

Finding and Securing Electronic Evidence

By Sharon D. Nelson and John W. Simek
© 2006 Sensei Enterprises, Inc.

Lawyers are notoriously slow to adopt change. The legal world has been a paper world for so long that adaptation to digital lawyering has proceeded slowly in relation to the digitization of the rest of the business world. In part, lawyers are simply so busy practicing law that learning the digital world seems oppressively time consuming.

However, lawyers love to win cases, and so do their clients. With increasing frequency, the pivotal evidence is electronic – and no, paper print-outs will not suffice. The “metadata” (hidden data that shows such things as pathing, times, the ID that was used to generate files, etc.) that goes along with e-mails and files is often the most compelling evidence of all – and it will not show up in printed copies of e-mails or documents. Word processing documents often contain non-printable data (revisions, comments, etc.), which may constitute pivotal evidence.

The trouble with this new world of electronic discovery is that it is an uncharted path for most attorneys. They don't quite know what to ask for – or what to do with it once procured. Below are some suggestions to guide attorneys through what may be unfamiliar territory.

- 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 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 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, 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.
- 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 are tapes 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 use 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 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, offer to "clone" the media and retain the originals for analysis. The opposing party can continue to operate on the "cloned" drives while the forensic acquisition occurs.
 - 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 "slack 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 image copy of the disk, which duplicates the hard disk's surface sector by sector.
 - Also bear in mind that "wiping" a disk may or may not overwrite it to the point that data cannot be restored. Very sophisticated utilities exist that effectively overwrite data, but there are plenty of unsophisticated utilities in use that may still allow recovery. Sometimes, attorneys are spooked by the presence of a wiping utility, but because using these utilities is a nuisance, it is often true that they are found on a machine and were only used several times before being abandoned as troublesome.

- 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. 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. Both the hardware and software utilized must meet industry standards of quality and reliability. Good examples are EnCase, FastBloc and the dd function of Unix, which are all utilized frequently by law enforcement authorities. The copying process must be repeatable as a means of independent verification. The media written to should also be write-protected during analysis to prevent spoliation. As always, evidence in the case should be kept securely, with very restricted access.
- 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 technologists – get a referral to a qualified technologist if you can, or ask the technologist for references. In this very new field, some folks simply hang out their shingle and pronounce themselves forensics technologists.
 - A good technologist has a "toolkit" which will allow maximum recovery and analysis of 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.

In the last few years, courts have begun to routinely admit electronic evidence, though always warily, knowing that electronic alteration is often simple and proving it is often hard. Frequently, the battle over electronic evidence becomes a battle between forensic technologists. Make sure yours is painstakingly careful and fully documents the forensics process so any challenge in court can be withstood!

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)