The Legal Intelligencer

Bits and Bytes: What Forensic Analysis Can Reveal

By **Philip N. Yannella**

The Legal Intelligencer

January 29, 2013

In the age of CSI, many civil litigators are aware that the secrets to unlocking a case may be buried deep within a party's computer, in the form of a deleted file, an incriminating Google search, or tell-tale cookie. But while litigators may be generally aware of the power of computer forensics, they do not always understand how forensic analysis works or when it is appropriate in civil litigation. This article will explain where deleted files and other important types of evidence can be located on a hard drive or mobile device, how forensic analysts actually track down hidden or deleted evidence, and the legal standard for conducting forensic examinations in civil cases.

What is Computer Forensics?

Computer forensics is a branch of computer science that focuses on the retrieval and analysis of data from hard drives and other media that are generally inaccessible to the layperson. One of the most common forensic techniques is "file-carving," which focuses on the identification and recovery of deleted files from a hard drive.

Some background: Computer operating systems typically store data in contiguous clusters on a user's hard drive. When the user deletes a file, the operating system notes on the hard drive that the file is now deleted and no longer accessible to the user. But the data in the file is not permanently deleted from the hard drive until the operating system assigns the clusters to new user-created files, which could be days or even months later. The space on the hard drive where the deleted file formerly resided is referred to as unallocated space. To recover and analyze deleted data that may occupy a hard drive's unallocated space, forensic analysts use very sophisticated tools, such as Encase, Scalpel and Magic Rescue. These tools metaphorically "carve" deleted data from the hard drive.

The power of file-carving was recently demonstrated in the case of the BTK killer in Kansas. Police obtained evidence against the infamous serial killer by checking the metadata of a deleted Microsoft Word file that was recovered from a floppy disk the killer sent to the police. The metadata showed that the document had been accessed by someone named "Dennis," and that the program was used by "Christ Lutheran Church." By searching the Internet for "Dennis Christ Lutheran Church," police were able to identify a suspect who was associated with the church – Dennis Rader, who was later arrested and ultimately pled guilty to 10 counts of murder.

File-carving, however, is not the only technique forensic analysts can use to locate potentially relevant evidence. Computer forensics has evolved into a cat-and-mouse game in which rogue employees, corporate thieves and criminals attempt to evade forensic analysis through a range of tricks – such as the use of anti-forensic software. Computer forensics, in turn, has responded by developing new software and incorporating new routines in standard analyses to expose these tricks. Summarized below are the more common steps that computer forensic analysts will take to locate potentially relevant evidence.

When the Evidence is Hidden in Plain Sight

One of the simplest ways in which criminals or malicious employees will attempt to hide illicit computer activity is by changing the file extension of important or revealing documents. For example, .xls is the extension for Microsoft Excel. To hide his or her digital footprint, a rogue employee might change the extension of an Excel spreadsheet from .xls to something else that would not be captured in a routine search for all .xls documents. To account for this possibility, forensic analysts will perform "header searches," instead of relying solely on file extensions to identify file type.

Another low-tech way in which criminals or malicious employees may attempt to hide key documents in plain sight is by changing the font size on a document to render it virtually unreadable. (Microsoft Word, for example, will allow you to save a file in 1-point font.) Changing the font color to white is another common way of hiding information within a file. Forensic analysts will take steps to spot these kinds of common tricks.

Encryption

Encrypting documents that might reveal illegal activity is another common means of evading detection. One of the most important steps that forensic analysts can take is to identify and crack encrypted files. The development of programs such as TrueCrypt, which allow users to hide encrypted files on a hard drive, makes detection of these files more difficult and in some ways even more critical.

Registry

The registry on a Windows operating system contains a trove of potentially important information, including a list of all hardware and software loaded onto the system, as well as user preferences. Forensic analysts can review the registry to determine when a flash drive was inserted into a computer, as well as the serial number on the flash drive – which can be very useful in uncovering the theft of intellectual property.

Temporary Files, Internet History and Cookies

Forensic analysts will also pay special attention to temporary files, which an operating system creates when a user is working on a particular document. Usually, the system will delete the temporary file once it is saved. But if the file is never saved – say, because the user is attempting to cover his or her tracks – the temporary file may be valuable evidence of nefarious conduct. Evidence that an employee has backdated a stock option, for example, may exist in such a file.

