

Computer Basics:

How Computer Forensic Investigation is Possible

Undeleting Deleted Files

Most users assume that deleting files from a computer actually removes the files. We only have to look as far as Ollie North and Bill Gates to see that even very sophisticated users can fall prey to this assumption.

A computer's operating system keeps a directory, much like a telephone directory, of the name and location of each file. When a user deletes a file, the operating system does not remove the data. Instead, it indicates that the space is available; the contents remain in place until they are over-written by some other process. The treatment of "deleted" files is comparable to a telephone company that deletes a subscriber from the phone book but leaves his/her service active. Someone who knows the phone number can still call the subscriber in question.

Similarly, someone who knows how to access these released-but-not-erased areas, and who has the proper tools, can recover their contents.

In computer forensics, the operating system is both friend and foe. Its friendly nature makes the system easy to use, but to do so it must keep track of information that it hides from the user. This hidden information is a rich source of details about what the user has been doing.

It contains information such as web sites visited, e-mail sent and received, Internet-based financial transactions, and letters. A computer forensics expert exploits these hidden pockets of data to acquire information and to evaluate its usefulness as evidence in a particular matter.

A user need not save documents on his/her computer for them to be accessible to forensic specialists—as one bank robber discovered. Involved in twelve bank robberies in San Diego in late 1999, the "Gap-Toothed Bandit" wrote threatening demand notes on his computer, but exited his word processor without saving them. A forensic investigation of his computer yielded five of his demand notes. How is that possible? In order to display the notes on his monitor, the system stored them in a temporary location; and, when he exited his word processor, the "friendly" operating system neglected to tell him the notes were still there.

Meta Data

Some applications, most notably Microsoft Word©, keep information about each document it accesses. Since these data, which describe the document, are stored within in the document itself, they are called *meta data*. The meta data can contain the history of the document, including all users who have modified and/or saved it, the directory structure of all machines it was saved on, and names of printers it was printed upon.

These data readily yield to forensics investigation techniques. Many theft-of-trade-secret cases have been decided because the meta data showed the original, and all intervening, possessors of protected documents.

A Proper Forensics Investigation

Evidence retrieved from electronic media requires the same chain of custody controls and assurance, as does other evidence. However, since electronic media are easily altered, special care must be taken to protect the evidence from changes, either deliberate or inadvertent. For example, merely starting a computer running a Windows system changes more than 160 files. It is imperative that the forensic investigator be able to demonstrate to the court that the electronic evidence was not altered in its acquisition and has not been altered since that time.

The work of the forensic specialist falls into three broad categories. The computer forensics community has developed tools for acquiring copies of disks without altering the contents. It is not sufficient merely to copy data files, the entire disk must be copied bit by bit.

This preserves all the hidden and temporary data on the disk.

Second, computer science has established techniques for identifying and securing computer files. The usual techniques involve applying numeric procedures to the disk to produce a number virtually unique to the disk. Computer forensic professionals use and document these techniques each time they access the disk to demonstrate its authenticity. The third task of the computer forensics specialist is to interpret temporary, hidden, and partial files. This interpretation requires in-depth knowledge of how computers and the various applications store and manage data. For example, a computer file usually records the date(s) on which it was created, last modified, and last accessed. It can happen that the “last accessed” date precedes the creation date. The specialist must be able to interpret these inconsistencies to the Court.