LAT LEGAL ASSISTANT TODAY
The only independent legal news resource covering the paralegal profession.

# E-discovery

Don't let electronic evidence bury your firm.

By Sharon D. Nelson, Esq. and John W. Simek

May/June 2004 Issue

## Electronic Evidence

How vastly the world has changed in the past decade. Today, more than 90 percent of our documents are electronic and most never will be converted to paper. We send e-mails at a frenzied pace — North America alone transmits more than 4 trillion e-mails a day. The daily average of non-spam e-mails received by the average worker is 20 to 80. No longer does the word "documents" 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 and can show up in two places you might not think of. First are in those e-mails 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 entire neighborhood sees it on a bulletin board on your nearest highway; 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 many lawyers and paralegals are blithely unaware of is metadata (hidden data showing things such as authors, dates of creation, modification and access, the last time the document was printed, tracked changes and more) that goes along with documents unbeknownst to senders. Metadata also is contained in the headers (message tracking information) that accompany an e-mail transmission. The headers might identify the sender's Internet Protocol address and the mail client used. This is often the most compelling evidence of all, and it doesn't show up in printed copies of documents or messages. You must obtain the evidence electronically, to the chagrin of those still happiest wading through boxes of documents.

Why should support staff care about electronic evidence and discovery? It's often the paralegals and other members of the legal team who end up sifting through the evidence and doing much of the work in selecting an expert to help when it comes to e-discovery.

## 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 drive 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, as well as application and e-mail use (including Web-based e-mail). Once the evidence is extracted and partially analyzed, the computer forensics portion is finished.

If the forensics company doesn't 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 can consist of Microsoft Word documents, PowerPoint presentations, Excel spreadsheets, Outlook e-mail, Intuit QuickBooks data, Web-based e-mail (such as Microsoft Hotmail) and so on. If the volume of evidence is small, it's often sent directly to the attorney. If the volume is large, it's usually sent to an electronic evidence company that then indexes, dedupes and sorts through the evidence, often importing it into software, such as

Summation, to help manage the vast amount of information.

### Why Hire a Forensic Technologist?

Speaking bluntly, amateurs step on themselves, and almost inevitably alter data and, in the worst cases, make it inadmissible in court. Even so, there are technologists and there are technologists. In this very new field of e-discovery, some folks simply hang out their shingle and pronounce themselves forensic technologists. A good technologist, as discussed later, has all kinds of certifications, a lot of technical experience, many instances of having qualified as a court expert, and possesses an extensive "toolkit" allowing 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 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 Information Technology staff member to explain the technical side of computer forensics and defend against common charges that the evidence is unreliable or might have been tampered with.

### Selecting a Computer Forensic/Electronic Evidence Company

Another reason for legal support staff to care about electronic evidence is they are frequently asked to locate appropriate forensic assistance. This can be a daunting task, and the right selection might depend on a number of factors including what is at issue in the case, the budget, the geographic location of the expert, and the credentials of the experts being considered.

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

- Ernst & Young, www.ey.com
- Deloitte Touche Tohmatsu, www.deloitte.com
- Applied Discovery (owned by LexisNexis), www.applieddiscovery.com
- Kroll Ontrack, www.krollontrack.com.

There are a host of other well-known firms in this burgeoning industry (see "E-discovery Services" on Page 66). As a general rule, the larger the firm, the larger the bill. It's not uncommon to pay as much as $500 per hour in the largest firms. In high-quality but smaller firms, $250 to $300 per hour might be a more common charge. If the firm you are looking at charges less than $250 per hour, you probably want to raise your eyebrows and seriously investigate the firm's credentials, references, number of courts it's qualified in, its standing in the industry and so forth.

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 *curriculum vitae* when the truth is 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 or 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 don't have an individual with a wealth of experience. If the expert is 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 have someone with an expansive technical background (just to name a few examples).
3. Get the expert's CV early on and study it. Ask questions. Does it show the expert has

spoken at a lot of seminars 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 costs spiraled out of control without notification to the law firm, resulting in a client highly perturbed with his or her law firm.

## Now You Have an Electronic Evidence Case — What Is Next?

If the hard drive or other media is in your possession (or your client's), do nothing. Don't even power it up. Booting up a typical Windows operating system changes the dates and times on approximately 400 to 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 could be critical dates, such as the date of last access, modification and so on. The trampled evidence might not be admitted in court at all, or it could be regarded as suspect because it was not acquired forensically.

If the evidence is in the other side's hands, first, make sure you send a preservation of evidence letter. The other side will 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 overly broad, so 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, 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 vanish or be 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 might be required; 4) network logs and audit trails; and 5) electronic calendars, task lists, telephone logs and contact managers. In your letter, make sure to note these things might 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 might 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 is acquired. Ask that the normal rotation and overwrite of backup media cease until copies are 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. Mention specifics in the order as well, so there can be no misunderstandings. When do you need one? The Enron/Arthur Andersen debacle is a good example. 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 spoliation might occur, you are very likely to be granted a protective order.

