

## **What You Need to Know About Digital Forensics\***

*By Beryl A. Howell and Samuel Rubin*

The management of a small regional company was concerned. They had just learned that its most important government contract had been lost to an out-of-nowhere startup. Management's concern grew to alarm, however, when they discovered the startup was staffed by former employees. They faced a scenario confronted too often by many businesses: Their company was a victim of intellectual property theft. The former employees had stolen proprietary business information, including inside knowledge of bidding prices, business methodologies and customer lists, and had used the information to "steal the deal." They decided to fight back.

A company can be placed in jeopardy by the theft of intellectual property, a lawsuit triggering electronic discovery obligations, an embarrassing security breach resulting in the loss of customers' personal data, an employee's improper or unlawful computer use to download child pornography or a myriad of other situations. In such cases, counsel may be called upon not just for legal advice but also for practical advice about what to do. Since most information created and received in an organization is generated electronically and stored on hard drives, attorneys should ideally know enough about digital forensics to make strategic decisions about its use in these situations, rather than forfeiting this evidence out of ignorance. They need to know the scope and types of information that digital forensic examinations can reveal so that counsel can know where to look for useful evidence to support a client's claims and also to anticipate its defensive applications.

### **When to Speed-Dial Computer Forensics Experts**

When the victim company decided to fight back, its first step was a wrong one. The company decided to investigate the situation itself by having in-house information technology personnel examine the workplace computers of the former employees. The IT personnel used off-the-shelf data recovery programs, which they installed on the target computers in an effort to recover deleted files, followed by further rummaging, copying and printing of files from the old computers.

After counsel was retained, the computer examination by in-house IT personnel was stopped. Though well-intentioned, turning on the computers, installing new software programs, searching and using other utilities on the computers resulted in the altering of active data and overwriting of deleted data that otherwise would have been recoverable and potentially probative. The task of convincing a client with an eager IT staff to wait and call in a more costly digital forensic expert, who can testify about the methodology and any positive findings on a target computer, may be difficult. The alternative, however, is that relevant or even case-dispositive evidence may be lost.

In this case, despite the actions of the company's IT staff, subsequent forensic analysis of the former employees' work computers established that they had conspired in Hotmail communications to take confidential client lists and other proprietary business information from the company, had accessed and copied information from restricted network locations without authorization and had copied confidential information to removable media, including CDs and thumb drives, all shortly before leaving the company. The findings were presented in expert testimony to gain court-ordered inspection of the work and home computers used by the former employees in their new business. Forensic examination of these computers confirmed that the former employees indeed had been using their former company's proprietary information to create "new" products and services. Moreover, the defendants had attempted to destroy this evidence by deleting data. These conclusions were presented in expert reports and deposition testimony and led directly to a favorable settlement for the victim company.

## **What to Look for on Computer Hard Drives**

The types of electronic storage media holding digital information that could be subject to forensic analysis vary greatly, and each type has specific forensic tools that are used to handle the data. The most common type of digital evidence encountered today is the personal computer paired with the Microsoft Windows operating system. Regardless of the media type, however, there are generally two types of information that can be gleaned from a forensic analysis: *content information*, which is textual data resident on the system, and *usage information*, which indicates how the system or data on it was used.

### **Content Information**

Content information on a computer hard drive includes not only the active files and e-mails readily accessible to the computer user but also data that is hidden and not readily accessible without the expert use of forensic tools. This hidden data may reside in unallocated, slack and swap space on the hard drive and may consist of information that the computer user has deleted or that the operating system has cached or automatically stored without the user's knowledge or active intervention. "Unallocated space" is the portion of the hard drive that the file system designates as available for the recording of new data and may contain data previously deleted or viewed. "Slack space" is area allocated to but not filled by an active file and may contain fragments of previously deleted files. "Swap space" is the portion of the hard drive that can be used to store information while an application or process is running. For example, information that the user has viewed on the computer screen or created without intentionally saving may nevertheless be automatically saved on the system and recoverable, though inaccessible to the normal computer user.

Sorting through the millions of pages of information stored on a hard drive to find relevant information for counsel to review can be simplified through use of forensic tools that enable searches filtered by keyword, timeframe or other criteria. In addition, the searches can be run across both voluminous active files and inaccessible or hidden data. For example, a keyword search of inaccessible data helped solve an investigation involving an anonymous letter containing derogatory and confidential information about a company. The company sought to identify the author. Forensic analysis of the company's computers revealed a draft of the letter in the swap space of a computer used by an employee who had drafted the document, printed it and then closed the document without saving it, thinking that the file was "gone." Unbeknownst to the employee, the document was cached on the hard drive and completely recoverable.

