

DIGITAL FORENSICS: SLEUTHING ON HARD DRIVES AND NETWORKS

The anonymous e-mail demand was blunt: "This is your notice that you are being given two weeks time to give \$17,000,000 cash" or else "I will NOT deactivate all those servers that have been programmed to deliver DDOS attacks to IP attorneys world-wide, salvo after salvo, with compromised proprietary information."¹ The company victimized by this extortion demand had been on the receiving end of a harassing e-mail campaign for over a year but this e-mail catapulted an annoying situation into a crisis.

The same anonymous perpetrator had sent hundreds of "spoofed" e-mails designed to appear as authentic messages from the company's officials to customers with derogatory text about the company and attachments containing stolen confidential information and offensive sexually explicit patent applications. The perpetrator had successfully cloaked his identity by using unauthorized access to unprotected wireless computer networks in homes and businesses and computer labs at local universities. In short, this was a sophisticated hacker and cyber-crook who appeared capable of making good on his extortion threat to unleash the company's confidential and sensitive data to the world while shutting down, through distributed denial of service (DDOS), attacks the computers of customers and potential customers.

In this case, tracking the suspect required the combined resources of law enforcement, a behavioral psychologist and a private digital forensic and investigations firm. Over the course of three months, after the author's firm was brought into the case, steps were taken to ascertain whether the perpetrator was a malicious insider or outside hacker; to close security vulnerabilities within the company's network subject to exploitation, profiling, and other techniques; to identify the suspect and whether he was working alone or with co-conspirators, and to monitor the suspect's movements and connect his whereabouts to the locations where anonymous e-mails originated. In the end, he was caught "red-handed" in his car with his laptop, computer equipment, and an antenna used to "surf" the airwaves to find open wireless Internet connections to hijack. More items related to the attempted extortion were located in a search of the perpetrator's house, including firearms, components for hand grenades, explosive powder and the ingredients, such as large quantities of castor beans, for making ricin, which is fatal in small quantities.²

In-house counsel and outside attorneys are

usually the first people called when companies or individuals confront problematic situations that put their businesses in jeopardy. These situations may range from the lawsuit triggering electronic discovery obligations or a document demand for electronic records, to a network intrusion, denial of service attack, theft of intellectual property, an employee using the company network to download child pornography, or other kinds of unauthorized or even criminal activity. In each of these situations, the attorney is called upon not just for legal advice but also practical advice about what to do. Since most information created and received in an organization is generated electronically and is stored on hard disks,³ attorneys would well-serve their clients to know enough about digital forensics to make strategic decisions about its use in these situations, rather than forfeiting this evidence out of ignorance.

Attorneys do not have to become computer scientists or professional cyber-sleuths to use digital forensics and, in fact, should leave to the independent forensic experts the performance of computer and network examinations. Yet, given the ubiquity of electronic information and electronic storage devices, every attorney should have an appreciation of the scope and types of information that digital forensic examinations can reveal from desktop and laptop computers, servers, personal digital assistants (PDAs), cellular telephones, and Blackberries, not only to avoid missing useful evidence to support a client's claims, but also to anticipate its defensive applications.

This article will survey the different types of evidence to search for on a computer or network, and the more common situations where such evidence may be probative and computer forensic expertise helpful. While it is the job of expert computer forensic examiners to preserve and examine digital evidence in a manner that does not damage, modify, or alter the data, attorneys should themselves be familiar with the kinds of evidence that can be found on a computer to help clients appreciate when such expertise would be helpful.

When to Speed-Dial Computer Forensics Experts

The situations where the assistance of a computer forensic expert may be helpful or even necessary are myriad, and just a few are highlighted here. For example, possible employee malfeasance may warrant

examination of the employee's workplace computer. If a company suspects an employee is stealing, or using in an unauthorized manner, trade secrets or other confidential business information, such as customer lists or pricing data, examining the employee's computer may show improper copying or transfers of the stolen digital property onto thumb drives or other removable media, or to web-based e-mail accounts to avoid the corporate e-mail account. If a company discovers violations of workplace computer use policies involving employee installation of highly insecure peer-to-peer file-sharing software, compounded by use of that program to download pirated music or child pornography, the company may itself face liability risks associated with copyright infringement or possession of contraband.⁴ Forensic imaging and examination of the employee's computer may reveal the extent of the liability exposure and bolster any administrative sanction the company determines is appropriate.

When confronted with document demands, subpoenas for records, or electronic discovery preservation and production obligations, attorneys must balance their clients' legitimate concerns over compliance costs with the risks of compliance shortfalls.⁵ Noncompliance—inadvertent or caused by the intentional disregard of a litigation hold by a rogue employee—can have serious adverse repercussions for a company, ranging from costly spoliation sanctions to criminal liability for document destruction, either of which may be accompanied by reputational harm.⁶ A company served, for example, with a document demand for all e-mails for the CFO, should preserve and search not only that employee's workplace computer and e-mailbox on the networked server, but should also preserve and search file servers for archived e-mail, old computers used by the employee, PDAs, and other areas depending on the network topography and scope of the request. Using digital forensics to preserve the relevant data, particularly of "key players" in the litigation, may counter any subsequent claims of insufficient search and preservation efforts and may provide exculpatory evidence to allay suspicions of improper deletion activity. Indeed, one court, which has issued a series of influential decisions on the scope of the preservation duty, has advised that keeping a set of existing backup tapes and a going-forward procedure for segregating later-created documents, "along with a mirror image of the computer system taken at the time the duty to preserve attached

