What Every Lawyer Needs to Know About Computer Forensic Evidence

by Sid Leach
Snell & Wilmer L.L.P.

Many years ago, a typical lawsuit would usually involve proofs in the form of documentary evidence. Hard copies of paper documents would be the focus of discovery and an important source of proof at trial.

Today, virtually everyone uses a computer at work, and a company's documents and business information are most likely to be contained in electronically stored files and databases. In today's world, the most relevant evidence is likely to be in the form of electronically stored information. Electronically stored email communications are likely to be relevant.

Trade secret misappropriation cases can often be high stakes litigation, involving significant damages claims and/or being directed to important products or proprietary technology. *See, e.g., DSC Communications Corp. v. Next Level Communications*, 107 F.3d 322, 325 (5th Cir. 1997) (jury awarded $369,200,000 in damages, which was subsequently reduced to $136,732,000, and the judgment on the reduced amount was affirmed on appeal). Computer forensic evidence may be key to proving a plaintiff's case. It can also make the difference between winning and losing for a defendant.

Many companies provide engineers and sales personnel with a company-owned laptop to use in connection with the employee's work, and employees are commonly allowed to take the laptop home. When the employee resigns or is discharged, the company-owned laptop typically must be returned to the company. If an employee is not provided with a company-owned laptop, then the employee typically uses a personal computer or workstation at work, and all such company-owned equipment is usually retained by the company upon the employee's departure. Crucial evidence of a departing employee's theft of trade secrets may be hidden on the company's computer equipment. A forensic examination of a departing employee's laptop or computer workstation can provide a goldmine of information concerning what the ex-employee was doing prior to departure. However, if a lawyer does not take timely measures to investigate or preserve such evidence, the relevant computer data can be lost because it may be over-written during normal use of the computer equipment subsequent to the ex-employee's date of departure.

In a copyright infringement case where the copyrighted subject matter involves computer files, computer forensic evidence may be crucial in proving that a defendant copied the plaintiff's copyrighted work. For example, in a case involving a claim that a defendant downloaded copyrighted music over the Internet, a forensic examination of the defendant's personal computer may show that file sharing software was present on the computer, that copyrighted songs were downloaded, when the copyrighted files were downloaded, and what username was used by the defendant to log onto filing sharing websites.

A lawyer representing a defendant on the receiving end of a lawsuit will often need to advise his or her client on how to best defend a lawsuit in which computer forensic evidence will be very important. In modern litigation, an ever increasing percentage of the relevant documents are in electronic form, rather than paper form. *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 427 (S.D.N.Y. 2002) ("Electronic documents are no less subject to disclosure than paper records.").

This paper is intended to provide lawyers with important information about the type of computer data that can be obtained from a forensic examination of computer equipment. In addition, this paper is intended to assist counsel in making better-informed decisions about electronically stored information when computer forensic evidence is a key factor in the case.

A. Example Cases

The case of *AdvantaCare Health Partners, L.P. v. Access IV*, 2004 WL 1837997 (N.D. Cal. Aug. 17, 2004), is a good example of why it can be advantageous for a plaintiff to have a computer forensic expert. In that case, two employees resigned and began a competing business. The defendants were served with a TRO on the afternoon of October 6, 2003. The TRO prohibited the defendants from using, copying, or destroying any of the plaintiff's data, and required the defendants to permit the plaintiff to make forensic copies of the hard drives and network servers of their new company. Later that day, after being served with the TRO, one of the defendants visited numerous websites searching for computer data deleting software. That evening, the defendant obtained an anti-forensic software program called BC Wipe, and over the next four days deleted more than 13,000 files from his home computer using BC Wipe. *Id.*, at *2.

The plaintiff hired a computer forensics expert. The forensic expert was able to show that one of the defendants had accessed his former employer's computer network and copied a large number of the company's files prior to leaving, including files containing company policies and procedures, patient databases, employee lists, and contracts. The forensic expert also determined that the defendant tried to conceal his copying activities by deleting copied files from his hard drive. Based on the evidence developed by the computer forensic expert, the plaintiff obtained a sanction instructing the jury to that they must find that the defendants copied all of the files on the plaintiff's computers. *Id.*, at *11.

The case of *New Hampshire Ball Bearings, Inc. v. Jackson*, 158 N.H. 421, 969 A.2d 351 (2009), is a good example of why it can be important for a defendant to have a computer forensic expert. In that case, the plaintiff company had a history of suing departing employees and accusing them of trade secret misappropriation. The plaintiff company had its own IT employees trained in computer forensics, and had the software and equipment to make a mirror image of the hard drive of every departing employee's computer so it could be examined for suspicious activity. Only a few months after losing the last case it filed against a departing employee, the plaintiff sued another departing employee, who was later found to be innocent of trade secret misappropriation by a jury.

Prior to filing the lawsuit, an IT employee was instructed to take the hard drive that had been used by the departing employee out of the safe in New Hampshire. Instead of using the software and equipment available in New Hampshire to make a forensic image of the hard drive, (which he was trained to do), this IT employee was instructed to get on a plane and take the hard drive out to the company's offices in California, allegedly so the hard drive could be used in yet another class that the employee attended to gain instruction on the use of computer forensic software. In this instance, a private class had allegedly been arranged for just two of the company's IT employees.

After arriving in California, the IT employee was told that the class had been cancelled, and to return back to New Hampshire. Although the director of IT had told him before he got on the plane not to let the hard drive out of his sight, those instructions were overruled by someone in California, and he was told to leave the hard drive in California where they would take good care of it. After he left, another IT employee in California accessed the hard drive without using a “write block” hardware device he had on hand, and which he knew he was required to use to prevent any changes being made to the contents of the hard drive.

After the hard drive was accessed without a write block device, the IT person in California made a forensic image of the hard drive before the class was rescheduled for the following week. Allegedly, when the forensic image made in California was examined during the class, they claimed that some files on the hard drive had sequential access times. A new forensic expert was retained who had never done any work for the company, (even though the company had an established relationship with a large nationwide reputable computer forensic firm that had been used in the company’s prior cases), and the expert was provided with the forensic image that the IT employee in California had made. No mention was made to the computer forensic expert of the fact that the hard drive had been accessed without a “write block” device. The computer forensic expert then signed an affidavit stating that, in his opinion, the sequential access times on the files was evidence that the former employee copied trade secret files from his company-owned laptop prior to departure from the company.

The plaintiff provided false interrogatory answers stating that no one had accessed the departing employee’s computer hard drive, and no data had been altered or modified on the hard drive. The plaintiff also provided false interrogatory answers that omitted the name of the IT employee in California from the list of people who had possession of, or access to, the former employee’s computer and hard drive after it was returned to the company.

The former employee and his new employer were sued for trade secret misappropriation. The defendants retained a computer forensic expert. The defendant’s expert discovered that the hard drive had been accessed without a write-block device after the employee turned it back in. The plaintiff was forced to amend its answers to interrogatories, and admit after the close of discovery, that the IT employee in California had accessed the hard drive, and had done so without a “write block” device. In addition, the defendants’ expert testified that the trade secret files allegedly copied by the former employee would not fit on the thumb drive he allegedly used, because it did not have sufficient memory capacity to store those files along with his personal files that were undisputedly copied at the same time. At trial, the jury found in favor of the defendants on the trade secret misappropriation claim. If the defendant had not had his own computer forensic expert, the evidence raising questions about the plaintiff’s forensic image of the former employee’s hard drive would never have come to light.

B. Computer Forensics

Computer forensics deals with the preservation, identification, extraction and documentation of computer evidence. Computer forensic investigations take advantage of the way computers store and retrieve data. Relevant computer data usually includes information stored in files on a hard drive, as well as information in files that were “erased” from the hard drive. Computer forensics also takes advantage of the way personal computers operate, and the temporary and/or permanent information recorded by the operating system during normal operation. During normal operation, a Windows operating system on a PC will record data identifying thumb drives that were connected to a computer, the date and time a file was last accessed or modified, Internet searches, Internet websites visited, email read or sent using the computer, and computer programs that were installed or used on the computer.

This paper will focus on computer forensic evidence available on a personal computer ("PC") employing Windows as the operating system. For simplicity of illustration, the specific examples and details discussed in this paper, unless otherwise noted, are for Windows XP because it is a common operating system used in business enterprises. However, much of the discussion also applies to Windows 95, Windows 2000, Windows Vista, Windows NT, Windows 7, and personal computers running other operating systems.

