

# Five Ways Computer Forensics Can Aid Discovery

by Robert L. Kardell

The art of discovery has changed drastically over the last two decades. The increased use of personal computers has added a significant burden to the process. Consider the average computer hard drive can hold approximately 61 million pages of text<sup>1</sup> or information or 50,000 photographs.<sup>2</sup> This is a lot of information being digitally stored and maintained by a single person. Couple this with the fact most people use two computers, a computer at home and a computer at work.

## Robert L. Kardell



Robert L. Kardell, JD, MBA, CFE is a managing consultant and member of the Forensics & Dispute Consulting division of BKD, LLP, one of the 10 largest CPA and advisory firms in the U.S. Based in BKD's Omaha office, he provides fraud investigation services, litigation support and expert testimony for a variety of business clients. Bob is a 1987 graduate of Benedictine College, Atchison, Kansas, with a B.S. degree in accounting, and a 1991 graduate of the University of Nebraska, Lincoln, with both MBA and Juris Doctor degrees. He is a member of the American Bar Association, Nebraska State Bar Association, Nebraska State Board of Public Accountancy and Association of Certified Fraud Examiners. Before joining BKD, Kardell spent 13 years with the Federal Bureau of Investigation in Chicago and Omaha. Contact the author at rkardell@bkd.com.



Photo courtesy of StockXchange.

The document you are looking for during discovery is most likely digitally stored on someone's computer hard drive or email mailbox as more than 171 million emails are sent every-day.<sup>3</sup> With the sheer number of emails and mailboxes, it is possible a witness may never remember seeing or receiving a particular email. This is a large amount of information which is excluded if e-discovery is not pursued during litigation. E-discovery generally refers to the process of harvesting, searching, reviewing and producing electronic documents during litigation in an agreed-upon format.

The question then for litigators is: when during the e-discovery process is it necessary or prudent to hire a computer forensics expert? There have been a number of ways in which computer forensics experts have aided in the discovery process, but five of the most common ways are: uncovering hidden evidence, uncovering evidence in intellectual property cases, reviewing meta-data, recovering emails and recovering deleted documents.

## Uncovering Hidden Evidence

The secrets to hidden assets may lie within the digital media of a computer. In a recent case, a computer forensics expert was asked to review the computer of an elderly person employing a caretaker. The caretaker had worked for the individual and had used a computer, which was owned by and located in the individual's house. After several years of employment, the caretaker was being accused of embezzling. The embezzlement allegations included the illegal transfer of certain real estate as well as the transfer of a large amount of money.

## COMPUTER FORENSICS AID DISCOVERY

The court hired a guardian ad litem on behalf of the individual who then sued the caretaker. As part of the investigation, the guardian asked for a computer forensics analysis of the computer used by the caretaker. After the initial search was complete, two different bank accounts were uncovered outside the U.S., which had been used to transfer money, as well as a copy of the Quitclaim Deed used to transfer the real estate.

### Computer Forensics vs. E-Discovery

**E-discovery:** Refers to the process of harvesting, searching, reviewing and producing electronic documents during litigation in an agreed upon format. These steps can be taken in many ways, such as reviewing and producing native documents, documents converted electronically to TIFF or PDF, paper copies or even a “load” file suitable for import into one of the many litigation support software programs.

**Computer forensics:** The process of harvesting, searching, reviewing and producing items where the authenticity of the document may be called into question. The computer forensics process preserves the authenticity of the documents and the associated meta-data. Computer forensics experts are needed to verify the authenticity of the documents and to verify and/or oversee the processes used to recover the documents. Documents can include active documents, deleted documents, file fragments, deleted emails and others.

This case worked well for the guardian and helped to show the court the transfers, which up to that point were merely allegations, had actually taken place. The attorney also was able to prove to the court the caretaker had been less than honest in the prior proceedings. Sometimes the information needed to bolster your case may lie within the information controlled by your client, but it may take a computer forensics expert to uncover it.

## Intellectual Property Cases

Intellectual property theft accounts for a large percentage of computer forensics cases. Computers are used to manage sales leads, maintain customer relationship databases, house proprietary programs and computer codes. Most, if not all, the information a business stores on its computers can be stored on any digital media and removed from the office. The entire database of customers, sales leads and other proprietary information which keeps a company in business may just fit on one employee’s MP3 player.

If your litigation involves the possible theft of intellectual property, computer forensics searches on the person’s old computer at his or her previous employer, who is usually the plaintiff in such cases and is still in possession of the computer, to see if it yields some significant evidence. Courts have been receptive to allowing forensics searches on computers at the

person’s new place of employment<sup>4</sup>, personal computers<sup>5</sup> and personal digital media<sup>6</sup> because this information can be so easily moved from one computer to another. A search of such a computer might yield proof information has been downloaded to a USB thumb drive, another computer, a CD or DVD, or possibly a transfer of a file over the Internet. There has even been precedent for the production, imaging and searching of a computer acquired by the defendant two years after leaving the company. The judge reasoned that it was likely the defendant would have placed the information on that computer if he were in possession of and using the information.<sup>7</sup>

Any computers remaining in the possession of your client at the time the case is initiated should be considered for forensics analysis. You may discover information to help your case but, you also may discover information which may be in the possession of the opposing party. Wouldn’t it be better to know this information going into the litigation rather than finding it at the time of trial?

