

DIGITAL FORENSICS:

As computers become an essential part of daily life, they also are increasingly used as accessories to crimes. Digital forensics helps the good guys keep up with the bad guys. / By Melissa Solomon



FIGHTING CRIME ONE BYTE AT A TIME

AFTER 7-YEAR-OLD DANIELLE van Dam went missing from her suburban San Diego home in February 2002, circumstantial evidence quickly led police to her neighbor, David Alan Westerfield. Initially, police were stumped by the motive.

However, when they seized his computer and disks, the police found that motive in the glow of the monitor. There were tens of thousands of pornographic images on Zip disks and CDs.

"It helped tie it up," recalls San Diego County Deputy District Attorney Jeff Dusek, who prosecuted the case along with Deputy District Attorney George Clarke. "The [digital images] explained why a seemingly normal 50-year-old guy, nice neighborhood, why somebody like that would do a crime like this. We think he finally got to the point where looking wasn't enough."

The defense team asserted that it was Westerfield's then 18-year-old son who downloaded the pornography. But experts from the San Diego Regional Computer Forensics Laboratory (RCFL), which helped seize and analyze the digital evidence, showed that factors such as the dates the pornography was accessed and the file-naming conventions pointed to the father, not the son.

That digital evidence helped seal the abduction and murder case against Westerfield.

"I don't understand computers," acknowledges Dusek. "That's why these guys [from the RCFL] are so helpful to us." He adds that in the van Dam case, the RCFL personnel were good witnesses and were able to explain all the computer-related technical details so the jury could understand them.

Closing the Gap

As computers have grown ubiquitous in everyday life and, in turn, criminal activities, the gap in scientifically sound methods to seize, search, preserve and analyze digital evidence has become glaringly obvious in the law-enforcement community. That gap has fueled the lightning-fast growth of the computer/digital forensics field.

"Law enforcement was behind the curve," says David Peters, commander of the University of Illinois at Chicago (UIC) Police Department.

"Technology is second nature to this generation of criminals. But it's very confusing to us old dinosaurs."

To address the problem, in 2003, the American Society of Crime Laboratory Directors recognized digital forensics (the application of science to the process of recovering legally sound evidence from computers, cell phones, video cameras and other forms of technology) as a distinct accredited discipline. Since then, the ranks of experts devoted solely to handling computer evidence have multiplied.

Earlier this year, the RCFL program was selected from a pool of more than 1,000 candidates as one of the top 50 innovations in American government by the Ash Institute for Democratic Governance and Innovation at Harvard University.

"It's a very young science," explains Rick Voss,

A YOUNG SCIENCE

Digital forensics is the new kid on the crime-fighting block, says Rick Voss of the Chicago RCFL.



DIGITAL FORENSICS

director of the Chicago RCFL. "It's the new kid on the block."

Child pornography is the most common type of case handled by RCFLs, but their workloads run the gamut from drugs to public corruption to terrorism, Voss says.

"I don't think there's a crime out there now that doesn't have some form of digital evidence," adds Peters of the UIC Police Department.

New Kid on the Block

When San Diego was hit by a string of bank robberies by the so-called "Gap-Toothed Bandit," the police brought a suspect's computer to the local RCFL. There was no evidence saved on the hard drive, but when the examiner looked in the print spooler and temporary word processor files, he found the demand notes that were used in the robberies.

"You would never think a bank robber would use a computer to write his demand note," says Assistant U.S. Attorney Mitch Dembin, cybercrime coordinator for the Southern District of California.

But they do. Drug dealers keep electronic ledgers, rapists e-mail their victims and murderers research their crimes on the Web. Digital forensics has been used in such recent high-profile cases as the Laci Peterson murder and the BTK serial killings.

As recently as the late 1990s, law-enforcement agencies were ill-equipped for the daily technology investigations they were facing, says Dembin. "The criminals were using computers, and we were not prepared to investigate them," he recalls.

Dembin, who had been prosecuting computer crime cases for the U.S. Attorney's Office since 1991 and taught a class on electronic evidence, knew what was needed: a central facility with experts who



EDUCATION IS KEY

To stay in the crime-fighting business, you need a lot of training, says David Hudspeth, a Chicago police sergeant.

knew not just how to find digital evidence, but how to satisfy legal authenticity requirements proving that the data had not been manipulated. "It is a very expensive proposition to have a

true forensic capability," he says.

Dembin convinced the San Diego agency heads to go along with his plan to pool efforts and create a cross-agency regional computer forensics facility. He didn't ask them for money. Instead, he asked for one employee from each agency who could be trained to work as an examiner at the new facility.

The FBI donated old office space and loaned trainers, the examiners requisitioned furniture from their host agencies, and a grant funded computers and equipment. When the San Diego RCFL opened in January 1999 then-Attorney General Janet Reno went out to christen it.

"We were instantly inundated with cases,"

Preparing America's Finest

Each year, the Regional Computer Forensics Laboratories train hundreds of law-enforcement professionals from their regions to examine digital evidence on their own and to work with the RCFLs.

The training and services provided by the RCFL are invaluable, says David Peters, commander of the University of Illinois at Chicago Police Department. It could cost up to \$100,000 to train one officer to the level of a certified computer forensics examiner, and the technology and information are changing at such a rapid rate that they can be out of date in six months, he says.

"To get to the point where you can extract evidence, preserve it and present it in court is a very costly proposition," Peters says. "Departments can't afford this, but you

can't ignore what's going on in the world."

"Not only does the technology change, the laws and rules also change," adds David Hudspeth, a Chicago police sergeant on a two-year assignment as an RCFL examiner. "If you want to stay in this business, you've got to do a lot of training."