1. Computer Forensic Images

A forensic image of a computer storage device, (*e.g.*, a hard drive of thumb drive), is an exact replica, bit for bit, of the contents of the original storage device. *New Hampshire Ball Bearings, Inc. v. Jackson*, 158 N.H. 421, 424, 969 A.2d 351, 356 (2009) ("A forensic image is an exact replica, bit for bit, of the original storage device that allows investigation of past use without altering the original evidence.").

The forensic image of a computer hard drive is sometimes referred to as an evidence file. The copy of the contents of a hard drive that is provided by a forensic image is different from the copy produced by copying all of the files saved on a hard drive using a program like Windows Explorer. A forensic image of a computer hard drive contains the entire contents of the hard drive.

Electronic data, including forensic imaging of hard drives, is within the scope of discoverable material. *In re Pharmatrak, Inc.*, 329 F.3d 9, 17 (1st Cir. 2003); *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 652 (D. Minn. 2002). Because electronic discovery can easily become broad and intrusive, "[c]ourts have been cautious in requiring the mirror imaging of computers where the request is extremely broad in nature and the connection between the computers and the claims in the lawsuit are unduly vague or unsubstantiated in nature." *Balboa Threadworks, Inc. v. Stucky*, No. 05-1157-JTM-DWB, 2006 U.S. Dist. LEXIS 29265, 2006 WL 763668, at *3 (D. Kan. Mar. 24, 2006). Without a sufficient showing of relevance and need, courts disallow the "drastic discovery measure" of permitting a party to image all of an opponent's electronic media. *McCurdy Group v. American Biomedical Group, Inc.*, 9 Fed. Appx. 822, 831 (10th Cir. 2001). Courts are more receptive, however, to circumscribed requests limited to specified individuals or computers expected to produce relevant information. *See Rowe Entertainment v. William Morris Agency*, 205 F.R.D. 421, 427-28, 432-33 (S.D.N.Y. 2002) (granting revised and limited request for defendants' backup tapes and emails and prescribing protocols for imaging); *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 641 (S.D. Ind. 2000) (granting access to computers used by four named individuals); *Playboy Enterprises, Inc. v. Welles*, 60 F. Supp.2d 1050, 1053 (S.D. Cal. 1999) (granting access to defendant's personal computer).

The most commonly used computer forensic software package is EnCase Forensic produced by Guidance Software, Inc. According to Guidance Software, EnCase software is used by more than 15,000 forensic experts and investigators. *State v. Butler*, 2005 Tenn. Crim. App. LEXIS 302, at *8 (Tenn. Ct. Crim. App. March 30, 2005) (Encase has been approved by several federal district and appellate courts as a “non-invasive forensic examination tool.”). EnCase is reliable software and may be used for the purpose of creating a forensic image of a hard drive. *State v. Plude*, 2007 Wisc. App. LEXIS 194, at *10 (Wis. Ct. App. March 6, 2007) (“EnCase makes a mirror image copy of a hard drive, without altering the original drive.”).

2. Computer Forensic Evidence

A computer forensic expert can analyze a forensic image of a storage device to determine what was stored on the device, what files were accessed, and when the files were last accessed or modified. In addition, a forensic image of a PC hard drive includes data from which an investigator can determine what peripheral devices have been connected to the PC. *New Hampshire Ball Bearings, Inc. v. Jackson*, 158 N.H. 421, 424-25, 969 A.2d 351, 356 (2009) (“Analysis of the forensic image with forensic software allows an investigator to determine what peripheral devices have been connected to the device, what a user accessed, what has been stored on the device, and when it was last accessed or modified. Because deleted files are not actually erased from storage media, analysts are able to determine both current and deleted files so long as the latter have not been completely overwritten with new data.”).

If you are a potential plaintiff in a case in which computer forensic evidence may be important, get a computer forensic expert at the outset, before a complaint is filed. Some companies have the software and equipment available to make a forensic image of a departing employee’s computer before anyone else uses the computer. This, of course, is the best practice, and the expense of doing so may be warranted in companies whose successful business operations depend heavily upon effective trade secret protection.

On the other hand, cases have been successfully litigated where evidence was obtained from a departing employee's computer even when no special efforts had been employed to preserve the computer forensic evidence that was later discovered on the ex-employee's computer. *See, e.g., DSC Communications Corp. v. Next Level Communications*, 107 F.3d 322, 325 (5th Cir. 1997)("DSC filed this lawsuit in April, after [a competitor] first announced its investment in Next Level, when it reviewed the files saved on [the ex-employee's] computer at DSC and found three pages of Next Level's May business proposal.").

Another reason for recommending that a plaintiff retain a computer forensic expert from the outset is the fact that, if the plaintiff intends to request that mirror images be made of the defendant's computers in order to obtain forensic evidence, it is advisable to image the computers sooner rather than later. An adversary's computers may have relevant information that may be lost through normal use of the computers. *Antioch Co. v. Scrapbook Borders, Inc*., 210 F.R.D. 645, 652 (D. Minn. 2002) (ordering defendants to allow plaintiff's expert to make a mirror image of defendants' computer hard drives because the computers may have relevant information which is being lost through normal use of the computers).

If you are a defendant in a case in which computer forensic evidence is an important part of the plaintiff's case, it is advisable to retain a computer forensic expert as soon as reasonably possible. Defendants have lost cases because they failed to retain a computer forensic expert at an early enough stage in the case. *See, e.g., State v. Plude,* 2007 Wisc. App. LEXIS 194, at *13 (Wis. Ct. App. March 6, 2007) (defendant's attempt to blame the prosecution for his failure to present exculpatory computer evidence at trial rejected on appeal, on grounds that it was the defendant's own fault due to "his failure to timely hire a computer expert.").

In addition, a defendant in a trade secret misappropriation case involving computer forensic evidence will want to comply with its obligation to preserve relevant evidence. "A party or anticipated party must retain all relevant documents ... in existence at the time the duty to preserve attaches, and any relevant documents created thereafter." *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003). Although there may be a "multitude" of ways to comply with the duty to preserve evidence, "a mirror-image of the computer system taken at the time the duty to preserve attaches" may be one component of a litigant's evidence preservation efforts. *Id*. Generally, someone skilled in computer forensic evidence must be retained to make the mirror images of the relevant computers.

An unscrupulous plaintiff can take advantage of a defendant's delay in retaining its own forensic expert. A defendant may be faced with a plaintiff's "Catch 22" strategy, *i.e.*, a litigation strategy based on allegations that the defendant misappropriated trade secrets, and even if there is no evidence of such misappropriation, the absence of such evidence "must" be the defendant's fault for failing to preserve the evidence.

3. The Recycle Bin

Although most people are familiar with the "Recycle Bin" used by Windows, a complete discussion of computer storage in a Windows operating system needs to include a brief mention of the Windows Recycle Bin.

When a file is deleted in Windows, the file is normally only moved from the folder where it was previously located to the Recycle Bin. The file is not actually deleted, and the space where the file is physically located on the hard disk continues to be regarded as used space that cannot be over-written by the operating system. If a hard drive does not have sufficient storage space to store a large file without emptying the Recycle Bin, the operating system will report to the user that the disk has insufficient space to store the file. In addition, a file in the Recycle Bin cannot be opened or used. Thus, a file moved to the Recycle Bin is actually preserved, cannot be used or opened, and can later be completely restored. *New Hampshire Ball Bearings, Inc. v. Jackson*, 158 N.H. 421, 426, 969 A.2d 351, 357 (2009) ("Jackson testified that after receiving a phone call about the suit on May 5, 2006, he had difficulty sleeping and searched his computer at 4:00 a.m. for any NHBB files he may have accidentally copied, found three, and placed them in the recycling bin — where they remained — with instructions not to erase them.").

4. Unallocated Storage Space

When a file is permanently deleted by a user, for example when the Recycle Bin is emptied, the data contained on a hard drive is not actually erased. All that Windows does is to designate that space on a hard drive as unallocated space, (and to mark the directory entry for the file as deleted). The next time that a file needs to be saved on the hard drive, some part of unallocated space will be used to store the electronic data. Whatever old data may be contained in the space used to record the new file will be over-written by the electronic data for the new file. However, until the storage space on the hard drive is reused, and the old data has not been over-written, the electronic data can be recovered in a forensic examination of the hard drive.

A forensic examination of unallocated space on a hard drive will uncover files and data that were once stored on the hard drive, and then permanently deleted, as long as the space on the hard drive has not been over-written. It is well-settled that discoverable “documents’ within the meaning of Rule 34 of the Federal Rules of Evidence include computer records that have been “deleted.” *Simon Property Group L.P. v. mySimon, Inc*., 194 F.R.D. 639, 640 (S.D. Ind. 2000) (“First, computer records, including records that have been ‘deleted,’ are documents discoverable under Fed.R.Civ.P. 34.”).

