

Computer Forensics: An Attorney's Primer

**By Sharon D. Nelson, Esq. and John W. Simek
© 2004 Sensei Enterprises, Inc.**

Electronic Evidence: Why care?

How vastly the world has changed in the last decade. Today, more than 95% of our documents are electronic and most will never be converted to paper. We send e-mails at a frenzied pace – North America alone now transmits more than 4 trillion e-mails per day. The daily average of non-spam e-mails received by the average worker is 20-80. No longer does the word “document” in discovery mean paper documents. The definition of document has been universally expanded to include electronic files.

With increasing frequency, the pivotal evidence in cases is electronic, often in those e-mails that we dash off with such abandon and so little thought. You should hit that “Send” button only if: 1) it's ok to see your e-mail on the front page of “The New York Times;” 2) you don't mind if your whole neighborhood sees it on a bulletin board on your nearest superhighway; 3) it would be perfectly agreeable for your mom to read it; and 4) if you have considered whether the transmission of the message could ever come back and bite you in the tush in a courtroom.

Another source of pivotal evidence that many lawyers are blithely unaware of: the “metadata” (hidden data that shows such things as authors, dates of creation, modification and access, last time that the document was printed, tracked changes, etc.) that goes along with documents unbeknownst to the senders. Another example of metadata are the headers (message tracking information) that accompany an e-mail transmission. The headers may identify the sender's IP address and the mail client that was used. This is often the most compelling evidence of all – and it will not show up in printed copies of documents or messages. You must have the evidence electronically, to the chagrin of those still happiest wading through boxes of documents.

If there was ever a day when attorneys could play ostrich and stick their heads in the sand ignoring electronic evidence, that day has long passed.

Computer Forensics and Electronic Evidence: The Dividing Lines

Understandably, many people are confused by the distinctions between electronic evidence and computer forensics, especially because the same companies often provide both services. Basically, a computer forensic technologist makes a bit by bit image of the hard drives(s) or other media in issue and identifies the relevant evidence, generally using search terms or data parameters provided by the attorneys. The forensic technologist will analyze Internet activity usage, application usage, and e-mail utilization, including web-based e-mail. Once the evidence has been extracted and partially analyzed, the computer forensics portion is finished.

If the forensics company does not also provide comprehensive evidence analysis, it will burn the electronic evidence onto CDs or DVDs, in a form readable to the attorney or to an electronic evidence company. The compilation may now consist of Word documents, spreadsheets, PowerPoints, Quickbooks data, Outlook e-mail, web-based e-mail (such as MS Hotmail), etc. If the volume of evidence is small, it is often sent directly to the attorney. If the volume is large, it is usually sent to an electronic evidence company which then indexes, dedupes and sorts through the evidence, often importing it into software such as Summation to facilitate managing the vast amount of information.

Why hire a forensics technologist?

Speaking bluntly, amateurs step on themselves, almost inevitably, altering data and, in the worst cases, making it inadmissible. Even at that, there are technologists and there are technologists. In this very new field, some folks simply hang out their shingle and pronounce themselves forensics technologists. A good technologist, as discussed below, has all kinds of certifications, lots of technical experience, multiple instances of having qualified as a court expert, and possesses an extensive “toolkit” which will allow maximum recovery and analysis of data, particularly deleted or obscure data.

Technologists know where to look for the information you need, and can help you tailor your discovery requests if you need to narrow discovery while procuring as much useful information as possible. A technologist is prepared with huge amounts of drive space and can recreate all sorts of native environments as needed to analyze evidence. Having an expert helps preserve the chain of custody and prove authenticity of the evidence – an expert is far better qualified than an attorney or an IT staffer to explain the technical side of computer forensics and defend against common charges that the evidence is unreliable or may have been tampered with.

Selecting a Computer Forensics/Electronic Evidence Company

So how do you find a good expert? This can be a daunting task and the right selection may depend upon a number of factors including what’s at issue in the case, the budget, the geographic location of the expert, and balancing the relative credentials of the experts under consideration.

