The Metropolitan Corporate Counsel®

The Quest To Uncover All The Facts: The Role Of Computer Forensics In Electronic Discovery

Jerry F. Barbanel and Bruce W. Pixley
Aon Consulting

Jerry F. Barbanel is the Executive Vice President in charge of IT Risk and Litigation Consulting for the Financial Advisory and Litigation Consulting Services practice at Aon Consulting. Mr. Barbanel can be reached at (201) 966-3494 or jerry_barbanel@aon.com. Bruce W. Pixley is a Senior Director in charge of the West Coast Computer Forensics group at Aon Consulting. Mr. Pixley can be reached at (805) 298-0031 or bruce_pixley@aon.com.

In today's corporate environment, the vast majority of business documents and communications are stored electronically. Given the relative ease of purging or overwriting electronic data, companies involved in litigation now need to go beyond traditional electronic discovery methods to uncover a case's "smoking gun."

When confronted with a litigation matter that requires electronic discovery, regardless of how complex it may be, the knowledge and skills of seasoned computer forensic or high-tech investigation experts can be invaluable. To be effective, these experts must have a thorough understanding of the forensic techniques utilized in electronic discovery matters.

Computer forensic specialists are typically retained by counsel to preserve, collect and maintain the integrity of the chain of evidence. Depending on the type of evidence that is being collected, there are a number of options available to forensically collect data so that it can, if needed, be produced and admitted into evidence during a legal proceeding.

Before starting the collection process, the computer forensic expert and counsel need to determine the most effective manner to collect needed information. Computer forensic experts are able to collect data from three tiers of information on a custodian's computer. The first tier, which contains the largest amount of data, is a mirror image of the custodian's hard drive. The second tier consists of all active files on the hard drive; while the third tier is limited to user-created files on the hard drive.

One of the most common collection methods used by computer forensic experts is to make a mirror image of the custodian's hard drive. This technique provides a replica of every sector on a hard drive and allows all data, including previously deleted data, to be recovered and reviewed. In instances when the custodian is a current employee, the forensic expert must shut down the individual's computer and then use forensic software to make the mirror image.

Another option for collecting electronic information is to leave the custodian's computer running and use forensic software to copy the hard drive data to either an external drive or a networked storage drive. One potential area of concern for counsel using this method is that unallocated space on the custodian's hard drive, the unused area of a hard drive where deleted files reside, might not be collected.

In situations where the computer forensic expert is requested to make a forensic collection of only active files from a custodian's hard drive, both of the above-referenced methodologies will produce the correct results. Active files are those files that can be readily accessed by the computer's operating system, such as program files, operating system files and user- created files.

However, if counsel requests the complete preservation of both active and deleted files, then it is important that unallocated space is captured during the collection process. As such, the preferred method of collection will involve making a complete mirror image of the custodian's hard drive. In the event that counsel requests only those active files that are user-created, then the forensic specialist will access the custodian's computer using forensic software and with applicable filters can collect only those files that match the specified criteria.

If counsel requests to limit the collection to user-created files, the smallest subset of the three tiers of information that can be collected, then there are potential risks that one needs to be aware of. When using

this technique it might be impossible to go back and collect data that has been deleted from the custodian's hard drive. Often times a company is compelled to preserve, by a court order, certain information that is contained on a custodian's computer. In order to avoid spoliation claims and potential sanctions, any strategic plan needs to clearly define the collection methodology to avoid potential pitfalls.

It is a common misconception that all corporate e-mail and electronic documents are automatically backed up to an archive as long as the computer is connected to the company's network. In reality, the archives may or may not exist depending on the company's policies. Unless a company makes a concerted effort to back-up the servers and employees' computers on a regular basis, the electronic documents contained on a custodian's computer may never be archived. Additionally, e-mails are only backed-up according to a company's archiving policies; therefore if e-mails are deleted by the custodian prior to being archived, they may not be recoverable. This holds true even when forensic software is used in an attempt to recover deleted e-mails, as they could have been overwritten.

For example, a forensic expert is instructed to only collect user-created files, however it is not specified that presentations should be collected. Then months later, counsel, after reviewing electronic documents such as spreadsheets, word processing documents and e-mails, inquires about the lack of presentations. At that time it is then realized that presentations were not collected, pursuant to counsel's original list. Due to the limited scope of the original request the data may no longer exist if the user deleted the presentations and the presentations were overwritten by other data through normal computer usage.

To avoid potential spoliation risks related to missing presentations or other data, counsel could have chosen to collect the second tier of information - all active files on the hard drive. Although the collection of all active files may be unnecessary, it ensures a safety net for preserving data. This second tier, however, does not address deleted files.

Counsel may opt to collect the first tier of information, a mirror image of the entire hard drive, to ensure that the most fail-safe method of preservation is performed. If during a deposition a custodian reveals that they deleted relevant documents prior to the date that the forensic collection process was conducted, it is possible that the forensic specialist can recover those deleted files for production. This can help counsel avoid a spoliation claim being proven against their client. However, possessing the full image of the hard drive could potentially open the door for the opposing party to gain access to data that was not contemplated as part of the original preservation order.

By having a full understanding and appreciation of the potential perils that can occur during the discovery phase and engaging a seasoned computer forensics expert to assist throughout the process, companies can obtain information that they would otherwise not know existed, while remaining within the confines of their electronic discovery budget.

Please email the authors at jerry_barbanel@aon.com or bruce_pixley@aon.com with questions about this article.