## Meta-Data

Meta-data is a way of describing the information kept by the operating system about the file itself, such as creation date, modification date, etc. Meta-data is also the term used to describe the information about the file kept by a computer program such as Microsoft Word. Computer programs can keep information such as author, reviewers, version changes, last print date and more. This second type of meta-data is stored within the file itself. Any or all of this information may be useful in your case.

Meta-data can be used to help provide a timeline for events by placing the documents in order of their creation date. A great use of this type of review is to look for document creation dates which may be after a date presented in the document itself. A review of a hard copy, scanned copy, TIFF or PDF version of a letter would not reveal this information. If there is a particular document or set of documents whose dates are cru-

### Fast Facts

- More than 1.4 million email mailboxes are in use today
- More than 171 million emails are sent everyday
- The average email size per user per day is approximately 14 MB<sup>10</sup>
- The average user sends or receives 8,400 pages worth of information each day
- A single megabyte of data can contain more than 600 pages of information
- A four gigabyte USB drive or MP3 player can store almost 2.5 MM pages of information

## COMPUTER FORENSICS AID DISCOVERY

cial to your case, consider asking for the associated meta-data. This information may still be present on the computer even if it has been several years since the item was deleted. The one caveat is that operating system meta-data such as time and date stamps are easily altered and may not be reliable.

### Search for Emails in Theft of Intellectual Property

In a case involving email on which I worked, I was asked to search the hard drive for any emails that might relate to a theft of intellectual property. Knowing the computer was used after the person had resigned, I thought the email file itself, and therefore the individual emails had remained untouched. I was wrong. The company had hired a local technology firm to install software upgrades. While performing the upgrades, the company asked the tech firm to covert the email file so that they could review the email. The software company attempted several times to convert the file and eventually did so, but the tools they used were not forensically sound. When I discovered the attempt, the company admitted someone else had tried to convert the file. Any hope of preserving the integrity of the file was now questionable.

Technology firms and their personnel may be good at managing software and hardware, but unless they are specifically trained in computer forensics and are aware of the issues concerning file integrity, they are not the right people to use for digital forensics procedures.

### Email and Deleted Items

The most common reasons for computer forensics examinations have been to retrieve emails and deleted items. There are many types of software out there that claim to be able to search and recover deleted files, but computer forensics software provides the necessary controls to maintain the integrity of the file for later use in a trial. Computer forensics software can provide documented proof of where the file resides on the hard drive, its starting point and ending point, and proof the file has not been altered.

Files can be deleted in several ways. After deletion, a file may still reside on the hard drive for several years in one form or another. The deletion of a file can take place by simply moving the file to the Recycle Bin or using the right-click menu to send the file to the Recycle Bin. In cases such as this, the file is not really deleted, but rather moved to a different folder. Files also can be deleted by bypassing the Recycle Bin by holding down on the shift key while the file is dragged to the Recycle Bin. If a file has been deleted in this manner, non-forensics recovery software may or may not find the file and

recover it. Forensics software is needed to be sure.

Parts of files also can remain on the hard drive for years as file fragments. Files are usually saved on a hard drive in several contiguous sectors. Sectors of a hard drive are overwritten as needed by the operating system, but the operating system may not need to overwrite an entire file, thus leaving part of a file on a hard drive to be recovered.

Under the newly revised Federal Rules of Civil Procedure, inaccessible files are not automatically discoverable by the opposing counsel and file fragments can be considered inaccessible files.<sup>8</sup> The review of such material can be expensive and time consuming, but if the computer is in your possession and the case may hinge on such data, it might well be worth the effort to search for it.

Emails are also a large part of e-discovery requests. The search, review and production of email can be time consuming, so it is in everyone's interest to make sure production is completed correctly. Emails are stored in a variety of places on a hard drive or on a central server and can be stored in a number of file formats. Some formats are easier to search and review than others. There are many tools for searching emails, but, to make sure the emails are not altered in any respect, it is usually best to preserve the files using forensics procedures first and then begin your search.

It is also important to note that, like files, emails can be retained on the hard drive in fragments for several years. For example, in another computer forensics case an email was recovered from 2001. In this case an email and the associated attachment were in question and the defendant denied creating either. Within a few minutes after an image of the hard drive was complete, several versions of the email were found intact on the hard drive from five years prior. The email contained a version of the spreadsheet and through a review of the meta-data created by the Microsoft Excel program, the author of the email and spreadsheet were shown to be an employee of the defendant. The case was settled shortly thereafter. Again, the computer was in the hands of the plaintiff so they took the chance of spending the money to review the data, which normally would not be discoverable by an opposing party under the new rules.