Among the largest players in the industry, companies provide both computer forensics and electronic evidence services. Some of the biggest firms include:

- Ernst & Young, LLP® <http://www.ey.com>
- Deloitte Touche® <http://www.deloitte.com>
- Applied Discovery® (owned by LexisNexis®)
<http://www.applieddiscovery.com/>
- Kroll OnTrack™ <http://www.krollontrack.com/>

Needless to say, there are a host of other well-known firms in this burgeoning industry. As a general rule, the larger the firm, the larger the bill. It is not uncommon to pay as much as \$500/hour in the largest firms. In high quality but smaller firms \$250-\$300/hour may be a more common charge. If the firm you're looking at charges less than \$250/hour, you probably want to raise your eyebrows and seriously investigate the firm credentials, references, number of courts qualified in, standing in the industry, etc.

Regardless of the size of the firm, here are some of the factors you should consider in selecting the specific forensic technologist for your case:

1. Review their forensics certifications. Currently, the most prestigious certification available to private firms is the EnCE (EnCase Certified Examiner) issued by Guidance Software. More certifications are emerging and will gain credibility over time, but in the private sector, the EnCE is the certification to look for. A caveat: many less than honest folks will claim certifications on their CV when the truth is that they took classes or had training courses – no real meaningful certification was granted, just a “certification of attendance.”
2. Look for technical certifications. A good forensic technologist will have a lot of letters after his/her name, indicating a broad range of certifications with a number of different technologies. If you see no certifications, or a “base-level” certification (such as A+), you do not have an individual with a wealth of experience. If the expert is (just by way of example – there are many, many valuable certifications) a Certified Novell Engineer, Certified Cisco Network Administrator, Microsoft Certified Professional + Internet, Microsoft Certified Systems Engineer, NT Certified Independent Professional and a Certified Internetwork Professional, you've got someone with an expansive technical background.
3. Get the CV early on and study it. Ask questions. Does it show that the expert has spoken at a lot of seminars and/or written a lot of articles? How many courts has the expert qualified in? What is the expert's educational and professional background?

4. Above all things, get several references and check them out. Did the expert do a thorough, professional job? Was the expert responsive when contacted? Was the work completed on time? Did the expert stay within budget (not always possible) or at least alert the client of additional costs before incurring them? Perhaps the number one complaint heard about experts involved in electronic evidence is that costs spiraled out of control without notification to the law firm, resulting in a client highly perturbed with its law firm.

So Now You've Got an Electronic Evidence Case – What Next?

If the hard drive or other media is in your possession (or your client's), do NOTHING. Do not even power it up. Booting up a typical Windows operating system changes the dates and times on approximately 400-600 files. NEVER, EVER let your IT folks or your client's IT folks do their own investigation. They are not forensically trained and will unwittingly trample on the evidence, changing what may be critical dates, such as the date of last access, modification, etc. The trampled evidence may not be admitted at all, or it may be regarded as suspect because it was not forensically acquired.

Make sure you send a preservation of evidence letter. The other side is going to be hard pressed to argue innocence when confronted with spoliation of evidence charges if they have received a preservation of evidence letter. Be as specific as possible in the letter and not overbroad, so that fair notice is given of the kind of evidence to be preserved. If you know or suspect where the information is located (on a particular machine or a specific media, or in a particular file location) say so. The more specifics you can give, the less excuse there is for having evidence that vanishes or is tampered with.

Normally, you will be asking them to preserve 1) e-mail (electronic versions), along with header information, archives and any logs of e-mail system usage; 2) data files created with word processing, spreadsheet, presentation or other software; 3) databases and all log files that may be required; 4) network logs and audit trails; and 5) electronic calendars, task lists, telephone logs, and contact managers. Make sure you note in your letter that these things may exist in active data storage, including servers, workstations, and laptops and in offline storage including backups, archives, floppy disks, zip disks, tapes, CD-ROM, DVDs, memory sticks and any other form of media. Caution that potentially discoverable data should not be deleted, moved, or modified.

With respect to users who may have discoverable information on their computers, new files should not be saved to existing drives or media, no new software should be loaded, and no data compression, encryption, defragging or disk optimization procedures should be run until an image of the hard drive has been acquired. Ask that the normal rotation and overwrite of backup media cease until copies can be made. Also mention that no media storage devices containing potentially discoverable information should be disposed of due to upgrades, failure, donation or for any other reason.

