



Takedowns: Legendary Successes in Computer Forensics

by Sharon D. Nelson and John W. Simek

Take•down (tāk'doun') *adj.* Sports. A move or maneuver in wrestling or the martial arts in which a standing opponent is forced to the floor.

—*American Heritage Dictionary of the English Language
Third Edition*

“Takedown” has had a new meaning since the publication of the book by the same name in 1996. The story of infamous hacker Kevin Mitnick, told by the hacker/hunter who finally found him (Tsutomu Shimomura) was a “takedown” heard around the globe. Forever after, “takedown” has developed another meaning—it’s a “gotcha” for computer forensic technologists when they find the pivotal electronic evidence that will bring a hacker or other criminal down.

Computer forensics has become quietly pervasive in the world of law enforcement. Though it is not always front and center in media reports, many of the most notorious cases of our times have hinged on electronic evidence. Here are some of the most highly publicized cases in forensic folklore.

Oliver North—Colonel Oliver North set out to conceal his involvement in the Iran Contra affair, doggedly shredding all pertinent papers and deleting all relevant e-mail. Unbeknownst to North, all his diligence was in vain because the government was using IBM’s Professional Office System (PROFS) and the mainframe support personnel were backing up his e-mail. All the incriminating e-mails were recovered. Gotcha Ollie.

Though Colonel North was convicted of accepting an illegal gratuity, aiding and abetting in the obstruction of a congressional inquiry, and destruction of documents in 1989, the conviction was overturned on appeal because immunized testimony had been used in his trial.

Robert Hanssen—A bizarre combination of low and high tech, the American spy and FBI counterintelligence agent Robert Hanssen favored old-fashioned mail drops to communicate information to his Russian handlers. In February 2001, he was arrested in Vienna,

Virginia, while in the process of making a drop in exchange for a \$50,000 payment. The arrest culminated a four-month FBI investigation in which the agency said it used “computer forensic analysis, substantial covert surveillance, court-authorized searches and other sensitive techniques.” Though the precise nature of the surveillance remained murky, reports suggested that the FBI had received court authority to monitor Hanssen’s computer usage, as well as to intercept his cell phone calls and to place a wiretap on his home and office phones.

Hanssen had some technical bona fides. According to an affidavit filed by the FBI, Hanssen used encrypted disks, flash memory cards and even a Palm Pilot to pass secrets to his Russian handlers. He could also program in C and Pascal, according to the *Washington Post*, which added that the “technologically sophisticated” Hanssen created a system to automate the teletype at the FBI’s Washington offices. *USA Today* reported that Hanssen hacked into the computer of the FBI’s top Russian counterintelligence officer in the early 1990s. Ironically, FBI logs showed that Hanssen surfed the FBI computers for references to his name in ongoing investigations.

In July 2001, he pleaded guilty to charges that included conspiracy to commit espionage, 19 counts of espionage, and one count of attempted espionage. Hanssen is currently serving a life sentence without possibility of parole, under a plea agreement in which he pledged full cooperation with authorities.

Wen Ho Lee—Though computer forensics was at the heart of this case, in the end what was not known was as fascinating as what was. It was undisputed that Los Alamos scientist Wen Ho

See Takedowns, continued on page 45

Takedowns, *continued from page 42*

Lee had copied certain computer tapes and that they contained information related to building nuclear weapons. Over 40 hours on 70 days in 1993, 1994 and 1997, Lee downloaded 1.4 gigabytes of data, the equivalent of about 400,000 pages, from the secure computer system at Los Alamos. Often working on nights and weekends, and circumventing security safeguards, he moved the data to his office desktop computer and to pocket-sized tapes that look like 8-mm videocassettes, a bit thicker than conventional audiocassettes. He then made copies of some of those tapes.

Lee maintained that the tapes copied were “crown junk” and not a “crown jewel.” He said he made the tapes for fear of losing material, although all manner of backups and keystroke logging are available at Los Alamos.

Lee claimed he threw approximately 17 tapes in a trash bin outside the lab in January 1999, after his security clearance was revoked. Although the FBI had this information in September of 2000, it unaccountably waited several months before searching the landfill where the laboratory dumps its garbage. Ten tapes were found in the New Mexico landfill, some of them crushed, but forensics specialists were able to recover much of the data on the tapes. After the entire hullabaloo, it turned out that the ten tapes were unrelated to the case. The tapes have never been found.

Ultimately, Lee admitted he had erased classified files that he had transferred to unclassified computers and removed secret data from three tapes that were later found in his office. He never acknowledged engaging in espionage, but said that he entered into a plea agreement because there was a 5% chance that he could be convicted, and he did not want to take that risk.

On September 13, 2000, the government dropped 58 of the 59 charges against Lee and he was sentenced to the nine months he had already served, and given his freedom in exchange for his cooperation with authorities. What emerged clearly in court proceedings was a bungled investigation—upon freeing Lee, U.S. District Judge Jim Parker took the unusual step of apologizing to Lee and sternly reprimanding the U.S. government for the conditions under which he was held.

Larry Ellison—Oracle employee Adelyn Lee won a \$100,000 out-of-court settlement against Oracle President, Larry Ellison, after claiming that she had been fired for refusing to have sex with him. Ellison’s often-colorful behavior made the scenario seem plausible. He was an easy target. There had in fact been an off-again, on-again romance between Ellison and Lee and it was undisputed that she was terminated five days after their last date.

