Computer Forensics

“Forensic data recovery can be a costly and time-consuming process.”
by Pete Choppin

Most of the time, computer problems are relatively minor—at the worst, hard drive crashes result in lost data, including pictures, spreadsheets and all-important client databases. Sometimes, though, data loss is more important.

To an individual user, perhaps, the loss of pictures and spreadsheets can be a serious problem. However, the science of computer forensics deals with the legal concerns of data that can be critical to the survival of a company.

In IT, we are talking about protecting the interests of the company, and it can involve litigation and criminal trials. If you find yourself needing forensic data recovery, it can be a costly and time-consuming process.

Why Use Forensics

Forensic data recovery isn't for everyone, obviously. If your home or business drive crashes and you need the data back without reconstructing it, a normal data-recovery service is by all means precisely what you need. Your IT department may even be able to recover that data without having to use outside sources.

If, however, you need to preserve the integrity of the data for legal reasons, or if you need to find out if a drive has been illegitimately tampered with, forensic data recovery is the only way to ensure that any information gained through the recovery process will hold up in a court of law. A knowledgeable lawyer will cut down any evidence presented without a full chain of custody report, and you may even need an expert witness to testify. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

Case in Point

A perfect example of computer forensics happened where I work. A former employee, who left on not-so-happy circumstances, began making threats about handing over proprietary information to another competing company. Because there was a non-compete contract in place, which he signed during his employment, this would mean he was breaching the contract and there was legal cause to not only prevent him from sharing the information to another company, but also to begin an investigation of the data to which he had access.

If we used our standard data recovery, the information we could retrieve would not be enough to stand up in court. By using e-discovery and systematically using computer forensics, the evidence was complete with a chain of custody and an explanation of what had to be done to retrieve the data. We were able to build a much stronger case. Even if the data isn't recoverable, a forensic data-recovery lab can prove that our employee purposely destroyed his e-mail, which is enough to end a case in many situations.

E-Discovery

E-Discovery refers to a legal process of finding or *discovering* information that is only available electronically. Electronic information is different from paper information because of its intangible form. Also, electronic information is usually accompanied by metadata, which is not present in paper documents, but plays an important part as evidence in litigation.

Examples of the types of data included in e-discovery are e-mail, instant messaging chats, documents, accounting databases, CAD/CAM files, Web sites, and any other electronically stored information that could be relevant evidence in a lawsuit.

How Does It Work

Most of the time, forensics cases don't involve physically damaged drives, but rather drives with deleted files or the like. The forensics company will make a clone of the drive, and then work on that clone for the remainder of the process; this ensures that there is no chance of losing any information from your original drive. Using a large number of programs, the company will analyze key files created by the operating system to reconstruct what a person used the computer to do.

Forensics experts can also undelete files in many situations if the hard drive used Windows formatting, retrieving key pieces of evidence such as e-mails or Microsoft Office documents. This is because files deleted in Windows aren't actually destroyed; the operating system merely marks these files as deleted and allows them to be overwritten. Other operating systems, in contrast, may overwrite the files immediately when the user selects them for deletion. Once a file has been overwritten, it is usually irretrievable, but since most users don't realize what needs to be done to permanently destroy a file, it is fairly common for files deleted in Windows to be retrieved unscathed.

In the case of e-discovery there are some rules about compliance, and evidence should be gathered as quickly as possible. With electronic message archiving in place for both e-mail and IM, it becomes a fairly simple task to retrieve any e-mail or IM chat that might be used in e-discovery. Some archiving systems apply a unique code to each archived message or chat to establish authenticity. The systems prevent alterations to original messages, messages cannot be deleted, and the messages cannot be accessed by unauthorized persons. Modern message-archival systems allow legal and technology professionals to store and retrieve electronic messages efficiently and in a timely manner.

It may seem easy to delete files or e-mails, but with the use of expert forensics it is extremely hard to beat a computer forensics company at their own game.

Protecting Yourself

I am not talking about covering your tracks when you are guilty of a crime. Once an investigation begins and the forensic evidence is being gathered, anyone can become a suspect. Computer data does not care whether or not you are guilty.

Because I was involved in the IT side of an investigation, I learned a few things in the process. I am much more aware of how and with whom data is transferred both within and outside of our network. Keep in mind the following:

1. Avoid personal correspondence using company e-mail. If you need to communicate with friends and family outside the organization, use a personal e-mail account that is Web-based if possible.

2. Never place company files on a personal laptop or computer. In fact, avoid taking files offsite if at all possible.

3. Be very conscientious of your communication. You may, without knowing it, share proprietary information over messengers or e-mail. This can be used against you in an investigation.

4. If you have signed a non-compete or nondisclosure contract with the company you work for, you are under legal contract not to share company secrets or information with anyone outside the company. Usually this extends for a specific period of time *after* you leave the company.

Even if you did not commit any crime or knowingly share information, you could be guilty by association or as an accomplice if evidence is found that information related to the investigation passed through you in any way.