Being the Better Expert Witness:
A Primer for Forensic Examiners

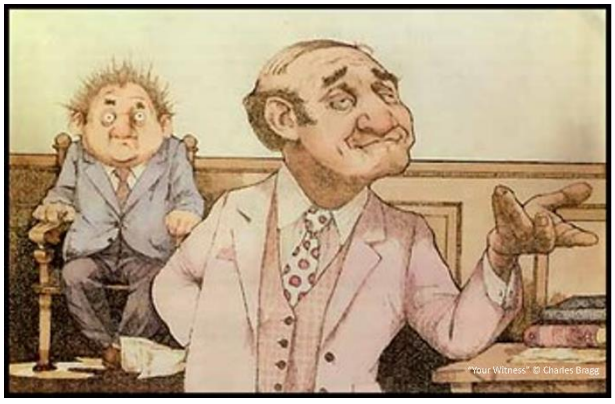
Craig Ball[1] © 2023

Link to: http://www.craigball.com/Ball_Expert_Witness_2023.pdf

I'm a lawyer *and* a certified computer forensic examiner: a weird duck, right? So weird that I *like* to testify—in court, at deposition, in declarations and affidavits—and I don't even mind writing reports about forensic exams.

I thrill to the confrontation—the chance to mix it up with skilled interrogators, defend my opinions and help the decision makers hear what the electronic evidence tells us. There's a compelling human drama playing out in those bits and bytes, and computer forensic examiners are fortunate to tell the story. It's our privilege to help the finders of fact understand the digital evidence.[2]

This paper covers ways to become an effective witness and pitfalls to avoid. They say lawyers make notoriously poor witnesses and I have no illusions that I'm a great witness. But after forty years of trial practice and thirty as a forensic examiner, I've learned a few lessons I hope might help other examiners build their skills in court.



It's difficult for computer forensic examiners to hone their testimonial abilities because it's rare to be interrogated by a lawyer who truly understands what we are talking about. Most interrogators are working from a script. They know the first question to ask, but not the next or the one after that. Pushed from their path, they're lost. Computer forensic examiners have it easy on the stand. Deep fakes notwithstanding, computer-generated evidence still enjoys an aura of accuracy and objectivity, and the hyper-technical nature of digital forensics awes and intimidates the uninitiated. Thank you, CSI, NCIS and all the rest! But sooner or later, computer forensic examiners will square off against interrogators able to skillfully undermine ability and credibility. So, it behooves us to strive to be better witnesses.

The Trick to Being a Good Witness isn't Tricky

Novice witnesses imagine there's a system they can follow to stay out of trouble on the stand, but no battle plan survives an encounter with the enemy. There are no "tricks" to testifying, except to **prepare**

[1] Craig Ball of Austin and New Orleans is a court-appointed special master, veteran Texas trial attorney, law professor and certified computer forensic examiner. More of Craig Ball's publications on computer forensics and electronic discovery are available at craigball.com and ballinyourcourt.com.

[2] Certainly, a few examiners make their living by trying to muddy the waters; but injecting confusion and doubt is like pulling the fire alarm to dodge an exam. It may work, but, it's nothing to be proud of, and they'll be in far worse shape when they're found out.

carefully, listen to the questions asked, answer the questions asked, stick to what you know and tell the truth. The corollaries are, don't imagine you can "wing it," don't anticipate the question, don't answer the question you think the examiner meant to ask, don't overreach your expertise, and don't try to snow the lawyers, the judge, or the jury.

Preparation is Key

Brilliant, articulate and honest expert witnesses will perform poorly on the stand when they aren't asked the right questions. Lawyers invest too little time prepping expert witnesses to facilitate a compelling direct examination,[3] and expert witnesses fret too much about cross-examination when, without a solid direct examination to lay out the key points, getting through cross-examination unscathed doesn't count for much. There are many reasons why lawyers don't spend sufficient time preparing expert witnesses: Lawyers and experts have demanding schedules, time spent with experts may be expensive and egos on both sides may not admit the need for preparation. Still, preparation for direct examination demands more than scripting a few questions and ad-libbing the rest. You and the lawyer should be in synch on what needs to be covered.