Even when data is deleted, overwritten and not recoverable, forensic analysis may be able to identify traces of the original files and prove that the files existed. One such method is to use information from the "shortcut" feature of Windows systems, which can leave pointers to files that no longer exist on a hard drive. In one case, these shortcut or "LNK" files were found still referring to important transactional documents that otherwise had been wiped clean from the suspect's computer.

### **Usage Information**

Often the content resident on a computer cannot be properly interpreted without an understanding of the context. This contextual information may be embedded in the file itself and reveal when a file was created, last modified, printed or accessed, and who authored and edited the file. Thus, for example, when the embedded information or "metadata" for a file reveals that the creation date is Jan. 1, 2006, but it was last printed a year earlier, this indicates that the file was likely moved and saved to its current location on Jan. 1, 2006. Significant clues about the authenticity of documents can be found through a metadata analysis and may reveal, for example, that a document was post-dated when the date reflected in the text of the document is inconsistent with the associated metadata in the electronic version.

Contextual information also includes details about system usage, such as when software applications were installed and used on the computer, file creation or deletion activity, manipulation of document time-stamps or access to certain Internet or network locations. Understanding the activities that transpired on a computer can be crucial to an investigation, yet the usage component of digital analysis may be neglected as counsel focuses on finding relevant data content. For example, searching a suspect's hard drive only for particular keywords may miss the fact that file-wiping software had been installed and then used to overwrite large portions of the hard drive just prior to review. This usage fact may show consciousness of guilt and be more highly probative than responsive files found as the result of keyword searches.

### **System Usage Report**

The user of a computer may not always be available or cooperative to assist counsel in assessing what is on a computer hard drive. In this situation, a useful first step after forensic acquisition of an image of the computer is to develop a general overview of its contents by requesting a system usage report. This report can detail for counsel the names and period of use of the primary users of the machine, the directory and folder structure the user employed to organize files, any wiping or unusual deletion activity, the presence of encrypted files, Internet history, applications installed, e-mail accounts used and use of external storage devices such as servers or USB thumb drives. These reports can assist in quickly pinpointing relevant files or areas that need drill-down analysis or further review.

### **Creation, Modification and Transfer of Files**

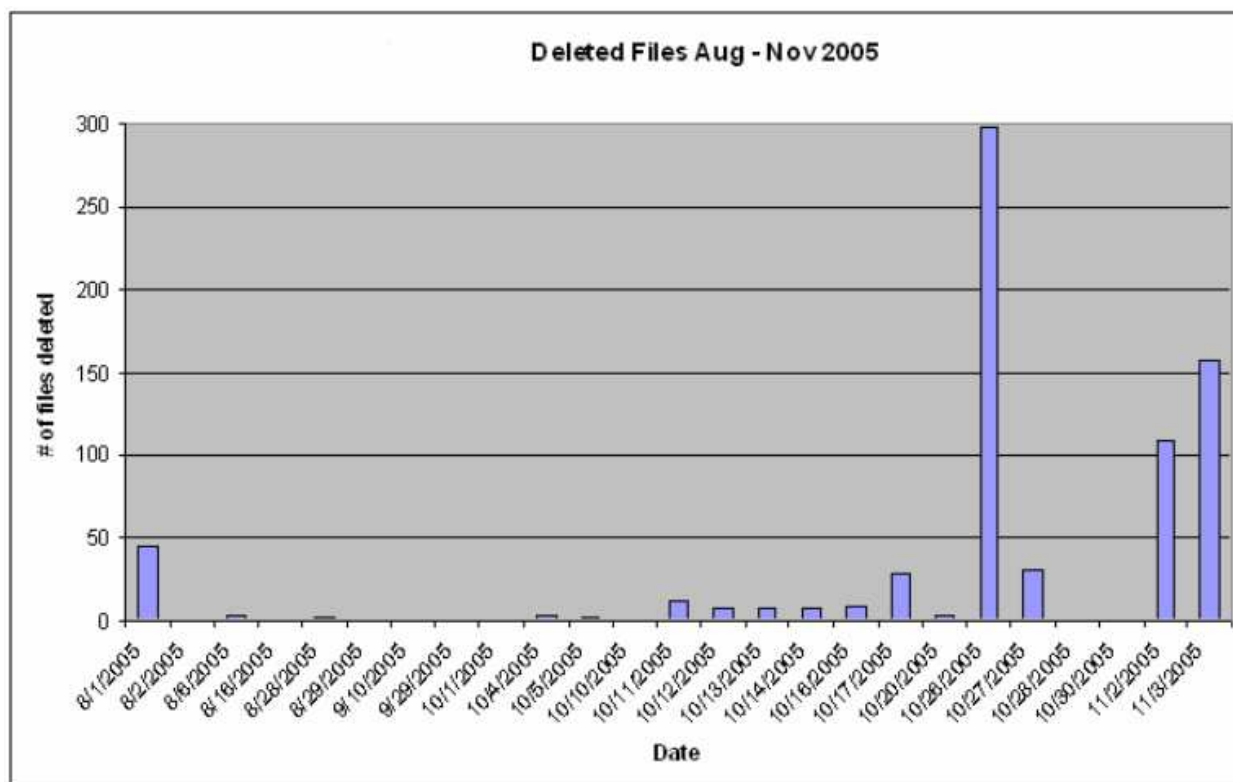
In intellectual property theft cases, it is essential to identify the proprietary information stolen and to establish when and how this information might have been removed. Digital forensic analysis of a suspect's hard drive can reveal evidence of the transfer of files to a USB storage device, CD-ROM, floppy disk, e-mail or even to a printer. Moreover, it is often possible to discern the serial number of the removable medium to which the data was transferred, what data was actually transferred and the date when the transfer occurred.

