Taking the Byte Out

It was a case that involved hundreds of manhours sitting in front of a computer, staring at a screen covered with computer codes from thousands of files. The investigator was looking for evidence on a juvenile who had set up shop via a computer bulletin board and was suspected of offering downloads of commercial software for a fee. The computer’s hard drive contained 100 megabytes of information, which was considered enormous at the time.

“There were three sets of files on the hard drive: the operating system, the software programs he was selling and all his communications and e-mail,” says Mark Pollitt, the case investigator and unit chief of the Federal Bureau of Investigation’s (FBI) Computer Analysis Response Team. “I had to go through that system by hand, directory by directory, file by file. It took 2 weeks of full-time work.”

Today, hard drives boast not megabytes but gigabytes of information, which could translate into several weeks of work, at a minimum, for an investigator. In addition, criminal cases involving electronic evidence have skyrocketed in the past decade. The FBI alone will investigate well over 5,000 cases this year, compared with a few hundred just 10 years ago. Other law enforcement agencies are in the same boat, investigating an increasing number of crimes involving electronic evidence that range from fraud and hacking to drug crime and child pornography. Investigators, however, are getting some new tools to help them keep pace.

National Software Reference Library

The Office of Law Enforcement Standards at the National Institute of Standards and Technology (NIST), with funding from the National Institute of Justice (NIJ) and working in cooperation with the FBI, the U.S. Customs Service, and the U.S. Department of Defense, has created the National Software Reference Library (NSRL). Recently established by NIST, NSRL will cut investigation time dramatically. Had the library been available nearly a decade ago when Pollitt was investigating his junior hacker, the case probably would have required 2 hours—not 2 weeks—of his time, with the computer doing all the work.

“A 10-gigabyte hard drive might have 50,000 files on it,” says Gary Fisher of NIST’s Information Technology Laboratory and project manager for NSRL. “Somebody has to go through those files for evidence. You may know what’s in 99 percent of the files, but still, somebody has to decide what to look at.

“The database that makes up our reference library gives investigators a set of ‘digital fingerprints’ for operating systems and about 1,000 software applications,” Fisher says. “The investigators can compare what’s on the hard drive of the computer they have seized with the file signatures in our database. What they’ll get is a list of files that don’t match up. Those are the ones they need to look at. The reference library is a tool that can cut an investigator’s time by 25 to 95 percent, depending on the number of files on the hard drive.”

The NSRL Reference Data Set database is available on CD-ROM through NIST’s Standard Reference Data program. There is an annual $90 subscription fee. For more information, log on to www.nsrl.nist.gov or call 301–975–8425.

Computer Forensics Tool Testing

The Computer Forensics Tool Testing (CFTT) project is a NIST/NIJ initiative that also will benefit computer crime investigators. CFTT helps determine the accuracy of computer forensics tools used to investigate or examine information found on seized computers.

According to Susan Ballou, program manager for forensic sciences at NIST, investigators use “imaging” tools to duplicate a disk drive, thereby enabling them to look for evidence on the “copy” without destroying or altering the original. As the number of these computer forensics tools proliferated in the late 1990s, however, defense attorneys, juries, and the courts began to focus more attention on this technology: its accuracy; and its part in investigation, evidence collection, and prosecution.
“How do you know the program you’re using is not altering evidence?” Ballou says. “We were aware of some of the difficulties of these imaging products—that the literature said it would do a certain thing and investigators found out later it wouldn’t, or it would but not to the extent the manufacturer claimed. Some individual agencies tested them on their own. They made up a mock computer system, ran an imaging tool, and then went back to compare the two. That was fine, but when you think of it on a national level, you have no unbiased person or agency testing these tools.”

CFTT is designed to provide a measure of assurance in the results of investigations based on automated tools used in computer forensics examinations. These tools are used not only by law enforcement but also by government and industry to examine electronic evidence. CFTT currently covers three functional areas:

- Disk imaging tools, which copy seized disk drives.
- Write blockers, which prevent the altering of or writing onto a seized disk.
- Analysis tools, which are used to examine information content within seized drives. More areas will be added as funds and capabilities for testing become available.

For more information about the Computer Forensics Tool Testing project, log on to www.cftt.nist.gov or call 301–975–8425.