Emails are difficult to review for two reasons; first, there are so many of them, and second, the manner in which they are stored on a computer. As pointed out previously, hundreds of millions of emails are sent every day. This makes for a large amount of data to review in discovery.

Emails also are stored in "container" files, which means a single email file can contain many emails. These containers need to be broken apart for individual email review. This takes special software, which will separate the individual emails while



### Tackling Issues In-house

One specific area of e-discovery that has become more common is searching for responsive files and producing the results using law firm employees. However, there are a variety of issues which law firms need to consider.

First, there is a distinction to be made between e-discovery and computer forensics. Computer forensics should be used any time the authenticity of the documents is called into question which includes deleted files. There have been a number of times in which I have been asked the question as to why computer forensics trained personnel are necessary when litigation support has software to do the job. The answer is that the software for litigation support is not the best software to use when the integrity of the file is at issue and harvesting the documents without computer forensics safeguards can inadvertently alter the meta-data. Computer forensics software and computer forensics personnel are much better equipped to deal with such issues.

Second, litigation support software does not always deal with the issues outlined in the article, such as deleted files and email conversion and preservation. For example, if a client searches a hard drive for files accessed between certain dates and an email file is part of the production, litigation support software will handle the issue if the file is a standard email file such as a Microsoft Outlook. But, if email is saved in an uncommon format and the production becomes a key document in the case, the integrity of the file will need to be proven. Without the preservation processes and checksums used in a computer forensics program, the file may not be admissible.

Finally, liability issues should be part of the decision process. In the well known case of the bankruptcy of the Denver based cable company Adelphia Communications Corporation (Adelphia), David Boies' firm, Boies Schiller & Flexner, recommended that Adelphia use the e-discovery firm, Amici LLC (Amici). As it turns out, the Boies family owned an interest in Amici. The attorneys representing the accounting firm KPMG, which was part of the bankruptcy litigation, pointed out to the bankruptcy court that Amici had collected millions in fees for e-discovery and litigation support all while the interest in the firm by the Boies family was never disclosed to the client or the bankruptcy court.<sup>9</sup> This is an ongoing case and it remains to be seen how the court will rule, but it highlights the liability issues of bringing such a production in-house or to a wholly owned or partially owned subsidiary. A mistake in the production may lead to arguments that the production firm lacked independence. Non-disclosure of the relationship of the production firm to the law firm may lead to arguments of a conflict of interest and ethics violations.

preserving the integrity, form and any attachments. There are many tools out there to open the container file or to convert the file from one format to another. Whichever tool you choose, it should be a forensics tool which has been shown in court to preserve the integrity of the data.

### Summary

The use of computer forensics can greatly aid in the discovery of material which may be pertinent to the case at hand. Computer forensics can help uncover hidden assets, intellectual property theft, meta-data and email and deleted files. Firms who would like to move the e-discovery process in-house to a subsidiary in which they own an interest should take great care in doing so as the move may expose the firm to greater liability.



### Endnotes

- <sup>1</sup> There are approximately 600 pages of unformatted text in 1 MB and approximately 614,000 pages of text in 1 GB. Formatted documents, such as Microsoft Word documents, would occupy significantly more space on a computer hard drive.
- <sup>2</sup> The statistic is based on the average digital photograph being approximately 2 MB in size.
- <sup>3</sup> "Hewlett-Packard: Taming the Growth of Email – An ROI Analysis" The Radicati Group, March 2005, <http://www.radicati.com/reports/whitepapers.asp>
- <sup>4</sup> Ibid.
- <sup>5</sup> *Balboa Threadworks, Inc. v. Stucky*, 2006 WL 763668 (D. Kan. Mar. 24, 2006)
- <sup>6</sup> Ibid.
- <sup>7</sup> Ibid.
- <sup>8</sup> *Frees, Inc. v. McMillian*, 2007 WL 184889 (W.D. La. Jan. 22, 2007)
- <sup>9</sup> FRCP. 26(b)(2)(B). See also, "The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production," A Project of The Sedona Conference Working Group on Best Practices for Electronic Document Retention & Production, July 2005 Version, p. 38, Comment 9.b. Deleted Data and Residual Data.
- <sup>10</sup> Lin, Anthony, "Adelphia Asked Boies Schiller to Resign Over Family Connection to Vendor," *New York Law Journal*, September 13, 2005, (<http://www.law.com/jsp/article.jsp?id=1126528530058>). See also Frank, Robert, "Adelphia, Boies Firm Agree to Split," *The Wall Street Journal*, August 30, 2005.

**“Five Ways Computer Forensics Can Aid Discovery,”** by Robert L. Kardell. This article, published on pages 5-8 in the October 2007 issue of **The Nebraska Lawyer**, appears here with the permission of the Nebraska State Bar Association.