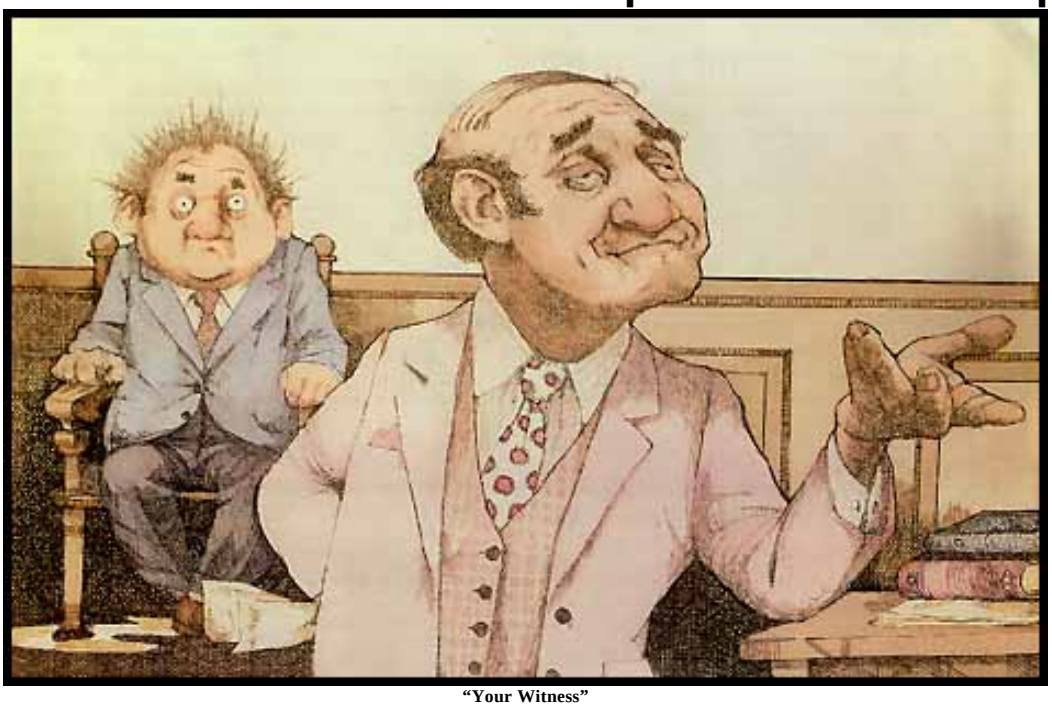
Cross-examination of the Computer Forensics Expert



"Your Witness"
(C) Charles Bragg

Craig D. Ball, P.C.

Craig Ball
Trial Lawyer
Technologist

E-Mail: craig@ball.net

Tel: 936/582.5040
Mbl: 713/320.6066
Fax: 936/582.5072

Helping Lawyers Master Technology

9795 Walden Rd., Suite 102
Montgomery, Texas 77356
www.craigball.com

Cross-examination of the Computer Forensic Expert

Today, some 95% of all documents are created using computers. Daily electronic mail traffic far outstrips postal mail and telephone usage *combined*. Computer technology impacts every facet of modern life, and the crimes, torts and disputes which carry us to the courthouse are no exception. The new field of computer forensics entails the identification, preservation, extraction, interpretation and presentation of computer-related evidence. Far more information is retained by a computer than most people realize, and without using the right tools and techniques to preserve, examine and extract data, you run the risk of losing something important, rendering what you find inadmissible, or even causing spoliation of evidence.

Though I've been immersed in computer forensics as a trial lawyer and as a computer forensics student, examiner, author and instructor for some time, I'd never come across an article that offered practical advice on the cross-examination of a computer forensics expert. The goal of this paper is to improve the caliber and candor of those who testify as computer forensics experts and to help lawyers get to the truth, not obscure it.

The Cops-and-Robbers Mindset

The world of computer forensics is heavily populated by former law enforcement officers from the Secret Service, FBI, Treasury, military investigative offices and local police forces. Many of these veteran officers--though generally well-trained and capable--have a good guy/bad guy mentality and regard computer forensics as a secret society where they don't want the "bad guys" to know their secrets. Lawyers are seen as aiding the bad guys, and the very last thing forensic examiners want is for lawyers to understand the process well enough to conduct an effective cross examination. With some justification, former cops view lawyers with suspicion and even disdain (how this makes them different from the rest of the world, I don't know). To their way of thinking, lawyers are contemptuous of the truth and bent on sowing the seeds of distraction, confusion and doubt.

This mindset can make forensic examiners guarded witnesses: not necessarily hostile, but reluctant, or quick to dive under cover of technical arcana and jargon to shake off a pursuer. A forensic examiner is dealing with largely objective observations and shouldn't come across as an advocate. If evasive or uncooperative on cross, give the witness enough rope for the jury to see it.

