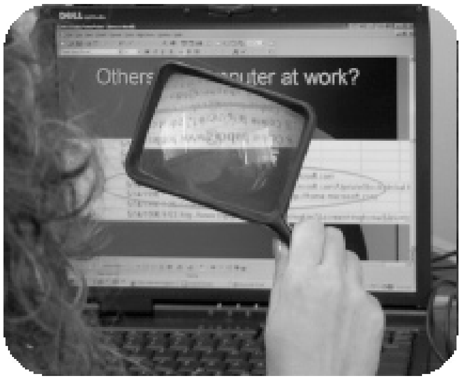
THE Institute

October 2001 Volume 25, Number 10

High-tech Sleuthing: Following Digital Trails

BY KATHY KOWALENKO
Editor, The Institute

Digital documents that were once thought to have disappeared by hitting the delete key or dragging them to the trash box could now end up as evidence in criminal or civil matters. Finding these documents is the job of IEEE senior member, Dr. Gordon Mitchell, a computer forensics expert and the founder of Future Focus, Woodinville, Wash., USA.



SOURCE: JAMES HANKARD

In a recent case, Mitchell helped prosecutors weave together clues found in an employee's office PC to convict the employee of killing his wife. Mitchell was able to provide testimony on what his company uncovered about the employee's Internet searches. The Internet search trail connected the employee to the location of the body and his preparations for the killing.

"The most hard-to-believe one was a search that was done for 'kill spouse,'" Mitchell said. "It's possible this is the first murder case where substantive evidence came from a machine," he noted. The employee was sentenced to 46 years in prison.

Mitchell admits this is one of his more unusual cases. He says he typically works with commercial clients who suspect employees of embezzling company funds, stealing intellectual property or issuing death threats. Individuals also have retained him when they suspect household employees of making unauthorized purchases or visiting inappropriate sites on their home computers. Not all of his work leads to criminal or civil action; employees might be simply disciplined or dismissed.

Computer forensics on the rise

U.S. companies spent US$118 million on computer forensics and other incident response services in 2000, and are expected to more than double that to US$277 million by 2004, according to International Data Corp., Framington, Mass., USA.

A forensics expert must have the "investigative skills of a detective, the legal skills of a lawyer, and the computing skills of the criminal."

The use of computers for criminal activity has become so pervasive that last November, the U.S. FBI dedicated the nation's first regional forensics laboratory in San Francisco, Calif., USA, devoted to interagency cooperation in gathering and assessing evidence from computers. Among the skills being taught at the lab are how to remove evidence from a computer without damaging the files, how to find ways around firewalls and secret passwords, and how to remove evidence from a computer without disabling it.

"There is a critical need for this all over the country and all over the world," said former FBI Director Louis Freeh at the lab's dedication.

Computer forensics is becoming a hot field for those desiring to become cyber sleuths. The 2nd Annual IEEE Systems, Man, and Cybernetics (SMC) Information Assurance Workshop, held in June and sponsored by IEEE SMC and the U.S. National Security Agency, conducted a session on "Policies to Enhance Computer and Network Forensics."

According to the conference proceedings, a forensics expert must have the "investigative skills of a detective, the legal skills of a lawyer, and the computing skills of the criminal."

The session covered such issues as how to retain information, establish and train a forensics team, formalize the investigative procedure and protect evidence.

Retaining information

Mitchell uses specially designed computer hardware running software that is not commonly used. This enables him to discover information on computer hard disks that is concealed from MS Windows utilities.

"It is critical that these investigations use forensic techniques that are designed to gather evidence from the computer hard drive without altering its contents," he explained. "Just turning on the PC will change files that are on the hard drive."

This can corrupt evidence, overwrite files and possibly wipe out critical portions of the hard drive. Normal backup techniques do not catch the important information that may lie in allocated clusters or deleted files.

According to Mitchell, if users delete files intending to cover nefarious activity, they will often leave traces. He can frequently find evidence in files that have been deleted and see information concealed in pictures, system files and mislabeled files. "We also try to knit together clues that are found in the computer -- that might be information in a history file connected with a fragment of a document that is still on the hard drive."

Privacy concerns

According to the American Management Association, 45 percent of large U.S. companies electronically monitor their workers, up from 35 percent three years ago.

What Mitchell is doing is perfectly legal because he is examining property that belongs to a client. Under U.S. federal law, companies have an almost unfettered right to monitor anything workers do on company-owned equipment.

"Privacy issues are something that are really important to us. We are not there sneaking around in the dark, looking at people's private stuff," said Mitchell. "We will never work on a computer except for the owner of the computer. We will never violate someone's privacy, for example, by having a company send us to the employee's house and snoop on their home computer."

Proves innocence as well as guilt

Computer forensics not only catches wrongdoers, but can also clear employees who are innocent.

"As often as not, we are able to exonerate employees without anyone doing an interview or something else that would cast suspicion on them when they really haven't done anything wrong," explained Mitchell. "This is very important. The computer is a more direct, practical, humane way to do investigations of important issues."

For more information about the IEEE SMC Information Assurance Workshop, visit "http://www.itoc. usma.edu/Workshop/2001/ Workshop2001.htm".

URL: http://www.spectrum.ieee.org/INST/ti.html (Modified:2001-September 30 1900 GM)