

Unlocking E-Evidence. Know How to Discover Computerized Information

By Paul French

Lawyers seeking electronic evidence through the discovery process cannot do so in the traditional way, which typically involves blanket requests for documents relating to a topic or issue. The volume of electronic information, along with the propensity for electronic data to replicate itself in multiple locations, makes generalized requests both impractical and ineffective. Lawyers must know exactly what information devices to target, or they risk missing large volumes of critically relevant information.

Lawyers, therefore, should approach this type of discovery by trying to understand the defendant company computers' layout, information flow and the way in which information is stored, in order to successfully retrieve the information that is being sought.

With the widespread use of computers, electronic evidence is everywhere. Not only are key documents stored on computers and servers, so are activity logs, deleted files and e-mail. Understanding electronic evidence, where it is stored and how to go about retrieving it, is imperative.

E-mails, for instance, can reside on personal computers as well as servers. How you go about retrieving this information may vary depending on the type of software used to store it and what type of storage media is used.

Also, depending on a company's backup policy, historical data can be retrieved from backup tapes. Backup tapes can provide a wealth of information but also can be very proprietary in nature and difficult to work with. In order to pull information off of backup tapes it is often necessary to duplicate the exact

operating environment in which the backup tapes were created. Once the data is removed, it often needs to be converted into a readable format.

With all these variables, it's important to get as much information as early in the discovery process as possible. Asking the right questions can help your litigation team gain access to the critical e-discovery that may very well make your case or give you access to the individuals in the organization who can point you to the crucial information.

The following is a road map of possible deposition questions that will leave few stones unturned in your quest for the electronic smoking gun.

"Can you describe in detail the data processing and data storage devices used by your company in the course of business?"

This question will help determine the quantity and accessibility of available data and will give computer forensic experts the information they'll need to duplicate original hardware configurations.

This question should elicit important information regarding the company's hardware including e-mail, file, fax and voice mail servers; operating systems; workstation hardware; personal digital assistants such as Palm Pilots; backup apparatus; electronic and optical storage devices; and office machines.

"Describe your network architecture and usage policies."

This will ascertain what users are allowed to do on the network, such as file sharing, file storage, running centralized applications activities, how many users are on the network and how user data is segmented and protected on the network.

Network configuration information is ultimately the road map you will use to pinpoint those electronic storage devices most likely to contain relevant data.

"Please identify the types of software used on your computer system or systems."

This question will provide you with information on their software applications, including industry-specific programs, word processing, spreadsheets, e-mail, calendaring, accounting, remote connection and any "chat" applications. This will enable you to determine the types of discoverable information to target. Additionally, your computer experts may need information regarding applications to explain processes that act upon data. For example, one backup utility might alter file dates while another does not, or one word processing program may track user changes while another ignores them.

"Who is responsible for the operation, maintenance, expansion, backup and upkeep of the computer systems, and how frequently do these activities occur?"

Although it is important to identify the individuals setting corporate policies and procedures related to information management, it is just as imperative to identify the people doing the hands-on work. You often will find discrepancies between a company's policies and its day-to-day practices. Talking to the folks on the front line will give you the best picture of what is and is not being done to the data you are seeking.

"What steps have you taken to ensure that electronic data is preserved?"

By determining how data was preserved, you will have a better sense of how to go after it. Ask the

deponent if mirror-image backups of relevant hard drives were created and if archived data was removed from the rotation cycle and securely preserved. Also, determine if broken or upgraded computer components were saved.

“What computer systems in the organization are backed up and how?”

You will want to gather information for each system, including backup software programs that are used, contents and frequency of backup, type of backup media used, location of backup media and any indexing procedures for backup tapes. Be sure to ask whether backup procedures have been at all modified to comply with discovery requests.

By gathering information on backup procedures, you will be able to effectively identify and address spoliation issues. This information also will help computer forensic experts in their data recovery and analysis efforts.

“Are files ever deleted from the computer system or systems?”

If the answer is yes, try to determine the file purge schedule and the methods used for file deletion. Also determine whether e-mail or user server accounts are closed or purged when an employee leaves. This will assist computer experts in reconstructing any lost information.

“What sort of maintenance is done on the organization’s computers?”

This question will help you identify processes and procedures that could contribute to spoliation of evidence. Be sure to ask whether utility programs have been used, and if so, have any of these programs been used to “wipe files.” Also, find out if any hardware or software has been upgraded. If hard drives were replaced, the old hard drives might still contain valuable data. Likewise, if software was upgraded, inquire whether the data was backed up and the location of the backup.

“What database management systems are used, and how are they used?”

Some information pertinent to

your case will reside in large, complex databases. Many database formats are proprietary and not easily recovered if damaged or altered. Understanding the deponent’s database management system will help you retrieve this information in an efficient and thorough manner.

Also, try to have the person identify the types of databases in use, such as customer relationship management or accounting databases; the database software used, such as Oracle or D:BASE; database architecture; the names of all data fields and the types of information they contain; and the names of the individuals responsible for designing, maintaining and operating the database. You also will want to learn how the database is accessed and the kind of reports that are routinely prepared.

“What are your organization’s e-mail protocols?”

In light of the Microsoft antitrust trial and more recently the Merrill Lynch debacle, everyone understands the significance of e-mail as a repository for telling evidence. You, therefore, will want to get as many details as possible from the deponent to gain access to archived e-mail.

Be sure to identify the personnel responsible for administering the electronic mail system and determine what e-mail programs are in use. Find out whether messages are stored in a central location or a desktop; e-mail is transferred via “point of presence” format or simple mail transfer protocol; e-mail can be accessed remotely; passwords are regularly changed or remain stagnant; or janitorial programs are used to periodically purge e-mail. Also inquire whether there are any special e-mail retention settings active, such as the “deleted items retention” setting in Microsoft Exchange.

Paul French is a computer forensics project manager with New Technologies Inc., a Gresham, Ore.-based company that provides tool development for computer forensics tool development, computer evidence consulting and

computer forensics training for firms. He can be reached at paul@forensics-intl.com.