The College of Labor and Employment Lawyers

LEADERSHIP FOR GREATER PURPOSE

ELEVENTH CIRCUIT THIRD ANNUAL CONFERENCE
CORAL GABLES, FLORIDA
FEBRUARY 1, 2014

AGENDA

9:00am	Welcome	Fred Ingram, Burr Forman
9:05am - 10:35am	**Aspiring to Civility Without Idealizing the Past: Civility and Professionalism in the Courtroom**	Tom Brooks, Moderator Meyer, Brooks, Demma & Blohm, P.A. Chief Judge Karon Bowdre, Panelist, USDC, Northern District of Alabama Judge José E. Martinez, Panelist, USDC, Southern District of Florida Judge Steve C. Jones, Panelist, USDC, Northern District of Georgia
10:35am – 10:45am	*Break*	
10:45am – 12:15pm	**Practicing in the Digital Age: From Social Media to E-Discovery**	Adam Sharp, President, E-Hounds, Inc.
12:15pm – 1:00pm	*Lunch*	

1997 Annapolis Exchange Parkway ■ Suite 300 ■ Annapolis MD ■ 21401 ■ Office 410 972 4711 ■ Fax 410 972 4701

On Encouraging Civility

William S. Duffey, Jr.

I remember that afternoon too well. I was the lead partner in a particularly difficult case – a commercial dispute between parties competing hard in a tough industry. The stakes were high and the clients demanded successful results. It was important to them. The lawyers on the other side were aggressive and, in my view, unreasonable. The litigation environment was unpleasant and nerves were frayed as we entered the last weeks of discovery.

The issue that afternoon was the scheduling and scope of a Rule 30(b)(6) deposition. The scheduling discussions were not going well. A younger lawyer from the opposing firm was charged with resolving this issue for his client, and he had to deal with me. He was at most a mid-level associate, and he had not been especially active in the litigation. Our client was being hard-nosed on this scheduling, and I had not enjoyed dealing with him on it. He insisted we resist what opposing counsel wanted at all costs. I was frustrated and my nerves were shot when my young adversary called to try to put this scheduling issue to rest. I resisted everything he suggested, probably for the sake of resisting. I remember being uncooperative and unpleasant. Then he said something that just struck me the wrong way. I do not recall that the comment was rude or angry, just that it did

not sit well. I let loose with what I am sure was received as an intemperate lecture to a young lawyer who was simply trying to do his best to deal with a difficult issue. While I hate to admit it now, I cut the conversation short and left the issue open.

As I got some distance from the conversation, I found myself wondering why it was so upsetting to me. In a moment of honest reflection, I realized how disappointed I was in myself. The more I replayed the conversation over in my mind, the more I recognized that I was not upset about failing to seek resolution to the issue but about how I had behaved. The more I considered the conversation, the more I regretted how I had treated a younger colleague who simply was given the assignment to do his best to resolve an issue.

I would like to say I acted immediately, but it took longer than it should have to make the call. I remember how tentative my young opponent was when he answered the phone, probably fearing he was in for more of the same from me. While I cannot remember our whole conversation, I remember two things very clearly. First, I told him plainly and unequivocally that I was sorry for how I had acted, and that I did not have any excuse for how I had treated him in our conversation. I told him that I knew I was impeding our ability to get beyond an issue we both needed to settle. I also told him that one of the things I had regretted

about our profession was the increasing acrimony that was evident among lawyers in litigation. And then I told him that I hoped he would remember my role in the conversation as a reminder of how not to act.

There is one other time I wish I had kept my tongue in check. I was involved in a matter after I became responsible for the United States Attorney's Office in Atlanta. We were prosecuting a case against a law enforcement agency employee who had disclosed confidential information which put other law enforcement officers and their investigative strategies at risk. The employee's actions were egregious, and he had been indicted for it. We were discussing with his lawyer the terms on which he might enter a plea. We were near the end of the negotiations, and the focus was on the term of imprisonment the defendant should face. His lawyer and I disagreed about what was appropriate. When I stated my view of a reasonable plea, the defense lawyer responded with a sarcastic, inappropriate attack on our office, our integrity, and me personally. I responded with several terse, biting remarks, and the meeting ended abruptly.