In another example, metadata date/time stamps were helpful in understanding the sequence of how an intellectual property theft was accomplished. In *Jackson v. Microsoft Corp.* 211 F.R.D. 423 (W.D. WA, 2002), the court credited the testimony of a computer forensic examiner who found identical confidential business data files on two CDs and a laptop in the possession of the plaintiff, a former employee. Based upon the creation dates of the files in question, the expert was able to determine that the data files on the CDs were created the day before the employee left employment at Microsoft and that the files from the CDs were placed on the employee's laptop later the same evening. The expert was further able to determine that, contrary to representations of the former employee, many of the confidential files had been last accessed on the laptop over the course of the plaintiff's two-day deposition. The court dismissed the plaintiff's suit due to his misrepresentations to the court and unlawful possession of Microsoft's proprietary information. See also *Leonard v. State of Texas*, 767 S.W.2d 171 (Tex. Crim. App. 1988).

### **Data Manipulation**

Electronic data is easily deleted, hidden and manipulated, but evidence of these actions can be found through forensic examination of the hard drive. Obstructive behavior can range from simple deletions or renaming of file extensions, to more sophisticated methods such as changing the computer clock to backdate files and the use of encryption software or software applications designed to overwrite files permanently. Without the scrutiny of trained eyes or if investigators choose to focus solely on a computer's content and not activities of the computer user, data obfuscation may go unnoticed.

Digital forensic analysis can identify this unscrupulous behavior. For example, deletion activity is recorded by the operating system and can be sorted chronologically, reviewed for periods of relevance and presented in a number of useful ways. The names of the files that have been deleted since the installation of the computer's operating system can be compiled in a spreadsheet format showing in chronological order the names of files that were deleted by the computer user and whether the files were overwritten. Alternatively, a graphic depiction of the deletion activity, shown in the deleted files histogram below, can help to pinpoint periods of mass deletion.



The spikes in the chart represent periods of high deletion activity. In this instance, the user of this computer deleted a high number of files on Oct. 28 and Nov. 3, 2005. Incidentally, Oct. 28 was the day the computer user was notified that his computer was to be imaged. Mass deletions of files, particularly those relevant to an investigation, on a day after the suspect received a subpoena or otherwise was alerted to an investigation would spell trouble for a suspect and provide probative evidence of the suspect's inculpatory state of mind. *Advantacare Health Partners, LP v. Access IV*, 2004 U.S. Dist. LEXIS 16835 (N.D. Cal.)

If data wiping is suspected, forensic review may be able to show whether wiping software is currently installed or was used and subsequently removed from the hard drive as well as when a wiping program was last used and the last file targeted for destruction.

### Conclusion

Digital forensics can provide a trove of evidence about a computer user's activities, state of mind and knowledge of and access to specific information. This evidence may be useful and sometimes critical to evaluating, authenticating and giving context to e-mails and other electronic records that are central to a case.

*Beryl Howell is a partner at Stroz Friedberg L.L.C., a technical services and consulting firm specializing in digital forensics, electronic discovery and cyber security investigations, and a member of the U.S. Sentencing Commission. Samuel Rubin is a digital forensic examiner and investigator at Stroz Friedberg.*

**\*As published in the November/December 2006 issue of *The Pennsylvania Lawyer* magazine.**