

BUSINESS LAW ADVISOR

Computer Forensics

By Ken Silverstein
May 4, 2002

Mission Impossible might need to be renamed if it was airing today. The 1960s hit television show used cutting-edge technologies to crack difficult cases but lacked the type of sophistication now present, specifically computer forensics. The ability to retrieve the digital fingerprints of any electronic information means that justice is better served.

With computers ubiquitous and information stored and moved digitally, forensics has become an essential science. Attorneys and their investigators can preserve almost any information that has ever been stored on a computer, even files that have been ostensibly deleted. It's a service once used exclusively by government investigators trying to crack major cases. Now, its commonplace among corporations of all sizes trying to prevent sabotage, the disruption of personnel records or the stealing of trade secrets.

"Discovery has been changed forever by data technology and recovery technology," says Mark Burge, partner in the firm of Bodoin, Burnside and Burge in Fort Worth, Texas. "It allows attorneys to prove their cases in ways they have not even thought about."

Burge worked a case where his client had been accused of keeping child pornography on his computer – a charge that didn't just jeopardize his good reputation and freedom but also his career and his financial stake in the company that he co-owned. After the initial

accusations, law enforcement confiscated the hardware and began to make its case. With such obscene pictures on his hard drive, it seemed like an easy one to prove.

But was it? The client, who never knew any pictures existed, insisted that it was sabotage. To aid the matter, Burge called in the Dallas-based computer forensics firm TLSI, which worked with police to establish the method and the time that those photographs were placed in the system – a process made more difficult because the hard drive had been tampered with.

But with lots of diligence, the forensics specialist determined that another party had planted the pictures illicitly. Moreover, they had been stored on the hard drive at a time when a major dispute was occurring between two of the firm's principals – one of whom was the accused and the other was the one who had wanted control of the business.

Through a combination of computer forensics and the circumstantial evidence, justice was done. In this case, Burge had represented the accused in a slander and defamation suit where he won \$1.25 million – and a moral victory. “Without the forensics, we could not have proved our case.”

The Science

A computer's operating system writes data and stores it on the hard drive. Hitting the 'delete' key only wipes it off the so-called file application table -- not the hard drive. It can only be permanently erased if the material is “written over” with new information or if a special utility program is installed that prevents it from staying on the hard drive.

With the size of today's hard drives, it is unlikely that any information will be "copied" over.

It's similar to the card catalogue system at the library. The card that details exactly where the information is and what its details contain can be lost but the books and other materials will still remain on the shelves. With the right skills and some detective work, the information can be captured.

Computer forensics is a growing science. U.S. companies spent \$118 million on it in 2000, says International Data Corp., a consulting firm in Framingham, Mass. That will jump to \$277 million by 2004, it says. Lost data is a huge problem, says TLSI, as 74 percent of all companies that have a major or complete loss of data will be out of business in 12 to 18 months.

Most such failures are the result of human error and hard drive failures. But others are the result of theft and sabotage. According to TLSI, only 10 percent to 20 percent of all attorneys are even aware that forensic evidence exists and that it is accessible to clients of almost any means. The cost to recover data depends on the size of the hard drive. But those between 10 gigabytes and 40 gigabytes – most sold in the market place today -- cost generally between \$550 and \$3,000 to analyze, says TLSI.

"Forensics has doubled our business," says John Wiechman, president of TLSI. "It's a matter of self defense for a lot of companies and it's a matter of catching criminals for law enforcement."

California investigators confiscated the computer of a man charged with child molestation and murder in a case now pending in San Diego. The accused had deleted all child pornography from his computer but the data was recaptured by forensics specialists. While the information is circumstantial, it is being used as evidence by prosecutors in combination with other and more direct evidence.

Similarly, investigators often pour through deleted emails in search of incriminating evidence. Deloitte & Touche has a whole computer forensics unit. In a recent case, an employee at a firm it represented had been fired and had demanded severance pay. The client, who argued that no such pay was deserved because the dismissal was for misconduct, turned the computer over to investigators. They found lots of pornography that been downloaded and then deleted. With such evidence in hand, the firm's denial of benefits was upheld.

Far Reaching Implications

To be sure, the field has its shortcomings. Investigations can be impeded or even stopped by new software that prevents data from being held on hard drives after it has been deleted. It's analogous to the criminal that wears gloves to prevent his fingerprints from appearing at a crime scene.

But a more prevalent issue is the lack of experts who know not just how to retrieve information on hard discs but also those who are savvy as to how to preserve and present evidence so that it holds up in court. At present, computer forensic companies are recruiting from the ranks of law enforcement and paying as much as \$100,000 annually.

But the free market will respond. Universities are starting forensics programs and companies are training those with the acumen to succeed. Companies like TLSI train their investigators to go to court and to testify so that judges and juries accept their findings. They further stay on the cusp of forensics methodologies by attending instructional programs for at least 100 hours a year.

Undoubtedly, the field will evolve and have far reaching implications. While it is the high profile cases that are now winning attention, – Kenneth Starr recapturing emails between President Clinton and Monica Lewinsky and the U.S. government preserving old emails within Microsoft to try and prove it plotted to thwart competition – it is the mainstream businesses that will constitute the expansion of this new industry. That growth will no doubt be fueled by lawyers trying to win justice for their clients. In doing so, they will continue to employ a powerful new tool in the court room.