

LAWYERS WEEKLY

Feature Story (6/10/02)

Electronic Evidence

It's Becoming Indispensable - But Most Lawyers Still Have No Idea What It Can Do

By Michael M. Bowden

Paper documents can be shredded; physical evidence can be "lost;" human testimony is only as strong as the witness's credibility - but electronic evidence is virtually impossible to destroy.

That's because the information (including attempts to delete it) is "remembered" by the computer at four levels of electronic storage. The average computer user can delete activity on the first level; the more advanced computer enthusiast might also be able to eliminate much of the second level. But the third and fourth levels belong strictly to the realm of the cybersleuths.

"If you are tremendously familiar with computers, it is possible to commit 'the perfect crime' - to totally hide your tracks," said Doug Rehman, a computer forensic expert in Mount Dora, Fla. "But to succeed, you've got to sequentially close about 13 'back doors' to the information, without a single error," he said. "If you make just one mistake, I can detect it. So my odds of success are vastly better than yours."

Furthermore, electronic evidence is increasingly accepted as gospel by the courts, thanks to its built-in time signatures and other highly reliable tracking data.

"If you want to see a real difference that's taken place over the last three years, look at the judges," said John Wiechman, president of TLSI, Inc., a computer forensics firm in Grand Prairie, Texas. "They're getting a lot more technically savvy about computers and electronic data. It's part of their jobs; they don't have an option."

That, he said, ups the ante for lawyers because they now have to face judges who expect a level of electronic sophistication.

But only 25 percent of all lawyers know "something" about electronic evidence and a mere 5 percent are "very knowledgeable," according to Joan Feldman, president of Computer Forensics Inc., in Seattle, Wash.

The fact is, the traditional world of paper evidence is quickly being replaced by electronic data, and the legal world has no choice but to catch up. To ignore these developments can be professionally disastrous, regardless of the merits of a given case.

"I have gone into cases where one side understood electronic evidence and the other side didn't," said Wiechman. "And the side that knew, literally tore up the side that had no understanding of information technology, and no idea of what to do with what was coming down the pike at them. We sent out a tremendous amount of data to these attorneys, in response to their interrogatories and requests for production - and they would get it and not have a clue about what to do with it."

What Kind Of Evidence

Digging for hidden and deleted documents remains the profession's bread and butter - almost always in cases involving business transactions, employment law or family law.

And this work is becoming more affordable thanks to better, faster technology. For example, three years ago, searching the hard-drive of a spouse's computer in a divorce action could cost up to \$10,000, effectively placing it beyond the reach of all but the wealthiest litigants. Today, the same examination can cost \$2,500 or less.

"In smaller civil cases, the expense still can't be justified sometimes," said Rehman. "But as it starts getting larger, it almost becomes a necessary expense - because without electronic discovery, you cannot know what evidence you missed that might have won the case for you."

Rehman cites a case in which the board of directors of a large corporation suspected that two high officers in the company had formed a secret agreement with a competing corporation.

Rehman found several deleted e-mails in which the officers alluded to the arrangement, one of which contained instructions to destroy the e-mail immediately upon reading it. Faced with this evidence, the officers immediately confessed to their double-dealing.

This illustrates the ubiquity of electronic evidence. People are using computers more than ever before - often for communications that would have once taken place in person or over the phone.

Factor in the growing popularity of cell phones (which store past-activity on their computer chips) and hand-held electronic devices like Palm Pilots and Blackberries, and future possibilities of electronic evidence recovery seem limitless.

"These devices are slowly coming into focus in the electronic discovery arena," Rehman said. "But they still have a way to go because the people at the top of a business - the ones we'd usually be targeting - aren't as technologically savvy as the lower-level people, and don't use the devices as much as those below."

Electronic building-access systems are another fast-growing source of electronic evidence in business litigation because these "electronic doormen" record who was where at a given time.

"This allows you to reconstruct someone's movements," said Rehman.

He said this could be used to establish that the person was present to commit the act in question, or to establish an alibi.

Perhaps the most fascinating aspect of computer forensics still involves the tracing of altered documents.

Ken Shear of Electronic Evidence Discovery in Seattle tells of a child rape case in which the alibi of prime suspect was that he was home typing e-mail during the two-hour window in which the attack occurred. By digging deep into the hard-drive records, Shear was able to prove that the suspect had reset the clock on his computer to shift the time signatures backward by several hours. Faced with this evidence, the rapist confessed to his crime.

Such alterations frequently figure in civil cases as well.

"You'll have litigation going on for two years and then suddenly some old memo miraculously appears that just happens to totally destroy the other side's case," Rehman said. "Then our issue becomes: Is this a genuine document, or was it created after the fact in order to win the case?"

Powerful Family Law Tool

Outside the world of business, electronic evidence has made its greatest impact in family law.

Typically, it comes into play in divorce cases, where one spouse believes the other is hiding assets. By burrowing into the depths of the opposing spouse's hard drive, cybersleuths have found secret bank accounts, real estate and other assets that their client never knew about.

But electronic evidence can affect more than just money matters. Hard drive contents are increasingly used in child custody battles to show that one spouse isn't a fit parent - often by showing that one parent has been downloading pornography and storing it where the children could see it.