The expert witness should help the lawyer understand what the digital evidence signifies and ensure that the lawyer won't stumble on the key terms and concepts. The lawyer should help the expert understand where the digital evidence fits into the case. Both must craft the flow and choreography of the direct examination, including what exhibits and demonstrative aids will be used and how to adapt when things don't go as planned (such as when the court excludes an exhibit or demonstrative aid). Preparation is key. The better prepared you are, the less anxious you'll be on the stand.

Pretrial Discovery: Expert Reports and Depositions

Decades ago, trial proceedings were exercises in ambush and a lawyer might have no clue what an expert witness would say. Today, the procedural rules governing the conduct of trials permit parties to obtain extensive discovery[4] of an expert's opinions and qualifications before trial. What that means is most of the courtroom theatrics familiar from movies and TV shows aren't permitted in real courtrooms. Discovery and procedures exist to suppress "gotchas" in the evidence. Surprises still occur, but less often than you'd think. The twin pillars of pretrial discovery expert witnesses face are reporting and deposition.

[3] A direct examination refers to the questioning of a witness by the lawyer who called the witness to testify. A key distinction between direct examination and cross examination (questioning by the other side) is that on direct examination, a lawyer is generally prohibited from asking leading questions that contain or suggest an answer, but leading questions may (and should) be used routinely to control a witness during cross examination. Because an opponent may elect not to cross-examine a witness, it's essential to get everything needing to be elicited from the witness into the record during the direct examination.

[4] "Discovery" is the pretrial phase of litigation where the parties learn more about the witnesses and evidence relevant to the dispute. In civil cases, the parties may seek and compel the turnover of relevant and non-privileged information held by their opponents.

Expert Reports

Typically, and well before trial, expert witnesses are obliged to prepare reports detailing the witnesses' work, the evidence examined and all opinions relating to the subject matter about which the witnesses will testify. The failure to report material opinions and the principal bases therefor may serve as grounds to exclude the witness' testimony.

In United States courts,[5] the Federal procedural rules require that a testifying expert prepare and sign a written report containing:
(i) a complete statement of all opinions the witness will express and the basis and reasons for them;
(ii) the facts or data considered by the witness in forming them;
(iii) any exhibits that will be used to summarize or support them;
(iv) the witness's qualifications, including a list of all publications authored in the previous 10 years;
(v) a list of all other cases in which, during the previous 4 years, the witness testified as an expert at trial or by deposition; and
(vi) a statement of the compensation to be paid for the study and testimony in the case.
Federal Rules of Civil Procedure Rule 26(a)(2)(B)

If an expert expresses an opinion not included in the expert's report, the Court may exclude the testimony and instruct the jury to ignore it or more likely will decide whether the unreported opinion is material to the dispute and if the opinion offered served to unfairly surprise the other side. If it's immaterial or not a surprise, the Court may allow it.

The Federal Rules of Civil Procedure protect draft reports prepared by expert witnesses from disclosure and shield communications between counsel and an expert witness from disclosure "except to the extent that the communications: *relate to compensation for the expert's study or testimony, identify facts or data that the party's attorney provided and that the expert considered in forming the opinions to be expressed or identify assumptions that the party's attorney provided and that the expert relied on in forming the opinions to be expressed*. ***Federal Rules of Civil Procedure Rule 26(b)(4)(C).***

The Federal Rules of Civil Procedure also require that expert witnesses supplement reports and testimony in a timely fashion if there are additions or changes or if the witness learns that the testimony or report is incomplete or incorrect in material respects. ***Federal Rules of Civil Procedure Rule 26(e)(2).*** As a rule of thumb, if it's not in your report, you can't talk about it on the stand (if the other side objects) or unless the other side broaches it on cross-examination (which may serve to "open the door" in legal parlance).