Within minutes after the meeting concluded, I thought about what had occurred. I, and the other lawyers from my office who were with me, all agreed that my response was justified, that we had been provoked, and that the defense lawyer was way out of line. While I concurred in their assessment, I knew it was

my job to create an environment where were could explore whether his client might plead to his offense. I knew I had to call the defense lawyer and schedule another meeting. We reconvened a few days later. I began by apologizing for my reaction during our prior meeting and we both acknowledged that we needed to get past our last conversation to determine if we could agree on a reasonable plea agreement to conclude the matter. Within a very short time, an agreement was struck.

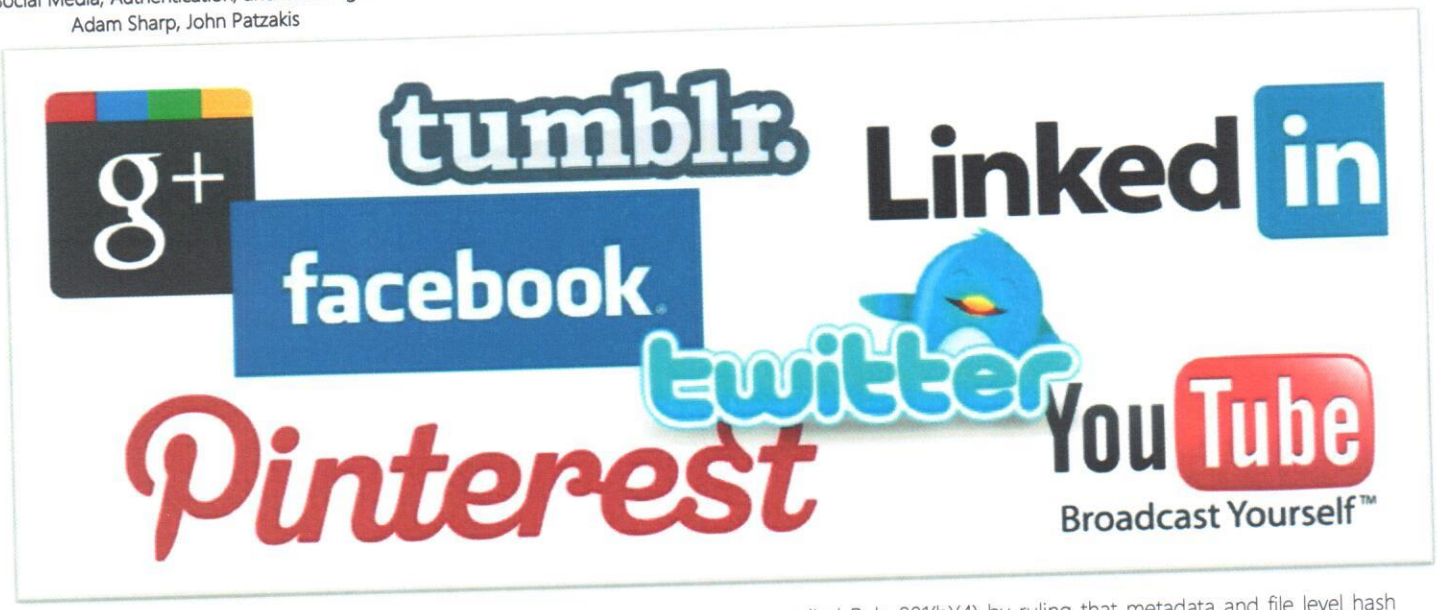
These are two very different examples. Thinking back on these two incidents, I know that my decision to reconcile these relationships was professionally, and personally, important. In the first, the conduct I modeled for my younger colleague was wrong. At that stage in my career, it was my responsibility to exhibit professionalism – grace under fire. If I could do that, I could at least model my willingness to make amends. In the second incident, I realized that in life there will be times when we are justified to act as we do. The question is whether our actions, while justified, are right. In my encounter with this defense counsel, I decided my public function required me to consider the interests of justice and the defendant's desire to accept responsibility for the crime that he had committed. It was irresponsible for me to allow his lawyer to interfere with my duty to serve justice, even if circumstances "justified" my response. My

ultimate decision in these two instances was to model professionalism to a young lawyer and to serve our justice system in a responsible way. These values prompted me to make two very difficult telephone calls. The calls simply were the right response to my errors in judgment.