5. Slack Storage Space

A cluster is the smallest amount of disk space on a hard drive that can be allocated to hold a file. “File slack” or “slack space” is the area on a hard drive between the end of a file and the end of the last cluster or sector used by that file. Slack space is wasted storage space on a hard drive. (File systems using smaller clusters utilize disk space more efficiently.) However, slack space on a hard drive can be searched and analyzed by forensic software.

In view of the fact that Windows does not actually erase data that was previously written on a hard drive, file fragments may still exist on a hard drive in slack space even when other files may have over-written that area on a hard drive. An expert can search a forensic image of a hard drive for fragments of a file, and may be able to detect that a file previously existed on the hard drive, even where the file was deleted and the storage space over-written by other files.

The best way to visualize this is to think of a hard drive as a stack of sheets of paper on which data can be written. Each time a file is recorded, a sheet of paper is selected from the stack and used to store the file. If a file does not completely fill up the page, the remaining space on the sheet of paper will not be used to store any other file, because it cannot be addressed by the operating system. If the remainder of that page has something recorded on it from a previous file, the information written on the piece of paper still exists and can be found by a forensic expert.

Let's say you are the plaintiff, and you want to know whether a departing employee copied a large database containing trade secret information onto his company-owned laptop so he could take it home and secretly copy it onto another storage device. And in this hypothetical example, assume the departing employee deleted the large database after he copied it, and then copied a large number of small files onto the hard drive in order to over-write the deleted file. An analysis of a forensic image of the hard drive in question could include a search for unique file fragments of the database. File fragments that uniquely correspond to the database may be found in slack space even when the employee saved a large number of smaller files on the hard drive after the database was deleted.

6. Metadata

A printout of a document does not include certain data that a Windows operating system stores about the "properties" of the document. This type of addition data about the computer file (that is maintained by the operating system) is generally referred to as "metadata." Electronic evidence that is discoverable includes relevant metadata. *Nova Measuring Instruments Ltd. v. Nanometrics, Inc*., 417 F. Supp.2d 1121 (N.D. Cal. 2006) (compelling production of documents in electronic format complete with metadata); *Williams v. Sprint/United Management Co.*, 230 F.R.D. 640, 653 (D. Kan. 2005); *In re Honeywell International, Inc.*, 230 F.R.D. 293, 296 (S.D.N.Y. 2003).

"In general, metadata is relevant when the process by which a document was created is in issue or there are questions concerning a document's authenticity; metadata may reveal when a document was created, how many times it was edited, when it was edited and the nature of the edits." *Kingsway Financial Services, Inc. v. Pricewaterhouse-Coopers, LLP*, 2008 WL 5423316, at *6 (S.D.N.Y. 2008).

(a) A PC's Internal Clock

A PC contains an internal clock that provides a date and time. This clock is accessible by the PC user, and can be readily set to any date and time chosen by the user. A user is asked to set the date and time for the PC's internal clock when Windows is started for the first time. The user may also select the time zone. If configured properly, Windows can automatically adjust the PC's clock for daylight saving time. A user can, at any time, change the date and time set for the PC's internal clock.

Windows uses the PC's internal clock to record three dates for each file, *i.e.*, a "date created," a "date accessed," and a "date modified." The data recorded by Windows for the time includes the hour, minute, and second.

You do not need special forensic software to view the dates recorded by Windows for PC files. The Windows Explorer program included with the Windows operating system can be configured to display "date created," "date accessed," and "date modified." If you have never seen these dates that Windows records for a computer file, I recommend that you do the following to familiarize yourself with these dates. In Windows Explorer, click "View" in order to display the drop down menu for "View." Select "Details" as the option under the "View" drop down menu. The default setting typically only displays the "date created" and "date modified." So once again go back to the “View” drop down menu and select “Choose Details...” in order to select which details will be displayed by Windows Explorer. This will open a dialog box in which you can select the details to display by checking the corresponding boxes. Check the box for “Date Accessed,” (and if they are not already checked, also check the boxes for “Date Created” and “Date Modified”), and then click “OK.” Windows Explorer will display the currently recorded values for these dates. A typical “date created” may be displayed by Windows Explorer as “3/12/2007 10:53 PM.”

If you want to play around with these dates and experiment with computer operations that change the dates, please note that Windows Explorer will not immediately update the date that is displayed. If you want to see whether a date shown in a currently displayed window has been changed by some computer action that occurred while the window has been displayed on the screen, you have to refresh the display. In Windows Explorer, in order to refresh the display, you click “View” (in order to show the drop down menu), and select “Refresh.” Alternatively, you can press the F5 key to refresh the display.

The date and time shown for files contained on a PC hard drive is taken directly from the PC’s internal clock. The Windows operating system (prior to Windows Vista) did not check the accuracy of the PC’s internal clock. When a forensic image is made, the date and time shown on the PC’s internal clock should be checked against the actual time to determine whether the PC’s clock was set to the correct time. *See State v. Cook*, 777 N.E.2d 882, 887 (Ohio Ct. App. 2002) (“When Detective Driscoll made the mirror image of the hard drive, he checked the date and time shown on the computer’s internal clock with the ‘real world’ time.”).

If the PC's internal clock is set incorrectly, the date and time of the files contained in the forensic image will be incorrect. Normally, the data recorded by the operating system will be offset from the correct time by the same amount that the PC's internal clock is in error. Therefore, the dates provided by a forensic examination of a hard drive cannot be immediately assumed to be accurate. In most cases, the dates need to be verified or otherwise authenticated before the recorded dates are relied upon to establish the time that the associated events actually took place.

(b) Date Created

The "date created" is the date the specific copy of the file contained at that location on the hard drive was created. Different copies of the same file can have different dates recorded for "date created." For example, if a file is opened and then saved with a new file name, the "date created" for the file with the new name will be the date it was saved with the new file name, even though the contents of the file may otherwise be identical to the original file that was opened. In this example, the original file will have a different "date created," which will be the date that the original file was first stored on the hard drive.

(c) Date Modified

The "date modified" is the last date that a file was altered. For example, if a Word file is opened, the document is edited, and then resaved, this will change the "data modified" for that file. When the "date modified" is changed, the previous date that had been recorded for the "date modified" is lost. Therefore, the "date modified" is more accurately the date the file was last modified.

The document ***contents*** need not be changed in order for the "date modified" to be changed. For example, if metadata saved with the file is changed, then the "date modified" will be changed for that file. For example, if the properties of a Word document are changed to change the author, and the file is saved, the "date modified" will be changed. If a fits image file is opened, and the information in the fits header is changed, the "date modified" will be changed even though the fits image itself was not changed.

Interestingly, a file can have a "date created" that is a later date for the "date modified," suggesting that something was modified before it was created. Thus, it is important to understand the significance of the "date created" and the "date modified" values, because it is not that uncommon for a file to have a "date created" that is a later date for the "date modified." This may happen of a file is copied to the hard drive from external media. The new copy of the file on the hard drive will have as its "date created" the date that the file was copied onto the hard drive. The "date modified" will usually not be changed when the file is copied,

(d) Date Accessed

Unfortunately, Windows does not specifically record the date a file is copied. The usefulness of forensic evidence would be significantly enhanced if Windows did so. The "date accessed" is sometimes important information from which an inference of copying may be drawn. This is because a file is "accessed" when it is copied. Therefore, the Windows operating system will change the "date accessed" to the date and time of the PC's internal clock when a file is copied. When the "date accessed" is changed, the previous value of the “date accessed” is lost. Thus, the “date accessed” is more specifically the last access date for the file in question.

The “date accessed” is sometimes used as evidence to support an inference that a file was copied. If a departing employee used Windows Explorer to copy several files containing proprietary information, a forensic examination of a hard drive may show that the files in question were sequentially accessed only a few seconds apart. If you are the plaintiff, you may argue that sequential access times for a large number of files containing proprietary information supports an inference that the files were copied by the ex-employee before he or she left the company.

If you are the defendant, it is important to know the many other computer actions that also change the “date accessed,” in addition to copying the file. If you are the plaintiff, you will want your forensic analysis to consider, and if possible eliminate, other potential reasons why a file’s “date accessed” might have been changed.