By the way, an expert report isn't generated by your tools, no matter what the software companies say. You, the expert, must prepare the report, crafting it to be understood by human beings lacking your

[5] In this paper, I'll refer to the Federal rules of procedure and evidence governing proceedings in federal courts, but keep in mind that most cases aren't filed in federal courts and each state has its own rules of procedure and evidence. Most state rules are similar or identical to their federal counterparts but be sure to check with counsel you're working with to understand the rules that apply.

technical acumen, and you must stand ready to prove anything you say is fact or a reasonable, rational inference grounded on fact.

While being cautious not to embrace "magic words," it's helpful to reference "industry standards," "accepted practices" and "reliable principles and methods." Be prepared to defend those characterizations. Lawyers and judges esteem citations to authoritative references but you should anticipate that when you cite a published authority, you may be confronted by other assertions in that publication.

I tend to include a one paragraph "Executive Summary" at the start of reports setting out key takeaways, on the theory that my subsequent discussion of LNK files and Registry entries will be easier to follow if the reader knows where I'm going. In terms of the level of detail, a good report serves as a sufficient road map of the examiner's work such that another competent examiner would be able to replicate the observations if afforded access to the same evidence. You should assume that your report will be critically assessed by an examiner seeking to fault your methodology and conclusions. So, proofread! You may groan, "OK, Boomer," but when I see misspellings or excruciating grammar, I wonder what else the "expert" botched. Many judges and counsel do, too.

There is nothing unethical about counsel suggesting language to include or omit in your report. Lawyers know the elements of proof required in their cases and addressing issues within your ambit is fine. *But never forget that it's your reputation at stake*. It's you who will be under oath. If you can't confidently stand behind the assertion or if an omission makes the report misleading or materially incomplete, reject the change! Be aware that drafts of reports and any back-and-forth with counsel are typically discoverable in state courts but largely shielded from discovery in federal forums. It's prudent to assume there's nothing "off the record" with the lawyers.

Depositions

In addition to a report, it's common for opposing parties to exercise their right to question an expert witness under oath in a pretrial proceeding called a "deposition." In connection with the deposition, a witness may receive a demand for production of information called a "*subpoena duces tecum*." These typically seek production of the witness' notes, records, evidence, and other work product relating to the matter. Let counsel know if you are served with a *subpoena duces tecum* (or any subpoena) and be sure to inquire if counsel received one in connection with your deposition. You don't want to get beat up in deposition because you failed to comply with a subpoena you knew nothing about.

The customary objectives of a deposition are to limit the scope of your findings and gather fodder to use to impeach you in court. If, at trial, you depart from what you said in deposition, opposing counsel uses the transcript or video of your deposition testimony to undermine your credibility. So, deposition testimony is not a "dry run;" prepare as you would for courtroom testimony. The other side is sizing you up to see if you can communicate in plain English and come across as qualified and credible.

The same rules apply to testimony in deposition as in the courtroom: listen to the question, answer the question posed and do not volunteer information. Don't guess or speculate. Answer "yes" or "no" where you can and explain if you must. Stop talking immediately when counsel object and listen to objections made by counsel presenting you should counsel be trying to steer you out of trouble.

Tips for Cross-Examination

Evidence professor John Henry Wigmore famously called cross-examination "the greatest legal engine ever invented for the discovery of truth." Apparently, every lawyer who writes about cross-examination is obliged to say that. Likewise, every trial lawyer aspires to do a great cross examination, and every judge and juror aspires to hear one. Yet, as I observed at the start, they are rare.