The work we do is hard. The pressure is often intense, and the demands unreasonable. None of these excuse impulsive, intemperate conduct. Ours is a profession of service to others and to clients. We are charged with addressing and resolving tough issues that often have important and substantial consequences. The incivility and hostility of litigation today not only makes this work more unpleasant, less satisfying, and less fulfilling, but it also serves as a barrier to what we are charged to do–to represent clients in the resolution of disputes by seeking just results. My conduct was a barrier, in both of these examples, to the service to our profession and the public. There will be times in one's professional life when an apology is in order because of the way we have treated someone in a case. Making the call to express your regret is hard. You have to swallow your pride and risk the vulnerability of admitting you were wrong. But it will be a necessary step to restore professional and personal relationships with another lawyer so progress in a case can be made and a resolution achieved. That is our duty: to seek justice and to treat others with dignity.

Social Media, Authentication, and Challenges

Adam Sharp, John Patzakis



Summary, by Adam Sharp:

Social Media, and the ubiquitous access to it in every aspect of daily life, is becoming highly relevant to legal disputes. The challenges today and in the years to come will focus on not only authentication, but on the best practices for collection, preservation and proper search. This paper is authored in conjunction with John Patzakis, President-CEO of X1 Discovery, and industry leading firm currently providing the most comprehensive tools for proper collection of the major social media sites, as well as web capture.

With over 800 million Facebook users and 300 million people with Twitter accounts, evidence from social media sites can be relevant to just about every litigation dispute and investigation matter. Social media evidence is widely discoverable and generally not subject to privacy constraints when established to be relevant to a case, particularly when that data is held by a party to litigation or even a key witness. However recent court decisions reflect that the main pressing concern for attorneys, eDiscovery practitioners and investigators is the authentication of social media data for admission into evidence in court.

Under US Federal Rule of Evidence 901(a), a proponent of evidence at trial must offer "evidence sufficient to support a finding that the matter in question is what its proponent claims." Unless uncontroverted and cooperative witness testimony is available, the proponent must rely on other means to establish a proper foundation. A party can authenticate electronically stored information ("ESI") per Rule 901(b)(4) with circumstantial evidence that reflects the "contents, substance, internal patterns, or other distinctive characteristics" of the evidence. Many courts have applied Rule 901(b)(4) by ruling that metadata and file level hash values associated with ESI can be sufficient circumstantial evidence to establish its authenticity.[2]

Given the transient and cloud-based nature of social media data, it generally cannot be collected and preserved by traditional computer forensics tools and processes. Full disk images of computers in the cloud is effectively impossible and the industry has lacked tools designed to collect social media items in a scalable manner while supporting litigation requirements such as the capture and preservation of all key metadata, read only access, and the generation of hash values and chain of custody. In fact, the proper and timely preservation of social media evidence is a major concern, with courts finding spoliation[3] or disallowing mere printouts of social media data as inadequate to establish a proper foundation.

In of State of Connecticut vs. Eleck,[4] the court rejected Facebook evidence in the form of a simple printout, for failure of adequate authentication. The court noted that it was incumbent on the party to seeking to admit the social media data to offer detailed "circumstantial evidence that tends to authenticate" the unique medium of social media evidence. Conversely, in State vs. Tienda,[5] the prosecution successfully admitted key MySpace evidence over the defendant's objection, laying a foundation through various circumstantial evidence. Among this key circumstantial evidence were relevant metadata fields, other evidence from defendant Tieda's MySpace page, including his username, which was consistent with Tienda's commonly known nick name, his email addresses registered to the account, user ID number, stated location (Dallas), communications with other suspects, and

numerous posted photos of Tienda with associated date and timestamps. The Texas appellate court determined that "this is ample circumstantial evidence—taken as a whole with all of the individual, particular details considered in combination—to support a finding that the MySpace pages belonged to the appellant and that he created and maintained them."

