

# Smoking microchip tells it all

**Computer forensic experts mine hard drives for data that too-clever users thought long deleted.**

*Sean Barry is a Computer Forensics Lab Manager for Gresham, Ore.-based New Technologies Inc. He can be reached at sean@forensics-intl.com.*

---

By Sean Barry

SPECIAL TO THE NATIONAL LAW JOURNAL

Documentary evidence can be the most compelling form of evidence in wrongful employment dismissals, sexual discrimination, racial discrimination, stock fraud and the theft of trade secret cases. Often, important communications are committed to writing, and such writings can make or break a case.

Traditional paper documents have been sought in the legal discovery process for hundreds of years; judges and attorneys are very familiar with documentary evidence in paper form. Litigators, however, are now beginning to understand the evidentiary value of computer-related evidence in the document discovery process. Litigators are turning their attention to the discovery of entire computer hard disk drives, floppy diskettes, zip disks and even cell phones and handheld computer devices. These new forms of documentary evidence have significantly broadened the potential for legal discovery, and have given birth to a new science—computer forensics. Computer forensics experts use sophisticated technology tools and investigative smarts to ferret out electronic smoking guns in a form that is acceptable for discovery purposes.

The role of computer forensics in the electronic evidence discovery process is essentially to mine the hard drives in desktop, laptop, and server computers for data beyond what the average user may be aware of. This data may reside in deleted files, temporary files, draft sequences, and results of other computer activity that can serve as discovery fodder. Computer forensics specialists have developed various tools and techniques to uncover this information in a form that is acceptable for discovery purposes.

When electronic documents are created, bits and pieces of the drafts leading up to the creation of the final document are written in temporary computer files, the Windows swap file and in file slack. The swap file is a special file that Windows-based computer operating systems use as a “scratch pad” to write data when additional random access memory is needed. In Windows, Windows 95 and Windows 98, these are called Windows Swap Files. In Windows NT and Windows 2000 they are called Windows Page Files, but both have essentially the same characteristics. Swap files are potentially huge and most computer users are unaware of their existence. The size of these files can range from 20 million bytes to over 200 million bytes and the potential exists for these huge files to contain remnants of word processing, E-Mail messages, Internet browsing activity, database entries and almost any other work that may have occurred during past Windows work sessions.

File slack can be explained as follows: Files are created in varying lengths depending on their contents. DOS, Windows and Windows NT-based computers store files in fixed length blocks of data called clusters. Rarely do file sizes exactly match the size of one or multiple clusters perfectly. The data storage space that exists from the end of the file to the end of the last cluster assigned to the file is called “file slack”. Cluster sizes vary in length depending on the operating system involved and, in the case of Windows 95, the size of the logical partition involved. File slack can be a significant source of evidence and leads. The computer user is usually not aware that this occurs.

Furthermore, when computer-created documents are updated or erased, remnants of the original version and drafts leading up to the creation of the original version remain behind on the computer hard disk drive. Most of this data is beyond the reach or knowledge of the computer user that created the data. As a result, these forms of ‘ambient data’ can become a valuable source of documentary evidence.

Computer Forensic specialists have specialized skills and tools that allow them to recover and examine this ambient data. They use powerful search utilities to look for keywords or phrases, whether it is contained within a file or not. These search terms can be names of people or companies the user may have been

communicating with; they can be known contents of documents that have disappeared from a computer they should be on or may be on one they shouldn't. Computer Forensics specialists build timelines of computer usage that go beyond simply listing the date stamps on the files in question. They can analyze a computer for internet usage, for example, in violation of employer policies, looking in places other than the temporary internet files and browser history files which the user may have cleaned.

Electronic evidence discovery can apply to a variety of litigations. Take, for example, a theft of trade secrets/violation of non-compete agreement case., The board of directors of Company X, a technical research company, demote the company's founder and chief executive officer. Disgruntled because of the demotion, the executive's productivity diminishes to the point that he is later fired. It is subsequently determined that at the time he was fired, the executive had already planned to quit Company X and establish a company that would compete with Company X. Company X files a suit. It's determined that at the time he was fired, the executive took home two computers and then returned them to the company four days later, along with a company computer he had previously used at home. Suspicious that critical information had been taken; the company immediately turned them over to their attorneys, who in turn contacted a computer forensics firm and sent them the computers for examination. Examining mirror image backups they made of the original hard drives, the firm identified a file directory that had been deleted during the aforementioned four-day period that had the same name as the suspected competitive company the executive had established. A specific search of the deleted files in this directory identified the executive's "to do" list file. The "to do" list indicated that the executive planned to copy Company X's \$100 million database for his personal use. Another "to do" item specified that the executive was to "learn how to destroy evidence on a computer".

The forensic firm's examination also proved that the executive had been communicating with other competing companies to establish alliances, in violation of the executive's nondisclosure agreement with Company X. It was also shown that numerous key files from Company X were located on removable computer storage media that had not been turned over by the executive to Company X. Company X was able to settle with the executive for all that it had originally requested in its lawsuit, enforcing the non-compete agreement previously in place and protecting their patents.

Another example of the usefulness of computer forensics is in fraud cases. Imagine a large agricultural firm that discovers that one of its competitors is selling a product with a similar brand name and composition, causing marketplace confusion. The agricultural firm, Company Y, files a lawsuit against the competitor, alleging patent infringement. The competitor claims that it had a written agreement signed in the late 1980's giving it the rights to sell Company Y's product and similar products in specific market segments and geographic areas. The competitor also produces another written document that allegedly validated the agreement.