Forty years ago, my boss was on the trial team of a lawsuit between Pennzoil and Texaco that resulted in the biggest plaintiff's verdict of the era and a three-billion-dollar settlement---back when that was a lot of money. The lawyer for Texaco, the big loser, was named Dick Miller, and my boss used to say of him, "Dick Miller has two speeds: OFF and KILL." I'll never forget that because it describes how some lawyers approach cross-examination. But a truly devastating cross examination flows from applying lessons learned from the raptors in Jurassic Park: *get the prey to look one way, while the attack comes from another.*

In court, that entails laying a trap and not springing it too early. Skilled cross examiners box witnesses in and seal off points of retreat before the witness recognizes the need to run. The very best cross examiners don't spring their traps during the cross; they save that for final argument.

The greatest teacher of cross-examination I've ever come across was a former prosecutor, judge and law professor named Irving Younger, who died about 35 years ago. Younger's famous lecture on the topic was called "The Ten Commandments of Cross-Examination." I've listened to multiple versions of his talk over the years and all are magnificent. Stirring. Funny. Unforgettable. Younger opined that a lawyer must try about 25 cases to begin to be skilled in cross-examination, but he GUARANTEED that any lawyer strictly adhering to his Ten Commandments would be able to conduct a reasonably effective cross-examination. Of course, he added, no lawyer is capable of sticking to all his commandments *until* the lawyer has about 25 trials under his belt!

I do not have ten surefire commandments that will guarantee you won't get in trouble on cross-examination, but I have a lifetime in court (much of one anyway) and many years teaching law to draw on in offering advice on what to expect on cross plus a few suggested techniques that I GUARANTEE will help you become a better witness.

Hypothetical Questions and Hearsay

In U.S. jurisprudence, there are two principal advantages afforded an expert witness. First, an expert witness is permitted to answer hypothetical questions; that is, questions where the interrogator lays out various assumptions and seeks the witness' opinions based on those assumptions. Second, an

expert witness is permitted to rely upon hearsay evidence when it's the sort of information on which experts in the field customarily rely.

Some cross-examiners take their hypotheticals too far and require you to assume unreasonable facts. In that event, push back. Point out that you can't express an opinion based on so implausible an assumption. Don't be reluctant to say, "I saw no evidence to support that assumption." Be wary of being bullied into offering opinions on hypotheticals incorporating elements outside your expertise and experience.

Just because you *can* rely upon hearsay doesn't mean that you *should*. Unassailable opinions are constructed from reliable evidence. Try not to build your testimony on assumptions that may buckle. Always ask yourself, "*Why do I take this to be true?*"

Compound Questions

A cross-examiner may pose two questions as one, such that an answer to one sounds like an answer to both. When this happens, the lawyer who handled direct examination should object to the compound question; but, if the lawyer doesn't object, it's up to you to be alert and keep the record clear. Seek clarification of the question (*e.g.,* "*Are you asking me whether I hashed the image or if the hash values matched?*") or address each part separately (e.g., "*Yes, I hashed the image, but the hash values did not match due to damaged sectors on the drive.*").

May I explain?

Effective cross-examiners use classic techniques to control witnesses. They pose leading questions that suggest the desired reply. They avoid repetition of damaging testimony. They ask only questions to which they already know the answer. And they seek to confine witnesses to "yes" or "no" responses to keep witnesses from explaining their answers. Skilled cross-examiners do this so well, you will be like a horse in harness. But skilled cross-examiners are rare. You are more likely to face cross-examiners who will try to insist on "yes" or "no" responses to questions that can't be answered that way.

You have a secret weapon when that happens. You can ask, "*May I explain please*?" Opposing counsel hates that. They want to scream, "*No, just say 'yes' or 'no!'*" But they recognize that if you've been candid and cooperative, refusing to let you explain will make them look bad to the judge and jury. Like any secret weapon, it's not very effective once the secret's out. So, you can only do this sparingly.

Don't Be Jekyll and Hyde

We communicate as much non-verbally as verbally, and it's fascinating to watch how a witness' body language and demeanor transform from direct to cross-examination. On direct, witnesses are forthcoming and helpful–their engagement and desire to please manifested in their words and appearance. On cross, they lean back, glowering, arms crossed, shifting in their seats, quarrelsome and evasive. Dr. Jekyll and Mr. Hyde.

