

# The 'Tools Proven in Court' Question

digg this storyDiscuss in Forums {mos\_smf\_discuss:/root}

By Steve Hailey, President, CEO, and Primary Analyst of the CyberSecurity Institute

This document is provided for informational purposes only, and represents the opinions of the author. It is not intended to represent legal advice, and should not be construed as such. If you are using the information contained within this document to help prepare for a computing investigation, review this document in its entirety with your legal counsel.

In the digital forensics community, you'll often hear talk about forensic tools "proven in court." On a pretty regular basis, I receive emails asking for our opinion on this topic, and whether or not "this particular tool" or "that particular tool" should be used based on whether or not its use has been "proven in court."

Vendors that sell digital forensics software will typically use statements such as "our tool has been proven in court" as a marketing technique. Really what these vendors are saying is that their tool was used in a case where the results of the tool as well as the underlying methodology and testimony of the forensic computer examiner were admitted. Understand that there are various tests that courts can apply to expert testimony, methodology and opinions in order to determine admissibility, reliability, and relevancy. The particular test(s) used will vary from state to state and even from court to court within the same state.

In the digital forensics business, we typically refer to an attack of the methods, tools and techniques we use as a "junk science" attack.

I do believe that commonly used commercial tools such as FTK, EnCASE, ProDiscover, and X-Ways Forensics should be used for forensic analysis, as the tools have already been authenticated by experts in many court cases. There is more to this equation however.

While I am not an attorney, I believe that the primary question that should be asked here is not whether a particular tool has been proven in court, but rather:

Does the analyst have the technical background to support the results of their investigation, have they properly authenticated their results, and was a sound investigation performed from start to finish?

Think about this for a moment. If the tools being used are the mechanism to find evidence on a computing device, and several different tools can replicate the process, then it doesn't matter what tools were used. The evidence is simply there and can be found by any competent forensic analyst using a variety of tools. Proper interpretation of the evidence, however, is another story - that's where the smarts of the forensic examiner come in to play.

Regardless of the tools that an analyst uses, the following questions should be pondered to help determine the likelihood of admissibility of evidence gathered during a forensic analysis. Whether or not evidence is admissible has more to do with factors other than the specific tools used for the technical processing.

If you are a digital forensics analyst, the following questions will most probably arise in some form during a deposition, hearing, pretrial or trial situation. Any attorney that you work for would be wise to affirm the answers to these questions with you, as they will go a long way in helping to determine whether or not the evidence gathered will be admissible in a court of law as well as whether or not your expert testimony will hold up under scrutiny. These questions can also be used as the basis for formulating additional questions to be asked of opposing experts:

1. Was the evidence gathered and verified in a sound manner?

One of the tenets of digital forensics is to assure that the original media is not altered, and that the methods used to create forensic quality copies of media and data assure that the integrity of the original is maintained. This is one of the most important steps. In situations where evidence must be gathered "live," we need to make sure that whatever process used has been verified beforehand to cause minimal changes to the overall system, and that other professionals given the same set of circumstances would have used the same methodology. Write blocking / prevention mechanisms should be used for imaging media, and thoroughly tested beforehand by the examiner to assure that the mechanism works without fail.

If you are going to use physical media for your working copy versus image files of the media, assure that the working copy media is sterile (contains no data) and has been verified as such before imaging the original to the working copy. I recommend that you write zeros to the entire drive using a program such as Sterilize ([www.csisite.net/software/](http://www.csisite.net/software/)).

Cryptographic hash functions should be used on the original media and/or data beforehand and then on the subsequent

copies in order to show that integrity was maintained as well as the fact that the copies are identical to the original. Contrary to what many forensic analysts have been taught, a simple checksum (a process that adds up byte values and outputs the result) is not recommended for this process. I recommend that an MD5 or SHA cryptographic hash function be used. As an aside, if you've heard that MD5 was "broken" and should no longer be used for digital forensics, I recommend that you read "MD5 collisions and the impact on digital forensics" by Eric Thompson of AccessData ([www.accessdata.com/support/](http://www.accessdata.com/support/)). Well done Eric.