Company Y hires a computer forensics firm to help it determine the source of the documents. In accordance with the discovery agreement, applicable hard drives of the competitor were obtained. After making mirror image backups, Company Y was able to identify the files that contained the alleged agreement by searching for unique words and phrases selected from the printed version. Based on the dates of the file, information found in the slack space at the end of the file, and other evidence, the forensic expert determines that the alleged agreement was actually written after the lawsuit commenced. The expert also determines that the alleged agreement was drafted by a corporate executive employed by the competition and was finalized by the executive's secretary. Moreover, the computer hardware and software used to create the purported agreement did not even exist during the period the alleged agreement was drafted. The computer the document was found on was manufactured after the date on the file. While it could have been copied from an earlier computer, the document contained information, unknown to the users, identifying the software used to create it. This software was also newer than the agreement.

Computer forensics is also extremely useful in cases alleging discrimination or harassment. For example, suppose a woman employed by a large defense contractor accuses her supervisor of sexually harassment. She is subsequently fired from her job for alleged poor performance. She then sues her ex-boss and former employer for sexual harassment.

The plaintiff hires a computer forensics expert, who through the discovery process, is able to obtain the ex-boss' hard drive. After making a mirror image backup of the ex-boss' hard drive, the computer forensics firm is able to recover deleted electronic messages that contained evidence that the ex-boss had a history of propositioning women under his supervision for "special favors". As a part of the settlement, the woman is reinstated, and the ex-boss is fired.

Computer evidence is very fragile and can easily and unintentionally be altered or destroyed, through normal use or even just turning on the computer. Therefore, it is important that only properly trained computer evidence specialists process computer evidence, so that the integrity of the evidence is maintained to eventually hold up in a court of law. Although there are no formal rules for processing computer evidence, the

computer forensics examination will generally include the following steps:

- Create photo documentation of the computer in question—photograph all angles and label wires to document the systems' hardware components and how they are connected.

- Mathematically authenticate data on all storage devices. This is done through the use of special software tools that calculate unique numerical signatures based on the contents of a drive. This is one way to ensure that your mirror image is just that, a mirror image of the original.

- Create an evidence grade mirror image backup (exact copy, down to the last bit of data) of a hard disk drive and other computer storage devices such as floppy disks, zip disks, etc. This guarantees the preservation of the best evidence, and is the basis for all later work.

- Store evidence in a highly secure location. Maintaining proper chain of custody is essential to any computer investigation. Depending on the discovery order for the case, the evidence may include the originals or just the mirror images.

- Create a list of key search terms which, depending on the nature of the case, will “red flag” sites visited by the computer-user in question; e-mail messages; internet chat messages; word processing documents, and other files.

Once the actual search begins, evaluate all data, including word processing documents, e-mail files, data from Internet use, Windows swap file, file slack, and unallocated space (when files are erased or deleted in DOS, Windows, Windows 95, Windows 98 and Windows NT, the content of the file is not actually erased; the ‘erased file’ remains behind in an area called unallocated storage space, which is available for discovery) for key words or questionable data. Determine frequency of e-mails to particular individuals, and of usage of particular documents.

Identify any file, program and storage anomalies, and document and report findings and anomalies. These anomalies might include indications that the entire drive is not being used and incorrect file type identifiers (i.e. a spreadsheet that is identified through the filename and extension as being a word processing document or picture file).

If called upon, provide expert witness testimony to clarify technical computer evidence issues in the litigation process.

The United States is a digital society, existing in an increasingly digital world. As computers take on an ever-expanding role in peoples' lives, computer evidence—and its application in civil litigation—will likewise increase. Computer forensics “experts” from a broad range of disciplines are springing up to meet this need. The specialists best suited for a particular case should satisfy certain criteria.

First, look for someone who has experience with forensics technology and the discovery process. While both litigation consultants and technology professionals bring something to the party, a litigator will do best with experts that are experienced with both disciplines, as they're closely entwined in the science of computer forensics.

Second, note that the software tools computer forensics experts use to uncover electronic evidence are constantly being refined. Make sure that your experts are using the best and most up-to-date utilities.

Third, knowing how to find something is important. Knowing what to look for can be much more important. A computer forensics expert who can run a search and return to an attorney's office with a report indexing search results has some value. An expert with an investigative background who can partner with a law firm to help define electronic evidence strategies and suggest alternative paths to isolating that electronic smoking gun, can be invaluable.

Finally, while mega-cases may foster a “find the evidence at any cost” attitude, this is not the norm. Electronic evidence discovery costs are not insubstantial, and can escalate if not closely monitored. A reputable computer forensics outfit will work closely with lead counsel at the outset of a project to define the scope of the discovery effort, and will update counsel at regular intervals to provide reports on project status vis-a-vis initial estimates. This way, counsel can determine if further inquiries are merited, and there are no unhappy surprises when an invoice is submitted at the project's completion.

Valuable evidence that can make or break a case is as likely to be stored on a computer today as it was on paper several years ago. Having a computer forensics expert on your team can ensure that this evidence is not missed or damaged.

Sean Barry is a Computer Forensics Lab Manager with New Technologies, Inc. ([www.forensics-intl.com](http://www.forensics-intl.com)), a Gresham, Oregon-based company that provides computer forensics tool development, computer evidence consulting and computer forensics training for law firms, corporations, and government entities. NTI is a wholly-owned subsidiary of Armor Holdings Company.