It's hard *not* to appear defensive when you're on the defensive, but *stay attuned to your demeanor and body language,* and don't change demeanor between examiners—at least not without a lot of provocation.

Open up your posture, unclench your fists and wipe that peevish look off your face. Try not to change the pace or tone of your answers. Patience is a virtue, so don't start jabbering just to fill an awkward silence. Be courteous. Of course, it's not your role to assist the other side; but being respectful and working cooperatively to move things along helps your side most. Some lawyers will work hard to get a rise out of you. Don't be drawn in. When you show anger, you squander credibility.

There may be times when anger or umbrage is unavoidable, but be slow to burn. Ideally, the jury or the judge should be awed by your restraint and rooting for you to push back long before you do.

Stay above the Fray

Nailing the bad guy isn't the point—not for you. You are the digital translator, not the prosecutor. The evidence speaks through you, and justice demands you not omit or embellish. As an expert witness, *you are not an advocate for either side*. That's the lawyers' role. *You are an advocate for your own findings and opinions*. You can and should vigorously support and defend the skill and integrity of your forensic process and of your reporting and the expert opinions you've drawn. Winning the case is not your objective. The only "win" for you is that the judge and jury listened to you, understood you and believed you.

Remember Who Matters

Court proceedings aren't about the lawyers. The lawyer for your side is *already* persuaded, and the other side's lawyer isn't going to come around. They don't matter.

Court proceedings aren't about you. Yes, you're a technical wizard and you've worked hard to uncover compelling evidence. But *you* don't matter—check your ego at the door.

The only people in the courtroom who matter are the judge and jury. So, speak to *them*, look at *them* and help *them* understand. Of course, you'll pay attention to the questioner while a question is asked; but orient yourself so that the jury can always see and hear you well, and endeavor to make eye contact with the jurors when giving longer answers. Be alert to cues from counsel, like questions that begin, "Please tell the jury…." That's how lawyers remind you that you're ignoring the most important people in the courtroom.

Couch your testimony in terms and analogies that judges and jurors understand. Never assume they know what the lawyers know about the evidence or that they come to court with any pre-existing technical expertise. Engage the judge and jury with references to common experiences and accessible analogies like, "We've all seen the hard drive activity light on our computer flash when we aren't doing

anything. That may be an instance where the computer is shifting information from RAM to its memory swap file on the hard drive, like leaving yourself a note."

Don't Quibble

Judges and juries hate witnesses who seem incapable of saying "yes" or "no." A skilled cross examiner frames questions that *sound* like they can be answered simply but are calculated to elicit quibbling from the witness. A skilled witness looks for opportunities to plainly respond "yes" or "no," or something close like:

"Yes, as a rule,"
"No, for the most part."
"There are exceptions, but that's true."
"Not in my experience."

Unless crucial to the case, let the lawyer chase the exceptions.

Avoid Absolutes

Lawyers like absolute responses like *"never," "impossible"* and *"always"* because they're easy targets for attacking a witness' credibility—even when those attacks are silly.

I was once asked to demonstrate cross-examination at a computer forensics conference. The witness was an expert of renown and an unquestionably capable examiner. He brought his laptop running the forensic software he'd written (like I said, a *serious* expert). I sparred with the witness long enough to make him defensive (and a bit cocky), then gave him a thumb drive holding two short text files. I asked him to calculate an MD5 hash for each. He glanced at the contents, saw that each contained my name and address, and quickly calculated identical MD5 hashes for the two. I asked him if, despite their different file names, the contents of the two files were identical. He said they were. I asked him if he was *sure* and tried to toss a little shade on his methodology to get him puffed up. The expert testified that he was *certain* the files were identical because they had matching hash values. I then had him explain how hashing was a technology central to his evidence authentication, deduplication, chain of custody, etc. I concluded by asking if he was as certain about the two files being identical as he was about the other opinions he'd expressed. He said he was, adding that it was *impossible* for the two to be different if they have matching hash values.