This is what happened in a pending case that Wiechman is investigating. But the husband hasn't conceded an inch. His lawyers came back with a technically sophisticated argument involving the use of "push" and "pull" technologies by pornographic websites.

The husband claims to have stumbled onto the notorious pornographic website, Whitehouse.com, which many innocent users have discovered while looking for the President of the United States (i.e., whitehouse.gov). The pornographic "Whitehouse" site employs "push" technology, meaning that, without any instructions from the user, it automatically opens a series of additional browser windows on the user's computer, opening related sites.

The result is a "popcorn" effect, in which the user watches as a half dozen porn sites suddenly open on his or her computer - and each time one is closed, it generates a few more. The only reliable way to stop the effect is to shut down the browser program entirely and restart it.

By the time that's done, however, the user's computer will have recorded all of the porn sites opened by the "push" technology as having been visited by the user. This, the father claims, is what happened to him.

"So we had to establish whether the spouse was being pushed to these sites by accident, or whether he'd actively sought them out," Wiechman explained.

To do that, he had to recreate everywhere the husband had gone on the Web, and the sequence of the sites opened, and then compare it against the "push" sequences employed by a number of porn sites.

The investigation is ongoing, and has been complicated by the fact that the husband has been caught deleting files in violation of a court order. In addition to the contempt issues, this creates an appearance of impropriety - and makes it almost impossible to determine the sequence.

"I think he's really hurt his case," Wiechman said.

In that case, the electronic data sought by litigants was very recent, and generally speaking, success is more likely when the investigation is done close to the time the files were created. However, it is not unusual for cybersleuths to dig up files that were created months or even years earlier.

In one case, for example, a woman had waited until the very end of a two-year statute of limitations to sue her former employer, saying she'd been pushed out by sexual harassment. Her evidence? A series of sexually explicit e-mails (printed out on paper while she was still employed at the company) received from male co-workers.

Wiechman located the computer the woman had used while employed there. Fortunately for the employer, it was in storage and subsequent employees had not overwritten its old files with new data. There in the forgotten depths of the hard drive, Wiechman found hundreds of raunchy letters (many with pornographic pictures attached) that the woman had written to provoke the sexually explicit responses.

When a stack of these were dropped in front of her at mediation, the woman immediately dropped her case.

Do-It-Yourselfers Beware

Computer forensics can be very expensive. The average expert charges between \$200 and \$300 per hour and the average case involves 10 to 50 hours of work. That's a range of \$2,000 to \$15,000 per case.

"You can run into some real numbers real fast," noted Wiechman.

Large corporate cases can cost even more, running up millions of dollars in forensic expert fees, according to Feldman. Even an average business case can run \$50,000 to \$100,000, he said.

As a result, there are a growing number of do-it-yourself programs available.

If you spend any time at all on the Web, you've probably come across numerous ads for these affordable software products that promise to reveal whether your spouse is having an online affair, whether your kids are looking at pornography or engaging in inappropriate online chats, etc.

That is, indeed, a form of cyber-sleuthing, and some of these programs work very well, experts say. One of the best is Computer COP (<http://www.computercop.com>), an easy-to-use program that can be purchased for as little as \$9.95 for the basic home-use version, up to \$495 for a professional suite designed to assist corporate IT departments, law enforcement professionals and private investigators.

But lawyers should proceed with caution. First, such programs can't provide nearly the same experience, instinct and creativity that a professional forensic expert can bring to the table.

"The problem isn't so much in using the software, but in knowing how to apply it, what to look for, and how to interpret what you find," Rehman said. "It really is very much a forensic science, as well an art form and a matter of gut instinct. It doesn't really lend itself to the do-it-yourself approach."

For lawyers, these programs are rife with dangers. For example, when you cybersleuth the information yourself, you risk becoming a witness in your own case. And if you have a paralegal or secretary in your firm do the job - or even your client - that can also create an appearance of bias that your opponent can exploit. Further, these individuals won't be able to authenticate the data like an expert can. If asked to explain fine points about the chain of evidence, they might be able to say little more than, "Well, I pushed 'Find' and this is what the program found."

A forensic expert, on the other hand, could explain why the information was found where it was, how it got there, how the computer generates copies, why the date and time stamps are reliable or why they are not.

Another danger is that it is very easy to break the golden rule of computer forensics, which is: Do not alter the data in any way, since this will destroy its value as evidence.

Every file on a computer contains a time and date signature that automatically notes when it was created, and when it was last opened or manipulated. If a forensic examiner touches the original file, that time signature is overwritten and lost, and the evidence is tainted or lost.

As a result, forensic experts first make a copy of the hard drive or database in question and leave the original intact. Also, the pros don't rely on any single "cyber-sleuthing program" in their work. Rather, they employ an entire "tool kit" that includes functions of the computer's own operating system, along with a host of other devices and techniques - tcpdump, Argus, NFR, tcpwrapper, sniffers, nstat, tripwire, etc. - that are incomprehensible to most laypeople.

"The concept is exciting to many people," said Feldman. "But the reality makes them say, 'Huh?'"

Questions or comments can be directed to the writer at: mbowden@lawyersweekly.com