DUNN ON DAMAGES

THE ECONOMIC DAMAGES REPORT FOR LITIGATORS AND EXPERTS

ROBERT L. DUNN

Publisher
Valuation Products & Services, LLC
James R. Hitchner, CPA/ABV/CFF, ASA
Editor in Chief
Robert L. Dunn, J.D.

Please enjoy the following article, reprinted from *Dunn on Damages*, with my compliments!

KELLY J. TODD, CPA/ABV/CFF, CFE

Kelly J. Todd is a shareholder at Forensic Strategic Solutions, Inc., specializing in forensic accounting, fraud examination and litigation support. She has experience in financial and white-collar investigations as well as investigation and analysis of large electronic databases. Ms. Todd has conducted forensic examinations for governmental agencies, including the second largest school district in the United States, and publicly held and closely held businesses. Her experience in litigation support includes services for plaintiffs or defendants in civil proceedings.

CONTENTS

Although the information in this journal has been obtained from sources that VPS believes to be reliable, we do not guarantee its accuracy, and such information may be condensed or incomplete. This journal is intended for information purposes only, and it is not intended as financial, investment, legal, or consulting advice. Valuation Products and Services, LLC, (VPS) disclaims all responsibility for its content.

Computer Forensics v. E-Discovery: What Every Expert Should Know

Kelly J. Todd
CPA, ABV, CFF, CFE
Forensic Strategic Solutions
Birmingham, AL
kelly@forensicstrategic.com

The Federal Rules of Civil Procedure were amended in 2006 to make clear that the discovery of electronically stored information (ESI) stands on equal footing with discovery of paper documents and require that any request for production of documents be understood to include a request for ESI.[1] This major change in the rules acknowledges the central role that computers and the Internet play in business and our lives.

In the six years since the FRCP changes, the perpetual explosion of ESI has been nothing short of a runaway train. The quantity and variety of ESI created daily by the typical person is astonishing.[2] Think for a minute about the trail you generate daily—from every swipe of your credit, debit, ATM and security access cards to your texts, tweets, pictures, e-mails, logins, keystrokes, websites, downloads, phone calls, voicemails, photocopies, print jobs, blogs and posts— you leave behind an astonishing electronic footprint that could tell a very compelling story. Forget the delete button…regardless of the number of times you press it, your trail will still follow you.

The evidence to answer the most fundamental litigation questions—the "who, what, where, when and why"— is increasingly contained within ESI.[3] However, merely knowing that the answers are buried somewhere in the mountain of potentially available ESI rarely proves helpful to your client's objectives.

A review of court rulings on electronic discovery (e-discovery) from the past decade shows that the most successful requests for ESI are those that demonstrate relevance and proportionality to the needs of the case. Yet how is this accomplished? An important first step is having practical knowledge of the two primary approaches to the discovery of ESI: computer forensics and e-discovery.

Computer Forensics v. Electronic Discovery

The differences between computer forensics and e-discovery are distinct. Requiring varying levels of technological sophistication, the processes for both computer forensics and e-discovery involve the identification, preservation, collection, review and production of ESI. The critical distinction, however, lies within the collection process and the type of ESI that is collected.

E-Discovery

The primary focus of standard e-discovery is the collection of active data and metadata from multiple hard drives and other storage media. Active data is the information readily available to the user and can be accessed and copied through file manager programs. Active data includes spreadsheets, databases, word processing files, business application files, e-mail, electronic calendars, and address books.

Metadata provide information about, or documentation of, other data managed within an application. Think of metadata as the "information about information." Metadata includes the date of creation, author, source, history, to name a few. This information seldom appears on the screen or in the printed version of a document and is often generated automatically by the software application without the user's knowledge or intent.

Common examples of metadata include the editing history in word processing programs, formulas in spreadsheets, email headers and routing information. For example, metadata is extremely helpful in constructing a timeline with emails and it can be critical in the examination of databases, which without metadata would be meaningless.

Computer Forensics

The collection of data in a computer forensic examination goes far beyond that of standard e-discovery. The goal of computer forensics is akin to conducting an autopsy of a computer hard drive – searching hidden folders and unallocated disk space for copies of deleted, fragmented or damaged files – attempting to identify the who, what, where, when and why from a specific computer.