## Onward to Discovery

When talking about electronic evidence, make your discovery illuminating and clear. Define everything at some length, encompassing all forms of media, all manner of things that could 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 is used?
- What class of machines is used?

- What applications, both off the shelf and custom, are used?
- What sort of backup system is used?
- When is backup media overwritten?
- Who is the systems administrator?
- Are home computers used for business?
- Do they use laptops, Palm handhelds or other personal digital assistants?
- Do they have a digital copier hooked up to their network?
- Do they use cell phones or pagers?

It's 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 systems administrator and other parties in the IT department likely to have relevant information about the computer systems. Again, make sure you receive full information about the backup system (often a treasure trove) and all possible data locations. It's common practice, though certainly not universal, to have monthly backup tapes (or other media) going back six months to several years. Make sure you have information about the hardware and software used to create the backups. Your forensic technologist might need to recreate the native environment to restore data from the backup 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 might exist.

Users themselves often are unaware of the extent to which their activities could be traced. Audit trails might tell you what ID accessed the system, when it was accessed, how long the individual was connected, what he or she did and more. These trails also could tell you which ID copied, printed, deleted or downloaded files and when it was done. Find out if the company uses monitoring software. If so, there might be a wealth of information indicating programs used, files accessed, e-mails sent or received by employees and records of the Internet sites visited. Find out how security access is structured, such as who has access to which files and programs, who has read-only access and who has write access. For relevant individuals, get user names, logons, passwords and
e-mail addresses. Find out about any encryption programs used and request the encryption keys.

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

Request to inspect and forensically acquire any relevant data. Note the words "forensically acquire." This does not mean copying a drive and doesn't mean "ghosting" a drive. The acquisition should be done by a trained forensic technologist using specialized equipment and 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.

Keep in mind, "deleted" doesn't really mean deleted. In computer terms, deleted means the space on the disk once occupied by a particular file now is 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) might be recovered from the area of the disk's surface that isn't allocated (this is known as unallocated space and it 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's captured by an imaged copy of the disk, which duplicates the hard disk's surface sector by sector.

During this process, you must maintain data integrity. Make sure you write-protect all media. A good forensic technologist will do the same thing as part of the acquisition, making sure 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 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 no information was added, deleted or altered; the forensic copy of the evidence is complete; the process used to copy the evidence was dependable and repeatable; and all media was secured. This harks back to preceding points. Write-protecting and virus-checking will help establish 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 the acquisition was complete. The hash is a form of digital fingerprint. Both the hardware and software used must meet industry standards of quality and reliability. Good examples are EnCase, FastBloc, SafeBack and the dd function of Linux, all of which law enforcement authorities use frequently. 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 secure, with very restricted access.

### Common Mistakes in Using Electronic Evidence

As most paralegals know, attorneys don't get it right unless you ride shotgun for them. So here are ways to keep your attorneys from sinking in courtroom quicksand.

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, he or she will do an end run around procedure and let the expert testify as a fact witness, but that is far and away the exception.

Another astonishing mistake 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 almost always is left until the bitter end, and often is given short shrift, if it's 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 or 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 returned original. The expert will carefully keep the imaged evidence under lock and key. Returning the original also helps defuse the business impact argument.

Another problem with electronic evidence is its just plain difficult to explain in lay language. It's important to get your expert, who undoubtedly speaks "geekspeak" very well, to speak the English language in simple declarative sentences when testifying in court. Even more helpful is coming up with images and analogies easily comprehended by both judges and juries. Judges are frequently as confused as juries by electronic evidence 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 isn't there as a soporific, but one would hope 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 your expert has written and spoken on particularly relevant topics or holds certifications directly pertinent to the case will make a jury find your expert more credible.

Finally, attorneys and support staff should remember how much they don't know. An electronic evidence expert should be questioned from a script and not on the fly. Heaven help attorneys who start thinking they know more than they actually do and decide to ad lib a question to which they don't know the answer.

In one case, we watched in horror as an attorney did a marvelous job establishing 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 could not 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 and e-discovery is filled with pitfalls that can potentially bury even the best of law firms and corporations. However, attorneys, paralegals and support staff can survive the encounter if they proceed slowly, carefully and thoughtfully with a plan. It's those who thrash and flail in a panic who often end up digging their own grave.

---

## E-discovery Services

### LexisNexis
**Applied Discovery**
*Contact: (877) 613-3010;*
*new_clients@applieddiscovery.com*
*www.lexisnexis.com/applieddiscovery*
*Pricing: Contact your local electronic discovery specialist.*
LexisNexis Applied Discovery is a leading provider of electronic discovery services to the nation's top law firms and corporations. From data gathering and media restoration through data processing, review and production, clients can search, organize, redact, Bates number and produce electronic documents.

