Computer forensics tips help you monitor investigations

Aug 6, 2002
Michael Jackman

Businesses today are all too vulnerable to high tech crime. PriceWaterhouseCoopers reported in June 2002 that 78 percent of the companies it surveyed had experienced a security incident and that 27 percent of the companies it surveyed had no plans to deal with security problems. Meanwhile, the average cost of a security incident in the U.K. was $50,000. The situation in the U.K. is typical for most of the industrial world.

The scope of the cybercrime problem is enormous. White-collar crimes aided by technology include identity theft, fraud, blackmail, bribery, counterfeiting, corporate espionage, and embezzlement. Employees use company computers to download porn, pirated software, and data; to hack other businesses' systems; and to steal corporate secrets.

Whether computers are used to commit felonies or simply to violate company policies, businesses can be inconvenienced, embarrassed, or even shut down. Given this situation, IT managers need to know something about computer forensics—the science of investigating computers for evidence. This brief introduction will give you the basics to understand what makes a valid computer investigation.

Investigation options

IT managers have three options if they think a crime or violation has been committed with a company computer:

- Ask for assistance from law enforcement. Many state and city police forces have established computer forensics units. Their trained investigators are often ready to assist businesses.
- Hire a forensics specialist. Companies such as Diogenes LLC have trained investigators aware of the many subtleties involved in cybercrime investigation.
- Train an in-house incident response team. Whether the goal is obtaining information, pursuing company discipline, or preparing for legal action, staff must know how to create a valid chain of evidence and how to avoid tampering with evidence.

Forensic tips

The worst thing a business can do is to proceed carelessly when investigating its machines. Keep these tips in mind when a computer is being investigated on your watch.

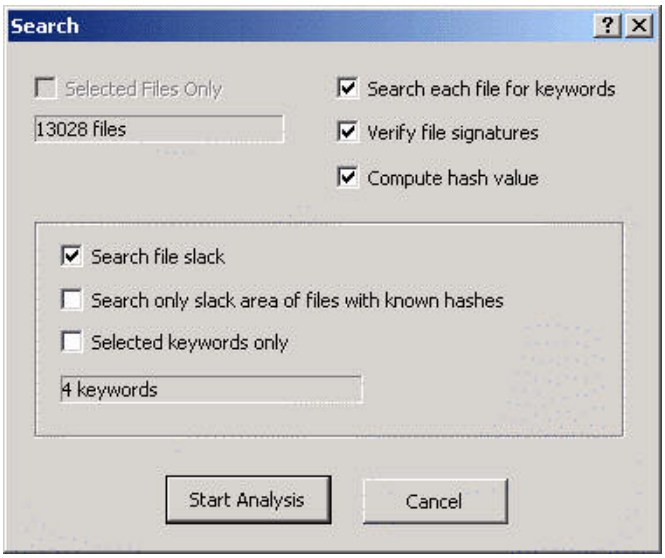
1. A computer is a crime scene, and it needs to be treated as such. All investigation activity needs to be logged and all the equipment inventoried.
2. The machine should be isolated from the network.
3. Investigators should almost never work with the original hard disk or media or any original files. Rare exceptions to this rule include situations when turning off the computer will destroy evidence. But most often, examiners should make copies—and not just any copies, but forensically sound ones, called clones or bit stream images. Just backing up a drive, for example, will not transfer slack space and deleted files that need to be searched.
4. Don't violate the chain of custody. If evidence is to be used in a legal case, it must be clearly established what the evidence is, where the evidence was, and what was done to it at all times. If there's any suspicion that the evidence was tampered with or altered, then you may be left without a case.
5. Don't be in a fixed frame of mind. No two investigations are alike. Because of this, investigators use training and experience to narrow the scope of an investigation.
6. Don't digress. Remember that the point of an investigation is to determine three things: whether a violation took place, the exact sequence of events that took place, and finally, who was responsible.

What investigators will do

You'll want to know if your forensic examiners are reliable. During an investigation, you can expect competent, trained examiners to do the following:

- **Use approved forensics tools**. The courts recognize certain tools to be reliable, such as Guidance Software's EnCase or Access Data's Forensic Toolkit.
- **Create a hash file**. Hashes are like fingerprints of the original data. It's accepted in court that if the hash value of the original matches the hash value of the copy, then (a) the copy is valid and (b) the original has not been tampered with since the copy was made. Hash files are also used to determine whether a perpetrator altered system binaries or other data. Even if a perpetrator was savvy enough to change the access time, size attribute, and checksum of a program, the hash values will not match a pristine version of the same program.
- **Perform noninvasive searches of files, unallocated drive space, slack space, and swap files**. Forensic tools will not alter data or file attributes. These tools can be used to search files, unallocated hard drive space, and slack space (see **Figure A**). Slack space is the space between the end of a file and the beginning of the next cluster on a hard drive. It contains remnants of previous files that occupied that cluster but were deleted or moved. The Windows Swap File is often a goldmine of file fragments.

Figure A



Accepted forensic tools such as EnCase provide the means to create hash files and search for keywords in files and in the slack space.
Search temporary files, logs, and other traces used by operating systems. Investigators use these methods to track and safeguard user activity.

Tricks of the trade

Incident response staff will need to understand the tricks used to thwart investigators and hide evidence. These tricks might include:

- Hiding data within files, such as .gif and .jpg pictures, a practice called *steganography*.
- Altering filenames and extensions to disguise evidence as innocent files, such as renaming a pornographic .jpg to gotmail.wav.
- Hiding files in unlikely places.
- Using Zero Link files (in Unix) that don't associate with any directory.
- Modifying operating system utilities so that certain data is not listed or found during keyword searches.
- Sabotaging a computer so that, if it is investigated, a logic bomb will be triggered. Saboteurs also give hostile programs friendly names such as find.exe.
- Erasing files or disk space with file shredding utilities.

These techniques represent just some of the tricks investigators are up against. Don't wait until an incident has happened—create an incident response procedure now and invest in training and tools. If you wait for an incident to happen before acting, your company (and your reputation) will be damaged. In the meantime, these tips will help you determine whether an investigation is being conducted professionally.

Additional resources

Web sites

- High Technology Crime Investigative Association—This organization accepts members from law enforcement, corporate management, and corporate security staff. However, anyone may download its newsletter containing forensic tips and information. The June 2002 issue, for example, contained tips on how to recover deleted Outlook e-mail by corrupting and then rebuilding a copied Outlook .pst file.
- LC Technology International, Inc. makes sophisticated data recovery tools and provides forensics training and investigative services.
- The Department of Justice offers guidelines for searching and seizing computers.
- SecurityStats.com provides digests of the latest statistics and analyses relating to computer security. These stats will help you justify a forensics budget to cover equipment, staff, and training.
- The Department of Justice Cybercrime Web site has news, articles, and other information.
- New Technologies makes software and offers computer forensics articles that are a model of clarity.

Books:

- *Computer Forensics: Incident Response Essentials*, by Warren G.Kruse, II and Jay G. Heiser.
- *Hacking Exposed: Network Security Secrets and Solutions*, by Stuart McClure, Joel Scambray, and George Kurtz.
- *Hacking Windows 2000 Exposed*, by Joel Scambray and Stuart McClure.