The hook was set.

I then asked the expert to pull the contents of the "identical" files into a hex editor, and I gave him the offset addresses of six places in the file where there were differences between them. He was floored to find the differences were real. I then wrote the names of the files on the board: *5h1t* and *5h1n0la*, and

I ended my cross-examination noting that he apparently wasn't expert enough to tell one from the other.[6]

All I'd done to set him up was append my name and address to tiny files engineered to demonstrate the feasibility of MD5 hash collisions, then brand new. The testifying expert forgot the difference between a collision being computationally infeasible and impossible. MD5 hash collisions are real, but *exceedingly* rare. Never having seen a hash collision and knowing the gargantuan odds against ever seeing one, the expert was maneuvered by hubris into making a categorical statement he couldn't defend and allowing his credibility to be tied to one point.

Expect the Unexpected

As a trial lawyer, my credo was that even adverse witnesses could do my case some good. I began each cross-examination by getting adverse experts to confirm the strengths of my case, sometimes to the point of their conceding things beyond their expertise. Medical doctors would corroborate liability facts, and engineering experts would concede my client was permanently disabled. I could do this because opposing counsel were loath to challenge their own witnesses' expertise, and the witnesses weren't prepped to expect the unexpected.

Even without pushing witnesses outside their expertise, I knew every opposing expert could concede *something* helpful to my case, even if just confirming the qualifications of my own expert or basic precepts of digital forensics. If they fought me on everything, it underscored their bias and hurt their credibility.

The lesson: The witnesses making concessions beyond their ken were too sure of themselves to say, "I don't know," and the combative witnesses were too invested in the outcome to concede the obvious.

Know What's Out-of-Bounds

In most jury trials, the court determines that there are matters that may not be disclosed to the jury. These may be a creature of statute, of custom, agreement or the consequence of a motion to exclude called a Motion *in Limine*.[7] You need to know what's out-of-bounds, and sometimes, counsel will forget to tell you. *Always ask about excluded matters before you take the stand!* Remember that the fact that certain evidence has been excluded is itself something you can't mention on the stand.

Occasionally, counsel for the party who sought to exclude the evidence will ask a question that necessitates mention of the excluded matter. This is called "opening the door;" but, don't be too quick to cross the threshold. Let the court and the attorneys see that you are hesitant to respond to allow the lawyers an opportunity to object and seek guidance from the Court. *You must carefully weigh the Court's intention to exclude the evidence against the obligation to answer a question that necessitates*

[6] In case it doesn't leap from the leetspeak, my point was that he couldn't tell "shit from Shinola," and, yes, I was being an ass.

[7] Examples include whether a party is insured in a liability case or trade secrets and other information subject to a protective order.

disclosure. Misjudgment can prompt a mistrial, so do all you reasonably can to afford the Court and counsel an opportunity to recognize and resolve the dilemma before disclosing excluded matter.

Dealing with Attacks Based on Compensation and Affiliation

A cross-examiner may point to an expert's compensation or affiliation to suggest bias, using questions like:

[to an independent expert]
"You're being paid to testify, aren't you?"
or
[to a government witness]
"It's true that you only testify in support of the prosecution?"

Many examiners would simply answer, "Yes," but better responses might be:

"No, I'm compensated for my professional time, not for my testimony."
or
"No, my opinions often support decisions not to prosecute and to dismiss charges. In those cases, there is no need for me to testify."

You are a well-trained and -experienced professional who has devoted many hours or days to collecting, authenticating, processing, and analyzing the digital evidence, as well as writing reports, briefing counsel and giving testimony. The jury understands that you are paid to do your job just as they are paid to do theirs; so, there is no need to be squeamish about it. The bits and bytes on the electronic media don't change based on who pays you or how much they pay.