Computer forensics takes advantage of the way computers operate and store information, including the temporary and/or permanent information recorded by the operating system during normal operation. For example, during normal operation many operating systems will record potentially valuable information such as the identification of thumb drives that were connected to the computer, the date and time a file was last accessed or modified, Internet searches, websites visited, email read or sent, and computer programs that were installed or used on the computer.

Although the data collection processes for standard e-discovery may involve the use of forensic software tools, do not confuse, however, the use of such tools with the outcome achieved in a computer forensic examination. The image of a computer storage device produced during a forensic examination produces an exact replica, bit for bit, of the original storage device that allows investigation of past use without altering the original evidence.[4] Referred to by various names, such as a mirror image, a forensic image, or a forensic copy, the computer forensic image is vastly different from a copy produced by merely copying all of the files and associated metadata. The computer forensic image captures not only readily accessible data such as active data and metadata from the storage device, but also less accessi-

Continued on next page

ble contents such as automatically stored files, deleted files, residual data, contents from unallocated space, and system data.

Automatically Stored Data
Computers store a great deal of data automatically. Many software manufacturers build in automatic backup features that create and periodically save copies of a file. These files are created and saved to help users recover data lost due to a computer malfunction. Typically, automatically stored files are not stored in the same directory as the active file. Moreover, on most networked systems, the automatically stored files are saved to the user's hard drive rather than to the network file server. As a result, a file (or some version of it) that was purged from the file server may exist as a copy on the user's hard drive.

Deleted Files
"Deleted" does not mean destroyed. The process of deleting merely indicates to the computer that the physical space belonging to the deleted file is available. The data can remain on the hard drive until it is overwritten by new data or "wiped" through the use of utility software. Unlike active data, the "deleted" data cannot be viewed with file manager programs.

"Ghost" or Residual Data
Residual data are information that remains recoverable from the computer system but does not appear as accessible data when performing a file or directory command. Residual data include deleted files or file fragments, file slack, and unallocated space.

System Data
System data is the electronic trail of activity on a computer or network and is typically generated without the user's knowledge. Computer logs generated by most systems track each time a user logs on or off, and may include information regarding the use of various applications, the web sites visited, passwords used, if and when a document was deleted, and whether a document was downloaded, copied, or printed and to what external device.

Computer Forensics v. Electronic Discovery

Factors	Computer Forensics	E-Discovery
Origins	Law enforcement	Civil litigation
Focus	Specific	General
Collection process	Bit by bit	Bit image only
Type of data collected	Accessible and inaccessible	Accessible
Active data	Yes	Yes
Metadata	Yes	Yes
Automatically stored data	Yes	Maybe
Deleted files	Yes	No
"Ghost" or residual data	Yes	No
System data	Yes	No
Evidence of wiping software	Yes	No
Testimony	Expert	Fact

Wiping Software
Anti-forensic software or "wiping software" is designed to remove all traces of data from a hard drive or other peripheral device. The wiping process can be a broad-brush wipe of the entire hard drive, or it can be limited to only the unallocated storage space. Leaving behind a characteristic pattern, the use of wiping software can be detected through the computer forensic process.

A summary of the differences between computer forensics and e-discovery is shown in the table above.

The Relevance of Computer Forensics in Discovery
Now that we have the picture of where the computer information resides, when does the deep-dive approach of computer forensics make sense? While not appropriate in all cases, the use of computer forensics is becoming increasingly relevant in a wide range of disputes. Originally developed by law enforcement for use in criminal matters, computer forensics has also become relevant in disputes involving significant damages claims, proprietary products or technology, employment disputes, fraud, marital disputes and cybercrime.

A good example of the deep-dive approach arises in the employment arena where a forensic examination of a departing employee's laptop, work computer or home computer can provide a wealth of information concerning the actions of the former employee in the days leading to their departure. The key is to take timely measures to preserve and investigate relevant ESI to avoid lost or over-written data. In *Keystone Fruit Mktg., Inc. v. Brownfield*, 2007 WL 788358 (E.D. Wash. Mar. 14, 2007) it was alleged that a former Keystone employee opened and used a key document for the benefit of her new employer (a competitor of Keystone). The former employee contended that while she did open and view the document, it was mere speculation that the document was given to or used by the defendant. The computer forensics analysis of her laptop, home and work computers told a different story. The forensic analysis showed that not only did Keystone's data reside on the former employee's home computer and

Continued on next page

e-mail, but also on computers at the defendant's company.