The lesson from these cases illustrates that to properly address these authentication and preservation challenges, social media data must be properly collected, preserved, searched and produced in a manner consistent with best practices so that all available circumstantial evidence is collected, including metadata. When social media is collected with a proper chain of custody and all associated metadata is preserved, authenticity is much easier to establish. For instance, the following are just some of the key metadata fields for individual Facebook posts (such as a photo or status update) that together provide important information to establish authenticity of the tweet, if properly collected and preserved:

Metadata Field	Description
Uri	Unified resource identifier of the subject item
fb_item_type	Identifies item as Wallitem, Newsitem, Photo, etc.
parent_itemnum	Parent item number-sub item are tracked to parent
thread_id	Unique identifier of a message thread
recipients	All recipients of a message listed by name
recipients_id	All recipients of a message listed by user id
album_id	Unique id number of a photo or video item
post_id	Unique id number of a wall post
application	Application used to post to Facebook (i.e, from an iPhone or social media client)
user_img	URL where user profile image is located
user_id	Unique id of the poster/author of a Facebook item
account_id	Unique id of a user's account
user_name	Display name of poster/author of a Facebook item
created_time	When a post or message was created
updated_time	When a post or message was revised/updated
To	Name of user whom a wall post is directed to
to_id	Unique id of user whom a wall post is directed to
Link	URL of any included links
comments_num	Number of comments to a post
picture_url	URL where picture is located

Any one or combination of these fields can be key circumstantial data to authenticate a social media item, or constitute substantive evidence in and of itself. Twitter and LinkedIn items have their own unique but generally comparable metadata[6]. In addition to collection of all such key metadata, it is important that MD5 hash values of each social media item are automatically generated at the time of their collection, and that unique case information is generated to support a proper chain of custody. However, many ad hoc measures currently used to collect social media for use in court do not meet these requirements. Screen capture tools and many archive services fail to collect most available metadata or generate hash values for individual social media items upon collection.

The Facebook self-collection mechanism currently will not collect most available metadata information, will not generate hash values, and will only provide content from the user's own account while omitting content contributed by that user to their friend's account, such as their "walls." eDiscovery leader KMPG provided a written release noting that the Facebook download feature "was not conceived to be a forensic collection tool. The only original timestamps that it preserves are in the HTML files which can be easily modified." There currently is no self-collection or even export feature for Twitter.

The Maryland Supreme Court in Griffin v. State[7] prognosticated that to address the compelling requirement to authenticate social media evidence, methods and technologies for authenticating social media data likely will develop "as the efforts to evidentially utilize information from [social networking] sites increases."

Notes:

1 John Patzakis is an attorney who frequently lectures and is extensively published on issues related to computer forensics, electronic discovery and the authentication of electronically stored information. He is the Founder and CEO of X1 Discovery. www.x1discovery.com. Previous to X1 Discovery, he was a co-founder of Guidance Software, Inc., the developer of EnCase.

2 Lorraine v. Markel American Insurance Company, 241 F.R.D. 534 (D.Md. May 4, 2007)

3 Lester vs. Allied Concrete Company (VA, 2011) is believed to represent he largest eDiscovery sanction ever imposed on an individual attorney (see http://wp.me/p1R4t2-49 for case details). See also, Katiroll Co., Inc. v. Kati Roll & Platters, Inc., 2011 WL 3583408 (D.N.J. Aug. 3, 2011)

4 2011 WL 3278663 (Conn.App. 2011)

5 --- S.W.3d ---- (Tx.App.2012); 2012 WL 385381

6 A full listing of metadata captured from Twitter by X1 Social Discovery is available here (X1 Discovery blog): http://wp.me/p1R4t2-1W and the product user manual

7 Griffin v. State of Maryland, 2011 WL 1586683, at *94 (Md. Apr. 28, 2011)

E-Hounds, Inc.
Computer Evidence Services

February 1, 2014

Commandments of Computer Evidence

A Guide for Judges and Attorneys on Computer Evidence, and Experts.

Adam Sharp, President of E-Hounds, Inc.

