

ARTICLES

The Boundaries of Computer Forensics

By John Mallery and Joan K. Archer, J.D., Ph.D.

It has been several years since the Federal Rules of Civil Procedure were modified to address electronically stored information (ESI) as part of the discovery process. Although not always viewed as pleasant, most lawyers have accepted that e-discovery is a necessary part of their practice.

One part of the e-discovery process—computer forensics investigation performed by experts—is not routinely used. Nevertheless, computer forensics can be a valuable tool in identifying relevant and responsive electronic data that may not be located using standard methodologies. One reason attorneys may be hesitant to use computer forensics is because they lack a true understanding of what can and cannot be done by a forensics expert. Moreover, the experts themselves may further confuse matters by providing varying information concerning the scope and limitations of the services they can provide. The only real common denominator is the price—they all seem quite expensive. Not surprisingly, it would be difficult to recommend that a client spend money on computer forensics when counsel cannot readily explain with clarity what the process will likely accomplish.

This article provides practical information concerning the scope and limitations of computer forensics. Key areas of forensic analysis and terminology are discussed, including explanations concerning the types of information that may be gathered through a forensic investigation. The topics discussed below are not intended to be exhaustive; rather, they provide a basic framework that attorneys can use as they work with experts and clients regarding what can and cannot be done through computer forensics.

What Can Be Done

Initially, when forensic preservation is deemed necessary, e.g., where complete preservation must be assured; in high stakes matters; when fraud or other misdeeds are under investigation; or when custodian "bad acts" may come into play, it is prudent to retain a knowledgeable and trustworthy forensics expert to preserve computer forensic evidence. A forensic copy of a hard drive (also called mirror image copy, exact copy, or bit-for-bit copy) should be made as soon as possible to preserve data at a particular point in time. This forensic copy can be held by an agreed-upon party while a search protocol is developed. The benefit is that the forensic copy "sets in stone" the data on the hard drive, with no chance of data destruction while the legal process moves forward. Another benefit is that if the forensic copy is stored in an EnCase evidence file (or other comparable format), the data is read-only, meaning the drive image can be searched many times without risk of modifying data. It is important to perform an investigation

that does not modify the data. If the evidence is altered through the investigation process, it may not be admissible.

The types of information that can be recovered during a computer forensics examination include active files such as word-processing documents, spreadsheets, presentations, email, memos, bank statements, contracts, financial statements, accounting databases, real estate materials, incorporation documents, receipts, and checks. Additional information that can be recovered includes Internet history, i.e., websites the person visited as well as web-based email, including hotmail, Gmail and Yahoo! Mail. Deleted files and fragments can often be recovered, including images, email, pdf files, Office documents, and the like. Despite the fact that some vendors may tell you they can get “everything” from a hard drive, there are some things that can make the process more challenging, even to the point of no longer being cost effective.

Computer forensics experts can identify many types of data or information through the examination of digital devices such as computer hard drives, USB devices, cell phones, and other handheld devices. The following are activities a computer forensics expert can perform.

Identify Spoliation or Data Destruction

This is one of the most commonly requested procedures during a forensic analysis of a computer hard drive. The following areas that store electronic data items may be examined to identify this type of activity (on a Microsoft Windows system):

- The Program Files folder
This is the first place to look, as many data destruction tools are installed in this location. CCleaner, one of the most commonly encountered tools, can be found here. This is a common first step when investigating whether a custodian employed a wiping tool to delete documents or destroy data.
- The Prefetch folder
This folder is located in the C:\Windows directory, and it contains files with a .pf extension. These files are created when applications are run on the system, theoretically to help an application open faster during subsequent uses of the application. The use of data destruction tools also can be recorded in this folder.
- The UserAssist key
Microsoft Windows uses a hierarchical database called the registry. One of the registry files called NTUSER.DAT can track application usage. The UserAssist key is an entry in this file.
- Unallocated clusters filled with zeroes, gibberish, or a specific character
Unallocated clusters is the area of the hard drive that can be thought of as “free space”; this is where deleted files or file fragments may be found. If a computer has been used for an extended period of time, this area of the drive should contain portions of files, some of

which will likely contain “human readable” text. If no files or file fragments can be found, it might be an indication that data destruction tools have been used.

- Operating system install date after the initiation of litigation
One mechanism used to attempt to cover one’s tracks is to reinstall the operating system.
- Hard drive manufacture date after initiation of litigation
Another mechanism used to cover one’s tracks is to install a new hard drive into the computer.
- Internet searches for data destruction tools

Identify Internet Activity

Internet browsers such as Internet Explorer and Mozilla Firefox record websites visited and searches performed on search engines like Google. Browsers track daily, weekly, and monthly activity, so Internet activity can be recorded in more than one location. Tools like NetAnalysis from Digital Detective can recover deleted history files for analysis.

Recover Chat Sessions

People can use the chat capabilities of social networking sites to bypass the monitoring of corporate communications systems. Chat sessions may be recorded on the local computer, not just the server hosting the session. This can be an invaluable source of information for multinational companies that use chat capabilities as a cost-saving mechanism.

Recover Web-Based Email

Web-based email messages are actually webpages and are cached on a hard drive just like any other webpage. As such, some web-based email messages often are recoverable, though such messages may be fragmented.

Identify Date and Author of Documents

Although date and time stamps on computers can be incredibly complex and convoluted, it often is possible to recover metadata from Microsoft Office documents showing the names of the last 10 authors (in older versions of Office), date and time the file was created, the date the document was last printed, and the company name of the organization to which the software is licensed.