THE COURT'S VIEW OF COMPUTER FORENSICS

Intrusiveness and Relevance

In the last decade, it has become common for the courts to enter an order requiring the mirror imaging of hard drives and peripheral devises that might contain responsive and relevant evidence to an opposing party's request for production. See e.g., *Communications Center, Inc. v. Hewitt,* 2005 WL 3277983 (E.D. Cal., April 5, 2005).

On the other hand, because electronic discovery can easily become broad and intrusive, the courts have exercised discretion in requiring the mirror imaging of hard drives and other peripheral devises where the request is "extremely broad in nature"[5] and the nexus between the need to mirror image and the claims are "unduly vague or unsubstantiated in nature."[6]

For example, in *McCurdy Group v. American Biomedical Group, Inc.* 9 Fed. Appx. 822, 2001 WL 536974 (10th Cir. 2001) American Biomedical failed to provide sufficient reason to require McCurdy to produce all of its computer hard drives. The District Court (and later the Court of Appeals) upheld the magistrate judge's ruling denying the request. The Court of Appeals noted that skepticism alone of a party to produce all copies of relevant and non-privileged documents "is not sufficient to warrant such a drastic discovery measure."

Conversely, in *Balboa Threadworks, Inc. v. Stucky,* No. 05-1157-JTM-DWB, 2006 U.S. Dist. LEXIS 29265, 2006 WL 763668 (D. Kan. Mar. 24, 2006), a matter involving copyright infringement, the court found that "the importance and relevance of computer evidence is particularly important" because the infringement claims arose from the use of computers to download copyrighted material. Additionally, the court ordered that all of the defendants' computers be made available for mirror image despite claims by one defendant that his computers were not used for the benefit of the business. The court noted, however, that because one of those computers was used to draft a document related to the alleged acts of infringement it was "reasonable to conclude that some relevant evidence concerning the claims and defenses raised by the parties" or "evidence relevant to the subject matter" may be found on any of the defendants' computers.

Specific and Limited Requests

The courts appear to be more receptive to specific and limited requests for a computer forensic approach to data collection. See e.g., *Rowe Entertainment v. William Morris Agency,* 205 F.R.D. 421, 427-28, 432-33 (S.D.N.Y. 2002) where the court granted revised and limited request for ESI, or *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 641 (S.D. Ind. 2000) where access was limited to computers of four specifically named individuals.

CONCLUSION

Understanding the difference between computer forensics and e-discovery can be critical to the outcome of a litigated matter. While both provide value, the differences are distinct and the decision to use either depends on the matter at hand. Because the discovery of ESI can easily become overly broad and intrusive, one must have a clear understanding of the issues when considering the deep-dive approach that computer forensics requires.

[1] Ball, Craig. "Hitting the High Points of the New EDD Rules," Law.com. 28 December 2006 *http://www2.law.columbia.edu/Johnson/syllabus/highpointsediscovery.htm.*

[2] Paul, George L.& Jason R. Baron. "Information Inflation: Can the Legal System Adapt?" *Richmond Journal of Law and Technology.* Vol. 13, Issue 3. 2007 *http://jolt.richmond.edu/v13i3/article10.pdf.*

[3] Borden, Bennett B., Monica McCarroll, Brian C. Vick, and Lauren M. Wheeling. "Four Years Later: How the 2006 Amendments to the Federal Rules have Reshaped the E-Discovery Landscape and are Revitalizing the Civil Justice System," *Richmond Journal of Law and Technology.* Vol. 17, Issue 3. *http://jolt.richmond.edu/v17i3/article10.pdf.*

[4] *New Hampshire Ball Bearings, Inc. v. Jackson*, 158 N.H. 421, 424, 969 A.2d 351,356 (2009).

[5] *Balboa Threadworks, Inc. v. Stucky,* No. 05-1157-JTM-DWB, 2006 U.S. Dist. LEXIS 29265, 2006 WL 763668, (D. Kan. Mar. 24, 2006).

[6] *Id.*