A file does not have to be altered for the “date accessed” to be changed. The file only has to be accessed. Dragging and dropping a file from one folder to another folder (using Windows Explorer) will change the “date accessed.” Right-clicking on a file, (for example, to view the file’s properties), will change the “date accessed.” Opening a file will change the “date accessed.” Printing a file will change the “date accessed.” Some virus checker programs will change the last access date when a virus scan is performed on a file. If a file is encrypted, the “date accessed” may change when the file is viewed (because the data must be unencrypted in order to view the file). If a file is an image file, and Windows Explorer “View” is set to “Thumbnails,” simply opening the folder containing the file will change the “date accessed” for that image file, because Windows Explorer accesses the file in order to display the thumbnail.

If a user merely hovers his or her mouse cursor over a file in Windows Explorer, a popup window will appear containing information about the “properties” of the file, such as the author, size, type, title, etc. This will change the “date accessed.” Windows Explorer does this for any Microsoft Office document, such as Excel, Word, Access, and PowerPoint. Windows Explorer will do this for Adobe “pdf” files, ASCII “txt” text files, and “jpeg” image files. Windows Explorer will even change the last access date of a temporary “tmp” file when a user hovers over his or her mouse over the file, if Windows Explorer is set to display hidden files.

EnCase allows an investigator to separately set the time zone for the evidence file. If this is incorrectly set, it may lead to incorrect inferences being drawn from the times recorded as “date created,” “date accessed,” and “date modified.” If you are the plaintiff, you will want to make sure this is set correctly, because incorrect times, for example, may turn out to be a time when the defendant can establish that he or she was somewhere else or may not mesh with the “date created” time for files contained on a thumb drive of other external media that the defendant may have used. If you are the defendant, you will want to double-check this setting, because an unscrupulous adversary could adjust the time zone setting in EnCase to make the times appear to coincide with the time of some other event.

(e) Dates for Files in the Recycle Bin

Files moved to the Recycle Bin have a “date created,” a “date accessed,” and a “date modified.” A file cannot be opened while it is in the Recycle Bin. Thus, no one can accuse a defendant of using or "accessing" a file during the time that the file was in the Recycle Bin. However, the "date accessed" will be changed if the Recycle Bin is opened, and someone right-clicks on the file to view the file's properties. The "date accessed" will also be changed if someone hovers over the file name in the Recycle Bin (and a popup window appears displaying the file's properties).

A forensic examination of files in the Recycle Bin will reveal the date and time that each file was "deleted," *i.e.*, moved to the Recycle Bin. It is possible to permanently delete a file by opening the Recycle Bin, selecting the file in the Recycle Bin, and then deleting the file. This will permanently delete the file, and the storage space occupied by that file will then be designated as unallocated space that can be over-written. However, Windows maintains a record for the Recycle Bin that shows every file that was permanently deleted from the Recycle Bin in this manner, every file that was moved into the Recycle Bin, and every file that was restored from the Recycle Bin, since the date and time that the Recycle Bin was last emptied**.** Once the Recycle Bin is emptied, this record is lost, and Windows creates a new record for the Recycle Bin from that time forward. A forensic examination will show the date and time when the Recycle Bin was last emptied, and will reveal the files that were contained in the Recycle Bin at any time subsequent to the last time it was emptied.

7. CRC and Hash Values

The integrity of the EnCase evidence file is protected by a hash value that is generated when the forensic image is created. The hash value that is generated represents a unique identifier for the data contained in the evidence file or forensic image. If anyone attempted to alter the data contained in the evidence file, the hash value for the altered evidence file would not be the same as the hash value that was generated for the original unaltered evidence file. Any time that the hash value of a suspect copy of an evidence file does not exactly match the hash value generated for the original evidence file, the suspect evidence file should be deemed to be unreliable and inadmissible because something in the data has been altered. *United States v. Heiser*, 2006 U.S. Dist. LEXIS 27886, at *22 (M.D. Pa. April 28, 2006) ("[I]f the hash value on the evidence images is one number off, compared to the hash value of purportedly the same evidence, then they are not reliable copies."). Therefore, if you are the defendant in a case involving computer forensic evidence, you should always double-check the hash value of the original forensic image of a hard drive against any evidence file that the opposing expert relies upon as the basis for his or her opinions.

EnCase software uses the 128-bit MD5 hashing algorithm, which has 2^{128} unique values. Although it is theoretically possible for two different data files to generate an identical MD5 hash value, the probability of this occurring is exceptionally small. According to Guidance Software, the odds of two different files generating the same MD5 hash value is roughly 10^{38}:1. It is much more likely that you will be struck by lightning – twice on the same day during a total eclipse of the sun – than it is likely that two data files will generate the same MD5 hash value.

One reason EnCase is preferred, and other software might be less reliable, is that every byte of the evidence file is verified using a 32-bit cyclical redundancy check ("CRC"), which is generated concurrent with acquisition. The CRC is in addition to the hash value. Rather than compute a CRC value for the entire disk image, EnCase computes a CRC for every block of 64 sectors (32KB) that it writes to the evidence file.

Thus, a typical disk image contains tens of thousands of CRC checks. A CRC is better than a checksum validation. The CRC is order sensitive. Thus, the string “1234” and “4321” would produce the same checksum, but not the same CRC. The CRC and MD5 hash values are stored in separate blocks in the EnCase evidence file, which is separate from the evidentiary forensic image itself. Those blocks containing the CRC and MD5 hash values are separately authenticated with separate CRC blocks. If any information is tampered with, the EnCase software will report a verification error.

The evidence file generated by EnCase software includes a Case Info header. That header contains information about the creation of the mirror image. The information includes system time and actual date and time of acquisition, the examiner name, notes regarding the acquisition, including case or search warrant identification numbers, and any password entered by the examiner prior to the acquisition of the computer evidence. There is no “backdoor” to the password protection. The acquisition MD5 hash value is included in the header. All the information contained in the Case Info file header, with the exception of the examiner password, is documented in the integrated written reporting feature of EnCase software. The Case Info file header is also authenticated with a separate CRC, making it impossible to alter without registering a verification error.

EnCase software is designed so that it is impossible to write to the evidence file once the evidence file has been created. As with any file, it is possible to alter an EnCase evidence file with a disk utility such as Norton Disk Edit. However, if one bit of data on the acquired evidentiary bit-stream image is altered after acquisition, even by adding a single space of text or changing the case of a single character, EnCase software will report a verification error in the report and identify the location where the error registers.

In view of the reliability of EnCase software, once a mirror image is made by EnCase, the evidence file is generally regarded as being beyond question in its representation of the contents of the hard drive or other storage device, at the time that the hard drive or storage device was imaged. All investigations into reliability, alteration, and fabrication, should focus on what happened to the storage device before the mirror image was made.

8. Write Blocker

A write blocker is a hardware device used to prevent any writes to a hard drive, while at the same time allowing a forensic investigator to read from the device. If you are the plaintiff, you have an interest in making sure that your computer forensic evidence is reliable and admissible. When a hard drive is imaged, it is imperative that a write blocker is used when connection is made to the hard drive during the imaging process. The write blocker allows a forensic expert to create a forensic image of the contents of the hard drive without altering the data in any way during the process.

If you are the defendant, you should question the reliability and accuracy of any forensic image that was created for a hard drive that was accessed without the protection of a write blocker, either during the imaging process or, even more importantly, before the forensic image was made. It is virtually impossible to alter the data in a forensic image made with EnCase software without such alteration being easily detected. The hash value generated by the EnCase 128-bit MD5 hashing algorithm for the altered forensic image will not be identical to the hash value generated for the original forensic image before the data was altered. Anytime the hash values do not agree, it is a red flag that someone has tampered with the evidence file.

On the other hand, it is relatively easy for a skilled IT person to alter the data on a hard drive ***before*** a forensic image is made to preserve the contents of the hard drive, if the hard drive is accessed without a write blocker. A skilled IT person can alter the data on a hard drive in ways that are difficult, and sometimes impossible, to detect. Sophisticated programs are available that can allow a skilled IT person to change the last access dates on files contained on a hard drive to make it appear as if the files were sequentially accessed and copied by the defendant on any particular date and at a particular time, (for example, the day before the defendant employee returned his or her company-owned laptop to the company). An unscrupulous plaintiff can fabricate evidence of sequential file access times, and then create a forensic image of the hard drive to provide to an independent expert. Even an independent computer forensic expert who examines such a forensic image would be likely to conclude that the sequential access times shown in the forensic image are evidence that the defendant employee copied the sequentially accessed files from his or her company-owned computer before the PC was return to the company.

