichael* (1999) furthered the scope of the *Daubert* requirements to cover technology expertise. This ruling set the precedent that the four rules described above would be used to measure the methodology of engineers and technologists when ascertaining the admissibility of their "technological" evidence. This extension of the *Daubert* requirements is another way computer forensics falls under the criteria. Computer forensics is difficult to classify as a disciple. It would appear that computer forensics itself is a science at the purest level. Investigators then use technologies to exercise the scientific principles to collect evidence. The *Daubert* criteria are applicable to computer forensics from both avenues.

The ruling in the *Daubert* case was intended to end the "battle of experts" (O'Conner, 2004). O'Conner states that:

> "Scientific fields that have been generally accepted by the professional forensic associations are proliferating, forensic this and forensic that; there must be some underlying reliability standards."

This statement leads well into the discussion of the field of computer forensics. How is the computer forensic community building a foundation of "reliability standards?"

Today's Computer Forensic Community

According to Rogers (2003), the area of computer forensic is "at a cross roads in its journey to become a recognized scientific discipline." This illustrates the fact that computer forensics is currently an immature scientific discipline. The community is missing some of the key elements that would make it mature. As shown, the *Daubert* criteria have been made the guidelines for technology, science and engineering to be

admissible. Does the field currently meet the requirements? In looking at each of the four criteria the discipline can be adjudicated on its compliance.

Testing

Testing of scientific tools according to *Daubert* is an important step in the maturation of a science. In order for evidence to be proven reliable, the tools used in its production should be tested to make sure that the results they report are accurate and uniform. This testing guideline subjects a tool to a battering of situations to insure accurate results (Carrier, 2002).

In the field of computer forensics there are two main types of tools; hardware and software. The hardware tools are mainly write blockers or other devices that interface with computer components. These can be easily tested to show they operate properly. It is more difficult with software tools. In Carrier's "Open Source Digital Forensics Tools: The Legal Argument" (2002) two types of software are discussed; open and closed source. Where does reliability testing on these types of software come from? For closed source software many times a forensic investigator and the courts must trust the vendor that the software was created accurately. These groups must also trust that the vendor has properly coded the software so that the results obtained from its application are reliable. Closed source testing can be done by the public, but only the vendor has access to the code, so only they can vouch for the accuracy of the underling process (Carrier, 2002). With an open source software tool one must also rely on the group or organization producing the software, but having access to the software's source code increases ones' ability to verify the integrity of the software and its results.

The National Instate of Standards and Technology (NIST) through the US Department of Commerce has a working group on Computer Forensic Tool Testing (CFTT). This group works to define requirements for disk imaging tools used in computer forensics (NIST, 2001). NIST reports that dependable computer forensics tools are required for reliable means of investigating crimes. It is important that the tools used are tested to make certain that the information they produce is accurate. This project is an important step for the forensic community but the testing is limited to tools that copy or image hard disk drives. Imaging hard disk drives is only one aspect of the forensic process, so this is only a part of what is needed.

Peer Review

The requirement of peer review under *Daubert* is a continuation from the *Frye*. Under *Frye* this was the main requirement for admissibility (Carrier 2002). With *Daubert* it is necessary that the methods and tools pass public and expert scrutiny before being considered admissible. The peer review process has long been used in the scientific community to facilitate this requirement and most of the publication and review comes from professional journals. These journals offer a researcher the ability to collaborate with peers and open research up to scrutiny, retesting, and analysis.

Steps have been taken in the area of peer review. Several journals have been created that have gained popularity in the computer forensic community. These journals are all in the first few volumes and most have not gained wide acceptance or readership outside of the community. This will change over time and the journals that are in existence are a step in the right direction.

A problem with the peer review system is that reviews must be done by experts. Currently, there is no one way for a computer forensic expert to be defined. The journals are created by academic institutions, companies and media outlets. They look to persons with extensive training and background to be considered experts. It is difficult to rely on the expertise of the individuals that are reviewing the published material when there is no common understanding of what makes one an expert.

Error Rates

The courts cite error rates as import for admissibility because truth is an import aspect of the United States legal system. The truth can only be found when no error is made in the collection, analysis, or presentation of evidence. With known error rates for the technologies used, the court can make a determination on the likelihood of a believed truth being false. If justice is blind then known error rates in the most import aspect of the *Daubert* test because justice will blindly follow evidence presented as truth.