1. Thou shall not stomp all over the evidence.

It is no accident that this is the First Commandment. When computer forensics specialists get together and swap war stories, one recurring theme is the number of times that clients have fouled themselves up by trampling electronic evidence. Typically, as soon as a potential legal matter is recognized, a law firm or corporation authorizes someone from its IT department to "look through" the evidence. Unbeknownst to them, while their IT staff is busy finding golden nuggets of evidence, they are also changing the dates and times of the files they are accessing and possibly altering information that indicates which user ID did what. While it may not entirely discredit the case, you have now given fodder to opposing counsel at the very least – and you will have to spend more money on the forensic examination because unraveling dates and times and explaining "the stomping" effect is now part of the examiner's job.

It is a very foolish client that contaminates evidence by having in-house folks look at it – from a judge's point of view, the client has a vested interest in that evidence. Far more credible is an initial, independent forensic examination by a certified third party.

2. Thou shall preserve the evidence.

The first rule of thumb when you suspect a workstation may contain significant evidence is to "pull the plug." No, the machine will not die by doing so. If the computer is powered up, forget the orderly shut down – this just changes dates and times again. Yank the doggone power cord. Also, savvy computer miscreants may plant a "bomb" so that shutting down without un-triggering the bomb causes the drive to be wiped. Servers are different beasts – it is very important to preserve log file entries and operational events on a server and "pulling the plug" may corrupt these files. Here, an orderly shutdown is mandatory.

Once a machine is taken out of commission, remove it and lock it up in a secure place. It is extraordinary how the machines will become the focal point of someone's attention if it is still publicly accessible. Whatever you do, don't adopt the attitude that someone else can still use the machine until you can get around to a forensic examination. Not only will usage change a world of dates and times, but deleted files which may be recoverable if the machine is decommissioned could be overwritten by continuing use.

A word about back-ups. They are invaluable. Don't continue rotating your tapes and loose evidence. Buy new tapes and take anything that may have evidence on it out of the rotation.

If the evidence you need is in the other side's possession, prioritize getting a preservation of evidence letter off to the appropriate parties. Courts are increasingly irritated with the spoliation of electronic evidence, so make sure the other side has early and clear notice of the evidence to be preserved, including back-up media!

3. Thou shall not copy and thou shall not "Ghost."

When you copy a drive, many of the dates are not preserved – not a good thing if those dates are important in court. By default, using Symantec's "Ghost" means that you will not retrieve information in unallocated space (all the wonderful deleted e-mails and documents that so often win a case reside in unallocated space). This is because "ghosting" results in a logical rather than a physical image.

If you are even remotely concerned that electronic evidence will end up in court, it is critical that a true forensic acquisition be performed. Using court-validated hardware and software such as EnCase, SafeBack, iLook and FastBloc means that your forensic image will be unchallengeable in court so long as the people that use them follow proper procedures.

4. Thou shall not covet the smoking gun.

As the country music lyrics tell us, "sometimes you're the windshield and sometimes you're the bug." There is nothing more gratifying than finding a digital smoking gun – it can be so exhilarating that we have been known to break into an enthusiastic if woefully off-key rendition of "We Are the Champions." Those are good days, but not all days are good days. Sometimes, after hours or days of searching and analyzing, it becomes painfully evident that what the client hoped to find is simply not there. On those days, we are the bugs.

Sometimes clients become agitated and even fixated on the notion that what they are looking for must be there. If you have a competent, certified forensic examiner, believe the examiner if they say they have followed all appropriate procedures and the evidence you are looking for is not there. Perhaps the evidence never existed at all, or it may have been overwritten (and therefore unrecoverable), or the drive/specific files may have been wiped, sometimes with a special utility.

5. Thou shall not be stingy, lest thee be stung.

When it comes to electronic evidence, clients frequently want the sun, the moon, and the stars – all for The Dollar Store bargain discount. That's an exaggeration, but the truth is that most lawyers do not seem to comprehend how complicated and painstaking a computer forensics examination is. Just documenting the evidence and process, setting the equipment up, taking digital photographs of the physical equipment, and opening a forensic case file takes more than an hour when done properly.