As well, always check your images to make sure that they can be read before returning the original media back to a client or owner. Don't take for granted that since the original and forensic copy hashes match that all is well. I have experienced images not being read properly when proprietary image formats were used for the working copies. When possible and practical, use the RAW format versus proprietary, and do not take for granted that everyone uses your format - especially when you have to provide forensic images to another party involved in a case. Remember - a competent forensic examiner verifies whenever possible, not taking anything for granted. Murphy's law is just as prevalent in digital forensics as anywhere else.

At this point you might be saying something like "if the hash value for the original and the hash value for the working copy match, that's all that matters." Not so. If you are the first to image a piece of media, you could have altered the original prior to the first hash. You have to show that your imaging process from start to finish did not alter the original in any way.

## 2. Was a chain of custody maintained?

All media, documents, and evidence related to a case or situation should be kept in your custody and closely controlled. Only those that have a right to see the information should see it and have access to it. We call this creating and maintaining a chain of custody.

Detailed documentation needs to be kept and readily available relevant to the chain of custody, and the analyst needs to have a secure location used to store all materials. I believe this goes beyond merely documenting when a particular item was received or returned. You should document when any information pertinent to a case or situation is removed as well as placed back into its secure location.

## 3. Is the ownership and licensing appropriate for the tools used?

Whatever software is used for the technical processing needs to be properly licensed. If you are in business for yourself, the software needs to be licensed to you or your company. If you are performing work as an employee, the software needs to be licensed to your company and you should have the authorization to use it. If you are going to use shareware for an analysis, pay the licensing fee.

The opposing experts for a case CSI was involved in used a "demo" version of software to process the Internet history of a particular computer. The repeated word DEMO could be clearly seen on the printed reports. How professional do you think these folks looked? They were being paid handsomely for their work on the case, yet were using demo versions of software.

In another case, the opposing attorney tried to impeach me by intimating that I had used software licensed to a college I instructed at to process a case. The attorney had failed to recognize that I also owned my own business and had properly licensed copies of all software used in my analysis.

## 4. Was the proper examination environment being maintained?

An analyst that is lackadaisical in this area will most assuredly have questions raised relevant to the efficacy of their overall methodology and procedures. For one, the workstation(s) used to process evidence must be kept in good working condition. Prior to a forensic analysis, I recommend that diagnostic software be run on the forensic system, and that the results be kept. When maintenance is performed on the system or upgrades are performed, keep documentation. Your forensic workstation is a tool used for your profession, and you need to show that it is in proper working condition.

Regularly scan your workstation for viruses and malware, and always scan the original media (with a write blocking / prevention method in place) or the resultant images for viruses and malware. Many forensic analysts fail to scan for viruses and other malware, thinking that their forensic software will find and identify all of these items. Don't make this mistake.

## 5. Can the results of the technical analysis be duplicated using other tools?

Any competent examiner knows that you do not use a single tool. Granted, we all have our favorite primary tools to use, but once the evidence has been extracted that is pertinent to the situation and will be used in some type of proceeding, it needs to be authenticated using other tools.

For example, at CSI, we use some of the popular GUI tools to process the bulk of information. When evidence is found pertinent to the situation, we then use several other tools to authenticate that specific evidence, such as the fact that it is

indeed on the media at this specific cluster, block, or sector, and that any time stamp information matches up.

The key is to use different tools from different vendors and different sources. DO NOT rely solely on tools from a particular vendor or source. Another competent forensic analyst should be able to find the same data at the same location on the working media or image using an appropriate tool.

6. Does the Analyst understand what the tools they use are actually doing, or are they merely taking for granted what an automated process is reporting?

With digital forensics having such a big "WOW" factor these days, we are seeing more and more people hanging out a shingle to do digital forensics work, with many of them being "point and click" analysts. In other words, using a GUI based tool with little knowledge concerning what the tool is actually doing.

