Title:
Computer Forensics vs. Electronic Discovery

Word Count:
436

Summary:
The field of computer forensics was developed primarily by law enforcement personnel for investigating drug and financial crimes. While Electronic discovery has its roots in the field of civil litigation support and deals with organizing electronic files using their attached metadata.

Keywords:
computer forensics, electronic discovery, litigation support, document imaging, document scanning, form processing

Article Body:
Computer Forensics

The field of computer forensics was developed primarily by law enforcement personnel for investigating drug and financial crimes. It employs strict protocols to gather information contained on a wide variety of electronic devices, using forensic procedures to locate deleted files and hidden information.

Computer forensics tasks include capturing all the information contained on a specific electronic device by using either a forensic copy technique or by making an image of all or a portion of the device. A forensic copy provides an exact duplicate of the hard drive or storage device. None of the metadata, including the าlast accessed date,ำis changed from the original. However, the copy is a าliveำversion, so accessing the data on the copy,even only to าsee what is there,ำcan change this sensitive metadata.

By contrast, making a forensic image of the required information puts a protective electronic wrapper around the entire collection. The collection can be viewed with special software, and the documents can be opened, extracted from the collection, and examined without changing the files or their metadata.

Other forensic tasks include locating and accessing deleted files, finding partial files, tracking Internet history, cracking passwords, and detecting

information located in the slack or unallocated space. Slack space is the area at the end of a specific cluster on a hard drive that contains no data; unallocated space contains the remnants of files that have been าdeletedำ but not erased from the device, as าdeletingำ simply removes the pointer to the location of a specific file on a hard drive, not the file itself.

Electronic Discovery

Electronic discovery has its roots in the field of civil litigation support and deals with organizing electronic files using their attached metadata. Because of the large volume encountered, these files are usually incorporated into a litigation retrieval system to allow review and production in an easy methodology. Legal data management principles are used, including redaction rules and production methodologies.

Electronic discovery tasks usually begin after the files are captured. File metadata is used to organize and cull the collections. Documents can be examined in their native file format or converted to TIF or PDF images to allow for redaction and easy production.

Common Capabilities, Different Philosophies

Computer forensics and electronic discovery methodologies share some common capabilities. One is the ability to produce an inventory of the collection, allowing reviewers to quickly see what is present. Another is the ability to determine a common time zone to standardize date and time stamps across a collection. Without this standardization, an e-mail response may appear to have been created before the original e-mail.