If the case seems to require it, get a protective order. Set out specifics here as well so there can be no misunderstandings. When do you need one? A good example was provided by the Enron/Arthur Andersen debacles, where it became known that shredding papers and wholesale electronic deletions were taking place. If you can present a judge with any sort of credible scenario suggesting that spoliation may occur, you are very likely to be granted a protective order.

Onward to Discovery

Make your discovery illuminating and clear. Define everything at some length, encompassing all forms of media, all manner of things that may be considered responsive, and all possible locations.

Use interrogatories to get relevant information about the target computer network. What kind of network are you dealing with? How is the network configured? What operating system? What class of machines? What applications, both off the shelf and custom? What sort of back-up system is used? When is backup media overwritten? Who is the systems administrator? Are home computers used for business? Do they use laptops? Do they have Palm Pilots or other PDAs? Do they have a digital copier hooked up to their network? Do they use cell phones? Pagers? It is a common error to focus solely on the server and the workstations and to forget other data sources. Is there remote access? What sort of e-mail package do they use? Is a firewall used? Is there an e-mail server? Who is the Internet network provider? Where is e-mail stored for transmission, retrieval and archiving?

Depose the system administrator and other parties in the IT department who are likely to have relevant information about the computer system. Again, make sure you receive full information about the back-up system (often a treasure trove) and all possible data locations. It is common practice, though certainly not universal, to have monthly back-up tapes (or other media) going back six months to several years. Make sure you have information about the hardware/software used to create the back-ups. Your forensic technologist may need to recreate the native environment in order to restore data from the back-up media. Get a copy of the backup schedule for both incremental and full backups. How is the backup media rotated? Understand what logging is done on the network and what audit trails may exist. Users themselves are often unaware of the extent to which their activities may be traced. Audit trails may tell you what ID accessed the system, when, how long they were connected, what they did, etc. They may also tell you which ID copied, printed, deleted or downloaded files and when it was done. Does the company use any monitoring software? If so, there may be a wealth of information indicating programs used, files accessed, e-mail that employees sent or received and records of the Internet sites they visited. Find out also how security access is structured. Who had access to which files and programs? Who had read-only access and who had write access? For relevant individuals, get user names, logons, passwords, and e-mail addresses. Find out about any encryption programs that may be utilized and request the encryption keys.

Ask every witness about his or her computing habits. Do they make individual back-ups of their system? Do they use floppy disks, zip disks, CD-ROMs or thumb drives to copy some information from their system as a back-up or for portability reasons? Do they use their home computer to check their business e-mail? Do they do business work on the home computer? Where do they store their documents? For instance, does an attorney save his/her work on a secretary's workstation? Do they use a laptop? A PDA? Cell phone? Pager?

Request to inspect and forensically acquire any relevant data. Note the words "forensically acquire." This does NOT mean copying a drive and does NOT mean "ghosting" a drive. The acquisition should be done by a trained forensic technologist using specialized equipment and/or software. If there is an objection because of the time element and disruption to business, your expert can help offer alternatives to minimize the disruption.

Bear in mind that "deleted" doesn't mean deleted. In computer terms, deleted means that the space on the disk once occupied by a particular file is now available to be overwritten. The pointers to the deleted file are gone, but bits and pieces of the file, or the whole file, will remain until they are overwritten. Whatever remains of the file (called "residual data") may be recovered from the area of the disk's surface that is not allocated (this is known as "unallocated space" and it is often contains valuable evidence if painstakingly searched). Again, residual data will not be captured in a file-by-file copy of a disk, but it is captured by an imaged copy of the disk, which duplicates the hard disk's surface sector by sector.

Maintain data integrity. Make sure that you write protect all media. A good forensics technologist will do the same thing as part of the acquisition, making sure that that nothing can be added, erased or altered on the original. For the same reasons, your forensic technologist will virus check all media. If a virus is found, the appropriate response is to record all relevant information and then notify the producing party of the virus' existence. The technologist will never clean the virus from the original media, but will do so from the acquired evidence instead if the virus impacts the data to be produced.