For example, regardless of the tool you use and the specific algorithms employed by your tool, the way in which computer forensic software tools perform the following is pretty much based on the same underlying principles:

- Creating forensic quality or sector-by-sector images of media
- Locating deleted/old partitions
- Ascertaining date/time stamp information
- Obtaining data from slack space
- Recovering or "undeleting" files and directories
- "Carving" or recovering data based on file headers/file footers
- Performing keyword searches
- Recovering Internet History information

If you lack the experience and technical knowledge to defend your use of a particular tool because you don't really understand what the tool is doing, then your results will not withstand scrutiny regardless of the tool used. If you do not understand how a tool could perform one of the functions mentioned above, I would recommend that you obtain some additional training. There are many fine training programs available. I would recommend Computer Forensics Core Competencies ([www.csisite.net/training/core.htm](http://www.csisite.net/training/core.htm)), Certified Computer Examiner ([www.cce-bootcamp.com/](http://www.cce-bootcamp.com/)), or NTI's 5 Day Computer Forensics Course ([www.forensics-intl.com/forensic.html](http://www.forensics-intl.com/forensic.html)) for starters.

All three courses are solid courses which teach the foundation knowledge that every forensic practitioner should possess. Once you've completed one of these, I recommend that you then take vendor specific training from one of the major forensic software vendors such as AccessData ([www.accessdata.com](http://www.accessdata.com)) or Guidance Software ([www.guidancesoftware.com/](http://www.guidancesoftware.com/)). I am also a firm supporter of X-Ways Forensics ([www.x-ways.net/training.html](http://www.x-ways.net/training.html)), and believe that every forensic examiner should be able to use the tool. At CSI, we use X-Ways Forensics to authenticate and verify the results of other tools.

There are also many fine training programs available at the Community College and University level these days. If you are after obtaining a certificate in computer forensics, I would highly recommend the Digital Forensics Certificate Program at Edmonds Community College ([cis.edcc.edu](http://cis.edcc.edu)). For a Bachelors degree, I recommend the Computer & Digital Forensics Program at Champlain College ([www.champlain.edu/majors/digitalforensics/](http://www.champlain.edu/majors/digitalforensics/)).

Truth be told, I'm the instructor for the certificate program at Edmonds Community College, so I'm a bit prejudiced.

Whatever you choice is for education, interview your instructor and make sure that they have experience not only teaching, but actually doing. This will make a world of difference in the education that you will receive.

7. Do other professionals use the same techniques and methodology?

If you are doing digital forensics related work and truly know what you are doing, you are using techniques that other professionals use. If you've developed your very own tool or methodology that no one else is in the profession is using yet, or that has not been subject to a review of your peers and thorough, documented testing, you're heading for trouble. Think about having to explain to a jury how your homegrown tool works...

Understand that when you have evidence that is damning to the other side, opposing counsel will bring up arguments that your software tool or methodology is not "generally accepted in the digital forensics community" and so forth. If you have authenticated your results using several different tools, really understand the meaning of what the evidence shows - and can prove it - you'll be fine. To help avoid problems in this area that will draw attention away from the real matter at hand, I do recommend (at the time of this writing) that your primary tool be a widely accepted commercial tool.

8. Is the Analyst technically capable of defending/supporting their interpretation of the evidence?

I could write an entire document citing instance of the opposing experts misinterpreting the results that their tools

presented to them. We'll cite one example.

The opposing experts in a case used a popular GUI tool that came with a script for finding Internet search engine activity. When they ran the script, they found literally hundreds and hundreds of "searches" that supposedly had been conducted by our client. Therefore, our client had intentionally accessed certain types of information related to these searches, because - in their interpretation - the searches showed intent.

On examination, I realized that each and every one of these "searches" were actually hyper links and not searches at all. The hyper links were formed in such a way that when a link was clicked, a database was searched to pull up the most current information related to the link. Our client had not conducted any searches whatsoever.

The opposing experts took for granted that their automated tool was accounting for any variables, and would only show them searches that had actually been conducted. A big mistake. The opposing experts lacked the technical skills to actually authenticate their results, so they depended entirely on a single automated tool.

Results from any tool should always be thoroughly checked by someone versed in the underlying technology to see if what appears to be a duck is actually a duck.

In the very same case, I recovered reams of email that the opposing experts did not find. This was because they simply did not know how to find it.

By the way, I used the same primary tool in our investigation as they did. The differences in what was found as well as the differences in interpretation was due to the inexperience of the opposing experts - it had nothing to do with the tool being used.

