

INVESTOR'S BUSINESS DAILY

TUESDAY, FEBRUARY 21, 2006

INTERNET & TECHNOLOGY

The Digital Evidence Left Behind In PCs Can Break Big Cases

Cyberforensics Evolving Fast

E-mails, Web pages and other documents can leave lasting impression for cops

BY MARILYN ALVA

INVESTOR'S BUSINESS DAILY

It helped to convict Scott Peterson of murdering his wife Laci and to indict Martha Stewart over a personal stock trade. And it's key evidence in the Enron case.

"It," in these cases, isn't a fingerprint or a tire track or DNA. It is information left on computers.

Whether a murder case, petty crime or corporate fraud, digital evidence left behind in e-mails, Web pages, online photos and cell phone calls often make or break a case.

Digital forensics — culling and preserving digital evidence for legal use — is a small but fast-growing subset of the \$6.4 billion computer-security software market.

The biggest catalyst has come from new software products that have come out in recent years to make computer forensic investigations easier, says Michael Menz, president of the High Technology Crime Investigation Association.

"Companies today are spending upward of \$500,000 on (computer forensic) software," he said.

Roughly \$5,000 Average Cost

Such software runs anywhere from \$600 to \$15,000, he says. A basic product can cost \$3,000 to \$5,000.

Menz says the top two software products are EnCase from industry leader Guidance Software, followed by AccessData's Forensic Toolkit. ProDiscover from Technical Pathways is a newer entrant that tends to offer lower prices, he says. Another outfit, Paraben, focuses on cell phones and PDAs. All four companies are privately held.

"There are literally dozens of other specialized tools out there," said Alan Brill, senior managing director of Kroll Ontrack, the technology services unit of business consultant Marsh & McLennan^{MC}.

For its mostly corporate clients,

Kroll uses products from the top vendors as well as proprietary software it's developed in-house.

It operates four in-house digital data labs in the U.S. and several more overseas. The labs do double duty in data recovery work.

Other consulting and accounting firms have added digital forensics to their practices.

Law enforcement agencies were early adopters of the technology, but now corporations are turning into cybersleuths to stem corporate mischief and fraud.

"We have relationships with Banc of America^{BAC}, Lockheed Martin^{LM} and several other large and small firms," said Scot Sessions, vice president of marketing for AccessData.

According to figures compiled by AccessData, the \$500 million corporate market in computer forensics is five times bigger than the law-enforcement side.

AccessData got its start in password protection. Only in the last four years did it become active in legal work, after police agencies started to use its password tracking software to nail suspected criminals.

"We saw that digital evidence was going to be a crucial factor in all law-enforcement cases, so we developed a tool that could basically review all the content within a computer, even files that have been deleted," Sessions said. "When you delete something on your computer, it's still on your hard disk until that space has something written over it."

Forensic tools can copy or index every bit and byte of information on a hard drive and assign mathematical values to files to verify that data haven't been changed. They can analyze PC and network logs and e-mails.

A growing number of companies want to pry into their employees' digital files to preserve data as evidence for possible lawsuits, such as those involving product liability or trade secrets.

Analysts from research firm Gartner wrote in a recent report that they are even seeing more requests to recover deleted documents during the due diligence phase in mergers and acquisitions.

Cybercrooks can try to cover up their tracks by using wiping programs such as Evidence Elimina-



This data recovery lab is similar to Kroll Ontrack's computer forensics labs. The company operates four in-house digital data labs in the U.S. and several more overseas that work on such tasks as recovering data from computers.

"When you delete something on your computer, it's still on your hard disk until that space has something written over it."

Scott Sessions, AccessData

tor, History Kill and Window Washer. But wiping tools can leave "forensic remnants," Brill said. And cybersleuths can determine whether and when a wiping program was used to a suspect's detriment.

In one recent criminal case, a forensic cyberanalyst showed that a suspect zapped about 5,000 files the night before he was scheduled to have his computer analyzed, using Evidence Eliminator.

The judge wasn't a "techie," Brill said, "but he had no problem saying that was not good."

Board Adds 'Multimedia'

Digital evidence is the newest of nine forensic disciplines cited by the American Society of Crime Laboratory Directors/Laboratory Accreditation Board. The board just added the word "multimedia" to the digital category so as to include cell phones and PDAs.

The older disciplines sound Sherlock Holmes-like by comparison: toxicology, biology, trace evidence such as fibers and residues, latent prints and questioned documents with handwriting and typewriting.

The group accredits the kind of crime labs seen on the TV series "CSI."

Of the hundreds of law enforcement labs it's accredited over the last 20 years, only 12 are digital labs — so far.

For the first time, two private-sector digital labs are going through the accreditation process, says the board's executive director, Ralph Keaton.

One is a large national bank based in North Carolina and the other is a major retail chain, he says, declining to name them.

Experts say it's wise to hire professional investigators who specialize in digital forensics to analyze the data retrieved.

They can determine whether there is sufficient incriminating evidence and can testify in court.

Some are better at tough crimes, and others at hacking-type cases, says Menz. He puts the number of digital forensic investigators at well over 20,000.

"I remember back in the early 1990s I had a piece of paper with the names of every one of the computer forensic people," he said. "Now anyone who graduates from college in computer science calls themselves a forensic expert."