JOURNAL OF ACCOUNTANCY
A Publication of the American Institute of Certified Public Accountants • SEPTEMBER 2006

DISCOVERY

Retrieving Electronic Documents

Electronic evidence often can provide vital information about the activities, motives and intent of individuals and businesses. Electronic documents thought to be deleted or lost by the user often can be recovered. In the case of electronic mail, casual and candid correspondence may be frozen in time. Additionally, the background information available with electronic data can provide the footprint necessary to develop the facts of an internal investigation.

Electronic discovery is challenging because relevant information may exist in a variety of locations and forms. Locating, searching and managing electronic evidence requires an understanding of technology beyond that of most experienced computer users. So calling in a computer forensic specialist is recommended. The specialist will have the expertise to properly handle and preserve evidence so that it is admissible in a court of law.

Hired computer forensic specialists can handle many aspects of electronic discovery, including

- Identification of likely sources of relevant information.
- Collection of data, taking care to avoid spoliation.
- Restoration of data to a readable and usable format.
- Examination of data (including concealed or destroyed data).
- Data analysis to determine the extent of fraudulent misconduct.
- Expert testimony.

Relevant data may exist in many forms, including the following.

Active data. Viewed through file management programs, active data are readily available and accessible.

Hidden files. Suspects may hide data to thwart an internal investigation. Typically, they rename files to appear as a part of the operating system (with file extensions such as ".com" or ".sys"). While on the surface these may appear to be legitimate files, the trained computer forensic specialist will examine an element of the file known as the file header which will show the true identity of the file.

Automatically stored data. Automatic backup features commonly create and save copies of the file being worked on in order to help users recover data lost due to a computer malfunction. Documents may exist on the user's hard drive.

Deleted files. "Deleted" does not mean destroyed. The process of deleting a file merely indicates to the computer that the physical space belonging to the deleted file is available. All or part of the deleted file may be recoverable.

Backup data. Network backups that capture data saved on the network server (typically excluding user drives) can provide valuable information, though restoring and locating relevant data can be expensive and time-consuming.

Locating relevant data. Data may be available on user drives, laptops, removable devices—such as thumb drives—compact discs and digital cameras, network computers, home computers and handheld devices

CPAs should advise clients to make every effort to safeguard computers and removable devices and complete forensic examinations as soon as possible. Complicit employees may attempt to cover their tracks by deleting incriminating evidence and can wreak havoc on information systems in a matter of seconds.

—***Kelly J. Todd,*** *CPA/ABV, CVA, director of forensic services, Summerford Accountancy PC, Birmingham, Ala.*