Electronic evidence discovery: From high-end litigation tactic to standard practice

By John M. Patzakis, Esq. *

Introduction

Electronic evidence discovery is increasingly becoming an indispensable component of civil litigation. This development is long overdue, as the majority of responsive documents – most now exist in electronic form – are typically not requested or produced in the course of discovery proceedings. The inadequate attention to computer-based evidence is a significant omission, and the changing ways of counsel and the courts need to continue.

Computer evidence is largely overlooked or ignored due to cost concerns, perceived procedural difficulties or plain ignorance of counsel. Traditionally, two barriers prevented the widespread practice of electronic evidence discovery in the civil litigation realm: 1) The enormous cost and burden associated with electronic evidence discovery due to a lack of effective tools to collect, process and manage electronic evidence, and 2) The lack of a defined procedural protocol to gain access to and regulate the inspection of computer systems not in the custody or control of a litigant. However, recent developments in both technology and the law have significantly reduced these constraints, allowing freer exchange of the treasure troves of relevant documents that invariably reside on opposing parties' computer drives.

Advancements in computer forensic tools

Computer forensics is commonly defined as the collection, preservation, analysis, and court presentation of computer-related evidence. As electronic evidence is fragile by nature and can easily be altered or erased without proper handing, the courts have correctly recognized that the necessary computer forensics tools and techniques must be employed in order to collect and process computer evidence. Computer forensic software also serves as the best means to recover all available evidence, including the deleted and temporary "buffer" files that are not normally visible to the user. and to preserve and authenticate the evidence with a documented chain of custody. Computer forensic software performs these functions by first creating a complete but non-invasive sector-by-sector "mirror image" backup of all data contained on the target computer media in order to recover all active, deleted and temporary files. This process allows the examiner to "freeze time" by having a complete snapshot of the subject drive at the time of acquisition.

After the mirror image copy is created, the latest generation of computer forensic software, namely EnCase, will then "mount" the mirror image as a readonly drive, thus allowing the examiner to conduct the examination on the mirror image of the target drive without ever altering the contents of the original. This process is essentially the only practical means of searching and analyzing computer files without altering date stamps or other information. Often times, a file date stamp (file creation date, last modified, or last accessed) is a critical piece of evidence that may weigh in the balance of a dispute.

The EnCase computer forensic software has helped foster a revolution in the field of computer forensics. Prior to the recent development of integrated tools with a graphic user interface, forensic investigators toiled with various procedures that required numerous nonintegrated DOS-based utilities in a process that was inefficient, costly, burdensome and, often times, incomplete and inaccurate. Under the old methodology, examiners often required weeks or months to examine a single computer involving, as noted by one court, a "highly technical process requiring expert skill and a properly controlled environment. The wide variety of computer hardware and software available [required] even computer experts to specialize in some systems and applications." (United States v. Campos - F.3d. -(10th Cir 2000), 2000 WL 1005262)

In Alexander v. Federal Bureau of Investigation, 188 F.R.D. 111, 117 (1998 D.C. Cir) an information technology specialist from the **Executive Office of the President** testified that the examination of a single hard drive to locate documents responsive to a subpoena (employing now-obsolete methodology) would require approximately 265 hours. If a law firm were to retain an expert to conduct a similar task at an average standard rate of \$300 per hour, the cost would exceed nearly \$80,000 for the examination alone. It is thus no (continued on next page)

* John M. Patzakis is general council to Guidance Software, Inc., the developer of the leading computer forensic software tool, EnCase. Currently, Guidance Software has over 3500 users from law enforcement agencies and the private sector worldwide, and EnCase now serves as the industry standard. wonder that the *Alexander* case and others like it often found their way into briefs submitted by litigants seeking to quash an adversary's subpoena for the production of computer evidence. As recent as July 1999, counsel advanced the argument in one wellpublicized federal litigation that e-mail discovery was "simply not feasible." (*Playboy Enterprises v. Welles*, 60 F.Supp.2d 1050, 1054 (S.D. CA 1999))

These previous methodologies, which required extensive training and overall mastery of the DOS operating system, limited the practice of computer forensics to a handful of experts in the private sector. Since the examiner performed the bulk of the examination from the DOS command prompt, the process mandated proficiency in crafting hundreds of arcane DOS commands and switches. The early pioneers of computer forensics believed that forensics examinations should never take place in a Windows environment, as Windows routinely alters data and writes to the hard drive whenever it is operated.

However, EnCase resolves this problem by acquiring the evidence in DOS and then "mounting" the resulting bit-stream mirror image as a read-only drive. The forensic software, not the operating system, then reconstructs the file system of the acquired drive by reading the logical data on the mirror image backup, thus allowing the examiner to view, sort and analyze the data though a Windows GUI in a completely noninvasive manner.

Additionally, all the necessary tools and functions are integrated into one application, further streamlining the investigation process and allowing the examiner to more effectively manage the evidence, and to build a case. The new generation of forensic software has redefined the practice of computer forensics by providing a means for dramatically more efficient and effective investigations by technical specialists who are reasonably skilled by no longer required to become highly trained and specialized computer engineers to properly recover computer evidence. Further, the new genre of integrated Windows-based forensic software, such as EnCase, allows more computer savvy attorneys and even judges to review the evidence and perform basic analysis of the mirror imaged drives after a computer forensics experts has acquired such evidence. This provides counsel and their staff with the opportunity to review the "box of documents" themselves without the necessity of exclusively and completely relying on the computer forensic expert to recover and interpret all the available information.

A coherent discovery order and model

The Simon Property Group v. mySimon, Inc. 2000 WL 963035 (S.D. Ind.), — F.R.D. —, decision is important as it presents a much needed, well-designed discovery protocol for the examination of computers to recover relevant documents, including deleted files. Simon Property demonstrates that a large-scale computer forensic analysis can be performed within a reasonable period of time and without enormous cost. Unlike Alexander v. F.B.I, the newer generation of computer forensic software (here EnCase) is being utilized to carry out the order of the Simon Property court.

Additionally, the appointment of a single computer forensic consulting firm to act as special master is another important recent trend in civil litigation that better serves judicial economy and efficiency. The alternative of each party retaining separate partisan computer forensic experts only invites prolonged litigation through objections and extensive motions, whereas a single expert acting as special master (using the appropriate computer forensic tools) can expedite the process by retaining custody of the evidence while providing the producing party an orderly means by which to address any claims of privilege. Further, with the computer forensic expert serving as a special master or officer of the court, any attorney-client or other privileges would not be waived by virtue of a mirror image of the drives being made.

Conclusion

Civil litigators cannot afford to continue to overlook electronic evidence, as computer files conceivably constitute the majority of responsive documents in any given demand for production of documents. Now that a support infrastructure of effective software tools and a vast and growing network of computer forensics experts is in place, attorneys have a heightened duty to incorporate electronic evidence discovery as a standard litigation practice.

Reprinted with permission from Federal Discovery News. Copyright 2000 by LRP Publications, 747 Dresher Road, P.O. Box 980, Horsham, PA 19044-0980. For more information on this or other products published by LRP Publications, please call 1-800-341-7874.