Computer forensics played a large role in the Casey Anthony trial. Among the forensic tricks that the public learned about from watching the trial was the ability of analysts to recover old Google searches from Internet browsers. Forensic searches of "cookies" – tiny text files sent from a website to a user's hard drive – can also be used to recreate a user's Internet searching habits.

Wiping Software

One of the more recent developments in the ongoing game of forensic evasion is the use of anti-forensic software, often called "wiping" software. Users can deploy this software to erase all forensic evidence of a deleted file from a hard drive. Think of this as the forensic version of nuking a hard drive.

But even this method is not foolproof. Trained computer analysts can sometimes detect the use of anti-forensic software (which can itself be strong evidence of computer theft) because malicious employees or criminals forget to delete the software itself from the system. The wiping software can also leave a digital signature that forensic analysts can sometimes detect.

Advanced computer forensic analysis incorporates many other routines. Without going into detail, examples include analysis of volatile data, such as RAM, pattern and activity analysis (which analyzes server logs to detect incriminating patterns of user activity) and the use of Shellbags, a Microsoft registry

program that caches the file names on a device plugged into the computer. Suffice to say, if data existed at one time on a hard drive, there is a good chance that a trained forensic analyst will be able to recover it, at least in part.

When is Forensic Analysis Appropriate in Civil Litigation?

As exciting and potentially revealing as computer forensics may be, it is an expensive and intrusive process. To conduct forensic examinations, a party must take a forensic image of the hard drive, capturing the slack and unallocated space (this is often called a bit-by-bit image), and then hand the image over to forensic analysts to poke and probe their way through the digital artifacts. Of course, for every piece of potentially relevant information an analyst may uncover, there are many more irrelevant ones – to say nothing of the private or potentially privileged documents that may be swept into the forensic dragnet.

For this reason, most courts take the view that a party in civil litigation is not generally entitled to a forensic examination. This position is echoed in the Sedona Principles, a leading treatise on electronic discovery often relied upon by state and federal courts. But that is not to say that forensic examinations are never appropriate. Most courts will permit a forensic examination upon a showing of special need.

Oftentimes, this burden can be met where there is evidence that a company or employee has purposefully deleted electronic documents. In such a case, forensic examination may be the only way to recover potentially relevant evidence. Sometimes the accidental deletion of electronic documents can be sufficient to trigger forensic examination, particularly if the deleted files are central to the litigation.

Forensic examinations are often ordered (or sometimes agreed to by the parties) when there is a specific allegation of employee wrongdoing. Cases involving misappropriation of trade secrets, for example, often hinge on forensic examinations. In these cases, side-switching employees are alleged to have stolen proprietary files from one company and smuggled them to their new employer. Plaintiffs in such cases will typically demand forensic examination of the employee's old computer as well as his or her new computer to locate evidence of data theft.

Other cases that may justify forensic examination include those where allegations of document shredding are central, as well as cases involving the alleged manipulation of data, document backdating, improper communications or suppression of negative information (such as bad clinical trial results).

Litigators who must comply with a court-ordered or agreed-upon forensic examination should take care to ensure that protocols are established to review potentially privileged documents, as well as confidential or private information. The use of clawback agreements, protective orders and the negotiation of search terms is a standard feature of negotiations concerning forensic examinations.

Civil litigators considering a potential forensic examination should know that there is a potential gold mine of evidence that can be retrieved from a hard drive or mobile device. But forensic examinations are expensive, highly intrusive and can end up being a wild goose chase, so choose your battles wisely. Understanding the basics of computer forensic analysis can help litigators articulate a reasonable basis for a forensic examination or defend against one.

Philip N. Yannella *is a partner in the litigation department and practice leader of the e-discovery and data management group at* ***Ballard Spahr****. He is also a member of the consumer financial services, commercial litigation and product liability and mass tort groups. He manages e-discovery issues in high-profile litigation, counseling clients worldwide on data preservation, retrieval and privacy matters. He has significant experience representing Fortune 500 companies on e-discovery and data management issues in bet-the-company litigation.*