It is possible that the independent forensic expert could detect that the hard drive was accessed without a write blocker after the date that the defendant last had possession of the computer. Whenever a Windows PC is turned on, the Windows operating system creates numerous temporary system files. *State v. Butler*, 2005 Tenn. Crim. App. LEXIS 302, at *8 (Tenn. Ct. Crim. App. March 30, 2005) (computer expert "agreed that in the process of booting up the Windows operating system the contents of the hard drive would be changed"); *State v. Plude*, 2007 Wisc. App. LEXIS 194, at *10 (Wis. Ct. App. March 6, 2007) ("every time a computer is even turned on, some change, however small, is made to the hard drive”). Those temporary files will remain on the hard drive after the PC is turned off, until they are over-written the next time that the PC is turned on and Windows is started.

EnCase can search and find all files contained in a forensic image that were created, accessed, or modified within a given date range. If you are the defendant, you will want to ask your expert to search for any files in the plaintiff’s forensic image that are dated after the defendant’s date of departure, in order to determine whether anyone powered on the PC or used it after the defendant turned in the PC. If the forensic image contains temporary system files created by Windows which are dated after the ex-employee’s date of departure, this would be evidence that the PC was powered on and the hard drive was accessed after the defendant no longer had possession of the PC. If you are the defendant, the existence of any such temporary system files raises a question about whether the data in the forensic image accurately reflects the relevant contents of the hard drive the last time that the defendant used the PC. Even a skilled forensic expert may not be able to find any evidence that electronic data was altered on the hard drive prior to the creation of the forensic image.

In view of the fact that a PC’s internal clock can be changed to any desired date and time, it is possible to manipulate the dates recorded for PC files by merely changing the setting on the internal clock. If a skilled IT person sets back the clock on the PC, and then turns on the PC again, the system files created by Windows the first time the PC was turned on will be over-written the second time the PC is turned on, and it will then appear that the PC was last used on the arbitrary date to which the clock was set back to by the skilled IT person.

If you are the defendant, and have some question about whether the PC clock was set back in an attempt to fabricate evidence, you may be able to detect such tampering with the PC clock. If you are the plaintiff, and are suspicious about whether the defendant changed the PC clock in order to cover up illegal activities, you may be able to detect this as well. Under these circumstances, you should know that other programs also create temporary files during normal operation of the computer. For example, Internet Explorer creates temporary files when Internet web pages are viewed. Microsoft Word may create temporary files that are back-up copies of draft Word documents, which are used to recover an unsaved document if Word terminates abnormally before the work copy of a document has been saved by the user. A forensic program like EnCase can be used to search for and locate any file that has a date that is after a specified date, or a date that falls within a specified range. Therefore, if there are temporary files created by other programs that are dated after the date of the temporary system files created by Windows the last time the PC was powered on, this would be evidence that the PC clock was set back or that someone had otherwise tampered with the PC clock setting.

It is unusual to have a case in which the plaintiff's computer forensic expert does not create the forensic image of the suspect hard drive that becomes the evidence file for the plaintiff's case. If a forensic expert is provided with a forensic image created by someone else, the reliability of the forensic image should be investigated. The reliability of the forensic expert's opinions will depend entirely upon the reliability of the data in the forensic image upon which such opinions are based. Therefore, if you are the defendant, you may find that your defense strategy should focus on the reliability of the forensic image, rather than the reliability of the forensic expert.

9. Registry Files

The registry files contained on a Windows PC should be included in any computer forensic examination. The registry is a database that contains the hardware and software settings for a Windows computer. When a software program is installed, entries are made for that software in the registry files. More importantly, when a thumb drive is connected to a computer, or any other hardware containing storage media is connected, entries are made in the registry files.

Windows stores information in the registry files that identifies every thumb drive or external storage device connected to the PC's USB ports. Windows records a serial number and other information specifically identifying a plug-and-play device that was connected to a USB port. For example, when a thumb drive is connected to a PC, a thumb drive iSerial number may be recorded that is unique to a particular thumb drive. The recorded data includes the date and time that the device was last plugged into the PC.

Of course, computer data on a hard drive is relatively easy to copy or transfer from a PC hard drive to other computer storage media. For example, data on a hard drive can be easily transferred to a thumb drive, floppy disk, ZIP disk, tape back-up drive, CD-R, or CD-RW. If you are the plaintiff attempting to locate data that has been copied or transferred to another storage device, you should seek access to all computer storage media that is or has been connected or attached to the PC in question. This would include any hard drives installed in the computer, any floppy diskettes used or accessed, CD-ROMs burned on the computer, and any ZIP disks that have been used or accessed. The registry files will usually identify the devices that were connected or attached to the PC. A forensic image of each such device may be performed to locate relevant electronic data that may be stored on them, as well as data that may have been stored on them and then deleted.

10. Link Files

If a person copies files onto a thumb drive, and then opens the copy on the thumb drive (*e.g.*, to make sure the file was copied correctly), Windows creates a shortcut to the original file, and the shortcut is stored as a "lnk" file. The "lnk" shortcut file is stored and it remains on the PC after the file is closed and the thumb drive is removed. Embedded within a shortcut file is information such as the date and time of the target file that the shortcut point to, and the volume label of the storage device. In an appropriate case, a "lnk" file may be solid evidence that a file was copied onto the thumb drive. For example, a "lnk" shortcut to "E:\trade secrets.doc" would indicate that a file named "trade secrets.doc" was on a thumb drive (assuming the PC assigned "E:" to thumb drives). The time that the file was opened on the thumb drive will be revealed by the "lnk" file.

A departing employee who is attempting to copy personal files onto a thumb drive before turning in his or her company-owned computer would be well-advised to make sure that files are personal files before copying the files to the thumb drive. In one case, the departing employee testified that he copied an entire folder that he thought contained only personal files, and then checked the copied files on the thumb drive after the files were copied and before the thumb drive was unplugged. He opened questionable files on the thumb drive, and if he thought it was not a personal file, he said he deleted it. However, a forensic examination of his company-owned laptop uncovered "lnk" files to the files on the thumb drive that he opened, and there was no proof other than his testimony that he deleted the files on the thumb drive after they were copied.

Under some circumstances, folders that may have existed on a hard drive, but which were erased and over-written, may be detected if there are “lnk” shortcut files that refer to the deleted folders. For example, assume a “lnk” file is found on a hard drive that is a shortcut to “C:\New Business Plan\projected market share.xls.” Even if the folder “New Business Plan” was deleted from the hard drive and any record of that folder was over-written, the “lnk” shortcut will reveal the prior existence of the folder.

11. Email

Modern litigation commonly involves the production of email messages. It has become a common form of communication. Sometimes people say things in an email message that they might not otherwise say in writing, because they assume that electronic communications are ephemeral things that disappear without a trace. Just the opposite is true.

Numerous copies of an email message are often stored in multiple locations, and copies of email messages are often preserved on the sender’s email server, on back-up tapes for the sender’s computer system, on the recipient’s computer, on the recipient’s email server (if the recipient is outside the company), and on back-up tapes for the recipient’s computer system. A copy of a sent email message is often included in a reply email message, and in a reply to the reply, and so forth, until copies of the same email message may be multiplied many times and can be found in scores of emails. In addition, an email message may be forwarded to others, which also may create additional copies of the email message.

Most companies use a centralized e-mail server. The logs on that e-mail server can record what email is sent or received by anyone using the system, even if the information was deleted via Outlook right after it was sent. Even when a message is deleted, the actual contents of the messages (such as file attachments) may still be stored on the server. Microsoft Exchange comes with an option that retains messages on the server or on backup media for a few days – even after emptying the deleted items – as an emergency recovery capability.

In addition, email messages may be preserved on back-up tapes of the centralized e-mail server. For example, if a message was sent on Monday and then deleted on Tuesday, the Monday night backup will still have a copy of the message – until the backup is over-written or erased.

Microsoft Outlook creates a "pst" file, which is a data file where electronic copies of email generated by Outlook is stored on a hard drive. In some cases, parties seeking discovery have been successful in compelling an adversary to produce electronic "pst" files. *See Optowave Co. v. Nikitin*, No. 6:05-cv-1803-Orl-22DAB, 2006 WL 3231422, at *9 (M.D. Fla. 2006) (compelling production of "pst" file containing email).