Tool Tykes

Poorly-trained experts rely on software tools without much understanding how they work. They're Tool Tykes. Of course, all of us trust and swear by tools we don't fully understand--do you really fathom how a quartz wristwatch tells time or a mouse moves the cursor?—but, an expert should be able to explain *how* a tool performs its magic, not offer it up as a black box oracle. Tool Tykes are trained to dodge attacks on their lack of fundamental skills by responding that, "The tool is not on trial" or citing how frequently the testimony of *other* witnesses using the same tool has been accepted as evidence in other courts. Don't let them get away with this evasion. A great tool in unskilled hands

is not reliable. Press the witness to either explain how the tool achieves its results or admit they don't know. Be advised that this technique will flush out only the pretenders to the throne of "expert." Real pros are going to know how their tools work down at the bit level and be able to explain it in a way any juror can grasp. Of course, *you* should be ready to distinguish the right explanation from technical doubletalk.

Computer forensics is a new discipline and many computer savvy persons without forensic training or experience offer their services as experts. Just as not every doctor is qualified as a coroner, not every systems administrator is a forensics expert. A background in law, law enforcement or investigation is important, whereas programming skills have little bearing on computer forensic skills. Be certain to obtain the witness' C.V. and check it for accuracy. Look for membership in professional associations of computer forensic examiners, formal training and certification. Find out if the witness has published articles on computer forensics or participated in list serves supporting the discipline, then find and read those contributions.

Chain-of-Custody Issues

Because of their law enforcement backgrounds, forensic experts tend to be very savvy about the importance of, and the proper procedures to maintain, a chain of custody. A chain of custody attack is warranted when you can level a credible charge that someone tampered with the evidence. The critical importance of the chain of custody is drilled into every computer forensic expert. If you can prove the witness botched the chain of custody, the witness will be shaken and defensive. Even when tampering isn't suspected, a sloppy chain of custody suggests a poorly qualified expert.

The Limits of Computer Forensics

Nearly everyone uses computers, but few users understand them well. A witness who's mastered the computer's deepest secrets may enjoy a Guru-like authority when testifying. If you're seeking to cast doubt on the witness or the "science" of computer forensics, you may gain traction by getting the witness to concede some of the things an examiner *can't* ascertain about how a particular computer was used or who used it.

Though computer forensics specialists can perform miraculous tasks, there are limits to what we can divine or resurrect. Some of these limits are oddly mundane. For example, it can be difficult to establish that a user altered the time on their computer, especially if the clock has been correctly reset by before the examiner arrives. Computers are pretty "stupid" where time is concerned. A toddler (at least one who doesn't live in Alaska) would challenge the assertion that it's midnight if the sun's still up, but, no matter what the actual time may be, a computer accepts any setting you give it as gospel. There are ways to ferret out time manipulation, but they aren't foolproof.

Similarly, a computer can't identify its user. At best, it can reveal that the user was someone with physical access to the machine or who perhaps knew a password, but it can't put a particular person at the keyboard. Usage analysis may provide other identity clues, but that, too, isn't foolproof. Establish the limits to what an examiner can say with

certainty, and afford the examiner an opportunity to concede those limits or overreach them.

Missing in Action

When hard drives were smaller, it was possible to thoroughly examine them by looking through the data. It was a tedious process, to be sure, and one where it was easy to grow tired and overlook something. Still, it was a pretty reliable process. Hard drives have grown to gargantuan volumes, e.g., the 60 gigabyte hard drive in my current laptop is *3,000 times larger* than the 20 megabyte drive in my first portable computer. It's all but impossible in the usual engagement for an examiner to look at all the data on the drive. It's overwhelming to thoroughly examine just the places where data most often hides.

Consequently, examiners must rely upon software tools to get the job done. Keyword searches are an integral part of computer forensic examinations and entail an examiner entering key words, phrases or word fragments into a program which then scours the drive data to find them. False positives or negatives are less of a problem than the literal way computers approach searches. A human eye will see the word "Confidential" though it be written C.o.n.f.i.d.e.n.t.i.a.l, Confidentail or _onfidential, but a computer can't make the connection unless it's been programmed to identify common variants or uses more advanced search algorithms. When the matter in dispute hinges on what *wasn't* found on the drive, the ingenuity and diligence applied to the search may be fodder for cross-examination. Of course, whatever points you score forcing the examiner to admit he didn't pursue certain searches can be lost when the witness returns the next day having completed those searches without finding anything.

Dealing with Digests

Disk drives are so vast and operating systems so complex, how can a forensic examiner be certain that someone hasn't slipped in incriminating data? A forensic examiner might respond that, when acquired, the data on the hard drive is "hashed" using sophisticated encryption algorithms and a message digest is calculated, functioning as a fingerprint of the drive. Once hashed, the chance that tampering would not be detected is one in 340 undecillion--and that's one in 340 followed by *36 zeroes*! That's FAR more reliable than DNA evidence! It's an impressive assertion, and even true…to a point.