To determine error rates requires extensive testing. This testing must be done not only on the tools used to create the evidence but also on the methodologies used. The community currently has done little in the way of determination of error rates. Testing must be done on all the tools used to create evidence. Vendors with proprietary information must be willing to share the results of error tests conducted or open their software up to outside scrutiny. Once extensive error testing has been done, a total possibility of error will be able to be determined from the known error rates of the tools chosen to gather the latent forensic evidence.

The many competing methods or “best practices” of computer forensic evidence collection need to be evaluated. There are currently several methods to accomplish the

same goal of collection. In order for a method to be accepted the potential error rates of the method, including where mistakes can be made and the possible error associated with those mistakes should be determined. After this the federal justice system will be able to make an educated decision on admissibility of evidence collected using the method.

Standards/Acceptance

Standards and acceptance are important because evidence needs to be of the highest quality. The scientific community that the evidence is coming from needs to be in agreement that the evidence was created in a standard and acceptable way. This has previously been accomplished by peer review and certification of methods and practices.

As mentioned, there are several methods widely used to collect latent computer evidence. Many institutions and organizations have released their own methodologies to collect evidence. These “best practices” while created with the best intentions have caused a problem because of some of their differences. The court does not have a true universally accepted method to rely upon. To further complicate the problem, many self-proclaimed computer forensics experts take what they feel are the best aspects of several approaches and create their own methodology. This proprietary method is kept secret and regarded as intellectual property.

The variety of methods has caused the problem of lack of universal acceptance. With each organization championing their method, a consensus approach can not be reached and no practice is considered standard.

The Battle: Computer Forensics v. Daubert

Where does the field of computer forensics fit today into the world of *Daubert*? It is certain that much work has yet to be done in the field, yet court cases that involve computer evidence go on daily. Are the courts not looking at the science and technology and comparing it to the *Daubert* criteria? Are lawyers not challenging the evidence presented? Both of these may be the case. It has been mentioned by several computer forensics "experts" that the reason these changes have not occurred is because much of the trial work that is coming in contact with computer forensic technologies is in civil courts. When it is not a matter of life and death most of the lawyers don't feel a need to challenge the evidence (R. Hendricks, personal interview, March 3, 2004). This type of challenge takes time and money. Hendricks went on to say that once computer evidence begins to make the move more to the criminal court room, especially in matters of capital crimes, there will be more challenges to the validity of the evidence.

So is the legal profession ready to challenge the admissibility of computer forensic evidence? Scott Ksander, computer forensics "expert" for the Purdue University police department says that most lawyers aren't prepared to understand the science behind the technology (Ksander, 2004). They take the testimony of the experts at face value and at most gather up their own expert. With this the jury and court are faced with the "dueling geeks" predicament. One expert says one thing while the other expert refutes those findings and presents different findings. In these cases who is the jury to believe? This type of situation is exactly what the *Daubert* rulings are supposed to have eliminated. Then why are these situations still occurring? Possibly the short comings of computer forensic science provides no grounds for the judge to rule on admissibility.

Without a "gold standard" in the field (Rogers, 2003) for training or methodology, how is a judge with little or no computer background able to rule if the method used is acceptable under *Daubert* criteria.

Why haven't more cases been forced to a *Daubert* hearing? Referring back to the thoughts of Rebecca Hendricks, these aren't life and death matters. Also many judges believe that the FRE rule #702 and the "gatekeeper" rules of *Daubert* should be applied liberally, and the court should use the rule when it feels it fits justice or the sprit of the law (Pfaffenbach, 2001). The US legal system is based on interpretation of law. When a judge believes that the criteria do not apply, they often will not enforce them. Another reason may be that 95% of cases that enter the United States legal system never make it to court (Cambanis, 2004). These are decided in a plea bargain or settlement. It is Ksander's (2004) experience that most defendants, upon hearing evidence that links them to the crime was collected from their computer, take a plea bargain or confess.

Many of these problems are discussed in the New Technologies Inc. (NTI) document; "*Defending Against Junk Science Attacks"* by Anderson (2003). NTI offers solutions to *Daubert* challenges. Their recommendations include expert training from several different sources and collection of evidence with multiple tools (Anderson, 2003). NTI's recommendations show that in computer forensics there is no one best method of collecting evidence and no standard in accreditation of experts. Their recommendation to use several tools proves that there are no good published error rates, so evidence collection using one tool with little known error is not possible. Also there are a large number of tools to choose from, with no uniform best practice. These recommendations show first had the necessary steps the community must take.