(to preserve documents in the state they existed at that time), creates a complete set of relevant documents.”⁷

In situations where electronic records appear to be missing, or exist in a form that is surprising to one party, a computer forensic examination may shed light on the discrepancy and even dispose of the case. For example, if examination of a computer shows that a wiping program was used to delete data and render the data unrecoverable, that fact alone may be sufficient, depending upon the timing of the use of the destructive program, to show consciousness of guilt in both civil and criminal cases.⁸ Where a “surprise” e-mail or other electronic record shows up in litigation, computer forensics can help establish its authenticity, or lack thereof, through examination not just of the record itself but the contextual clues found in critical areas of the hard drive, described in more detail below.⁹

What to Look for on Computer Hard Drives

The activities of a computer user can be revealed by examining the data in both the active file directories, which are accessible to the user, and hidden files, which are accessible only through expert analysis and use of forensic tools. Hidden data includes data stored in unallocated, slack, and swap space on the hard drive;¹⁰ files that the computer user has deleted; operating system logs; data from Internet surfing that the operating system has cached or automatically stored (without the user’s knowledge or active intervention), and unsaved data, which the user has viewed or created without intentionally saving, but the operating system automatically saved.

Caution must be exercised in getting to any of this information, since every time a computer is turned on and booted-up—or turned off—the data on the computer may be altered, modified, or even lost. For example, when a computer is turned on, the operating system automatically resets the clock and modifies the dates on documents and Excel spreadsheets that have been set by the computer user for automatic date setting. In addition, data stored in temporary memory is lost and new data can overwrite deleted data, making it unrecoverable. In many corporate networks, virus scans are triggered to run automatically upon boot-up, a process that can also alter metadata associated with files subject to the scan and over-write deleted data that might otherwise be recoverable. Computer forensic examiners use specialized tools to block a computer’s operating system from triggering these automatic processes that can alter data so that an exact bit-stream image of what is on a hard drive at a particular time is obtained for examination.

Computer Usage Overview

After a computer hard drive has been forensically preserved, a useful first step is to develop a general overview of its contents. A *System Usage 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.

Active Files

Active files are accessible to the computer user. Although finding the data that a user has either deleted from, or does not know has been saved automatically to, a hard drive is often the most revealing part of a computer forensic examination, active files provide valuable information, including information that a user has tried to hide in plain view by changing the file extension, applying a misleading name, or storing the file in an unusual location on the hard drive.

File System Metadata

Metadata, or “data about data,” is maintained about each file both by the operating system and in the file itself. Recent versions of the Windows operating system maintain three date and time stamps for each file: the *creation* date, when the file was first saved on the hard drive upon creation, downloaded from the Internet, or transferred from another media source; the *last modified* date, when the data within the file was last changed; and the *last accessed* date, when the file was last opened and viewed. These date/time stamps are known as “file system metadata” and are generally hidden from view, but can be accessed in Windows by clicking “File,” then “Properties.” The act of checking the “Properties” of a file, even if the file is not opened, will actually modify the system metadata of the file reviewed, absent the use of forensic tools.

The file system metadata stamps are applied to each file according to the computer clock, which can be reset or may not be accurate. If possible, computer forensic examiners often compare the subject computer’s clock setting upon seizure or acquisition of an image to evaluate the accuracy of the date/time settings.¹¹

The file system metadata can provide useful information about how the computer was used and when. The active files on a computer may be sorted by forensic examiners into chronological order by the date created, modified, or accessed to give an investigator a time-line of the activity on a computer. If, for example, criminal activity is documented on a computer during periods

when an employee has a confirmed alibi or is not on duty, investigators may want to expand the list of possible suspects or co-conspirators to other persons with access to the computer.

Embedded Metadata

In addition to date/time stamps maintained by the operating system, other metadata characteristics are embedded in the file itself, and therefore carried with the file no matter where it is stored or transferred. This aptly-named “embedded metadata” may contain additional details about a file that would otherwise be hidden. Embedded metadata is accessible in full only through use of specialized forensic tools. For example, many word processing and e-mail programs contain the author, revisions, and even names of people who made changes to a document.

Embedded metadata can be illuminating, as the British government learned to its embarrassment in February of 2003. During the debate about British participation in the Iraq war, the Blair administration published a dossier on Iraqi intelligence written in Microsoft Word on their web site. As shown below, the metadata embedded in the Word document revealed the last ten revisions to the document, the names of the people who worked on the document, and previous names of the file.¹²

In the report above [Image 1], the first section of metadata shows that this Word document was stored on a computer associated with Stroz Friedberg (the author’s firm). The second section of the metadata reflects the title of the document, while the third section shows that the document was created and last saved on “2/3/2003,” by the author “MKhan.” The last section of metadata displays the names of the last ten authors, who worked on the document and made each of the ten revisions, along with the file directory locations where each author saved the file, including the last of the ten authors, “MKhan.”

