NOVEMBER 2004

TechLink

Covering technology, biotechnology and telecommunications in Maryland

Inspector Tech

Maryland's legal community embraces electronic evidence

Page 9

ALSO INSIDE:

Maryland biotech firms are working overtime to snag VC funding.

If the game (or game developer) ain't broke, why invent an all-new game?

Funders interested in Maryland companies have been roused from slumber.

In the cutthroat world of wireless, users want handheld offices and entertainment centers.

A supplement to THE DAILY RECORD

ILLUSTRATION BY ROBIN ALLEN

Inspector tech

Though slowly, legal community embraces electronic evidence

BY ROBERT L. RAGER
Special to The Daily Record

"As a profession, they're just starting to come into the '90s."

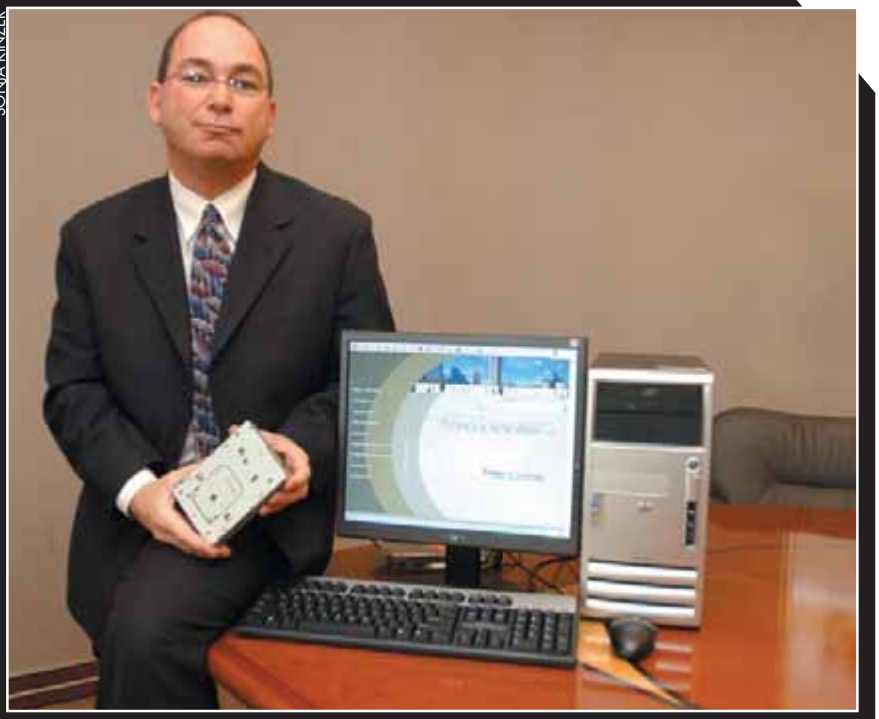
John W. Simek, vice president of **Sensei Enterprises** Inc. in Fairfax, Va., was somewhat joking when he said this about the country's legal community. But his point was clear: In the legal world, the digital divide is being bridged much slower than elsewhere in America.

Where "electronic evidence" is concerned, the meshing of law enforcement, courts and attorneys with technology and computer forensics has produced a steep learning curve, forcing judges and lawyers alike to wade slowly through some of the most complex evidentiary issues in the U.S. legal system's history.

The Internet, the trillions of e-mails that are sent each year and the countless electronic documents have formed an enormously complicated and volatile area of law that has unsure attorneys firing burdensome electronic discovery salvos at their opponents, and judges grasping for a road map to navigate territory that often neither they, nor the attorneys presenting cases, fully understand.

"There was a time when the only kinds of cases that presented electronic discovery issues were cases that were, on their face, high-technology," said Harold Walter, attorney and partner with the Baltimore office of **Tydings & Rosenberg** LLP.

SONIA KINZER



Harold Walter, attorney and partner with the Baltimore office of Tydings & Rosenberg LLP, says that while most attorneys have a good understanding of e-mail and word processing programs, they also should learn more about the dos and don'ts of electronic discovery and computer forensics.

But with most businesses today using e-mail and word processing programs, Walter says attorneys must understand the dos and don'ts of electronic discovery and computer forensics.

"Lawyers are beginning to understand the technology better ... to know that a printout of an e-mail is not nearly the same thing as receiving an electronic copy in native format," said Walter, adding, "If you don't have the metadata (computer-generated file information that most users never see), you've got the tip of the iceberg, and the rest is still below the surface."