It costs about \$60,000 in software, hardware, background investigations for top-secret clearance and education (nine to 12 months of training) to prepare an examiner, explains New Jersey RCFL Director Larry Depew. So he asks for at least a two-year commitment from examiners, who are paid by the agencies that assign them to the lab.

There are 18 examiners at the Chicago lab. Some are FBI employees, and others have been detailed from various federal,

state and local agencies. They include officers and civilians, IT experts, police sergeants and administrative professionals.

While all officers are trained in Microsoft Windows, there are also experts in specific types of technology, such as personal digital assistants, Apple computers, Linux and video enhancement. "Computer forensics is getting to be a team sport," says Hudspeth. "Everybody can't know everything."

The mix of backgrounds and skills makes the lab network more effective, adds Rick Voss of the Chicago RCFL. "It's that synergy that works because the person who has the extensive law-enforcement background sits next to the person who has 20 years of experience in IT," he says. "There's a lot of collaboration and discussion."

Dembin recalls. "And success bred other successes."

From its inception, the San Diego RCFL received national praise for its work. But on Sept. 11, 2001, digital forensics became a matter of national security.

"When you have a large event like Sept. 11, you wind up with a glut of digital evidence, and you've got to be able to get the key information out," Voss says.

If a person were to take a 100-gigabyte hard drive and fill it with text documents, it would produce about 4,000 boxes of paper, he explains. A terabyte is 1,000 gigabytes. Sept. 11 produced multiple terabytes of data from police departments, airline companies and others. How do you begin to mine the important stuff? Voss says the term used to describe that dilemma is data glut/information famine.

The San Diego and North Texas RCFLs helped sort and categorize that data, and the administration took notice. The USA Patriot Act of 2001 allocated funding to build three more RCFLs, and additional ones followed soon after. At press time, nine RCFLs were in operation across the country, and five are planned for 2005 and 2006.

Measuring the Value

The value of digital forensics is threefold, according to law-enforcement professionals.

First, computer forensic examiners are trained to look for digital evidence that might otherwise go unnoticed. They use software to run keyword searches and sort endless amounts of data on hard drives. They can recover deleted files, find registry data, restore video images, expand photo frames and analyze cell phones.

Examiners can help investigators plan their searches. They can advise them on what equipment can be accessed, how invasive a search can be and how long equipment can be kept within the legal boundaries of search warrants.

The examiner may even go with the investigator to seize equipment. RCFLs have transportable storage area networks that can hold approximately eight terabytes of data, so if investigators can't remove evidence, they can copy it on the scene.

A second factor that makes digital forensics so valuable is that it preserves data exactly as it was found, so the integrity of the evidence isn't compromised. Just turning on a computer can destroy evidence, because hundreds of files are altered when a computer boots into Microsoft Windows. Files can be accidentally deleted, or the dates they were last modified can be changed, leaving law enforcement with little ammunition to refute the "I was framed by investigators" defense.

Digital forensic examiners remove hard drives from computers and image them in a forensically sound manner without ever turning them on. An algorithm ensures with mathematical certainty that

New Jersey Joins the Team

The video frame on the computer doesn't look like much of anything—just darkness with some grey shades. But later in the video, a light flashes and someone runs past the camera.

"It's extremely poor quality," explains Ray Salapka, a certified computer forensic examiner assigned to the Regional Computer Forensic Laboratory in Hamilton, N.J., who's extending his certification to become a video forensics expert. "It's 15 minutes before dawn."

Salapka, a civilian specialist employed by the FBI, is trying to enhance the video to find clues in an open arson investigation. He is one of the 22 examiners who have been assigned to the New Jersey RCFL from local, state and federal agencies since it opened in November 2004.

The New Jersey RCFL has Attorney General Peter Harvey to thank for its existence, says Larry Depew, an FBI supervisory special agent who directs the lab. After watching the digital work that went into the Sept. 11 investigation, he decided to compete for a local RCFL. He gave free office space and offered to cover much of the build-out cost.

The investment seems to be paying off. In 2003 and 2004, the New Jersey State Police and FBI together handled about 340 computer cases. Between the time the RCFL opened in November 2004 and August 2005, the RCFL handled 450 cases—more than the two agencies did in the previous two years.

Nevertheless, Depew notes that there are three major challenges the RCFL faces.

One is bringing together agencies, many of which are unionized, with different work methods and rules. But since everyone at the RCFL is a forensic examiner, they share interests as well as differences.


The sheer volume of work coming in poses another challenge, he says. RCFL cases must be high quality with measurable and repeatable outcomes, but that can conflict with time-sensitive cases.

Third, there's a technical challenge due to the capacity required to acquire and analyze the evidence. Examiners are constantly faced with new hardware devices, software applications and storage devices, Depew explains. "But people who come into this line of work persevere," he says. "They won't quit."

the data on the duplicate is an exact replica of the original. The original then goes into a tamper-proof bag in the evidence room and is preserved in the state in which it was found. "We're never going to touch that if we don't have to," Voss says.

The third valuable aspect of digital forensics is that examiners can serve as expert witnesses at trials. They can refute defense experts, advise prosecutors on technical aspects and explain complex technical details to juries in layman's terms.

One concern voiced by Assistant U.S. Attorney Dembin is that the use of encryption by criminals will become widespread, making it harder for law enforcement to access data related to crimes.

Despite this caveat, technology continues to benefit law enforcement. "I'm happy to see that we are keeping pace with criminals," Dembin says. 

You can find this issue's stories, plus past *StateTech* editorial content, at STATETECHMAG.com