This otherwise hidden information in Microsoft Word documents can be used to track a document across both multiple computers and multiple authors. In this example, the metadata lists the users “P. Hamill,” “J. Pratt,” “A. Blackshaw,” “M. Khan,” and “cic22” as previous authors. The path listings of revision numbers 5 and 8 show that the file was saved to a floppy drive (A:\), which is most likely how the document made its way to the listed computers. In fact, the hearings before Parliament on this matter have since disclosed that the dossier was provided on a floppy disk to Mr. Blackshaw and subsequently to then-Secretary of State Colin Powell for his presentation before the United Nations.

Soon after the dossier was posted on the Internet a reader reported that the document was at least partially plagiarized from an

American researcher on Iraq and that the "intelligence" dossier had been edited by various press officers within the Blair administration. The Blair administration was subjected to hearings to explain to the British Parliament both the plagiarism and the role of the communications and press officials in the preparation of the dossier.

The date/time stamps can also be helpful in intellectual property theft cases in understanding the sequence of how the theft was accomplished. In *Jackson v. Microsoft Corp.*,¹³ 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 his 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.¹⁴

Shortcuts

Windows operating systems have a "shortcut" feature that appears as icons on the desktop. Shortcuts may be created for specific applications or files to which a computer user would like easy and quick access. Once created on the desktop, the shortcut icons provide access to the application or file with a double-click. The presence of a shortcut for a file or application can be highly probative of the user's knowledge of, familiarity with, and use of those files or applications. For example, in an online music piracy case, a defendant's denial of downloading copyrighted music may be refuted by the presence of a shortcut icon to Kazaa, Morpheus, or other peer-to-peer file sharing program on his or her computer. The dates of creation of a shortcut may also be recovered from the computer hard drive and may itself be probative of the user's state of mind. Installation of a shortcut to a "wipe" program on the date a document demand was delivered would be probative to show improper deletion activity, even if the wipe program itself had been installed months before.

Application Registry

Forensic examiners are able to recover from computer hard drives a list of all the systems or applications installed on a computer, including the dates of installation, use, and deletion. This can be useful information depending on

Image 1 - Embedded Metadata in Publicly-Available British Iraqi Intelligence Dossier



the nature of the case and circumstances of the activity under investigation. For example, evidence of the use of a de-fragmentation program to re-organize data on a hard drive (which over-writes data on portions of the hard drive and can make recovery of deleted data more difficult),¹⁵ or of a wipe program to erase data on a hard drive at around the same time that a suspect became aware of an investigation, would be probative of the user's state of mind.¹⁶ In embezzlement, fraud, or theft of intellectual property cases, the installation on a user's computer during a relevant time period of key-logging software used to collect user passwords and access codes remotely via computer networks, could provide key evidence as to how the crime was executed and the user's role in the crime.

Search History

The registry also maintains a list of searches conducted by a user on the computer and the date the search was done. The Windows search tool is accessed by using the search feature on the "start" menu or the "find" feature on the Microsoft Outlook e-mail program. Accessing this search history and finding out what searches a user conducted may reveal the preparatory steps taken to identify files to delete or copy from a computer. For example, an employee targeted in an internal fraud investigation who wants to delete all references to files related to the malfeasance, may first do a search for associated words and then proceed to delete each file containing a reference.

Renamed Files

Some users may try to hide files in plain view by re-naming the files or moving them to buried directories within the active files. As one court noted, "a computer user can mislabel or deliberately label files to avoid detection."¹⁷ Indeed, the web site of one vendor of a key-logging software program, which can be remotely installed on a target's computer and has been used to gain unauthorized access to computers, expressly counsels purchasers of its program on how to hide its installation, stating:

You may wish to change the NAME of this INSTALL file to something like MyPhotos.exe or CompanyUpdate.exe or another name you think will make it more likely that the child or employee will click on.¹⁸

The Windows operating system and other application programs automatically apply file extensions to the ends of file names to identify the type of file it is. Microsoft Word document files are automatically designated with the extension ".doc" at the end of the file name; Excel spreadsheets carry the extension ".xls"; picture or graphic files carry the extensions .gif, .jpg, .tif, .pdf, or .emf, as well as others. These naming convention extensions may be manually modified by a computer user in an effort to hide them, but forensic tools may be employed to check the files and determine whether there is a mismatch between the type of file and the extension and identify those files for which the extensions have been intentionally modified or renamed. For example, a former employee who has

stolen a "CUSTOMER LIST.xls" may attempt to hide the file by renaming it "BIRTHDAY.PIX.gif" with a different file name and extension. This effort can boomerang if it is discovered and provide valuable confirmation of the employee's culpable state-of-mind and knowledge of inculpatory files.

Keyword Searches and Other Filters

Hard drives may hold millions of pages of files and present an overwhelming volume of information for counsel to review. This task is made more manageable by developing a list of keywords or other filters designed to identify those files with information relevant to the case or investigation. Keyword searches can be conducted not only on the active files in allocated space on the hard drive, but also on other spaces on the hard drive that are only accessible through use of forensic tools.

A powerful search program, called dtSearch, may also be used by forensic examiners to index every word in active files, including e-mail, on a hard drive, or associated network, to facilitate searches. The index will show the number of times a word (or its synonyms, phonetic spellings, or misspellings) appears and in which files, with the "hits" highlighted and displayed for easy access. This search utility allows rapid searches for words or phrases over many gigabytes of data since the search is conducted on the index, rather than by accessing the actual files.

