Demystifying Computer Forensics

Johnette Hassell, Ph.D.
Susan Steen

Introduction

When the Lieutenant on a television show—usually at a murder scene—says “Get forensics in here!” the viewer knows what to expect. Soon the scene will be filled with technicians who will dust for fingerprints, examine blood splatters, and determine bullet trajectories. Whether or not this representation is accurate, we, the viewers, understand the goal of such forensic activities.

What then is “Computer Forensics?” In this article we explain what computer forensics involves and how it relates to the legal system. We review computer principles as they impact forensic investigations; describe a proper forensic investigation; and advise interested parties, such as attorneys and information technology staff, of what they can do to secure the best results from a forensic investigation of computer media.

What is Computer Forensics?

Computer forensics is a collection of multi-faceted, multi-disciplined specialties that are used to extract useful information from computer media.

When retained in a current or potential legal matter, the computer forensic specialist helps determine if a computer disk contains potential evidence. The specialist also oversees the extraction of information from the computer media and evaluates the information for its evidentiary value. Throughout the process, the forensics practitioner provides assurance of chain of custody. The following examples illustrate the results of some real world computer forensic investigations.

Two partners in the business of developing certain telecommunication services separated. Within a few months, one of the partners formed a new company and was marketing a product that was a virtual clone of the partnership product. A computer forensic specialist compared the two products and, using statistical techniques, showed that the partnership's computer code had indeed been used in the new product and that their copyright had been infringed upon.

A group of employees of a high tech company decided to raid the market share of their employer. They formed another company, and using their employer's technology, developed a product that competed directly with that of the employer, all the while remaining as employees of the company! A computer forensic analysis revealed that they had copied the employer's designs, charts, and specification documents, and showed the trail of the documents as they moved from one conspirator's computer to the next.

Computer forensic analysis is often useful in matters that, on the surface, seem unrelated to computers. In one case, an alleged bomber had kept downloaded files that described the bomb-making techniques he used. In another case, a bitterly fought divorce and child custody dispute, one party had scanned questionable pictures of herself into her company computer and then attempted to delete them.

In all these cases—and many others—computer forensics techniques were able to retrieve data that ultimately played a pivotal role in the outcome of the case.

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.

While accessing the Internet, browsers keep records of the sites a user has visited. If a user permits *cookies*, small files used by browsers to keep track of a user’s visits, the cookies may yield passwords and other information about the user’s Internet practices. These records can be deleted <u>if</u> the user knows about them, is zealous in regularly deleting them, and overwrites their locations. If not, forensics investigations can disclose clear evidence of sites the user has visited.

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.

What You Should Do

When you suspect that a computer holds information about illegal activities, the most natural reaction is to want to check it out, both to avoid public knowledge of security breeches and in a desire to avoid false accusations. However, remember that merely starting the computer changes files, and many of those changes affect significant dates. Any access to the disk risks overwriting relevant information and destroys the chain of custody. In addition, there is no protection in booting from another disk or trying to examine the computer over a network.

The best course of action is to leave the computer alone and have a qualified forensics specialist create a certified, bit-by-bit copy of the disk(s). The copy can then be examined without jeopardizing the investigation. It is not sufficient to use utilities, such as Norton's Ghost, to image a disk because accessing the disk in the usual fashion alters it.

But what if you have already tried looking at the disk? Stop and leave the computer exactly as it is, do not even turn it off or on. Confess to your forensic specialist what you have done and let him/her work from there. The worst course of action would be for you not to tell the specialist, who eventually is called in to investigate the matter, that you have accessed the disk!

A Final Word

If a matter you are working on has potential evidence on computer disks, we recommend that you engage a qualified computer forensics professional as early as possible. Not only can such professionals conduct the proper investigation we have described herein; they can assist with preparing and answering interrogatories, drafting language for a search warrants, and carrying out preliminary "stealth" investigations to assess the potential evidence. In choosing a computer forensic specialist, be certain too that your choice not only knows how to conduct the disk acquisition and data retrieval, but can also provide expert reports, depositions, and testimony. Chosing a specialist who is qualified and experienced in all of these matters will be more cost effective and will simplify the coordination of professionals involved in preparing the case.

About the Authors

The authors are partners in Electronic Evidence Retrieval, L.L.C., a company specializing in computer forensics and other expert consultation and testimony in computer science. They have more than twenty years of experience in computer consultation and testimony, computer forensics, software and technical manual copyright infringement support, and programmatic research and evaluation. They can be reached at info@ElectronicEvidenceRetrieval.com or 504.483.0201 on the Gulf Coast and *970.922.7250* in the Rocky Mountain area.