

Seeking the Treasure Trove of Data

Electronic evidence must be preserved before the investigation even begins.

BY KENNETH A. MENDELSON AND DON ALLISON

It does not take a computer scientist or a legal scholar to realize that information at the heart of most internal corporate investigations, civil litigation, and criminal investigations is created on a computer and stored on hard drives, removable media, and in electronic files. In the hands of a specialist, digital data can provide a treasure trove of case-making (or -breaking) evidence.

Consider what happened when Martha Stewart ordered her secretary to change her electronic calendar and then change it back to the original: All versions could be recovered. We've all read about the cases of theft of proprietary corporate data, e-mail harassment or extortion, peer-to-peer file sharing abuses, Internet child-pornography trafficking, and disputes over which version of an e-mailed contract is the "original."

These cases have two things in common: the need to extract data from some form of digital storage media, and the need to ensure that the data can be authenticated to ensure its admissibility in court. Whether you are trying to prove an employee forged the e-mail giving him a large bonus, or attempting to track down the source of extortion messages anonymously being sent to your client, you might find yourself considering the need to hire a computer forensic examiner.

When properly examined by a professional computer forensic examiner, a hard drive, for example, can be a source of information the computer's user did not even know existed. Computer hard drives retain many types of information the user cannot see—deleted files and e-mails, fragments of files, Internet use history, and even Web pages that the user simply viewed, but never saved—as long as the data is not overwritten by new data. If the data has been written over, even the most experienced computer forensic examiner will probably not be able to get it back.

Nevertheless, even when the data has been overwritten, expert examiners are often able to recover evidence that the information used to be there. Whether the computer forensic examiner can extract this wealth of information depends on many factors.

Perhaps the most important factor is what happens to the computer before the examiner arrives.

Once you have determined that information on a computer is relevant to an investigation or would be useful to a lawsuit, and concluded that you need a qualified computer forensic examiner to analyze the information and ensure its admissibility, what should you do first?

Ensuring that critical electronic evidence is not destroyed, modified, or otherwise rendered inadmissible by well-meaning systems administrators or others requires a minimal amount of training. The goal is simple: to ensure that the information is not compromised before the forensic analysis happens.

The name of the game here is "preservation." Before anything else, it is vital to preserve the data to overcome any potential assertion that the information was altered after it was last accessed by the suspected wrongdoer. This preservation is best done by a computer forensic professional, and not the organization's system administrator or IT staff. Once it's preserved, the examiner can then locate the relevant information and prepare it for presentation in court or other proceedings. What needs to be done as a first step is to ensure that the data is not compromised even before this preservation can occur.

In most cases, each time a computer is powered up, or a file accessed, information is written to the computer's hard drive, potentially overwriting important evidence or changing dates that may become significant as an investigation or litigation unfolds. Accordingly, if there is even a remote possibility that the information on a computer system or peripheral would be useful, the organization should ensure that the data is ready to be preserved in a manner that will ensure its value as evidence.

Here are 10 steps to take when you determine that information possibly relevant to an investigation or litigation may be on a specific computer system. While the natural inclination of most forensic examiners would be to say "just don't touch it," these practical suggestions will facilitate the forensic preservation and examination, improve the likelihood that relevant data will be

found, expedite the examination process, and may even reduce overall costs.

10 RULES OF THUMB

1. If the computer is off, leave it off. If the computer is on, leave it on.

2. If a computer process is running (for instance, if the user is escorted from his desk while the computer is in use), consult with a forensics professional before shutting down and securing the machine, to ensure that the relevant data is not inadvertently overwritten by the shutdown process. If no one is available for advice, the accepted practice is to pull the plug of a Microsoft Windows-based system (to prevent data from being overwritten during shutdown), but powering down the computer of a non-Windows system (e.g. Macintosh or Linux systems), which operate differently.

3. Secure the computer to prevent unauthorized access, as well as other digital storage devices that may hold relevant data, including BlackBerrys or other mobile communications devices and removable media (such as CDs, DVDs, or MP3 players) that the suspect might have used.

4. Do not run any programs or otherwise attempt to access any data on the computer (for example, running the Windows “search” tool can destroy evidence in the swap file).

5. Do not allow the user to help open or turn on the computer. The examiner will be able to do this without assistance and with appropriate tools to prevent data overwriting or damage from static electricity. The best help a user can give is to provide passwords to access encrypted or password-protected files.

6. Once the machine is secured, the system administrator or other qualified person should obtain information about the machine, peripherals, and the network to which it is connected that may be subject to examination, including:

a. the make/model/serial number of all equipment and materials to be examined;

b. a description of the e-mail, instant messaging, or other communications systems used, with details about the network configuration for storage of e-mails and files on servers and workstations, and identification of all e-mail and file servers potentially used by the subject;

c. a list of other applications generally used by the organization (such as Microsoft Office or Corel);

d. a description of the job function of the user. Why? A person with a technical job or someone who is considered “techni-

cally saavy” may try to “cover his tracks.” Often, these steps are detectable.

7. If the computer was accessed before the forensic preservation, note:

a. what was done to the computer(s) already;

b. who tried to access what kinds of files;

c. when this was done;

d. what was found; and

e. why the computer was accessed.

8. Begin a “chain of custody” document for each piece of original evidence (physical and electronic) that identifies each individual and organization handling the evidence. If the evidence is shipped, the tracking numbers should be recorded.

9. Start defining the tasks for the examiner by describing the type of relevant data that may be found on the computer (for example, e-mail, proprietary data, a “smoking gun”) and the potential uses of the data (for instance, injunction, settlement, specific performance, jury award). The more context the examiner has at the outset, the more effective the examination will be. In addition, the urgency level (and the level of detail of the analysis) will vary according to how much time the examiner has to finish. Compile the names, e-mail addresses, or other identifying information about those with whom the subject might have communicated.

10. Prepare a list of specific terms or words (key words) that may be used to search for relevant data on the computer.

This is not an exhaustive list of the topics that should be addressed or the steps that would work in every situation, but it does provide some general ideas about what would be useful at the outset of a digital forensic investigation. The more information provided at the start, the more likely the examination will yield the right information. In addition, the examiner will be able to give a more accurate assessment of the work to be done and its estimated cost.

Like anything else, the more information sought and the more iterative the process, the more time it takes, and the more it will cost. The earlier in the process the forensic examiner is brought into it, the greater the likelihood of success.

Kenneth A. Mendelson is vice president, deputy general counsel, of the D.C. office of Stroz Friedberg, LLC, a consulting and technical services firm specializing in digital forensics, electronic discovery, and investigations. Don Allison is a senior forensics examiner there.