Instead of looking for a specific keyword on the hard drive, it may be more important to identify all telephone numbers, e-mail addresses, or physical street addresses that may be present on the hard drive. Even when the specific number or address being searched for is unknown, forensic examiners are able to use a sophisticated UNIX search utility, called the generalized regular expression parser (GREP), to identify forms of text rather than a specific text, and cull from a hard drive, lists of physical addresses, e-mail addresses, or telephone numbers that are stored on the computer.

For example, if a company wants to locate the persons who have been acting in collusion with a disgruntled employee to post derogatory or confidential information about the company, a forensic examiner could use a GREP search on the hard drive for any telephone numbers, physical addresses, or e-mail addresses, without any specific information on the precise numbers or addresses. Similarly, in an identity theft case, in which an investigator was interested in finding all social security numbers and birth dates on a hard drive to determine whom the suspect may have victimized, the forensic examiner would be able to use a GREP search to identify any such personal information present on the hard drive.

Deleted Files

Deletion of files from computers using the

Windows operating system changes the file path, or location, of the files from the active directory to the recycling bin, where the file may be recovered until the user empties the bin or the bin fills up and the system overwrites the oldest files. Users are also able to program the settings for the recycle bin to empty automatically at set periods of time of the user's choice. Booting up a computer in a non-forensically sound manner can trigger the dumping of deleted data from the recycling bin.

Files that are emptied from the recycling bin are not accessible without a forensic examination. Using forensic tools, a forensic examiner can profile a computer for the names of the files that have been deleted since the installation of the computer's operating system. This profile can be compiled in a spreadsheet format showing in chronological order the names of files that were deleted by the computer user or automatically by system files and whether the files were overwritten. 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.¹⁹

Deleted files that have not been overwritten in unallocated or slack space may be recoverable in full or in fragments, although these recovered files may not have clear creation or deletion dates associated with them. [Image 2]

Unsaved Data

Data that has appeared on the computer screen but not saved by the user is oftentimes cached on the hard drive and still accessible through forensic analysis. This data can include: web pages the user has viewed on the Internet; e-mails that the user has opened but not saved to the hard drive; any data, such as text, graphics, or spreadsheet cells, which a user has pasted and moved from one file to another; or text that a user has created on the computer but stored to a floppy disc or a network server, rather than to the hard drive. Generally, the greater the frequency of new data being saved to the hard drive and the longer a computer is in use, the higher the probability that older, deleted data will be overwritten.

This feature of computers helped solve an investigation in which an anonymous letter containing derogatory and confidential information about the company was received, and the company sought to identify the author before the information was disseminated more widely. Forensic analysis of the company's computers revealed a draft of the letter in the swap space of a computer used by one 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.

Internet History

When a computer user surfs the Internet, the Windows operating system captures URLs or addresses on the Internet that the user views, along with the date and time the viewing occurred. In addition, the operating system saves every search that the user types into the Internet Explorer browser. Forensic examiners are able to capture the URLs accessed from a particular computer and produce that history in both text form and in HTML format so that the URLs that are still operative may actually be accessed.

The Internet history can provide valuable information about a computer user's interests and access to information that may be relevant to a case. Bookmarks on the Internet search engine highlight for investigators those online sites in which the user has particular interests.²⁰ For example, a suspect in a harassment or stalking case, who claims not to know that the victim lived at 3400 International Drive, would have a difficult time explaining why the Internet history from his computer hard drive showed him searching a map site for directions to that specific address, which he had typed into his browser. [Image 3]

The hard drive will regularly cache the code constituting web site pages visited in a series of temporary files. These temporary files will in part still exist as active files on the disk. However, since the size of the storage area assigned to house these files on the disk is limited in size by a number of factors, cached temporary Internet files tend to be deleted and overwritten; but they may be recovered in whole or in fragments using forensic tools. Since this data is not organized in any fashion, the best way to find this data in unallocated space on the hard drive is by doing customized searches, including for specific URLs that have been identified as those visited by the user or for keywords that may have appeared in the URLs.

Printer Spool History

The fact that a computer user printed a particular document or information from a computer may be relevant to the user's knowledge of the document's existence and its importance or to an understanding of what a user did with the document. For example, in an economic espionage, theft of trade secrets, or intellectual property case, the fact that a suspect printed key information from a company computer in order to remove it from the premises is important information that can be gleaned from a log maintained on the computer of the temporary files created for files printed from both the computer hard drive and removable media installed on the machine.

