

# Deploy Computer Forensics Early to Find the Smoking Gun

BY SCOTT STEVENS

**C**onsider the following scenario: a company has been tipped off that some recently departed employees may have left with more than they were entitled to – namely, proprietary information that might amount to a theft of trade secrets. After a month of strategic planning, the litigation team retains a third party computer forensics consultant to analyze the company's server. Their efforts are successful; evidence of wrongdoing is discovered on the server. The next step is to corroborate the information found on the server with corresponding evidence on the former employees' workstations.

As it turns out, the company in question has a perk that allows employees to purchase their computers (the policy was designed to cull out obsolete machines). The employees in question purchased their 'old' work computers and took them home when they gave notice. The plaintiff party and their forensics experts are eventually able to gain access to these machines through a court order. However, by the time they got there, much of the data they were seeking had been overwritten and otherwise "scrubbed", rendering it irretrievable...and irrelevant.

Had the plaintiff had the foresight to have the court quarantine these computers at the very outset, damning evidence might very well have been preserved in an admissible format.

## Early Intervention

There are a number of logical reasons for conducting a level of forensics analysis and intervention at the outset of a case. From a case management standpoint, deploying forensics

experts can constitute a wise allocation of a litigator's most valuable commodity: time. While a litigator will be well-versed in his or her chosen specialty area (say securities), a forensics expert will possess a strong understanding of common *digital evidence issues that arise in securities litigation*. After all, every case that a computer forensic expert gets involved in will entail computer forensics. There's little question that most litigators could get up to speed on e-discovery issues. The question is, does such prep work constitute a good use of their time? Thanks to their focused experience, forensics consultants can offer some unique perspectives and strategies that the attorney may not have thought of or been exposed to.

From a case strategy standpoint, early computer forensics consultation can prove invaluable, as it might prevent you from accidentally bargaining away digital evidence that's integral to your case. In a number of cases, my firm has been called in mid-way through a litigation only to find that key evidence is beyond our grasp, unattainable because of discovery deals that had been struck between opposing counsel. Without knowing what data you're interested in, it's easy to concede certain pieces of potential evidence. Many unknown factors can come into play at a later date that can affect where pertinent information may reside. Specifically, different applications and operating environments store information in different places. It's often hard to know up front if the smoking gun we're looking for is on the server or on the individual's workstation. If one or the other is bargained away up front, your forensic expert may be limited in his/her ability to help. Through depositions the ques-



tion as to where to focus the search can often be answered, but it's important to preserve the data before these factors are known.

## The Smoking Gun

Perhaps more compelling are the technical and legal implications that recommend early computer forensics intercession. With digital evidence, there are several layers of information interest to the litigator. Of course, there's the smoking gun – the email showing sexual harassment or the spreadsheet displaying financial irregularities. The second layer of "meaning" comes in the form of metadata – information *about* the data, such as when it was created, how many times it was revised, etc. This metadata can be a wonderful tool in illustrating how a computer may have been used to perpetrate a crime or harbor evidence. What's more, metadata remains intact *even after the smoking gun file has been deleted*. However, it is extremely fragile; the metadata changes each time the computer is used.

Every time a user turns on a computer and goes into Windows, thousands of pieces of information are changed. Most of this data relates to times/dates, system resources and, to a lesser extent, deleted files. All of these affected areas contain critical information related to the activities of the user in question. Besides the potential for data to be overwritten, it is also possible for data to be compromised or tainted even if it is still retrievable. This often occurs when proper procedures are not followed while analyzing computer media. For instance, if the requestor of electronic discovery entrusts the other side with

that process, they may be unwittingly compromising data integrity. Often, the producing party will simply print electronic files to be produced or at best burn them to a C.D. Although this seems to be a good solution, any manipulation of the file in question (even printing the file without opening it or just right clicking on the file) can change attributes of the file and compromise the chain of custody and its evidentiary potency, potentially resulting in data spoliation.

Many don't realize that preservation is the most important part of any electronic discovery plan, more so than the discovery itself. A common mistake in the electronic discovery process is to fail to quarantine a machine or put the other side on notice with a well crafted preservation letter. It's far more preferable to preserve everything and process a small portion of the available universe of data than to allow portions of potentially critical information to disappear forever. Besides, it usually takes more time to figure out where your key information resides than it does to find hardware and media of potential significance. For example, your targeted computer may reside in a company that has 20 computer systems. It's not unreasonable to spend a day or two on-site creating mirror image backups of all the office computers until depositions are conducted to find out which systems/workstations your defendant accessed. The time spent up front is great insurance for potential discoveries down the road. If your litigation team is not able to access those 20 computers until a year has passed, it might be too late.