See Takedowns, continued on page 46

Takedowns, *continued from page 46*

One of the compelling pieces of evidence was a 1993 e-mail from Lee's boss, Vice President Craig Ramsey, to Ellison, confirming that Lee had been terminated at Ellison's request. Electronic records revealed that Ramsey could not have sent the e-mail because he was driving (according to cell phone records) at the time that the network recorded the e-mail transmission. As it turned out, Lee knew Ramsey's passwords and sent the e-mail herself. In 1997, she was convicted of felony perjury and the falsification of evidence.

Kevin Mitnick—Few Americans have not heard the name of the world's most famous hacker. "Free Kevin" t-shirts and Web sites proliferated at an astonishing rate during the height of Kevin's fame. As is so often true, the real Kevin wasn't much of a hero. Mitnick had a problem distinguishing between simple concepts of right and wrong. Breaking into other people's technology for his own self-interest was something he continually justified. If he wanted free phone time or free computer time, he used his technical skills to trespass on other people's technology and stole it. His rap sheet lengthened over time.

As a teenager, he was a phone "phreaker" making free long distance calls before Pacific Bell caught him stealing computer manuals. He was placed on probation. Mitnick first came to national attention in 1982 when he hacked into the North American Aerospace Defense Command (NORAD). Remember the movie "War Games?" Kevin Mitnick was the inspiration for that movie.

During the 80s, Mitnick also took control of three central telephone offices in New York City and all the phone switching centers in California. In 1989, he was charged with computer fraud and possession of unauthorized access devices that he used to hack into MCI and Digital Equipment Corp., from whom he lifted \$1 million in proprietary software. He was sentenced to and served a year's time. A series of arrests ensued over the next several years and he served two more prison stretches. In 1991, he violated probation by hacking into voice mail systems at Pacific Bell. The government got a warrant for his arrest in 1992, and Mitnick became a fugitive on the run.

Mitnick went behind bars again in February 1995 on a 25-count indictment that included charges of wire fraud and illegal possession of computer files stolen from such companies as Motorola and Sun Microsystems. His arrest followed a national hacking spree that finally earned him a spot on the FBI's most wanted list. During the 2 years preceding his arrest, he hacked into computers, stole corporate secrets, scrambled phone networks, and broke into the national defense warning system. During his years on the run, when he adopted the moniker "Condor" from the Robert Redford film "Three Days of the Condor," he allegedly hacked into computers at Motorola, Nokia Mobile Phones, Fujitsu, Novell, NEC, Sun Microsystems, Colorado SuperNet and the University of Southern California. Damages were estimated to be as high as \$80 million. He was finally found, not by the government, that he successfully eluded time and again, but by computer savant Tsutomu Shimomura. Mitnick finally made a mistake that would prove fatal.

He arrogantly broke into Shimomura's home computer network, taunting a man whose skills proved to be more formidable than Mitnick may have imagined. Shimomura, then a security specialist at the San Diego Supercomputer Center, had originally declined to assist authorities. But when Mitnick broke into Shimomura's system, he was infuriated by the intrusion and resolved to find him.

Mitnick had stashed some of his data in a dormant account at *The Well*, an on-line forum with 11,000 subscribers, some of whom were well known Net activists. A technical manager there noted a possible hack into the company's systems. The owner of the dormant account recognized one of the e-mail addresses as belonging to Shimomura and noted that the data that had been stashed included serious software hacking tools.

Working with the FBI, Shimomura determined that the hacker was probably Mitnick and that he was making telephone calls with a cellular modem to a Netcom phone bank in Raleigh N.C. The calls were intricately looped from a GTE Corp. office to a Sprint cellular phone switch in such a way that neither company could identify the caller. Shimomura and the investigative team were able to narrow the location to somewhere near the Raleigh-Durham International Airport.

How did they do that? Part of a cellular transmission is an "electronic serial number" of the originating device. The investigation involved searching the communications logs for the ESN and phone number of the caller. The phone number was not assigned to any entry in the cellular databases. By first checking the logs for the phone-switching network and searching on the phony number, it was determined that the call was coming from the Raleigh-Durham area. After determining the switch, each cell attached to the switch was checked to determine the appropriate cellular cell that was receiving the appropriate ESN that was associated with the bogus number. Arriving in Raleigh, Shimomura, Sprint technicians and the FBI used cellular frequency detection devices to find Mitnick. Armed with the ESN/phone number combination, the hunt was on. Monitoring hardware can track the transmission signals and determine the ESN "tag" associated with the communication session. The detection equipment senses the strength of the signal. Basically, the team drove around in the area until they had a "fix." Mitnick was found and arrested in a nondescript apartment complex, where he was arrested. At precisely the same time as the surveillance team was closing in on Mitnick, technicians at *The Well* recorded the last unauthorized intrusion into their network. *Takedown*.

Mitnick ultimately signed a plea agreement and was released from prison on January 21, 2001, after being incarcerated for five years. He is prohibited from using a computer and from acting as a consultant or advisor in computer-related matters until January 20, 2003. ☞

(To be continued . . . Next: "What is the ComputerForensic Process?")