Establish and maintain a chain of custody. Make sure you can track the evidence from its original source to its introduction in court. This means being able to prove that no information was added, deleted or altered, that the forensic copy of the evidence is complete, that the process used to copy the evidence was dependable and repeatable, and that all media was secured. This harks back to preceding points. Write protecting and virus checking will help establish that nothing was added, deleted or altered. Making a pure forensic copy of the evidence (with matching "hash" values between the original and image copy) will help prove that the acquisition was complete. The hash is a form of digital fingerprint. Both the hardware and software utilized must meet industry standards of quality and reliability. Good examples are EnCase, FastBloc, SafeBack and the dd function of Linux, which are all utilized frequently by law enforcement authorities. The image is then analyzed in a read-only mode to prevent spoliation. The copying process

must be repeatable as a means of independent verification. As always, evidence in the case should be kept securely, with very restricted access.

Common Mistakes in Using Electronic Evidence

How do you avoid sandtraps in the courtroom?

Believe it or not, the most common mistake is failing to designate the expert. The number of times this happens is truly amazing. Occasionally, you will find a judge so eager to hear the expert that he/she will do an end run around procedure and let the evidence testify as a fact witness, but that is far and away the exception.

Right on the heels of that error in prevalence is the failure to lay a proper foundation for the expert's testimony. As an example, suppose you are in a custody battle and the electronic evidence manifests an obsessive interest by the husband in bondage and discipline. Since that interest, assuming all the models are 18, is perfectly legal, you are going to need to lay a foundation by, for instance, having the children's therapist testify that the father is tying them up, locking them in dark rooms, holding pillows over their faces, etc. before your expert can then tie the bondage and discipline obsession to the way the father is interacting with the children.

Another astonishing failure is the failure to prepare the expert. Regardless of the expert's skill, the absence of preparation time with the attorney can be catastrophic. For some reason, this task is almost always left until the bitter end, and is often given short shrift, if it is done at all. Likewise, if electronic evidence is at issue, why would an attorney fail to prepare for cross-examination of the opposing expert without consultation with his/her expert?

As silly as it sounds, the failure to maintain a proper chain of custody frequently comes into play. The smartest move, once you know electronic evidence is involved, is to get it into the hands of your expert, sign a chain of custody form, have the evidence forensically imaged, and then return the original evidence, again with the chain of custody form. Once the expert has imaged the original evidence, it doesn't matter what happens to the original that is returned – and the expert will carefully keep the imaged evidence under lock and key. Returning the original also helps to defuse the business impact argument.

Electronic evidence is just plain difficult to explain in lay language. It is important to get your expert, who undoubtedly speaks "geekspeak" very well indeed, to speak the English language in simple declarative sentences. Even more helpful is coming up with images and analogies that are easily comprehended by both judges and juries. Judges are frequently as confounded by electronic evidence as juries and often pepper the expert with questions in an attempt to make sure they understand the true nature of the testimony.

Keep the expert's testimony as short as possible. Dragging out technical testimony will make the listeners' eyes glaze over. Your expert is not there as a soporific, but hopefully to provide illumination.

If you have a great expert, the other side will quickly stipulate to qualification as an expert. Don't let that deter you from deftly sliding in your expert's qualifications wherever possible, particularly in a jury trial. Hearing that your expert has written and spoken on particularly relevant topics or holds certifications that are directly pertinent to the case will make a jury find your expert more credible.

Attorneys should remember how much they don't know and how much trouble ignorance can cause. An electronic evidence expert should be questioned from a script and not on the fly. Heaven help the attorney who starts thinking he or she knows more than they actually do and decides to ad lib a question to which they do not know the answer. In one case, we watched in horror as an attorney did a marvelous job establishing that the prosecution's expert had totally failed in his official report to validate the date and time of the computer that was the source of his evidence. It was a good place to quit, but, sensing advantage, the attorney couldn't let it go. He asked how the jury was supposed to consider the dates and times relevant at all given the report's complete failure to validate them. The witness was then able to point out to great effect that, notwithstanding the expert's omission, three different server logs all corroborated the dates and times. Oops.

The world of electronic evidence contains a lot of quicksand. But just as most encounters with quicksand are not ultimately fatal, attorneys can survive the encounter if they proceed slowly, carefully and with a plan. Just as with quicksand, it is those who thrash and flail in panic that sink.

The authors are the President and Vice President of Sensei Enterprises, Inc., a computer forensics and legal technology firm based in Fairfax, VA. 703-359-0700 (phone) 703-359-8434 (fax) sensei@senseient.com (e-mail), <http://www.senseient.com> (web site)