### Planet Data Solutions
**Electronic Data Discovery Services/Targeted Data Extraction**
***Contact: Zoltan Horvath, president;***
*(914) 333-0670; zhorvath@planetds.com*
*www.planetds.com*
Pricing: EDD is $0.12 per page processed; TDE is $0.10 per page processed; Total is $0.22 per page processed; or traditional EDD with
manual coding for attachments and
e-files is $1.05 per page.
Planet Data Solutions' Electronic Data Discovery Services in conjunction with its Targeted Data Extraction process, provide clients with more than the traditional metadata extracted from e-mails, attachments and e-files. Planet Data provides automatic objective coding of the e-mail attachments and e-files. TDE extracts all names, organizations, dates, sites, address and unlimited keywords or phrases from the text of the data.

### Data Discovery Direct
**Division of SPI Litigation Direct**
*Contact: Tom Barnett; (206) 909-7978; t.barnett@spitech.com*
*www.spitech.com/litdirect.html*
*Pricing: Varies by size of case and services requested.*
Data Discovery Direct is a one-stop shop for EDD services, including collection, processing, review and production of electronic data, all using industry-standard processes, with output to any standard litigation support application.

### Fast Track Litigation Support
**Paramount and Electronic Discovery**
*Contact: (800) 515-3278; info@ftls.com*
*www.ftls.com*
*Pricing: Pricing depends on size, scope and requirements of a project.*
Fast Track is the integrated, single-source solution for complete electronic discovery services, including consulting, computer forensics, restoration, processing, management and more. Fast Track's Paramount system transforms e-mail, attachments and more than 300 application file-types into an image-enabled, fielded, fully searchable, full-text and metadata database linked to images and is viewable in the litigation support software of your choice.

### Cricket Technologies
*Contact: (888) 635-1554; (703) 391-1020; info@crickettechnologies.com*
*www.crickettechnologies.com*
*Pricing: Cricket creates custom bids on each case document project based on the size of the document population and other variables.*
Cricket offers one-stop shopping for all the technology services you need to capture, convert, produce, manage and store large volumes of documents, whether physical documents or complex electronic files. Cricket supports and produces for all litigation software management systems. Using Cricket Extranet Solutions, clients easily can retrieve and share information. Cricket manages huge volumes of documents and provides complete security.

### Kroll Ontrack
**Electronic Dataviewer**
*Contact: Nicolle Martin; (952) 949-4137; nmartin@krollontrack.com*
*www.krollontrack.com*
*Pricing: Contact Kroll Ontrack for pricing.*
Kroll Ontrack Inc. provides electronic evidence and data recovery solutions to help individuals, companies, law firms and federal agencies quickly and cost-effectively recover electronic information.

### Quorum Litigation Services
**Electronic Data Discovery and Reddoc II**
*Contact: Barry Dop, director of sales;*
*(800) 328-4454; bdop@quorum.com*
*www.quorum.com*
Pricing: Call for free consultation.
Quorum is the industry leader in EDD and Web-based repository services. You can extract text and metadata and convert to TIFF or link to original document. Hundreds of file types are supported. Search, review and print using just your Web browser with RedDoc II online document repository. Increase productivity; decrease the cost of managing your discovery documents.

### Daticon
**Virtual Partner and Discovery OnDemand**
*Contact: (860) 823-4400; info@daticon.com*
*www.daticon.com*
Virtual Partner is a Web-based document management system allowing you to perform online document review, document organization and collaboration, and research information in large volume document collections. It features full-text and relational database components, and the viewer uses TIFF images. Discovery OnDemand is an in-house e-discovery tool for converting native files, Microsoft Outlook/Exchange and Lotus Notes files to common litigation support software load files with corresponding TIFF images.

### Forensics Consulting Solutions
*Contact: (602) 354-2772; kbrown@forensicsconsulting.com*
*www.forensicsconsulting.com*
*Pricing: Hourly for consulting, volume based for process work.*
Forensics Consulting Solutions offers electronic discovery consulting and litigation support. Services include case analysis and strategy development; pre-project cost analysis and planning; electronic discovery processes; concept search electronic discovery service; litigation support

services; e-discovery for pre-merger and acquisition due diligence, and Department of Justice second requests; in-house and remote data gathering teams; secure data hosting facilities with remote access; and free continuing legal education.

**Fios Inc.**
**Prevail**
*Contact: Brian Rose, director of business development; (877) 700-3467; (503) 265-0730*
*Pricing: Pricing for Prevail is based on a per megabyte basis. The standard rate is $4 per megabyte.*
Prevail is an easy-to-use, online tool facilitating the review of electronic documents associated with legal and government proceedings. Prevail's Web-based platform provides remote and secure access to electronic data, permitting legal teams to search, organize, categorize, annotate, cull and produce information quickly and effectively. Prevail also offers concept-based searching and e-mail chain review.

** Vendors provided the e-discovery services information above. Listings are in no particular order.*

---

***Sharon D. Nelson, Esq. and John W. Simek*** *are the President and Vice President of Sensei Enterprises, Inc., a computer forensics and legal technology firm based in Fairfax, Ca. (703) 359-0700 (phone); (703) 357-8434 (fax); sensei@senseient.com; www.senseient.com.*

---



Updated 04/22/04

editorlat@jamespublishing.com
www.legalassistanttoday.com
(800) 394-2626