Computer forensics

Abstracted to a series of ones and zeros, digital information seems elusive and easily hidden. Yet each time it is stored, read, written, transmitted, or printed, data multiplies promiscuously. Solving computer crime can often be a simple matter of tracking down concealed or forgotten copies of incriminating digital information.

Computer forensics, once specialized, is now mainstream due to our total dependence on data. Experts deal not only with computer-related crime, such as hacking, software piracy, and viruses, but also with "conventional" crimes including fraud, embezzlement, organized crime, and child pornography.

The term "computer" extends beyond desktops, laptops, and pocket computers. It applies to anything containing a microprocessor. Cell phones, fax machines, cameras, video recorders—even washing machines—contain chips to process and store data records. All of them are potential sources of evidence.

Where is that smoking gun?

However, the majority of computer crimes concern conventional PCs. An aid to investigating these crimes is the inherent insecurity of computer hardware and software. For example, deleting a file does not irreversibly remove it from the hard disk. "Deleting" simply changes the file's name, to hide it from the user.

Data that will not die

Sophisticated criminal computer users are aware of the security loopholes, and use encryption and more secure deletion programs to hide incriminating data.

All computer operating systems use virtual memory to speed programs up. Storing data in RAM (on-chip random access memory) makes software very responsive, but RAM is a scarce resource. The computer's operating system makes RAM work harder by constantly swapping rarely used data from RAM on to a hard disk, which is slower but has a greater storage capacity. This process creates a "swap file" containing as much data as the computer's installed RAM—usually enough to hold the text of 200 novels.

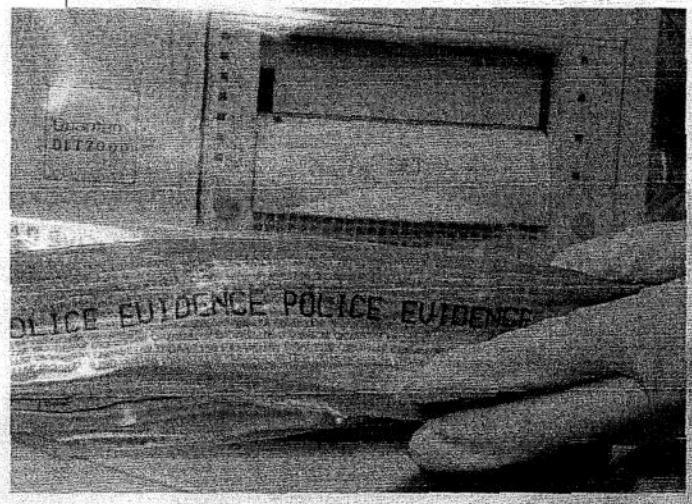
When a file has been securely deleted, its contents may persist in the swap file. However, it does not remain there indefinitely. Each time a computer is switched on and used, new data replaces some of the old contents in the swap file.

This presents the investigator with an interesting problem: evidence may exist on a computer's hard disk, but simply switching the machine on might be enough to erase it.

Fortunately, there is a simple solution. With specialist equipment, it is possible to completely duplicate the contents of a computer's hard disk without switching the suspect machine on. Investigators can then examine files on the copy without running the risk of destroying data on the original. This approach has a secondary advantage—working on a copy avoids

TYPES OF COMPUTER CRIME:

1. *Software piracy—when computer programs are illegally reproduced and sold.*
2. *Hacking—unauthorized computer access and sabotage, either mischievously or maliciously.*
3. *Computer fraud deals with assets—for example, illegal bank transfers and credit card transactions.*
4. *Computer forgery involves creating false documents using computers, such as laser-printed checks.*
5. *Incidental use of computers in the course of other crimes.*



SEALED AND PROTECTED ▲
When investigators seize computers, they must treat them just like any other physical evidence. Careful storage and documentation is essential to avoid defense challenges when a case comes to court.

DELVING WITHIN ▲
Forensic investigators dismantle and study seized hardware. They identify and photograph each component part before examining the stored data.

DIGITAL DATA ▲
As well as recovering data, investigators often have to reconstruct the operating system and programs to untangle digital evidence.

BOUNCING DISKS ▶
Computer hard disks, such as this one, can be remarkably resilient. Even throwing a computer from a second-floor window may fail to damage the data.

accusations of evidence tampering. It also allows a third party, perhaps an expert working on the suspect's behalf, to repeat and verify any steps that investigators take to recover deleted or encrypted data.

Internet fraud

Controlling cyber-crime presents investigators with a completely different set of problems. In addition, financial institutions are coy about revealing that they have been the victims of cyber-fraud. Even when they do, tracking down the perpetrators is not easy, as one of the few large cases to be made public illustrates. In 1994, computer hackers broke into the supposedly secure network of the world's largest bank, Citibank, and stole more than $10 million. The thieves used a modem to dial up and gain access to Citibank's payment network, but tracing the rogue calls was far from easy, since the transactions were completed so rapidly. In the end, investigators traced the mastermind of the operation, Russian Vladimir Levin, partly from telephone company records, but also by monitoring the bank accounts into which the stolen money had been electronically transferred. When one of the cyber-gang tried to cash a multi-million-dollar check, he was arrested, and helped police in exchange for a lighter sentence.

"Follow the money"

This combination of cyber-sleuthing and tracing financial transactions has also paid dividends in tracking down criminals who use the Internet to exchange pornographic images of children. For example, in spring 2002, British police used special software to monitor Internet chatrooms used by members of a pedophile ring. However, the suspects were eventually identified from credit cards, used to pay for access to child pornography websites.

Encryption

Criminals may use encryption to try to cover their tracks in computer crime. But, until recently, the commercial password-protection programs they could use offered very weak safeguards against even moderately knowledgeable investigators. Strong encryption is becoming more widely available, but ironically, this may provide little help to cyber-criminals. Whether sent over the Internet as emails or stored on a hard disk, encrypted data has an eye-catching signature that shouts "suspicious." Using encryption can be tantamount to an admission of guilt.

CASE STUDY

In early May 2000, millions of computer users opened an email headed "I Love You" and got a nasty shock. The message emailed itself to every contact in their address books. By multiplying explosively, this "Love Bug" brought the Internet to a standstill. Investigators found the word "Barok" in the virus code. This word had also appeared in a less damaging virus four months earlier—along with the claim that its author was studying at AMACC, a computer college in the Philippines. The school confirmed that a student, Onel de Guzman, had submitted a similar program as a term paper shortly before dropping out. Manila police raided his apartment and found disks that proved he was one of the authors. However, at that time, the Philippines had no laws against computer hacking. By June, new legislation had been introduced, but it was too late to apply to the "Love Bug" case. So the author of the most destructive virus ever written escaped unpunished.

◀ ONEL DE GUZMAN
24-year-old Onel de Guzman denied authoring the virus, but said he may have released it by accident.