How to Successfully Obtain Computer-Based Discovery in 10 Steps

Identifying pertinent evidence on computer systems is essential to the discovery process in today's world, as it is believed that over 70% of information stored in computer systems is never reproduced in hard copy form. Often, a significant amount of data, such as date and time information, can only be viewed electronically, causing the discovery of computer-related evidence to become even more critical.

Simply asking for electronic evidence will not necessarily result in all relevant information being supplied. Therefore, it is important to understand the proper collection processes involved with ensuring that electronic evidence will be authenticated and admissible in a court of law. The following ten steps are meant to provide clarity with respect to the collection of electronic evidence:

Step 1: Send a letter to all involved parties notifying them that electronic evidence will be sought.

Essential to the discovery process, such a letter will seek to ensure that electronic information will be preserved. In addition, a protective order may be sought at this time that compels all parties to safeguard electronic information that may be relevant to the case.

Step 2: Specifications regarding electronic information must be included in the written discovery request.

Definitions of the precise documents requested, instructions, and specific questions must be included in this request, as well as the form of production requested, whether only electronically or in hard copy form. In addition, at this time a request for experts to physically examine and analyze the computer hard drive(s) in question should be admitted and interrogatories may be sent in an attempt to gain an overview of the target computer system(s).

Step 3: IT staff should be deposed via 30(b)(6).

Throughout the course of these depositions, if asked, employees will be required to provide information regarding the manner in which electronic evidence is stored, the types of hardware and software utilized, and how the organization backs up electronic information.

Step 4: Gather backup tapes

Backup tapes contain information that would help the organization recover from a disaster. Backup tapes are generally made on a routine basis and often contain information that is no longer readily available on a computer system's hard drive.

Step 5: Gather removable media, such as CD-ROMs and zip drives

Such as the case with backup tapes, removable media often contains information that is not available on a computer system's hard drive. In addition, such removable media may contain ad hoc backups of files and email messages.

Step 6: Question all available witnesses about their specific computer usage

All witnesses can be asked how they specifically store data on their computer systems. In addition, witnesses should be questioned with regards to their home computer systems as it is possible that they have removed information from their work systems and transferred them to their home systems.

Step 7: Make a mirror image copy of the hard drive(s) in question

A mirror image is an exact duplication of a computer hard drive that is completed sector by sector to secure residual data, such as deleted files, partial deleted files, and other information that still exists on the disk.

Step 8: Uphold the integrity of the data by write protecting all media and checking for viruses

Write protecting the media keeps the data from being distorted or obliterated. In addition, all media should be checked for viruses to ensure evidence is not tainted. If a virus is found, a record should be made and the opposing party must be notified.

Step 9: Ensure the proper chain of custody is followed

A proper chain of custody ensures that the data presented is "as originally acquired" and has not been altered prior to admission into evidence. An electronic chain of custody link should be maintained between all electronic data and its original physical media throughout the production process.

Step 10: Understand your limitations

Due to the intricacy of the computer forensic process and the complexity involved with electronic discovery, outside expertise is often warranted to maximize the discovery of electronic evidence and ensure its admissibility in a court of law.