Scientific Evidence

The legal standard most courts use to determine if a witness may testify as an expert and offer opinions is admirably flexible and practical. Rule 702 of the Federal Rules of Evidence states:
"A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
(a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
(b) the testimony is based on sufficient facts or data;
(c) the testimony is the product of reliable principles and methods; and
(d) the expert has reliably applied the principles and methods to the facts of the case." [8]

Just because a witness meets the low bar to qualify as an expert doesn't give a witness *carte blanche* to offer any opinion, no matter how controversial or speculative it might be. The judge serves as a

[8] Once again, every state has its own rules of evidence and procedure which govern proceedings in state court, though most of these are similar or identical to the Federal rules.

gatekeeper charged to limit testimony based on so-called "junk" science, a catchall term describing opinions based more on achieving a certain result in court than in conforming to the reasonable measures of scientific integrity. The leading case is the thirty-year-old United States Supreme Court opinion, *Daubert v. Merrell Dow Pharmaceuticals Inc.,* 509 U.S. 579, 595 (1993). The pre-trial process employed to seek exclusion of flaky expert opinions is termed a "Daubert challenge."

In brief, the *Daubert* standard inquires into:
(1) **Testing:** Has the scientific procedure been independently tested?
(2) **Peer Review:** Has the scientific procedure been published and subjected to peer review?
(3) **Error rate:** Is there a known error rate, or potential to know the error rate, associated with the use of the scientific procedure?
(4) **Standards:** Are there standards and protocols for the execution of the methodology of the scientific procedure?
(5) **Acceptance:** Is the scientific procedure generally accepted by the relevant scientific community?

Perhaps because the *Daubert* case concerned issues of medical causation (did this drug cause that injury?) the *Daubert* standard is couched in terms with little apparent connection to digital forensics. *What's the error rate of a hash calculation?* Who knows?!? The potential for a spontaneous MD5 hash collision is estimated to be one-in-340 undecillion. Do you trust it more now?

Much of what we report on in digital forensics are observations of objective, verifiable data (this region of media contained this information). It's not opinion; it's observation--the application of tools that enable the identification and interpretation of the content. The techniques employed—*e.g*., imaging and verification, file carving, hash matching, linear or indexed search, even just the binary-hex-ASCII encodings employed—are well-documented and -supported by the professional literature as trusted, verifiable, and standard. Your education, training, and experience, bolstered by that of others in our discipline bear that out. The tools serve to replicate and expedite processes that examiners could do (and once did) painstakingly and manually.[9] We *cross-validate* key findings to guard against error, but *there are no established error rates* for much of what we do because, when it comes to the key evidence found on the media, there should be no room for error concerning content and location.

Where we must be prepared to show accuracy and acceptance is in the *interpretation* of the data and how the data observed serves as a reliable analog to human behavior. This is where we turn to authoritative references and our training, experience, and testing. It boils down to "*why should we trust what you say?"* It demands extensive familiarity with the processes attendant to the systems we analyze and the tools we employ. We must be able to explain not just *what* our tools tell us but *why*.

[9] One advantage of coming to forensics during the Dark Ages is you learn analysis at the sector and file table levels armed with only a hex editor. That atomic, granular perspective spawns a reluctance to let tools do the all the work.

Hoist by your own Petard

A very effective way to undermine an expert's testimony is to prevent the expert from testifying at all. That's accomplished by challenging the expert's qualifications, and examiners make that easy when they claim sham credentials. Lawyers closely scrutinize experts' curricula vitae (CVs) looking for bogus degrees, specious or outdated certifications, lack of required licensure, training courses claimed but not attended and all manner of exaggerated achievement.