A corollary commandment might be: Thou shall not attempt to break the laws of physics. Imaging takes as long as imaging takes, and no amount of persuasion will make it go faster. Depending on the amount of data written to the media, the technology and methods that must be used to perform the acquisition, etc., the amount of time required will vary widely. Perhaps one of the least understood aspects of pricing is the difference between acquisitions that take place in a computer forensics lab and an acquisition that must be done on site. It is far faster (and therefore cheaper) to acquire in a lab. People who are unfamiliar with forensics assume that a forensic acquisition is the equivalent of "copying." They are aware of the time involved to copy a drive and simply cannot comprehend why a forensic acquisition takes so much longer. Remember that a copy is a logical copy, whereas a forensic acquisition produces a physical bit-by-bit image.

On-site acquisitions are not just a little longer but a lot longer, because the portable computer used for the acquisition doesn't have the processing power or memory that the lab devices do. The data transfer rate for evidence storage is much slower because the evidence must now be held on an external drive versus one directly attached to a lab acquisition machine. By way of example, an acquisition that took 4 hours in the lab might take 8-10 hours on-site, though one can never pinpoint the exact time because it is unknown how much data is written on the hard drive or the impact of the speed of the subject computer. There are a lot of variables. Moreover, the technologist may run into specific issues where he/she needs to consult reference materials or needs a particular utility from the forensic toolkit. It is impossible to take everything on-site, so the expert will make a "best guess" based on the information that has been provided.

Most often, technologists are asked to acquire servers on site, and the client will not obligingly ship them to the forensics lab. Clients have angst about letting servers out of their possession and sometimes are determined that the acquisition will be done on-site no matter how great the advantages of shipping them out. If this is the client's determination, simply be aware that the costs are likely to be 2-3 times as great, even before travel is included.

6. Thou shall not bear false witness, nor ask thy witness to bear false witness.

You wouldn't think this admonition would need to be in here, would you? Lawyers are governed by codes of ethics, yes? Officers of the court and all that? And yet, it seems to be so tempting to constantly ask the expert to slant testimony. While there are clearly "experts for hire," good experts are seekers of truth and will report their findings regardless of what those findings may be. Having a forensic technologist examine a drive can certainly be a double-edged sword. You may find exculpatory evidence –

or you may find incriminating evidence. An expert can't pretend a search on a particular term wasn't conducted. You may put your expert on the stand and limit the scope of your questions, but if anything you've asked exposes a soft underbelly to the evidence and opposing counsel has the acumen to strike at it, well, so it goes.

It is perfectly understandable that counsel would like its expert to say explicitly: "Mr. Jones sent this defamatory e-mail" when all the expert can really say is that "this e-mail was transmitted from this machine, which Mr. Jones shares with his wife and children." Even if it was done under Mr. Jones' ID, did any of his family members have access to that ID? In a large number of cases, the best you can hope for is testimony that the evidence in question came from a specific machine that a specific person had access to.

While it's certainly fair to ask "Are you comfortable testifying to blah, blah, blah?," a "no" should be accepted gracefully, no matter how much "yes" was the answer you wanted to hear. Ditto for those expert reports – while all experts will labor to say whatever they can on behalf of the side that employed them, they will and should exercise extreme care in making sure they don't say anything that they are not comfortable they can fully back up. The good news is that employing experts who are known to be precise and careful in their reports and testimony frequently means that they have added credibility. Note well that this is especially true in an area where judges walk in unfamiliar, alien territory, as most of them do in the field of electronic evidence.

7. Thou shalt not kill forests.

Why, why, why do lawyers want to take electronic evidence and have us produce it to them in paper format? There is nothing more unwieldy than paper. It is stupefying that we are so often asked to produce boxes and boxes of paper when the complete forensic analysis report can easily be held on a single CD-ROM. Moreover, paper production puts the attorney in the same miserable place they have always been with respect to reviewing documents. Our most comic moment came when a firm wanted the entire forensic report converted to paper (two big boxes worth!) and then insisted that we transport it all to a conference we were speaking at so we could review the paper in their stead in order to meet their looming discovery deadline. Good thing one of us is a lawyer! How much simpler it is to manage the evidence in electronic form, where it is filed, cross-referenced, indexed, etc. This can be done using standard tools available to law firms or using sophisticated document management software, such as Summation or its counterparts. Subsequent searching and manipulation of the evidence is a relative breeze compared to traditional paper methods.