Emails commonly include attachments. Attachments to email messages must also be produced when production of the email is required. *United States v. New York Metropolitan Transportation Authority*, No. CV-2004-4237(SLT)(MDG), 2006 WL 3833120, at *3 (E.D.N.Y. Dec. 29, 2006) ("attachments must be produced."); *CP Solutions PTE, Ltd. v. General Electric Co*., No. 3:04cv2150(JBA)(WIG), 2006 WL 1272615, at *4 (D. Conn. Feb. 6, 2006) ("Attachments should have been produced with their corresponding emails.). Programs other than Outlook may be required to open or print an attachment. For example, an “xls” file attached to an email will typically require Microsoft Excel, a “pdf” file will typically require Adobe Reader, a “doc” file may require Microsoft Word, *etc*. The “pst” file also includes copies of attachments to email messages.

A “pst” file is searchable by a forensic expert, and can be used to locate email messages that are sent to specified people, that use specified words, that were sent within a given date range, as well as other search parameters. The “pst” file makes it relatively easy to match up attachments with emails.

If a company-owned computer is used to log onto a personal email server, such as a Yahoo! account, Outlook will make a “pst” file for that email server. A former employee’s personal email can be retrieved from the hard drive if the company-owned computer was used to send and receive personal email. There have been cases where a departing employee used his personal email account to send email relating to his or her planned departure and job interviews. If the company-owned laptop is used to access the departing employee’s personal email from home, Outlook will create a “pst” file for the personal email account. That “pst” file will still be on the laptop when the departing employee returns the company-owned laptop to his former employer. The former employer will be able to retrieve the former employee’s personal email from the hard drive, and read every email, including any emails in the inbox folder, sent folder, or deleted folder.

Apart from the commonly used email client software like Outlook or Outlook Express, many people use web-based e-mail like Gmail or Hotmail that only rely on a web browser to work. Most of these services use secure protocols (https), so the browser takes extra steps to avoid caching temporary copies of the mail contents. The web-based email is designed to work this way in case the user accesses the web-based email using a public terminal; it wants to prevent the next user of the public terminal from seeing the prior user's email. Because of this, the various accounts used by a former employee should be identified quickly and subpoenas issued to the e-mail service providers in order to preserve any mailbox contents.

12. Other Data Recorded by the Operating System

If a departing employee prints out documents from his or her company-owned laptop before turning it back in, a forensic examination of the laptop will usually show the last documents that were printed. A typical printer will print at a speed that is much slower than the rate at which the data to be printed can be sent to the printer. When a document is printed, Windows usually sends a copy of the document to a print spool so that the PC is not tied up and unable to respond while the document is printing.

After a document has been printed, a copy of the document remains in the print spooler. The last document printed can be retrieved from the print spooler, even if the original document itself was deleted from the computer. The copy of the printed document remains in the print spooler until the data in the print spooler is over-written by subsequent documents that are printed.

A departing employee may use the company-owned laptop to burn a CD in order to copy files from the company-owned laptop. However, CD burning can also leave traces, since the burning process usually makes a temporary copy on the hard drive of the files being burned. The CD burning process also creates a "project" or "session" for the contents of the CD. The burning software may also keep its own log of the CD, or at least a record that a CD was made, (even if the contents of what was copied are not known).

Windows stores a record of the several searches that were performed searching for files of documents. The date each search was performed is also available.

Windows stores temporary copies of web pages when someone uses Internet Explorer to browse the Internet. A forensic examination of a computer can reveal the Internet websites visited by a user, and reconstruct copies of the actual web pages that were viewed. A forensic expert can determine what search terms were used to search the Internet. If a former employee searched the Internet to find wiping software to use for the purpose of cleaning off of his or her hard drive any traces of misappropriated trade secret data, a computer forensic expert can detect what websites were visited, what wiping software was purchased, installed, and used, and how much data was wiped from the hard drive. *See AdvantaCare Health Partners, L.P. v. Access IV*, 2004 WL 1837997, at *1-2 (N.D. Cal. Aug. 17, 2004) (computer expert determined when the ex-employee visited websites and what websites were visited, what wiping software he installed, and when he used the wiping software to delete data from his computer).

If an employee uses his or her company-owned PC to synch a PDA, such as a Palm Pilot, the PC hard drive will have a copy of the synched files stored on it. Thus, relevant information contained on a former employee's PDA may, under those circumstances, be obtained even if discovery of the contents of the PDA is not possible, because the information was subsequently erased or modified by the ex-employee.

13. Formatting a Disk

In spite of the fact that a user receives a warning that formatting a hard drive will erase any data on the hard drive, the formatting process does not do so. A computer forensic expert can usually recover data from a reformatted hard drive, as long as the data has not been over written.

14. Network Records

Most company networks maintain records of users who remotely access the network. Such records typically record the time a user logs in, and the time the user logs out. More importantly, the total bytes of data transmitted will also be recorded.

If the plaintiff company controlled access to materials on one or more central server computers, logs should have been kept on those servers recording both failed and successful accesses to critical information. Those logs typically record the time of an access attempt, the user's identification (account or user name) and the location the attempt came from (such as an IP address). If a company is concerned enough to restrict access to certain information, they should also have enabled such access logging to ensure they can identify attempts to take information.

The departing employee's computer may also record access to the company network of his former employer after hours, any attempts to access information on that company's servers, and may also record time and date when the ex-employee accessed the new employer's computer systems.

From the plaintiff's standpoint, network access logs and other data recorded by a company network may collaborate other evidence of file transfers, or evidence of an employee emailing materials to his or her home email. From the defendant's standpoint, data showing how many bytes were transmitted may show that the total bytes transmitted were insufficient to have been the trade secret files allegedly misappropriated.

15. Back-up Tapes

If a PC or workstation is connected to a network, data can be easily transferred across the network, and either copied from one PC to another, or from one PC to a network server or a network hard drive. If the PC in question was connected to a network during a relevant time period, it may be desirable to obtain a forensic image of the network storage space that was accessible to the user in question. However, shutting down a company’s network in order to obtain forensic discovery of electronic information during litigation may not be practical, and a defendant can make strong arguments against such burdensome discovery, especially if a more narrow discovery request can be formulated to reduce the burdensome scope of the requested discovery. *See generally New Hampshire Ball Bearings, Inc. v. Jackson*, 158 N.H. 421, 969 A.2d 351 (2009) (sustained trial court refusal to allow plaintiff to image 250 computers and all servers at a competitor, where trial court had allowed narrower request to image 35 computers of potentially relevant employees and ordered production of back-up tapes for the servers).

You can often tell from a forensic examination of the PC that was connected to a specific network, what user name was used when the PC was connected to the network. If the user name can be identified, then the network areas accessible to that user name during the relevant time periods would potentially contain relevant information. In addition, back-up tapes for the relevant server space that was accessible to the user name in question may contain copies of files that were stored by that user on the network, but which were subsequently deleted and are no longer present on the server.

It is not uncommon for a company to have a policy requiring employees to save their work on network servers, rather than on the hard drive contained in their PC or workstation. Consequently, if a user of the network adheres to such a policy, the documents and data files created by the user would be stored on the network servers rather than the user’s PC or workstation. If a user copies files or data from a thumb drive plugged into his PC directly to a network server, normally there would be no evidence of those computer files on the user’s PC. If you are the plaintiff, you will want to determine during discovery whether the defendant company has such a policy.

Most companies operating a computer network have information technology employees who periodically back-up data on company servers using back-up tapes. A back-up tape captures data on a network server at a particular point in time. The data contained on back-up tapes may differ from the current data contained on a computer system. If a new employee brought computer files with him that were taken from his prior employer, the files could have been copied to storage space accessible by the employee on his current employer’s network servers. When a lawsuit is filed naming the new employee as a defendant, he may attempt to erase the files he copied onto his current employer’s network server. The data on a network server is fluid and typically changes on a daily basis as network users create, modify, and delete files and data stored on the network. A subsequent search of the network servers may not reveal evidence of files or data that was erased or deleted. However, a back-up tape of the relevant storage space on the network server, made prior to the erasure of the files or data, would contain evidence of the files or data.

A back-up tape must be restored to a computer hard drive in order to use the data on the tape. If necessary, experts are available who can recover data off of back-up tapes.

Email files are typically recorded on back-up tapes. It is not uncommon for IT departments to make back-up tapes of email files separately from back-up tapes of other information. Email servers may be backed up on a daily basis, whereas other network servers may be backed up less frequently. Email messages deleted from a departing employee's computer may still be recorded on back-up tapes.