Its time to grow up

When Rogers (2003) speaks of the “cross roads” he is talking about the next steps or the direction that the field must go for it to be accepted. The steps a field must take to become mature are not a standard path. The field of DNA testing has gone through the same processes that computer forensics is now facing. Computer forensics can use the knowledge gained from the DNA evidence maturation process as a roadmap for its own development. In 1996 Conners and others outlined some key goals that the DNA community must strive for;

> Among the tasks ahead are the following: maintaining the highest standards for the collection and preservation of DNA evidence; ensuring that the DNA testing methodology meets rigorous scientific criteria for reliability and accuracy; and ensuring proficiency and credibility of forensic scientists so that their results and testimony are of the highest caliber and are capable of withstanding exacting scrutiny.
>
> Meeting these scientific challenges requires continued support for research that contributes to the advancement of the forensic sciences. The research agenda must also enable criminal justice practitioners to understand and to make appropriate use of the rapidly advancing and increasingly available technology.
>
> (Conners, 1996)

These goals for the DNA community are the same that are now necessary for computer forensics to become a decisive science.

The field must be willing to unify behind a common methodology of collection. This method does not have to be set it stone, it can evolve with time as technologies and tools change. A standard does need to be established and certified by the justice system. A negative effect of this may be similar to what happened in the world of DNA evidence,

once a standard was chosen, many previous cases that had been decided on by what now would be considered an incorrect scientific method were overturned in an appeal. Additionally many innocent individuals who were convicted were able to prove their innocence through the use of the DNA (Conners, 1996). Yet until a standard is chosen the situation described will never occur and the problem will always exist.

Another reason a standard must be chosen is so the courts and law enforcement don't face similar problems to that which recently occurred in the fingerprinting community. The judge in the case *United States v. Plaza* (2002) ruled that the evidence of fingerprints in the case came from a "junk science" and that witnesses could not offer expert testimony on the conclusions drawn from the evidence (Smith, 2003). The judge had inadvertently set a precedent that all fingerprint evidence ever argued by expert witnesses using the same methodology was now inadmissible. Consequently two months later the judge came back with a reversed ruling where he admitted he had made a mistake and after further review the science was valid and the testimony would be allowed. This case nearly had devastating effects to the criminal justice system. Without a certified standard a similar ruling maybe made towards computer forensics.

Greater efforts need to be made for classification and testing of tools. The work done by the CFTT is good, but it is not enough. Too often investigators must rely on vender data to explain why tools act the way they do. Vendors often find many problems with a system or errors in code. How these errors affect the results from using the tool maybe unknown and great effort needs to be made in testing tools to find out error rates before patches and updates are released. Imagine the situation where computer evidence is collected and the case is put on hold for several months. During that time period the

vendor whose tool was used to collect the evidence comes out with a newer version or a patch for the current version. This patch, they boldly advertise, fixes know issues with the previous version. Is the evidence that was collected using the version that has “known issues” now inadmissible? Only the judge will be able to decide this matter, but it illustrates a reason why the evidence collected could be flawed and raises significant doubts on its quality. With proper error testing before and after a patch or new version is released, confidence in evidence that was collected using any version can be maintained.

The next step in the peer review process is providing the journals with certified experts to review the research of the community. How will experts be established? In a field as large as computers it is difficult for one to be an expert in all areas; one who may be good in programming may have little knowledge in risk assessment. An accreditation or certification of an expert needs to be developed that would allow the court to trust ones background and ascertain that they have the required knowledge to be considered a person who has expertise in the science and technology of computer forensics. First steps have been taken by universities and other institutions to develop programs to train individuals in computer forensics.

With a standard methodology resources can be focused on research and development of new ideas. Those with the most training, knowledge, experience and certification can in turn be considered experts and recognized by the judicial system to provide accurate testimony based on the knowledge accepted and standardized by the scientific community.

