Becoming a Better Witness on Digital Forensics

Craig Ball

"Your Witness"
© Charles Bragg

I love to testify—in court, at deposition, in declarations and affidavits—and I even like writing reports about my findings in forensic exams.

I love the challenge—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 is a compelling human drama being played out in those bits and bytes, and computer forensic examiners are the fortunate few who get to tell the story. It's our privilege to help the finders of fact understand the digital evidence.[1]

This article outlines ways to become a more effective witness and common pitfalls you can avoid.

It's difficult for computer forensic examiners to hone their testimonial skills because it's rare to be interrogated by a lawyer who 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 off their path, they're lost. Computer forensic examiners have it pretty easy on the stand. Computer-

[1] Certainly, some 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.

generated evidence still enjoys an aura of accuracy and objectivity, and the hyper-technical nature of digital forensics awes and intimidates the uninitiated. But, it won't always be this way. 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 great witnesses.

The Trick to Being a Great Witness

Novice witnesses think there's a system they can follow to stay out of trouble on cross-examination, but no battle plan survives an encounter with the enemy. There are no "tricks" to testifying, except to prepare 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 on technical matters.

It's All About Preparation

Even brilliant, articulate and honest expert witnesses will perform poorly on the stand when they aren't asked the right questions in the right way. Lawyers invest too little time working with expert witnesses to present a compelling direct examination, and expert witnesses worry too much about cross-examination. 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 enough 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.

The expert witness must help the lawyer understand what the digital evidence signifies and insure that the lawyer won't stumble on the key terms and concepts. The lawyer must help the expert understand where the digital evidence fits into the overall theme of 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 according to plan (such as when the court excludes an exhibit or demonstrative aid). There is no such thing as over-prepared when it comes to direct examination.

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, 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 pushed 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 a cross-examiners who will try to bully you into "yes" or "no" responses to questions that can't be answered that way.

You have a secret weapon when this happens. You can ask, "May I explain please?" Opposing counsel hate 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 once (or twice). Don't waste it.

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 physiognomy. On cross, they lean back, glowering, arms crossed, shifting in their seats, quarrelsome and evasive. Jekyll and 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 whole lot of provocation.

Open up your posture, unclench your fists and wipe that peevish look off your face. Endeavor not to alter the pace or tone of your answers. Patience is a virtue, so don't start jabbering just to fill an awkward silence. Be courteous and helpful. Yes, *helpful*. 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 behind and integrity of your forensic process, 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 very 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 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 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:

"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 the Absolute

Lawyers like absolute responses like *"never," "impossible"* and *"always"* because they're easy targets for attacking a witness' credibility—even when those attacks are pretty 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 simple 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 certain and tried to toss a little mud 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.[2]

[2] 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 a jerk.

All I'd done to set him up was append my name and address to tiny files engineered by Chinese researchers to demonstrate the feasibility of a MD5 hash collision. 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 stress 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 expert could concede *something* about my case—"Y*ou would agree that my client's computer was powered by electricity, correct?"* If they fought me on everything, it underscored their bias and hurt their credibility.

The lesson: The witnesses making concessions 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 or the consequence of a motion to exclude called a Motion in Limine. 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 may itself be 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 enter. Let the court and the attorneys see that you are hesitant to respond so as to allow the lawyers an opportunity to seek guidance from the Court. You must carefully balance the Court's intention to exclude the evidence against the obligation to answer a question that necessitates disclosure. Misjudgment can prompt a mistrial. Accordingly, do all you reasonably can to afford the Court and counsel an opportunity to resolve this 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 or to dismiss charges. In those cases, there is no need for me to testify."

You are a highly-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 prosecutors 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.

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 bogus credentials. Lawyers closely scrutinize experts' curricula vitae (CVs) looking for phony degrees, unearned or outdated certifications, lack of required licensure, training courses claimed but not attended and all manner of exaggerated accomplishments.

The risk is real. In January, 2014, a "computer forensic examiner" testifying for the defense in the U.S. state of 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, an electronic evidence expert was savaged on cross-examination when it turned out his law license had been suspended and he didn't even 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.

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 to your Feet

If you have important points to make, try to make them standing up 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 up 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 dress like Steve Jobs just because you're testifying about an iPad.

What Comes to Court

Where I come to court to testify, I want access to all the data I've examined. That typically means all of the evidence data in compressed formats housed on a portable NAS, with my principal forensic tools running on a powerful laptop. When data volumes grow beyond several terabytes, 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 bare essentials I'd need if nothing worked, and these items—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 that technologist who couldn't get his PowerPoint to work.

If paper records may be offered as evidence, be sure to bring copies for the lawyers and the judge. Recognize that evidence that comes as a surprise is evidence that may be excluded, so avoid surprises. Be sure the attorney presenting you 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 deep dedication to and infectious enthusiasm for your 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. Be passionate about the evidence and the integrity of your process so the judge and jury want to follow you, and use accessible language and simple analogies to help them keep up.

Craig Ball, of Austin, Texas, is a court-appointed special master, Board-certified 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.