Drive hashing and the creation of those message digest "fingerprints" is indeed one of the slickest tools in a forensic examiner's arsenal. The reliability assertion is genuine (though the probabilities vary among commentators). But, the probative value of hashing depends upon the points in time during the acquisition and analysis process when hashing is done and, ultimately, upon the veracity of the examiner who claims to have hashed the drive. Two identical message digests of a drive tell you only that no tampering occurred between the time those two digests were computed, but tell you nothing about tampering at other times. If a drive is altered, then hashed, subsequent hashes can be a perfect match without revealing the earlier alteration. Likewise, an earlier hash can't tell you anything about subsequent handling; at least, not until the

drive is hashed again and the digests compared. The point is, be sure you know when the hashing was done and where that activity falls with respect to the entire chain of custody. Also, consider whether the hashing was done by someone telling the truth. A cross-examiner might score some cheap points by getting the witness to attest to the importance of hashing, and then asking the witness to explain the mathematical process by which such a critical step is accomplished. Some experts understand cryptography and can explain it, but I suspect their ranks are small.

Pornographic Images

Aside from the scourge of child pornography, the law makes a person's proclivity for pornography their own affair; unless, of course, that person is my employee and dumps their trash on my computer system. Pornography, the bread-and-butter of law enforcement computer forensic examinations, is a civil litigation issue in cases of wrongful termination or harassment. When used as grounds for discipline or termination, or when the presence of smut will otherwise be used to impeach, it's essential to be able to reliably link the objectionable imagery to its true owner.

It's a simple matter to load a computer with dirty pictures unbeknownst to the owner. One sneaky way to do this is to embed the pictures in an innocuous e-mail but specify the dimensions of the image to be a single pixel. That way, all of the image data gets downloaded to their computer, but the recipient didn't see a thing. The porn file or other electronic contraband now resides on the recipient's computer and there's no reason to believe the recipient didn't put it there unless you go looking for other avenues. The same insidious result can be accomplished using an outwardly-benign web site or precipitated by a malevolent virus. The upshot is that an amateur examination of the computer reveals megabytes of porn or other incriminating material, and management goes ballistic.

Fortunately, a skilled and cautious investigator can spot the difference between an unwitting victim and avid accumulator. Sheer volume is a factor, but the location of the images and efforts to conceal or delete them, as well as their creation and access times, format and context all tend to reveal the truth. Any skilled examiner should be able to authoritatively address the question, "How do you know my client put these files on the computer?" A reply of, "It was his computer and the pictures were on it" is always an inadequate explanation.

Checklists and Notes

Thoroughly analyzing a hard drive is a long, detailed and complicated process. It's easy to overlook or fail to follow up on something. Those who undertake other critical, complex and repetitive tasks are aided by checklists (survival tip: never fly with a pilot who doesn't take the preflight checklist very seriously). However, computer forensic analysts are sometimes taught to avoid employing checklists for fear criminal defense lawyers will crucify the examiner for skipping a step, even when the shortcut is justified. Spanning the realms of art and science, and dealing as we do with human frailty, computer forensics examiners are aided by instinct and gut feeling--skills which don't lend themselves to checklists.

The twin goals of cross-examination are to secure helpful concessions and blunt the impact of whatever hurts your case. If an examiner uses checklists or a published methodology, obtain copies of those items and search for the overlooked step suggesting carelessness. If the examiner doesn't use some written system to insure a consistent analytic approach, then the examiner might be taken to task for that. An experienced witness isn't going down in flames this way, but it may flush out charlatans and novices.

In a similar vein, all the literature emphasizes, and veteran examiners agree upon, the importance of carefully documenting a forensic analysis. If the witness claims to have no notes, there's something amiss. Inquire if the witness' analysis tools track activities like keyword searches and whether those logs have been saved or altered. Obtain and check logs for matters overlooked, such as results omitted from reports or incomplete follow up.

Get Help

Cross-examining a technical expert on matters you don't understand is playing with fire. Though you can't quickly become the equal of someone who's spent years mastering an esoteric specialty, you can learn a great deal about one or two specific aspects of that specialty. Pick your battles and do your homework to win the day. You can pick up the fundamentals from my article, "*Computer Forensics for Lawyers Who Can't Set the Clock on their VCR,*" found at http://www.craigball.com/cf.pdf. For top notch online information about computer forensics, visit the Electronic Evidence Information Center at http://www.e-evidence.info/index.html or the resource library areas of the following vendor sites: New Technologies, Inc. (www.forensics-intl.com), Computer Forensics, Inc. (www.forensics.com) or Kroll Ontrack, Inc. (www.krollontrack.com).

Finally, don't charge into battle alone. Even if you haven't invested in your own computer forensic analysis, it might be worthwhile to engage an expert to review the other side's findings or back you up at deposition or trial.

Craig Ball is a Texas trial lawyer and computer forensics expert. He can be contacted via e-mail at craig@ball.net.