Similar to traditional physical evidence, electronic evidence — which includes e-mails, computer files, memory cards, hard drives and other computer-related hardware and software — must stand up to certain admissibility standards that are laid out in federal and state rules of evidence.

But unlike traditional physical evidence, digital data is subject to easy and quick manipulation. Electronic information that might normally seem

SEE **EVIDENCE** PAGE 12

Computer forensic analysis can reveal:

- What Web sites have been visited
- What files have been downloaded
- When files were last accessed
- When files were deleted
- Attempts to conceal or destroy evidence
- Attempts to fabricate evidence

Evidence

Continued from page 9

unimpeachable can become suspect the instant a link in the evidentiary chain of custody is broken.

Hands off

In criminal cases, procuring electronic evidence begins much the same way any other evidence is collected. Search warrants usually need to be executed, with the reasonable expectation that relevant information resides somewhere in a suspect's (or witness') digital realm.

But this is where electronic evidence collection usually diverges from the usual, physical "smoking gun" search.

The **U.S. Secret Service**'s "Best Practices for Seizing Electronic Evidence" instructs law enforcement officials that if a computer to be seized is turned on, an investigator generally can't just pull the plug and go. The information on the screen has to be recorded. Evidence tape has to be placed over each drive slot, and photographs have to be taken to show all components and connections.

Similarly, if the computer (or PDA or other storage device) is off, an investigator should leave it off because a boot-up can change information on hundreds of system files and possibly break the evidentiary chain of custody before the equipment ever makes it back to the computer forensic lab.

Even in civil cases, where electronic discovery is becoming more and more common, the task of maintaining an evidentiary chain of custody is daunting. Simek says the No. 1 problem he finds as a computer forensics consultant and expert witness is that clients simply feel compelled to know what's on a hard drive or other storage device.

"The client or lawyer can't help but see what's going on ... in other words, they stomp on the evidence," said Simek, explaining that most lawyers and their staffs "are not educated [in electronic evidence], and they don't have the skill sets to do it forensically ... but they can't help themselves.

"So now they've compromised the evidence," continued Simek. Simply by turning a computer on, "they've altered dates and times. And that makes my job harder as an expert ... now I have to explain that away."

Tydings & Rosenberg's Walter notes it's often just as difficult for judges to understand what to do with proposed evidence gathered from an electronic source.

"You have some judges who are technophobes ... but even judges who are very interested in this, and are willing to take the time, have difficulty getting good information," he said.

Computer forensic companies, such as Sensei Enterprises, specialize in the preservation, recovery, duplication and storage of electronic media. While the need for such services is on the rise nationwide, Walter speculates that the specialized skills and tools needed for data recovery, analysis and preservation make it unlikely that law firms will rush to add a computer forensics investigator to the payroll.

"I rely on outside consultants that I hire on a case-by-case basis. ... I deal with a number of them, the same way you might need experts in the field of medicine," said Walter.

He adds that while his firm has a talented in-house IT department, "IT people don't deal with forensic computer issues, and I believe it's a mistake to rely upon even competent IT people when what you need is a forensic expert."

Walter and Simek agree the proper way to deal with electronic evidence is to make a "forensic copy" of the hard drive, also known as a "mirror image copy" or "bitstream copy," to preserve it in its original state. "Then all the [evidence] searches are done based on this copy," said Walter.

What is electronic evidence?:

- Data that may not exist in hard copy, including e-mail text, e-mail headers, e-mail file attachments, electronic calendars, Web site log files or "cookies," and browser information.
- "Deleted" documents. When a computer user deletes a document, it does not necessarily disappear. Although reference to the deleted file is removed from the computer's directory, file information often remains on the hard drive until new data overwrites it.
- Password-protected files or encrypted files.
- Hardcopy's electronic counterpart, which is better evidence than, say, a printout of an e-mail. Network and personal computer operating systems create information in addition to the text, which may prove the hard copy's authenticity or provide additional information, including:
- Author, date, time of creation
- Information about the document's review or modification
- File names and changes
- Alterations, versions and earlier drafts.

Source: www.sociablemedia.com.

Before hitting send consider:

- People tend to write things in e-mail they never would consider writing in a memo or letter. What happens if your e-mail were to be seen by unintended audiences?
- E-mail has been used successfully in civil cases as well as criminal cases.
- E-mail is often backed up on tapes that are generally kept for months or years.