Image 2 - Example of a deleted file spreadsheet

File Name	File Ext	Description	Last Accessed	Last Written	File Created	Evidence File	Original Path
LC420c.doc	doc	File, Deleted, Overwritten	2/12/2002	10/14/99 02:32:54PM	02/12/02 10:07:10AM	GatewayGT	GatewayC:\Program Files\Norton AntiVirus\Q_LDVP_VDBV\D10A8D7_VDBWLD\swex15.exe
LC420b.doc	doc	File, Deleted	2/12/2002	10/14/99 02:32:30PM	02/12/02 10:07:10AM	GatewayGT	
LC420a.doc	doc	File, Deleted	2/12/2002	10/14/99 02:32:14PM	02/12/02 10:07:10AM	GatewayGT	
LC419h.doc	doc	File, Deleted, Overwritten	2/12/2002	10/14/99 02:40:22PM	02/12/02 10:07:08AM	GatewayGT	GatewayC:\Program Files\Norton AntiVirus\Q_LDVP_VDBV\D10A8D7_VDBWLD\swex15.exe
LC419g.doc	doc	File, Deleted	2/12/2002	09/03/99 11:02:54AM	02/12/02 10:07:16AM	GatewayGT	
LC419f.doc	doc	File, Deleted	2/12/2002	09/03/99 11:25:20AM	02/12/02 10:07:14AM	GatewayGT	
LC419e.doc	doc	File, Deleted	2/12/2002	09/03/99 10:42:02AM	02/12/02 10:07:16AM	GatewayGT	
LC419d.doc	doc	File, Deleted	2/12/2002	09/03/99 10:30:52AM	02/12/02 10:07:16AM	GatewayGT	
LC419c.doc	doc	File, Deleted, Overwritten	2/12/2002	09/03/99 10:36:30AM	02/12/02 10:07:16AM	GatewayGT	GatewayC:\Program Files\Norton AntiVirus\Q_LDVP_VDBV\D10A8D7_VDBWLD\swex15.exe
LC419b.doc	doc	File, Deleted, Overwritten	2/12/2002	09/03/99 10:32:42AM	02/12/02 10:07:20AM	GatewayGT	GatewayC:\Program Files\Norton AntiVirus\Q_LDVP_VDBV\D10A8D7_VDBWLD\swex15.exe
LC419a.doc	doc	File, Deleted, Overwritten	2/12/2002	09/03/99 10:27:19AM	02/12/02 10:07:20AM	GatewayGT	GatewayC:\Program Files\Norton AntiVirus\Q_LDVP_VDBV\D10A8D7_VDBWLD\swex15.exe
LC409h.doc	doc	File, Deleted, Overwritten	2/12/2002	09/03/99 10:22:38AM	02/12/02 10:07:20AM	GatewayGT	GatewayC:\Program Files\Norton AntiVirus\Q_LDVP_VDBV\D10A8D7_VDBWLD\swex15.exe
LC409g.doc	doc	File, Deleted	2/12/2002	12/15/97 11:04:02AM	02/12/02 10:07:48AM	GatewayGT	
LC409f.doc	doc	File, Deleted	2/12/2002	12/15/97 10:56:58AM	02/12/02 10:07:48AM	GatewayGT	
LC409e.doc	doc	File, Deleted	2/12/2002	12/15/97 10:46:15AM	02/12/02 10:07:48AM	GatewayGT	
LC409d.doc	doc	File, Deleted	2/12/2002	12/15/97 10:44:10AM	02/12/02 10:07:55AM	GatewayGT	
LC409c.doc	doc	File, Deleted	2/12/2002	12/15/97 10:36:40AM	02/12/02 10:07:55AM	GatewayGT	
LC390 Dust Free.doc	doc	File, Deleted, Overwritten	2/12/2002	12/15/97 09:36:46AM	02/12/02 10:07:52AM	GatewayGT	GatewayC:\Program Files\Common Files\Dynastec\Shared\Views\Defn_MP3184_TbP\swex15.exe
LC140.doc	doc	File, Deleted	2/12/2002	02/07/00 08:27:20PM	02/12/02 10:06:24AM	GatewayGT	
LC1400.doc	doc	File, Deleted	2/12/2002	10/14/99 01:49:14PM	02/12/02 10:07:12AM	GatewayGT	
LC128 Kleen.doc	doc	File, Deleted	2/12/2002	02/15/00 01:47:02AM	02/12/02 10:06:24AM	GatewayGT	
Piney Bows.doc	doc	File, Deleted, Overwritten	2/12/2002	09/15/99 07:57:26AM	02/12/02 10:07:12AM	GatewayGT	GatewayC:\Program Files\Norton AntiVirus\Q_LDVP_VDBV\D10A8D7_VDBWLD\swex15.exe
M98 1.doc	doc	File, Deleted, Overwritten	2/12/2002	09/15/99 09:11:12AM	02/12/02 10:07:24AM	GatewayGT	GatewayC:\Program Files\Norton AntiVirus\Q_LDVP_VDBV\D10A8D7_VDBWLD\swex15.exe
MASTER LIST.doc	doc	File, Deleted	2/12/2002	09/14/99 03:06:44PM	02/12/02 10:07:14AM	GatewayGT	
MASTER LIST PRIVATE.doc	doc	File, Deleted	2/12/2002	01/12/99 12:34:16PM	02/12/02 10:07:48AM	GatewayGT	
MASTER LIST CLEANTEXT.doc	doc	File, Deleted, Overwritten	2/12/2002	04/10/99 07:36:54AM	02/12/02 10:07:26AM	GatewayGT	GatewayC:\Program Files\Common Files\Dynastec\Shared\Views\Defn_MP3184_TbP\swex15.exe
REBATE.doc	doc	File, Deleted	2/12/2002	07/25/97 01:15:03PM	02/12/02 10:07:58AM	GatewayGT	
ASSESSMENT.doc	doc	File, Deleted, Overwritten, Archive	2/12/2002	02/11/02 11:38:14AM	02/11/02 11:38:12AM	GatewayGT	GatewayC:\Program Files\Common Files\Dynastec\Shared\Views\Defn00000000_00VWRSCA8 DAT
Letter to Bill	ink	File, Deleted, Overwritten, Archive	2/12/2002	02/11/02 11:38:14AM	02/11/02 11:38:12AM	GatewayGT	GatewayC:\Program Files\Common Files\Dynastec\Shared\Views\Defn00000000_00VWRSCA8 DAT
Cleaner.doc	doc	File, Deleted, Archive	2/12/2002	02/11/02 04:45:30PM	02/11/02 04:45:28PM	GatewayGT	
Airlines.doc	doc	File, Deleted, Overwritten	2/12/2002	03/09/99 09:17:46AM	02/12/02 10:06:54AM	GatewayGT	GatewayC:\Program Files\Norton AntiVirus\Q_LDVP_VDBV\D10A8D7_VDBWLD\swex15.exe
Comp.doc	doc	File, Deleted	2/12/2002	01/03/99 11:06:02AM	02/12/02 10:07:42AM	GatewayGT	
Microdot.doc	doc	File, Deleted, Overwritten	2/12/2002	12/14/99 02:24:48PM	02/12/02 10:07:06AM	GatewayGT	GatewayC:\Program Files\Norton AntiVirus\Q_LDVP_VDBV\D10A8D7_VDBWLD\swex15.exe
COMPACT2 COMP.doc	doc	File, Deleted, Overwritten	2/12/2002	12/14/99 02:12:10PM	02/12/02 10:07:06AM	GatewayGT	GatewayC:\Program Files\Norton AntiVirus\Q_LDVP_VDBV\D10A8D7_VDBWLD\swex15.exe
COMP1407.doc	doc	File, Deleted, Overwritten	2/12/2002	12/14/99 02:12:58PM	02/12/02 10:06:58AM	GatewayGT	GatewayC:\Program Files\Norton AntiVirus\Q_LDVP_VDBV\D10A8D7_VDBWLD\swex15.exe

