

Using Computer Forensics To Manage Electronic Evidence

by Scott Stevens of New Technologies, Inc.

More often than not, digital discovery is treated much like the traditional paper discovery model. With paper discovery, documents are scanned (perhaps OCR-ed), converted to TIFF files, linked to corresponding records in a database and then searched and categorized using a litigation support program.

Digital documents fall into three broad categories: active files, archival/legacy data and residual data (which include file fragments, deleted files and metadata). Using the paper model, each category is treated differently. A litigation team might proceed like this:

Active Files — Print out and review, scan and OCR, then convert to TIFF file and commit to database

Archival Files — Convert to printable format, print and review, scan and OCR, then convert to TIFF file and commit to database

Residual Data — Perform forensic processing to identify deleted files and telling computer-user activity, report findings, selectively convert to TIFF file and commit to database

While litigators are beginning to recognize the benefit of using computer forensics to uncover unknown evidence (the residual data mentioned above), many do not realize that forensics can be used to complement—or in some cases, replace—conventional digital discovery efforts. The computer forensics approach departs from the paper model in that all data is reviewed in electronic format with forensic software tools. Many conversion steps are removed from the process, all data is reviewed, and the litigation team receives preliminary results with much faster turnaround for a fraction of the cost.

Meeting Difficult Discovery Demands

In an actual case on which our firm has been working, a government agency alleged that a company had violated its agreement and filed a lawsuit.

Production of over one terabyte of data (1,000 gigabytes, the equivalent of 375,000,000 document pages) was mandated by the court—*within a week*. Almost all the data resided on backup tapes. It would be impossible for the company to meet this request using manual methods, and they lacked the internal technical expertise to produce the massive amounts of data involved in a cohesive electronic format.

Applying the paper-based approach, all data would have to be converted from its native tape format to a universal format (generally as TIFF files) and placed in a database, where it could be searched and categorized. Obviously, file conversion would be the bottleneck in this scenario—not to mention how extremely expensive the process would be.

To narrow the scope of meaningful data earlier in the process, forensics utilities were used to search the universe of data in its native format for relevance and responsiveness, a necessity in a discovery request of this magnitude under the given time constraints. Using further forensics processes, the company's MS Exchange database (which housed the company's e-mail archives, the focus of the discovery efforts) was converted to PST files, sorted by user and searched for responsiveness. The company was able to meet its deadline; ongoing analyses have been conducted to keep the company in compliance with the discovery mandate.

When to Consider Forensics as an E-Discovery Management Tool

While computer forensics can be applied to any situation in which there's a need to make sense of e-discovery, there are certain situations where it offers definite advantages:

Searches across a variety of file formats: To conduct a search across a variety of file formats (e.g., PST files, legacy databases, PDF files), the files must undergo time-intensive file-conversion. Computer

forensics allows you to circumvent the conversion process, as all files can be searched in their native format.

A narrow search across a broad amount of data: In many cases counsel may be looking for only a few key documents or pieces of correspondence across a large computer hard drive or server. Forensics will allow for a search across an entire hard drive or logical partition thereof, quickly surfacing only those documents most likely to be responsive.

Searches where confidentiality is an issue: Counsel will often try to block discovery of a client's business or personal computers on the basis that these machines contain confidential information that has nothing to do with the case at hand. By permitting discovery, so their reasoning goes, all client data will be reviewed, and confidentiality will be violated. Because computer forensics searches are conducted independently of file format, individual files are not opened or viewed in the searching process, and confidentiality can be maintained. Counsel seeking discovery can conduct a forensics search, identify a finite amount of files that contain key words (or files that were accessed during a pivotal time period in the case), and present that list to the court, citing their relevance.

The litigation community is just beginning to understand how computer forensics can help uncover "unknown evidence"—deleted files, usage patterns, and the like. The efficacies of forensics for the management of "known" evidence represent a whole new and potentially much broader-based use of this technology.

About our author . . .

Scott Stevens is Director of Business Development at Gresham-based New Technologies, Inc. (www.dataforensics.com) Contact him at scott@dataforensics.com or 503.661.6912.