

## Gaining Access to Forensic Computer Images

by Gregory Fordham

Although parties to litigation have a duty to preserve data, they may not be required to produce the data that has been preserved. Whether data is producible still turns on its relevance to the case as well as other factors.

One of the most common means used by litigants for preserving electronic data is the forensic imaging of computer hard drives as well as other media like diskettes, thumbdrives, flash cards, cell phones, etc.

The process of forensic imaging captures the relevant evidence for the case as well as many other items that may have no relationship to the case. In fact, imaging can be analogized to preserving an entire filing cabinet as well as the trash can.

Despite its breadth, imaging is used for preservation because it can be more economical than sifting through documents at the start of a case without firm knowledge of what will or will not be relevant to the matter. Also by imaging, like preserving the entire filing cabinet, other attributes about the data it contains can be preserved such as the timing of the preservation, the last access to the evidence and even the absence of previously existing evidence.

Despite the breadth of data captured by forensic imaging, courts have allowed production and discovery of entire computer hard drives under protocols like those described in *Cenveo Corp. v. Slater*, Slip Copy, 2007 WL 527720 (E.D.Pa.) and its predecessors.

Even so, production and discovery of imaged hard drives is not an inherent right of the requesting party even if the data is easily accessible. (See, *Peskoff v. Faber*, 2007 WL 2416119 (D.D.C.))

Furthermore, one court has denied production of the entire hard drive in order to protect privacy and confidentiality of the producing party unless there has been a showing by the requesting party of:

- discovery “discrepancies and inconsistencies”; or
- a nexus between the computer hard drive and the act initiating the lawsuit; or that
- the producing party was not capable or willing to produce the requested information.

(See, *Calyon v. Mizuho Securities USA, Inc.*, Slip Copy, 2007 WL 1468889 (S.D.N.Y.))

With decisions like *Peskoff* and *Calyon*, litigators are likely to encounter greater resistance to production of entire computer hard drives. As a result, requesting parties will need to show relevancy as required in *Peskoff* and better justify their requests with the three criteria discussed in *Calyon*.

Although *Calyon*'s first two criteria should be easily understood by both requesters and courts, the third is more involved. In making their arguments, requesters may want to consider three facets to their argument.

First, the court may envision the forensic analysis that will be performed on the hard drive image as simply a series of simple word searches. The reality is that the analysis will likely also include various examinations of file system and system usage metadata in order to authenticate and validate the word search results. So, it will be incumbent on the litigator to properly orient the court's conceptual model of the examination so that it can understand the need for a particular type of examination and examiner.

Second, while simple word searching is a skill commonly held by many, the examination of file system and system usage metadata involves both skills and tools that are not as commonly available. So, the litigator will need to adequately differentiate the producing party's resources and skills from the requesting party's resources and skills.

Third, other than metadata analysis there are still other processes like signature analysis, hash analysis, data carving, malware analysis as well as other techniques designed to detect and defeat data hiding techniques or efficiently locate the relevant needle in the haystack. These processes can also be used to differentiate the parties' experts and justify production of computer hard drives.

If the requester's arguments are still unpersuasive there are still other steps that requesters can undertake. For example, the file system and much system usage metadata are contained in discrete files on the hard drive. These files (such as the Master File Table, the Registry, Event logs, and application logs to mention a few) could be requested separately for examination.

Also, the requester could develop a protocol where its expert is able to monitor or validate the analysis performed by the producing party's expert.

In the end, there may be no substitute for production of the entire hard drive. In those cases, the requester will simply need to be persistent and use every opportunity to incrementally convince the court of the merits of its requests and gain access to the evidence so crucial to its case.

§§§

*Gregory Fordham has written extensively on this subject. His papers are available for download from the K&F website [www.knfcon.com](http://www.knfcon.com). He regularly advises clients on how to structure their e-discovery plans in order to minimize cost and maximize return. The Georgia Bar has approved his e-discovery presentation for CLE credit. He has been an expert witness in state and federal cases involving e-discovery and computer forensics. His e-mail is [greg@knfcon.com](mailto:greg@knfcon.com)*