Removable Media History

Forensic examiners are able to determine from an examination of a hard drive whether and when any programs were installed to use external media, such as compact discs or floppy discs. In addition, analysis can often reveal what data was copied to removable media and when. This information may be relevant in intellectual property theft cases, where evidence that an employee copied sensitive business files on a removable media would be highly probative of how and when the data was stolen.

Logging

Log file analysis is an essential tool for forensic examiners in cases that involve suspicious modification of or alterations to a computer system. These cases can include the backdating of electronic documents, installation or use of wiping software, or hacked computer networks. The types of log files that exist are as varied as the computers and servers from which they are produced. User activities on newer Windows-based laptop or desktop computers are logged in the *Windows Event Logs*. Similarly, UNIX-based operating systems, which are used on many servers and Linux-based PCs, also log user activities entered in a file called a history file. These logs track significant occurrences on the computer system and, in the case of event logs, include errors logged by applications, valid and invalid logon attempts, installation or removal of software programs, and the deletion of files. Depending on the requirements of the case, log files can be used by the forensic examiner to corroborate computer use at a certain period of time, examine possible tampering with the system clock to back-date documents, or look for the installation of a particular program like a key logger, which captures all the keystrokes

made by a computer user, or a root-kit, which is a set of hacker tools to gain administrator level access and control over computer functions.

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 evaluate, authenticate, and give context to e-mails and other electronic records that are central to a case. Moreover, as the rules governing electronic discovery continue to evolve and the sanctions for spoliation make headlines, the use of forensic methods to preserve electronic data, particularly for key players, should be considered, as such preservation can provide exculpatory demonstrations that data was not improperly deleted, and is a recommended option for the most risk-sensitive situations, including law enforcement and regulatory agency investigations.

Digital forensics also plays an important role in investigating malicious and criminal computer activity. The case of the extortion demand mentioned at the outset of the article ended happily for the victimized company: digital forensic analyses, combined with other investigative methods, were able to provide assurance that no disgruntled insider was involved and established the perpetrator's guilt beyond any doubt. After pleading guilty, he is currently serving sixty-three months in prison on the cyber-extortion charges and was sentenced in another district on September 13, 2005, to a consecutive term of forty-one months in prison for his possession of ricin and improvised hand grenades.²¹

Beryl A. Howell, Esq., is the Managing

Director and General Counsel of the Washington, DC office of Stroz Friedberg, a consulting and technical services firm specializing in computer forensics and cybersecurity investigations. Samuel Rubin, Consultant and Computer Forensic Examiner at the firm, assisted in the preparation of this article.

¹ News Release, U.S. Attorney's Office, Eastern District of Virginia, with attached STATEMENT OF FACTS, §11 (June 8, 2004) in matter of U.S. v. Tereshchuk, Crim. No. 04-149-A (emphasis in original e-mail). This cyber-extortion investigation by Stroz Friedberg was featured in Timothy O'Brien, *The Rise of the Digital Thugs*, N.Y. TIMES, Aug. 7, 2005, available at <http://www.nytimes.com/2005/08/07/business/yourmoney/07stalk.html?ex=1130299200&en=64615c52165e842f&ei=5070>.

² News Release, "Hyattsville Man Sentenced for Possession of Destructive Device, Biological Weapon," U.S. Attorney's Office, District of Maryland (Sept. 13, 2005) available at http://www.usdoj.gov/usao/md/press_releases/press05/TereshchukSentencePR.pdf.

