Imaging Hard Drives – Will you get what you expect?

August 19th, 2008

If you or a partnering service bureau need to be able to process or review your client's files from an imaged hard drive, you may be in for a surprise. The results of an imaged hard drive are often stored in a forensic image format or what is referred to as an "evidence file" container. Common evidence file formats include Encase, DD (RAW), SMART, AFF and Safeback, just to name a few.

These forensic image formats are designed to allow access to the files from computer forensic software. Most electronic discovery and litigation support applications are unable to access the file contents of an imaged drive that is stored as a forensic image. If you need to access the copied files, you have three options.

1. Request a "clone" of the source hard drive rather than a forensic image. A clone is created by copying source media to another drive in the same format.
2. Ask that the forensic image be restored to a clone.
3. Purchase "Mount Image Pro" (http://www.mountimage.com/), which will allow you to view the contents of several popular forensic image formats.

It is important to talk to the company or individual performing the collection to ensure that the collected files can be accessed by those performing the electronic discovery processing and review.