## Data Integrity

Maintaining data integrity goes hand-in-hand with maintaining the admissibility of electronic evidence. To preserve admissibility, it is critical that proper procedures be followed and that the expert in question has the proper knowledge and background to understand where the data is coming from and how it got there. If a smoking gun document is found, but there are doubts as to how the data was procured or where the data originated, the validity of the evidence can easily be compromised. This often occurs when

issues are handled internally rather than involving a 3<sup>rd</sup> party. A well meaning employee may want to 'poke around' the computer or network to see if they can find something before an expert is hired and 'wastes money'. In my opinion, the WORST thing that can happen in this scenario is that the hypothetical employee will actually find the smoking gun, as that employee becomes, de facto, the forensics expert. If the other side feels they can discredit your 'expert', they can very well discredit the evidence.

Involving a competent computer forensics consultant early on will allow you to assess which computer media is important to your case as early as possible, and can help you develop a "rapid response" plan to present to the court to ensure key information is preserved. Convincing the court to support discovery requests can be tricky. I've faced a number of occasions where opposing counsel has battled discovery requests, on the basis that digital data requested will infringe upon attorney-client privilege, divulge trade secrets and generally cause interruption to business as usual. On most of these occasions, we've been able to articulate a discovery request that assuages the court's concerns. For example, we've had success in making our case to the court that attaining a mirror image backup is the only way to ensure proper chain of custody, allow for access to all potential evidence and avoid data spoliation. Once these issues are clearly outlined and we've resolved the issue of privilege through protective orders and an have compiled an agreed list of key words with which we will search, the road to accessing pertinent computer media is generally smooth and straightforward.

Thus far, I have presented some strategic and technical reasons for deploying the expertise of forensics consultants early in the process. There's another reason that may be equally compelling.

It's easier, and in many cases, cheaper.

More often than not, digital discovery is treated in a manner based closely on the traditional paper discovery model. With paper discovery, documents are scanned (perhaps OCR'd),

converted to TIFF files which are linked to corresponding records in a database, and then searched and categorized using a litigation support program like Summation or Concordance.

## Earlier Is Cheaper

Digital documents fall into three broad categories: active files, archival/legacy data, and residual data (which includes file fragments, deleted files and metadata). Using the "paper" model, litigation teams will proceed as follows:

- ACTIVE FILES – print out and review, scan and OCR, and convert to TIFF file and commit to database
- ARCHIVAL FILES – convert to printable format, print and review, scan and OCR, and 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

The computer forensics approach departs from the "paper" model in that all data is reviewed in electronic format, using various forensic software tools. Many 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.

Let's take a concrete example, returning to the case mentioned at the outset of this story. The computers of several employees suspected of theft of trade secrets and the server used for these machines contain 20 gigabytes of data. Applying the "paper" approach, all data – approximately 7,500,000 pages – is printed and reviewed, scanned, converted to TIFF file format, and placed in a database, where it can be searched, categorized, etc. Based on a conservative estimate of five cents a page for printing/scanning/file conversion, the cost of performing this task would be \$375,000. Processing data of this magnitude would take a minimum of two weeks, and perhaps much more time.

Reviewing the 20 gigs of data using computer forensics, the process would go as follows:

- Make a mirror image bit-stream back-up of the machines in question

(so data is preserved in admissible format)

- Work with counsel to determine short list of key words for searching
- Use forensics tools to provide counsel with a preliminary report that includes a complete list of file names (including times and dates), and results of key word searches

The results of key word searches will generally serve to narrow the potential electronic discovery universe at the outset of the case, illuminating the path for further discovery efforts. Resources are not wasted processing and converting data that has little impact upon the case. Time and date information may help pinpoint telling computer activity, such as when the suspected employee downloaded a group of proprietary designs from the server to his local machine.

Cost for this forensics service will generally run from \$15,000 to \$20,000.

And if you're lucky, preliminary searches might even unveil the smoking gun.

**Scott Stevens is Director of Business Development for NTI-Breakwater Inc. (www.dataforensics.com), based in Seattle, WA. He can be reached at 503.661-6912, or via email at scott@dataforensics.com.**