³ THE SEDONA GUIDELINES: BEST PRACTICE GUIDELINES & COMMENTARY FOR MANAGING INFORMATION & RECORDS IN THE ELECTRONIC AGE (Sept. 2005), at vi, available at http://www.thosedonaconference.org/content/miscFiles/TSG9_05.pdf.

⁴ In the past year, half of Fortune 500 companies experienced at least one workplace Internet pornography incident. Delta Consulting, "Survey: Inappropriate Images in the Workplace" (June, 2005). For fuller discussion of liability risks, see B.A. Howell & P.H. Luehr, *Child Porn Poses Risks to Companies that Discover it in the Workplace*, N.Y. L.J., Oct. 4, 2004, available at <http://www.strozllc.com/ChildPornPosesRisks.pdf>.

⁵ For fuller discussion of digital forensics use in electronic discovery, see B.A. Howell, *Strategic Planning at Outset of E-discovery Can Save Money in the End*, DIGITAL DISCOVERY & E-EVIDENCE, Feb. 2005, at 6.

⁶ *Coleman Holdings, Inc. v. Morgan Stanley*, 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005) (adverse jury instruction imposed as sanction for discovery abuse, contributing to \$1.5 billion verdict against the defendant); *U.S. Phillip Morris USA Inc.*, 327 F. Supp. 21 (D.D.C. 2004) (deletion of e-mail subject to preservation resulted in \$2,750,000 fine for

Image 3 - Example of an Internet history spreadsheet

B1	URL	08/17/01	0 08/20/01	0	2001081320010820	lcats@http://hw15fd.law15.hotmail.msn.com/cgi-bin/premail/4173			
B2	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@http://hw15fd.law15.hotmail.msn.com/cgi-bin/getmsg?cumbox=F000000001&a=3240bd081c014c			
B3	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@http://hw15fd.law15.hotmail.msn.com/cgi-bin/hmhome?cumbox=F000000001&a=4b4d3691b05f1			
B4	URL	08/17/01	0 08/20/01	0	2001081320010820	lcats@Host: 64.4.22.23			
B5	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@Host: www.reliaquote.com			
B6	URL	08/17/01	0 08/20/01	0	2001081320010820	lcats@http://hw15fd.law15.hotmail.msn.com/cgi-bin/HotMail?cumbox=F000000001&a=457432a1bdaa			
B7	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@http://www.yahoo.com/r/m/p			
B8	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@http://64.4.22.23/reidlog/hmhinbox?url=http%3a%2f%2b15fd%2elaw15%2ehotmail%2emsn%			
B9	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@http://maps.yahoo.com/py/maps.py?Pyt=Tmap&addr=3400+International+Drive+NW&city=Wash			
B0	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@http://maps.yahoo.com/py/maps.py?Pyt=Tmap&addr=3400+International+Drive+NW&city=Wash			
B1	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@http://hw15fd.law15.hotmail.msn.com/cgi-bin/HotMail?cumbox=F000000001&a=4b4d3691b05f1			
B2	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@http://64.4.22.23/reidlog/hmhinbox?url=http%3a%2f%2b15fd%2elaw15%2ehotmail%2emsn%			
B3	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@Host: popup.msn.com			
B4	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@http://maps.yahoo.com			
B5	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@http://maps.yahoo.com/py/maps.py?Pyt=Tmap&addr=3400+International+Drive+NW&city=Wash			
B6	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@Host: maps.yahoo.com			
B7	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@http://hw15fd.law15.hotmail.msn.com/cgi-bin/saferd/867329.DOC? lang=EN&hm_tg=http%3a%			
B8	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@http://maps.yahoo.com/py/maps.py?BFCat=&Pyt=Tmap&newFL=Use+Address+Below&addr=3-			
B9	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@http://hw15fd.law15.hotmail.msn.com/cgi-bin/hmhome?cumbox=F000000001&a=3240bd081c014c			
B0	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@http://hw15fd.law15.hotmail.msn.com/cgi-bin/HotMail?cumbox=F000000001&a=3240bd081c014c			
B1	URL	08/16/01	0 08/20/01	0	2001081320010820	lcats@http://maps.yahoo.com/py/maps.py?Pyt=Tmap&addr=3400+International+Drive+NW&city=Wash			
B2	URL	08/17/01	0 08/20/01	0	2001081320010820	lcats@http://hw15fd.law15.hotmail.msn.com/cgi-bin/hmhome?cumbox=F000000001&a=bd1c1a843159a			
B3	URL	08/17/01	0 08/20/01	0	2001081320010820	lcats@http://hw15fd.law15.hotmail.msn.com/cgi-bin/HotMail?cumbox=F000000001&a=9085b6e6570fd			
B4	URL	08/17/01	0 08/20/01	0	2001081320010820	lcats@http://hw15fd.law15.hotmail.msn.com/cgi-bin/HotMail?cumbox=F000000001&a=fa0b80aa2077c			
B5	URL	08/17/01	0 08/20/01	0	2001081320010820	lcats@http://hw15fd.law15.hotmail.msn.com/cgi-bin/getmsg?cumbox=F000000001&a=fa0b80aa2077c			
B6	URL	08/17/01	0 08/20/01	0	2001081320010820	lcats@http://hw15fd.law15.hotmail.msn.com/cgi-bin/getmsg?cumbox=F000000001&a=9085b6e6570fd			

spoliation sanction); see also *U.S. v. Lundwall*, 1 F. Supp. 2d 249 (S.D.N.Y. 1998) (general obstruction statute, 18 U.S.C. § 1503 reaches the willful destruction of documents during civil litigation).