Unsophisticated users may sometimes think they have deleted an email message, but the email is still preserved by Microsoft Outlook. When Microsoft Outlook "deletes" an email message, the message is only moved to the "Deleted Items" folder. The email is not permanently deleted and can be restored, as long as the "Deleted Items" folder is not emptied. A user can manually empty the "Deleted Items" folder by selecting "Mailbox Cleanup" under the "Tools" drop down menu on Outlook. In addition, under the "Tools" drop down menu, you can select "Options…", which permits a user to select the "Other" tab and check the box to "Empty the Deleted Items folder upon exiting." Then every time Outlook is closed, it was empty the "Deleted Items" folder. However, if this box is not checked, and the user does not use "Mailbox Cleanup" to empty the "Deleted Items" folder, emails that the user had "deleted" can be easily recovered and restored.

16. Anti-Forensic Software

In view of the fact that Windows does not actually erase electronic data on a hard drive when the files containing that electronic data are permanently deleted, software is available to remove the electronic data so it can never be recovered by a forensic examination of the hard drive. Commonly called “wiping software,” many versions are available. The U.S. Defense Department has developed standards and procedures for wiping hard drives on which classified information was stored. Commercially available wiping software typically allows the user to select various procedures, including DOD standard methods, that include multiple passes to completely remove any detectable trace of the electronic information formally stored on a hard drive.

There are many legitimate uses of wiping software. A company’s IT department should use wiping software whenever a PC containing a hard drive, or any other storage media, is sold, discarded or donated to charity.

Wiping software can be used to remove all traces of electronic data that may have once been stored on a hard drive or thumb drive. The entire hard drive can be wiped, or the wiping process can be limited to only the unallocated storage space. However, if a hard drive has been wiped, the use of wiping software can be detected. Most wiping software will leave a characteristic pattern on the wiped storage space of the hard drive; and this pattern will be different from the expected contents of a new hard drive that has never been used. If wiping software has been installed on a PC, the registry file will usually reveal that fact. In addition, the “accessed date” for the “exe” program files of the wiping software program will usually be the date that the wiping software was last used. The registry file may also contain the date the wiping software was installed on the computer. A computer forensic expert can examine a PC to determine whether wiping software has ever been used on the PC.

C. Pre-Litigation Procedures and Spoliation Claims

Given the ease with which electronic data can be altered, and the numerous locations where it can reside, litigants face a daunting task when they are asked to preserve all potentially relevant electronically stored information (“ESI”). With the heighten interest in spoliation claims as a result of recent court rulings, troublesome attorneys may be quick to try to exploit any shortcomings in an opposing party’s efforts to preserve evidence. In view of the difficulty and expense involved in attempting to achieve the perfect preservation of all ESI, especially at an early stage when the full scope of a potential claim is not known, claims of spoliation are frequently made and adverse sanctions are often sought against the imperfect party.

While there is no way to absolutely guard against the impossible and non-existent standard of perfection, a party’s efforts to avoid spoliation claims may be strengthened if an action plan is in place before issues arise. With recent rule changes and judicial decisions that have raised the stakes for companies and their counsel regarding the preservation of electronic evidence, planning for potential litigation has become essential. In order to deal with evidence preservation issues in a cost-effective and defensible manner, it is helpful to have procedures in place that enable a company to respond promptly and appropriately should a claim arise. These procedures may provide guidance for key employees on what they should, and should not do.

Recent rulings have shown that those parties that are unprepared for litigation and do not take the necessary steps to ensure preservation will be punished and held accountable. The analysis of whether a party has taken appropriate steps to preserve electronic evidence, and whether it could be subject to sanctions for failure to do so, is a reasonableness analysis that takes into account the day-to-day operation of a company's electronic information system. *See* Fed. R. Civ. P. 37(f). Because ESI is much more volatile than hard copy documents, action must be taken much earlier in the process to ensure that ESI is not deleted or altered.

To defend against claims of spoliation while accounting for the unique nature of ESI, it is important to understand that a company will be operating in one of three phases at all times during its existence and may actually be operating in more than one phase at the same time. The three phases are (1) prior to receipt of notice of a claim, *i.e.*, during the day-to-day operation of a company; (2) after the company has received notice of a claim and preservation obligations have been triggered; and (3) after litigation has been filed against the company, and the rules of civil procedure then go into effect and govern ESI.

1. Reasonable Document Retention Policy

During phase 1, a company can help protect itself and avoid sanctions during subsequent litigation if it has a reasonable document retention policy that is broadly communicated and implemented. *See Lewy v. Remington Arms Co.*, 836 F.2d 1104, 1112 (8th Cir. 1988) (stating that to determine whether to issue an adverse jury instruction for failure to preserve evidence a court should consider such things as whether a company's "document retention policy is reasonable considering the facts and circumstances surrounding the relevant documents" and "whether the document retention policy was instituted in bad faith.").

A company should be vigilant to ensure that there are mechanisms in place for reporting and reviewing possible claims in the work place. *See In re Adelphi Comm.*

Corp., 327 B.R. 175, 180 (Bankr. S.D.N.Y. 2005) (In the event that a corporation has policies and procedures in place for ensuring that all documents are preserved, a company may not be held liable for the independent actions of one employee.). A pre-claim procedure need not be complicated. It simply requires a reporting mechanism for employees that is suited to the company's structure and reporting procedures. The reporting procedure may include consultation with in-house counsel, especially when there is ***any*** question about whether litigation can reasonably be anticipated.

2. "Litigation Hold" After Notice of a Claim

The duty to preserve evidence arises when a party reasonably anticipates litigation. *Pension Committee of the University of Montreal Pension Plan v Banc of America Securities, LLC*, No. 05 Civ. 9016 (SAS), slip op. at 12 (S.D.N.Y. Jan. 11, 2010) ("It is well established that the duty to preserve evidence arises when a party reasonably anticipates litigation."). "Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents." *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003)("*Zubulake IV*").

Receipt of notice of a claim or potential litigation should prompt action, as the duty to preserve "known relevant evidence" will arise at this time. *Zubulake IV*, 220 F.R.D. at 216. At a minimum, the company should have: (1) a procedure in place to determine if notice has been given; and (2) a stop gap plan to rely upon while determining if it needs to move forward with a formal investigation and to retain outside counsel. *Id*. at 218. Consultation with in-house or outside counsel should be a step in the reporting procedure to ensure that an appropriate investigation is undertaken at the direction of counsel.

An immediate "litigation hold" is important after notice of a claim is received. *See, e.g., ACORN v. County of Nassau*, 2009 U.S. Dist. LEXIS 19459 (E.D.N.Y. Mar. 9, 2009) (holding that failure to issue a litigation hold once you have notice of a claim will serve as the necessary culpable state of mind to sustain a claim of spoliation.); *Zubulake IV*, 220 F.R.D. at 218. At this point, six years after the *Zubulake V* opinion, the failure to issue a written litigation hold is now considered to be gross negligence. *Pension Committee of the University of Montreal Pension Plan v Banc of America Securities, LLC*, No. 05 Civ. 9016 (SAS), slip op. at 24 (S.D.N.Y. Jan. 11, 2010).

A preliminary litigation hold may be critical in many cases to make sure that documents are preserved, though they may not need to be gathered before a lawsuit has been filed. In some circumstances, a preliminary litigation hold may also include instructions to specific individual employees concerning the task of gathering documents, and, in the event gathering is necessary, such employees should receive further instructions outlining the procedure to be followed.

However, a party's obligations for preservation of evidence do not end with a "litigation hold." The "litigation hold" is only the beginning. *Zubulake v. UBS Warburg, LLC*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) ("*Zubulake V*") ("A party's discovery obligations do not end with the implementation of a 'litigation hold' - to the contrary, that's only the beginning. Counsel must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce the relevant documents.").

3. Identification of the Key Players

An initial step in the post-notice investigation should be to identify and contact the key individuals with substantive knowledge relating to the claim. *See Zubulake V*, 229 F.R.D. at 434-35. This is important, because these persons are most likely to be in possession of the pertinent documentation, or they will likely know who is.

A stop gap notice should go to the key players and to the company's information technology department ("IT") to preserve critical systems and backup data. *See Zubulake V*, 229 F.R.D. at 432 (A lawyers responsibilities include "communicating with the 'key players' in the litigation"). This notice is an important first step to avoid the destruction of significant data. The failure to identify the key players and to ensure that their electronic and paper records are preserved is now considered to be gross negligence. *Pension Committee of the University of Montreal Pension Plan v Banc of America Securities, LLC*, No. 05 Civ. 9016 (SAS), slip op. at 24 (S.D.N.Y. Jan. 11, 2010).

Information from the key players will assist the IT department in complying with preservation obligations. In interviewing key players, the focus should include identifying other individuals who may have knowledge and locating potentially relevant documents. If the claim further develops, and additional relevant persons and documents are identified, a broader, more comprehensive preservation notice should be timely issued to those individuals as well in order to ensure coverage of all main players and databases identified during the investigation.