The risk is real. As early as 2014, a "computer forensic examiner" testifying for the defense in New Hampshire narrowly avoided jail time for falsely representing that she held CCE and CHFI digital forensics certifications. And in a high-profile Chicago federal court case a few years ago, an electronic evidence expert was savaged on cross-examination when it turned out his law license had been suspended and he didn't know it. The lesson is simple: *If it isn't accurate in letter and spirit, it doesn't belong in your CV.* You will get caught.

More important than not exaggerating your qualifications is acquiring suitable professional credentials and staying current with your training in the first place. When I started in digital forensics, it was my hobby; there were no computer forensics training courses open to the public. Making the same point, legendary examiner Andy Rosen likes to testify that that he "attended the same flight school as Orville and Wilbur Wright." That won't fly anymore. Unless you wrote the software (like Andy), you should be formally trained and/or -certified in the use of your principal analysis platform.

Technology changes rapidly, so don't fail to get formal training in the discipline and tools and attend refresher courses to stay abreast of new developments. Professional examiners invest in their expertise: in training, tools, software and certification. Acquisition and analysis of data is their full-time focus.

Show *and* Tell

An effective expert witness is a good teacher, and good teachers use visuals to support instruction. We believe what we see. So never just tell when you can show and tell. I endeavor to prove points using the electronic evidence and my forensics software, but I also come armed with PowerPoint presentations allowing me to graphically depict the key evidence and the grounds for my opinions.

Juries get bored. Judges, too. Give them something to look at, and they'll reward you with their keen attention.

Get on Up!

If you have important points to make, try to make them while standing and facing the jury. If you are using a PowerPoint, ask if you can leave the witness stand to point something out. Use a flip chart, dry erase board or whatever, but *where feasible and important*, break up the monotony of a talking head and get to your feet. Not every court will allow it—and you will need to articulate cause to leave the

stand—but most courts won't hesitate to let you rise to illustrate a point. It's not a stunt. It's a chance to refocus everyone on crucial evidence.

Appearance

Every trial lawyer has a view as to what an expert witness should wear to court. Some take it to the point of asking witnesses to wear bow ties and glasses to look nerdier. My preferred "uniform" is a suit and tie. But if your suit's too tight or you just can't breathe wearing a necktie, wear what you'd put on for a job interview or a funeral. Always wear socks or hose, closed-toe dress shoes and (for men) long sleeves. For both men and women, be sure what you wear is clean, pressed, comfortable and *unremarkable.* Courtrooms are no place for fashion statements, so don't don a black turtleneck just because you're testifying about an iPhone.

What to Bring to Court

When I come to court to testify, I typically want access to all the data I've examined. That means all of the evidence data in compressed formats housed on a portable storage device, with my principal forensic tools running on a powerful laptop. When data volumes make that infeasible, I have to select sources; but I still strive to have real time access to as much evidence as possible. Then, I try to anticipate what essentials I'll need if nothing works. Then, file and metadata inventories, screen shots, Registry output, reports, etc.—get dropped into a PowerPoint and printed to paper.

Before I head to court, I confirm that I can bring my electronics into the courtroom and that I will have access to power and, as needed, video projection. I bring all necessary cables and adapters, and then add a spare for everything. Overkill? Sure, but I don't want to be the technologist who couldn't get his PowerPoint to run.

If paper records will be offered into evidence, be sure to bring copies for the lawyers and the judge. Remember that evidence that comes as a surprise is evidence that may be excluded, so be sure the attorney presenting your testimony knows what you plan to present and has met all disclosure requirements for that material. Don't be shocked if the other side is permitted to inspect your file. Plan for it.

The Most Important Thing to Bring

The most important thing to bring to court as a computer forensic examiner is your dedication to and enthusiasm for our craft. Digital evidence touches us all. Digital forensics is *fascinating*. You are the court's guide through a complex, alien world of metadata, shadow volumes, Registry hives and unallocated clusters. Share your joy at explaining how it works. Be passionate about the evidence and the integrity of your processes so the judge and jury will want to learn from you while you use accessible language and simple analogies to help them understand.