⁷ *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003); but see *In Re First Energy Corp. Securities Litigation*, 2004 U.S. Dist. LEXIS 28317 (N.D. Ohio) (defendant's refusal to comply with plaintiff's request that a computer forensic expert create an exact duplicate of computers and other electronic storage devices to protect the stored data from alteration, was not sufficient to show preservation risk warranting lift of discovery stay in securities class action lawsuit).

⁸ *Bond v. Polycycle*, 732 A.2d 970, 976-77 (Md. Ct. Special App. 1999) (former employee who downloaded onto floppy disks and then erased from company's computers all his work product on the night before his resignation, misappropriated trade secret information); *LeJeune v. Coin Acceptors, Inc.*, 849 A. 2d 451 (Ct. of App. 2004) (former employer copied confidential files from work laptop to CD and then erased over 400 files from laptop suggesting that he "was attempting to hide his conduct and was aware that transferring the files was improper"); see also *State of Vermont v. Voorheis*, 844 A.2d 294, 800-801 (Super. Ct. 2004) (forensic analysis of defendant's computer showed that "shortly after the police investigation started, defendant installed and ran a software program ... which makes files completely unrecoverable" and was part of the "compelling" evidence of a conspiracy); *State of Missouri v. Tripp*, 2005 Mo. App. LEXIS 848 (Ct. App., W.D.) (forensic examination of defendant's laptop showed he had deleted a Microsoft Office suite of programs on the night of the murder, resulting in deletion of related files, raising an inference of consciousness of guilt).

⁹ See, e.g., *Munshani v. Signal Lake Venture Fund II*, 2001 Mass. Super. LEXIS 496 (Suffolk Super. Ct.) (forensic expert determined that e-mail proffered by plaintiff to avoid a statute of frauds defense was not authentic, resulting in dismissal of \$25 million lawsuit).

¹⁰ "Unallocated space" is the portion of the hard drive that the file system designates as unused and available for the recording of new data. When a file is deleted, the file system marks the space previously occupied by the file as unallocated and available for

reuse. Data is written to the hard drive in uniform chunks called "clusters." When the size of a file is smaller than the size of the cluster it occupies, the remaining area is called "slack space." This space can contain fragments of previously deleted files. "Swap space" is the portion of the disk that can be used to store information while an application or process is running.

¹¹ *State of Ohio v. Cook*, 149 Ohio App. 3d 422, 428 (2d App. Dist. 2002) (detective who made image of hard drive "checked the date and time shown on the computer's internal clock with the 'real world' time" and determined the "computer's clock was within five minutes of the actual date and time").

¹² An analysis of the original dossier from February 5, 2003 is posted online at <http://www.casi.org.uk/discuss/2003/msg00457.html>.

¹³ 211 F.R.D. 423 (W.D. WA, 2002).

¹⁴ See also *Leonard v. State of Texas*, 767 S.W.2d 171 (Tex. Crim. App. 1988) (defendant's conviction for theft of trade secrets upheld where, *inter alia*, creation dates of proprietary files in defendant's possession were prior to defendant leaving the complainant's employment).

¹⁵ Files are laid down contiguously on hard drive tracks, but as older files are deleted and over-written with new files, the new files may be laid down in fragmented clusters rather than contiguously. This fragmentation of active files can slow down the retrieval of files and operation of the computer. Defragmentation of, or defragging, the hard drive moves the fragments of active files into contiguous tracks and clusters and can speed up the operation of the computer.

¹⁶ See, e.g., *U.S. v. Triumph Capital Group, Inc.*, 211 F.R.D. 31, 55 (D. Conn. 2002) (installation shortly after investigation began of software wiping program Destroy-it on company computer corroborated cooperator's information that the defendants planned to delete incriminating data and confirmed reasonableness of government's use of forthwith subpoena).

¹⁷ *U.S. v. Triumph Capital Group, Inc.*, 211 F.2d at 62; see also *U.S. v. Hill*, 322 F. Supp. 2d 1081, 1090 (C.D. CA 2004) (computer search that was not limited to certain file extensions or keywords upheld since "images can be hidden in all manner of files," and data can be concealed by "the simple expedient of changing the names and extensions

of files to disguise their content from the casual observer."); *U.S. v. Hunter*, 13 F. Supp. 2d 574, 483 (D.Vt. 1998).

¹⁸ See www.spectersoft.com.

¹⁹ *Advantacare Health Partners, LP v. Access IV*, 2004 U.S. Dist. LEXIS 16835 (N.D. Cal.) (forensic examination showed that former employees tried to conceal their copying of business information by searching online and downloading BC Wipe, a computer file deletion program, shortly after service of a cease-and-desist order by their former employer, and then using that wipe program to delete over 13,000 files from a hard drive, warranting monetary and adverse jury instruction sanctions).

²⁰ See, e.g., *U.S. v. Al-Marri*, 230 F. Supp. 2d 535, 537 (S.D.N.Y. 2002) (FBI examination of defendant's laptop revealed files containing credit card numbers and expiration dates and "bookmarks to several web sites that could be used to assist a person conducting credit card fraud").

²¹ News Release, *supra* note 2.