8. Thou shalt not think like thy parents, but like thy children.

How well one of the authors remembers the day when her 11 year old daughter called from elementary school the week before school opened. She had gone in for half a day to help the teachers get their classrooms ready. At noon, she called and said "Mom, I'm going to have to be here all day – the teachers all have new computers and they have no idea how to configure them. Can you pick me up at 5 instead?" Nearly everyone has marveled at how youngsters tool around the Internet, manipulate computer programs, and even master the simultaneous use of the four or five remote controls for the TV/DVD/VHS/Stereo systems we all seem to have.

Those of us who come from the paper era seem to have enough trouble simply converting a paper function into an electronic one. Our kids, on the other hand, see the whole vista of new possibilities opened up by the electronic world. When you deal with electronic evidence, it helps to think like a child. Everyone knows that the kids are swapping music files with the like of Kazaa, Morpheus, and Bearshare, but it was out of the box thinking by our young interns, who said "hey, they might be using file-swapping to exchange other illegal stuff," that led us to realize that those same file-swappers were used by pedophiles and others who wanted to swap contraband files rather than copyrighted music.

It is the younger generation that cottoned to steganography first (hiding text files within the white space of graphics) and soon we began to realize that terrorists might also be using steganography. In time, it became obvious that all sorts of miscreants might have uses for steganography. Though it's old hat now, it took a long time for law enforcement to realize what kids knew right along. If you want to hide particular kinds of files from mom and dad, give them innocent names and change the file extension so (for instance) your extensive .jpg collection of porn appears as .doc (Word) files bearing such innocuous names as historyreport.doc. These days, competent forensic examiners look for such mechanisms, which are very easy to discover. In the electronic arena, innovative thinking is frequently the way to unearth critical evidence.

9. Thou shall not honor false prophets.

Caveat emptor. The world of computer forensics is rife with "wannabes" who hang out their shingle and proclaim themselves forensic technologists. Be skeptical. Good forensic technologists have a lot of experience and credentials, have been involved in litigation many times, and are happy to give you referrals and to cite some of the cases in which they've been involved. Are they certified? By whom? Did they simply pay dollars for a certification that is essentially meaningless? What is there training and experience level? Have they been previously qualified as an expert? How many times? Which courts? Have they written expert reports? How many? Have they served as court appointed computer forensic experts? What certifications do they have? How long have they been engaged in computer forensics? How many cases have they personally handled? Make sure you carefully review their CV with all of the above in mind.

Also keep in mind that certified forensic technologists generally charge somewhere between $200-$500 an hour. If the price is significantly lower, be wary and ask questions.

10. Honor thy expert.

Though it might sound a little silly, it is astonishing how often lawyers treat forensics experts with cavalier disregard, as though they were mechanics engaged to change the oil. Not only do they often want the world on a platter, and delivered to them yesterday, but frequently their own lack of timely preparation is foisted onto their experts, who must now abandon everything else on their dockets in order to produce what the attorney needs when he/she needs it or has promised the client/court it will be delivered.

Making your expert part of the team can only help the end result. In a remarkable number of cases, forensic technologists are given directions for searching the evidence without any briefing as to the facts of the case. Needless to say, this is a patently absurd use of an expert. The more the technologist understands the case, the greater his/her sense is of the next logical step for achieving useful results. It is also striking that many attorneys fail to return calls from their experts. There are few things more frustrating than reaching a point in evidence analysis where guidance is required and being completely unable to get it.

Just as attorneys have their favorite and least favorite experts, so experts have their favorite and least favorite attorneys. While most experts will do their level best for everyone, there are some attorneys who are so consistently gracious, collaborative and responsive that the experts will work around the clock if necessary to be a part of a winning team. As with most things, success in the world of electronic evidence is a combination of the right people and the right process. If you've picked good forensic technologists, trust them, be responsive to them, and involve them in your litigation strategy. If you ignore the Ten Commandments, you do so at your own peril!

- Last Revised October 10, 2013
  Adam Sharp, President-CEO
  E-Hounds, Inc. Computer Evidence Services