4. Locating the Relevant Documents

In order to effectively comply with evidence preservation obligations relating to ESI, a lawyer must become familiar with a client's computer storage systems and data retention architecture. *G.T.F.M., Inc. v. Wal-Mart Stores, Inc.*, 2000 U.S. Dist. LEXIS 3804 (S.D.N.Y. 2000) (court-imposed monetary sanctions on Wal-Mart for electronic discovery abuses and further found that "counsel's inquiries about defendant's computer capacity were certainly deficient."). An attorney's obligations in locating relevant documents were described by one court as follows:

> "[C]ounsel must become familiar with her client's document retention policies, as well as the client's data retention architecture. This will invariably involve speaking with information technology personnel, who can explain system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm's recycling policy. It will also involve communicating with the 'key players' in the litigation, in order to understand how they stored information."

Zubulake V, 229 F.R.D. at 432.

Consultation with a company's IT department will provide invaluable information helpful in counsel's efforts to preserve electronic evidence. The IT department can assist in: mapping the flow of documentation throughout the company's system; identifying the location of the relevant information identified above; and preserving any active reasonably accessible documents (*i.e.*, first tier information). The IT department also will be able to identify the company's policies and procedures in backing up computer data, and can assist in the preservation of information that is not reasonably accessible (*i.e.*, second tier information) as the rules require.

The failure to cease the deletion of email or to preserve the records of former employees that are in a party's possession, custody or control is now considered to be gross negligence. *Pension Committee of the University of Montreal Pension Plan v Banc of America Securities, LLC,* No. 05 Civ. 9016 (SAS), slip op. at 24 (S.D.N.Y. Jan. 11, 2010). So is the failure to preserve backup tapes when they are the sole source of relevant information or relate to key players. *Id*.

5. Confirming Adequacy of Litigation Hold

Once investigating counsel has confirmed the identity of the key players and the location of relevant data, the preliminary "litigation hold" should be reviewed to ensure it is sufficiently comprehensive. Counsel should oversee compliance with the "litigation hold." *Zubulake V*, 229 F.R.D. at 432. By this point, more details should be available about the nature and scope of the claim, and additional individuals in possession of potentially relevant information are often identified who were not known at the outset of the investigation. The review should confirm that the litigation hold: includes an adequate description of the nature of the claim; identifies key players with substantive knowledge; provides detailed information relating to the preservation and potential collection of information; and identifies the individual(s) who have the authority to lift the hold. *See The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production* (Sedona Conference Working Group Series July 2005).

In addition to the written preservation instructions, counsel should personally contact key players (including IT personnel in charge of the deletion of data) to ensure compliance with the order. *Zubulake IV*, 220 F.R.D. at 232 (S.D.N.Y. 2003) ("A party's discovery obligations do not end with the implementation of a 'litigation hold' -- to the contrary, that's only the beginning. Counsel must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce the relevant documents."). Because it is important that all employees understand and follow the written instructions, individual follow up may be necessary, especially with the key players.

The key focus at this stage is twofold: first to satisfy the reasonableness test of Rule 37 of the Federal Rules of Civil Procedure, and second to ensure that important evidence truly is being preserved. If a complaint has not been filed, there may be no formal duty to move forward with gathering the relevant documents that have been preserved and to incur the associated costs of gathering such documents.

If a company is a potential defendant, the company may have an independent interest in preserving evidence relevant to its defense. If a company cannot locate relevant evidence that it has reason to believe exists on its computer system, the company may wish to consult a forensics expert. A computer forensic expert may be able to locate data and files that were deleted, for example, by a departing employee who is now an adverse party. Otherwise, the company's ability to defend a claim may be compromised without the preservation of relevant evidence.

6. Safe Harbor

Rule 37(f), Fed.R.Civ.P., sets forth a good faith standard to be applied in reviewing the culpability of a company for the destruction of documents relevant to litigation. Although the Rule focuses on the good faith operation of an "electronic information system," this section is essentially an inquiry into whether the company took good faith efforts to preserve relevant evidence once it had notice of the claim. Accordingly, to seek protection under the new safe harbor provisions of this rule, a company will likely be judged on the totality of its response once it has received notice of a claim. *See* Fed. R. Civ. P. 37.

Once the company determines it has notice of a claim, or even that the company may have notice, it should seriously consider retaining outside counsel to assist with pre-litigation steps. Although the involvement of outside counsel will not relieve the company of liability for data destruction, it could demonstrate that the company took reasonable steps to ensure preservation. *See Zubulake V,* 229 F.R.D. at 433-34 (S.D.N.Y. 2004) (stating that both the company and outside counsel have an independent duty to ensure that relevant documents are preserved upon notice of claim); *Report of the Advisory Committee on the Federal Rules of Civil Procedure to the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States*, at 125-29 (May 27 2005; rev. ed. July 25, 2005), available at www.uscourts.gov (a company's effort to pose a litigation hold should be considered in determining if a company acted in good faith).

7. Heightened Discovery Obligations

During phase 3, after litigation has been filed against the company, the Federal Rules of Civil Procedure will govern electronic discovery, and will have an impact on any claim of spoliation that arises based upon post-filing conduct. Although litigants are not required to be perfect in discovery, any shortcomings in electronic discovery often lead to a claim of spoliation against the imperfect party.

Although the e-discovery changes to the federal rules addressing ESI do not create new obligations to preserve evidence, they highlight the need to preserve documents in day-to-day operations. Once litigation has been instituted, a company will want to take additional steps to ensure that it can comply with its disclosure and discovery obligations. Gathering, reviewing and production of electronic documents come into play in light of these obligations. A detailed discussion of company's disclosure and discovery obligations are beyond the scope of this article, and a company will need to consider the new amendments to the federal rules that now govern the discovery of ESI and how they affect the gathering and production of ESI.

In any event, it is now abundantly clear that appropriate efforts must be taken in order to avoid the spoliation of electronic evidence. *Pension Committee of the University of Montreal Pension Plan v Banc of America Securities, LLC,* No. 05 Civ. 9016 (SAS), slip op. at 2 (S.D.N.Y. Jan. 11, 2010) ("By now, it should be abundantly clear that the duty to preserve means what it says and that a failure to preserve records – paper or electronic – and to search in the right places for those records, will inevitably result in the spoliation of evidence.").

In an ever-growing trend, courts expect the parties to work out electronic discovery issues as much as possible without court intervention. *Covad Communications Co. v. Revonet, Inc.*, 254 F.R.D. 147, 151 (D.D.C. 2008) ("[T]he courts have reached the limits of their patience with having to resolve electronic discovery controversies that are expensive, time consuming, and so easily avoided by the lawyers' conferring with each other on such a fundamental question as the format of their productions of electronically stored information."). With the growing importance of electronic discovery, courts are at risk of being swamped with too many discovery disputes if the courts do not require counsel to resolve routine issues themselves; and the imposition of sanctions is seen as a way of providing the incentive to approach discovery in a different way. *Mancia v. Mayflower Textile Services Company*, 253 F.R.D. 354, 361 (D. Md. 2008) ("[C]ourts repeatedly have noted the need for attorneys to work cooperatively to conduct electronic discovery, and sanctioned lawyers and parties for failing to do so.").

Retaining a computer forensic expert may be helpful in resolving discovery disputes in cases where ESI evidence is important. Computer forensic experts can be helpful in developing search protocols, procedures for privilege review of a forensic image, and preserving evidence.

D. Conclusion

Knowledge of computer forensic evidence can be crucial in intellectual property cases where the most important evidence is electronically stored information. In particular, trade secret misappropriation suits and copyright infringement cases often involve computer forensic evidence. It is becoming increasingly important for lawyers to know as much as possible about computer forensic evidence in order to deal with issues in IP litigation involving electronically stored information. Knowing what kind of computer forensic evidence may be available can be helpful to a lawyer in knowing when to retain the services of a computer forensic expert. A lawyer representing a defendant in intellectual property litigation involving computer forensic evidence must know how to effectively defend the plaintiff's claims. A defendant who does not know how easily electronic evidence can be fabricated or destroyed, may find himself or herself at the mercy of an unscrupulous plaintiff who may have no qualms about altering relevant electronic data.

Sid Leach
Snell & Wilmer
L.L.P.
One Arizona Center
400 East Van Buren
Phoenix, Arizona 85004-2202
(602) 382-6372
(602) 382-6070 (facsimile)
sleach@swlaw.com