At CSI, we use a variety of tools to process cases. We use the well-known and popular GUI tools, command line tools, and open source tools. The fact of the matter is, many of the tools "already proven in court" are fantastic tools and do a great job. I want you to realize however that if you feel you must use a specific tool to defend your results, you are probably in need of additional technical training more than you are a specific tool.

Methodology and technical knowledge is far more important, in my opinion, than the tool.

As you can see, whether the tool being used has been "proven in court" or not, the digital forensics practitioner needs to know what he or she is doing, and should have a technical background that includes more than just a course or two in digital forensics.

There are situations in which a particular tool has been chosen as the primary tool for a company or law enforcement agency. So if you work there, you'll be using the tool that has been accepted and adopted. Even in this situation however, you'll find the experienced forensic practitioners will use additional tools to authenticate the results of the primary tool.

If you have a positive answer to the 8 items presented above, then you have done your job and are prepared. It is now up to the attorneys to argue whether or not the evidence you have recovered is admissible based on its relevancy to the situation amongst other factors.

The Tests

As mentioned previously, there are various tests that courts can apply to the methodology and testimony of an expert in order to determine admissibility, reliability, and relevancy. The particular test(s) used will vary from state to state and even from court to court within the same state.

The Frye test (Frye v USA, 1923) used to be the standard for the admissibility of expert witness testimony. Frye indicated that scientific evidence would not be admissible unless the scientific community to which it was related had generally accepted it. Some states still use the Frye test.

The Frye test remained the standard for about 50 years.

In 1973, Congress adopted the Federal Rules of Evidence. The rules relevant to our document here are:

FRE 401 and 402: All relevant evidence is admissible, except as otherwise provided ... Evidence which is not relevant is not admissible. Relevant evidence is defined as that which has any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.

FRE 403: Although relevant, evidence may be excluded if its probative value (serving as proof) is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.

FRE 702: 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. Please see <http://www.law.cornell.edu/rules/fre/overview.html> if you need more information on the Federal Rules of Evidence.

Stemming from the Federal Rules of Evidence, came the Daubert (Daubert vs. Merrell Dow Pharmaceuticals, 1993) reliability test. The Daubert reliability test requires special pretrial hearings for scientific evidence and special procedures on discovery. The Supreme Court in Daubert declared that the more flexible Federal Rules of Evidence had completely replaced the Frye test in determining whether an expert's testimony was admissible, and that the Frye test would no longer be used in federal courts.

In its basic form, Daubert says that experts must use objective methodological principles in their work, and that they should also be qualified to testify as a true expert in their field. Federal trial judges were granted the right to screen an expert's qualifications and test the reliability of the expert's methodology.

A number of reliability factors can enter into the Daubert reliability test:

- Whether the expert's technique or theory can be or has been tested -- that is, whether the expert's theory can be challenged in some objective sense, or whether it is instead simply a subjective, conclusory approach that cannot reasonably be assessed for reliability
- Whether the technique or theory has been subject to peer review and publication
- The known or potential rate of error of the technique or theory when applied
- The existence and maintenance of standards controlling the technique's operation
- Whether the theory or method has been generally accepted by the scientific community

Individual states and even jurisdictions within these states have their own rules of evidence, and you'll find many are based on the Federal Rules of Evidence: States accepting Daubert: States accepting Frye: States with their own tests:

Connecticut  
Indiana  
Kentucky  
Louisiana  
Massachusetts  
New Mexico  
Oklahoma  
South Dakota  
Texas  
West Virginia  
Alaska  
Arizona  
California  
Colorado  
Florida  
Illinois  
Kansas  
Maryland  
Michigan  
Missouri  
Nebraska  
New York  
Pennsylvania  
Washington  
Arkansas  
Delaware  
Georgia  
Iowa  
Military  
Minnesota  
Montana  
North Carolina  
Oregon  
Utah  
Vermont  
Wyoming

It is our belief that as a digital forensics expert, you should be aware of the Federal Rules of Evidence, as well as those for your state or jurisdiction. You'll want to go over these with the legal counsel you are working with.

As you begin to work on a case and process the evidence, you'll want to ask yourself and legal counsel if your methods will survive the rules of evidence tests for your particular situation. All of your work will mean nothing if the evidence you recover is not admissible.