Identify Make, Model, and Serial Number of USB Device

This information is captured in the Windows Registry. USB devices are often used to copy material. There are, however, some limitations, which are listed below.

Thus, there are many potentially fruitful types of information that may be retrieved if a forensic analysis of electronic data is used during discovery. This list is not exhaustive, but is just a sample of the areas of inquiry that may be useful in many cases. Now we will discuss some of the common misconceptions about computer forensics.



What Can't Be Done

There are a number of misconceptions regarding what types of activity can be identified and recovered during a forensic investigation. What follows is a list of items that are often requested, but are not typically possible to identify.

Identify Files Copied or Moved to a USB Device

Unfortunately, Microsoft Windows does not track this type of information. It is often possible, however, to identify files stored on a USB device by looking at "link files." Link files are files with the file extension of .lnk; they are essentially shortcut files pointing to the full path of the storage location of a particular file. A .lnk file can point to a file stored on a removable drive, potentially showing a file that was moved or copied to a device.

Identify Users at a Specific Date and Time

Even though data can often be matched to a specific user profile, it is not possible to say with certainty who performed a particular action on a computer. In certain situations, it is possible to identify who was in a particular work space by examining closed circuit television footage or log files from other security tools.

Identify Attributes of Data in Unallocated Clusters

Because data in unallocated clusters is not intended to be seen or accessed by computer users, the data is unstructured. There are file fragments, complete files, and system data deleted during computer use. Therefore, it often is not possible to determine when data in this area was deleted or when activities identified in this area were performed. It also may not be possible to comply with a court order limiting the recovery of Internet searches to a specific date range. Internet search activity can be recovered, but it cannot generally be tied to a specific date.

Determine the Creation Date of a Document Using Metadata

Date and time stamps are generated by the system clock, which is actually stored on the motherboard of the computer, not on the hard drive. It is a trivial matter to change the date and time on a computer. Because of this, it is important to verify the accuracy of the system clock when collecting documents that are to be used in litigation. In addition to being easy to change, system clocks can gain or lose time just like a clock in your house.

Conduct a Full Forensic Analysis in a Short Period of Time

A computer hard drive can contain 65,000 files or more. Unallocated clusters can contain gigabytes worth of information. A computer forensics examination can take 15 hours or more, depending on the scope and the analysis requested.

Attorneys should arm themselves with this information when retaining forensics experts. If an expert suggests that these types of information can be found, a second expert opinion is advisable.

Other Issues

There are a few other issues that should also be considered as part of an attorney's education in computer forensics. One challenge that can present itself is "whole disk encryption." This means that the entire hard disk is encrypted, and the contents cannot be accessed without having the appropriate password or key. In an enterprise environment, this can be overcome, as the IT department will likely have a "master key" that can provide access to the encrypted drive. But if an individual has his or her personal computer encrypted using whole disk encryption, it might not be possible to gain access to the drive, although a court order requiring the password could be helpful. You may more commonly encounter encrypted files. Although there are tools that can help crack the password for many of these files, if the password is complex, it could take days or even weeks for the password to be cracked.

Damaged hard drives may require the skills of a data recovery company before the forensic analysis is conducted. A seriously damaged drive may be in a condition where some or all of the data is no longer recoverable. A forensics expert cannot work miracles, after all.

Another challenge is when the subject under investigation is bilingual or multilingual. Searching the computer using English search terms may not detect the material you are seeking. If a person is using another language to "cover his tracks," determining what that language is crucial to recovering evidence. If the person is using an obscure or uncommon language, finding someone to help with the analysis may be an essential part of the process.

Just as lawyers are starting to understand e-discovery and the pros and cons of a computer forensics examination, new technologies are developed that add a whole new wrinkle to the process. Our cell phones have become "smart phones," which are simply small computers with the ability to send and receive email; take pictures; send and receive text messages; and create, store, and transmit word-processing documents, spreadsheets, and PDF files. They have become another source of ESI, as requesting and analyzing a phone during the discovery process is becoming more common. In addition to the phone itself, some phones, like the iPhone in particular, make a backup copy of everything on the phone (except email) every time it is synced to a computer. These backups may contain historical communications that no longer reside on the phone.

Finally, social networks are another important area for e-discovery that should not be overlooked. Members of social networks will often use a site's chat capabilities to "covertly communicate," thinking that their sessions are stored on the site's server or disappear in the "cloud." What most people fail to realize is that their communications may actually get stored on their computer. It may be easier to recover deleted chat sessions from someone's hard drive as opposed to sending a subpoena to the social networking site. Other social networking artifacts that can be recovered from a computer include status updates, full webpages, and user IDs.



Technology for the Litigator

FROM THE SECTION OF LITIGATION TECHNOLOGY FOR THE LITIGATOR COMMITTEE

Spring 2011, Vol. 5 No. 3

Armed with a few basic facts, forensic discovery is not so complicated after all. With some basic knowledge, terms, and concepts, one should be able to sort out fact from fiction when dealing with computer forensics experts. Once a competent and trustworthy expert is selected, counsel can rest assured that clients will benefit from their e-discovery investment.

Keywords: computer forensics, discovery, expert, e-discovery, hard drive, data, recovery, delete

[John Mallery](#) is the president of Mallery Technical Training and Consulting, Inc. in Overland Park, Kansas. [Joan K. Archer](#), J.D., Ph.D. practices with Lathrop & Gage LLP in Kansas City, Missouri.