It really is Elementary

These ideas are large steps for the computer forensic community. For something that will have drastic effects on how the world operates it is difficulty to understand why theses steps have not already been taken. A lack of funding in this area is a poor excuse for lack of progress. In a society where more then 70% of information never makes it to paper, computer forensics should be a top priority for progress (R. Hendricks, personal interview, March 3, 2004). These challenges need to be faced head on and approached from the top down with those in power gathering together the right information to make the decisions that have to be made. Until the first steps of unification and development are made, the community will continue in a state of limbo. The courts will not be able to rely on the evidence collected and criminals may go free, or worse yet the innocent may be incarcerated. The understanding being gained by the community is less useful if it is not considered a good science.

A vial step in the maturation process is acceptance and validation. This right of passage must be undertaken for it will not come to one on its own. Until the modern community of computer forensics is willing to undertake the vital steps for acceptance, the United States Judicial system, an institution that has been in place for over 220 years, will be unable to constitute the science that the community practices as valid and will refer to this juvenile art as “junk science.” As a “junk science” Mr. Holmes would have no choose but to pack up and move on to the next case, knowing full well that his “smoking gun” of computer evidence would not be admissible at trial. Those who practice the computer forensics of today must take on the challenge of proving to their own Doctor Watson that computer forensic science is elementary.

References

Anderson, M. R. (2003). *Defending Against Junk Science Attacks*. New Technologies Inc. Retrieved 3/10/2004, 2004, from http://www.forensics-intl.com/art20.html

Bernstein, D. E. (2001). Frye, Frye, Again: The Past, Present, and Future of the General Acceptance Test (No. 01-07): George Mason University School of Law: Law and Economics Research Papers Series.

Cambanis, T. (2004, 2/1/2004). Trials rise in US court as plea deals are spurned. The Boston Globe.

Carrier, B. (2002). *Open Source Digital Forensics Tools: The Legal Argument* (Research Report): @stake.

Carrier, B., & Spafford, E. H. (2003). Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence, 2*(2).

Connors, E., Lundregan, T., Miller, N., & McEwen, T. (1996). *Case Studies in Use of DNA Evidence*. Retrieved 3/11/2004, 2004, from http://www.ncjrs.org/txtfiles/dnaevid.txt

Daubert v. Merrell Dow Pharmaceuticals, 509 US 579 (1993).

Federal Rules of Evidence. (2004). Retrieved 3/11/2004, 2004, from http://www.law.cornell.edu/rules/fre/overview.html

Frye v. United States, 293 F. 1013 (1923).

Gates Rubber Co. v. Bando Chemical Industries, Ltd., 167 F.R.D. 90, D.Colo. (1996).

General Elec. Co. v. Joiner, 522 U.S. 136, 149 (1997).

Kumho Tire Co. Ltd. v. Carmichael, 526 US 137 (1999).

Kruse, W. G., & Heiser, J. G. (2002). *Computer Forensics: Incident Response Essentials*: Addison-Wesley.

Ksander, S. (2004, January 20). Forensics and the Law. Presented at a TECH 581G lecture at Purdue University.

National Institute of Standards and Technology. (2001). *Disk Imaging Tool Specification* (No. Version 3.1.6): National Institute of Standards and Technology.

New Technologies Inc. *Junk Science Legal Challenge Explained*. Retrieved 3/11/2004, 2004, from http://www.forensics-intl.com/def14.html

O'Connor, T. R. (2004, 3/4/04). *Admissibility of Scientific Evidence Under Daubert*. Retrieved 3/15/2004, 2004, from http://faculty.ncwc.edu/toconnor/daubert.htm

Pfaffenbach, W. L. (2001, 1/8/2001). Statistics In Age Bias Case Survive 'Daubert' test. *Massachusetts Lawyers Weekly*, 29.

Rogers, M. K., & Seigfried, K. (2003). *The future of computer forensics: A needs analysis survey* (Tech Report). West Lafayette: Center for Education and Research in Information Assurance and Security, Purdue University.

Rogers, M. (2003). Computer Forensics: Science or fad. *Security Wire Digest*, Vol 5. No. 55, July 24.

State v. Cook, 149 Ohio App.3d 422 (2002).

Smith, F. C., & Bace, R. (2002). *A guide to forensic testimony: The art and practice of presenting testimony as an expert technical witness* (1st ed.): Addison-Wesley Pub Co.

United States v. Llera Plaza, 181 F. Supp. 2d 414 E.D. Pa. (2002).