Chapter 3

Computer Forensics

Margaret A. (Peggy) Daley
Duff & Phelps, LLC; Chicago

Since almost all communications in the modern world occur electronically, computer forensics is a fundamental component of fraud investigations. The computer forensic examiner works as part of a collaborative team. Often attorneys or law enforcement officials are primarily responsible for identifying which computers and other equipment are relevant to an investigation, but the preservation and collection of the data residing on the relevant machines should be accomplished by qualified computer-forensic specialists. After establishing proper chain of custody, computer forensic examiners then preserve, recover and analyze the data for information relevant to the investigation. The examiner, guided and informed by the investigative team, seeks to identify relevant data and to determine whether any actions were taken on the systems (*i.e.,* wiping, deletions, forwarding corporate data to third parties) that may implicate users in the fraudulent activity.

Computer forensics requires systematic examination of data. It is not enough to think about what might reside within the hard drive of a laptop. In order to complete a thorough investigation, the forensic examiner must determine whether relevant data may reside in a variety of devices and locations, such as:

- printers
- fax machines
- IP telephones
- personal digital assistants
- cell phones
- scanners
- copiers
- iPods and MP3 players
- copiers
- notebooks
- PCs and workstations
- mainframes and servers
- removable disks
- solid-state storage
- thumb drives
- tapes
- removable disks
- CDs and DVDs

- e-mail (server or remotely stored)
- voicemail on telephone systems
- recycle bin
- instant messenger
- data stored on a "cloud."

This chapter won't make you a computer forensic expert. It takes years of study and experience in order to reach that goal. It will, however, provide you with the basic tools and vocabulary necessary to effectively communicate with and work with a computer forensic examiner. It will also help you determine how to efficiently ferret out any relevant or incriminating evidence residing on computers and other electronic devices that might have been associated with the fraud. Conducting this work in a defensible and auditable manner is critical, as computer forensic examinations often unearth the "smoking gun" evidence that makes or breaks a case.

I. What Is Computer Forensics?

Computer forensics is a systematic examination of data residing on digital media. This examination may result in an expert report, deposition or trial testimony. Most often, the computer forensic examiner will work in collaboration with fraud attorneys and forensic accountants to develop evidence and strategies to find the evidence relating to the fraudulent acts of the persons or entities under examination.

Computer forensic analysis can be conducted on any electronic device or storage media. The examination can retrieve and analyze Internet history, Web-based e-mail, lost or deleted files, logging and registry files and cloud-based data. Computer forensic analysis might be based on examination of data seized from the subject of the investigation such as hard drives, cell phones or thumb drives. It can also be conducted on data produced in electronic discovery such as Word documents, e-mail and other documents. Different approaches apply to each of these activities.

Best practices in computer forensics are systematic rather than ad hoc. A systematic computer forensic analysis is characterized by:

- utilization of best practices
- utilization of forensic software that is generally accepted in the forensic industry
- documentation of all switches and settings used for the examination
- exact results that can be reproduced
- systematic documentation
- maintenance of data in a documented evidentiary chain of custody
- preservation of data without compromise in the course of examination.

II. Magnetic Media: Central to Computer Forensics

An understanding of magnetic media is fundamental to understanding the methodology employed by and the findings of computer forensic experts. Most people understand that computer data resides in "hard drives." Few understand that the hard drive is essentially an electronic filing cabinet for the zeros and ones that make up the binary data that comprises our Excel spreadsheets, digital photographs, PowerPoints and Word documents. The "platter" of the hard drive holds the data. The "head" of the hard drive reads the data. The hard drive is formatted into sectors. Adjacent sectors are referred to as a cluster. Electronic files, which so neatly—or sometimes not-so-neatly—appear in the "My Computer" file are not organized so neatly on the hard drive platter. This is because the data may be stored in clusters, which are not particularly well organized or adjacent to one another. In order for the computer to be able to access the data in a file, it must make use of a file allocation table that is created by the operating system of the computer.

Deleting a file does not necessarily erase data. File deletion simply eliminates the directory reference to the file within the computer's operating system. The data is not necessarily lost unless and until the file sector in which the data resides is overwritten. Frequently, file deletions can be reversed because of the multiple restoration points that could exist on a computer's hard drive. It is a popular belief that electronic evidence can be "shredded" or physically destroyed. However, this is not as easy as it may appear. "Shredding software" does exist, and it can

permanently delete a file, making recovery impossible. However, the use of such shredding software is stored in log and registry files, making it clear to the examiner that those documents were intentionally deleted. Intentional deletion of data, particularly after a preservation order has been issued or a fraud investigation commenced, is considered "spoliation" of evidence and is subject to sanctions. Often courts will allow the opposing party a negative inference to be drawn as a result of the spoliation. Such negative inference could be used to bar a debtor's discharge in bankruptcy. While permanently shredded files are often irretrievable, many users try less-sophisticated methods of data destruction or use the software tools incorrectly, making it possible to restore data that had been intended for destruction. This is the best of both worlds for the fraud investigator, as it allows for the examination of the deleted documents and also provides proof of the user's intent to destroy relevant documents.

III. Using Electronic Forensic Data

Financial experts use forensics in investigations and in assessing damages. Computer data can be utilized to:

- establish scienter or knowledge
- identify related parties
- identify hidden assets
- identify otherwise-unknown relationships
- identify e-mail accounts, addresses, phone information
- identify patterns of a target's day-to-day activity
- establish wrongful or fraudulent conduct
- establish culpability of third parties
- establish deletion of data leading to possible criminal charges or civil sanctions for withholding or destroying data.

IV. Gathering Electronic Data

Be sure that your computer forensic examiner uses tools that are sound from a forensic standpoint. Some of the software that is currently in use includes:

- EnCase, published by Guidance Software, www.guidancesoftware.com.
- Forensic Tool Kit, published by Access Data, www.accessdata.com/.
- LogiCube Talon or Dossier, information for which is found at www.logicubeforensics.com/.
- Forensic Boot CDs (Helix or Raptor) pcquest.ciol.com/content/enterprise/2006/106050502.asp.
- ASR Smart www.asrdata.com/.

The tools not only allow for the gathering of data, but they also assist in analyzing the data in an effective matter. Think of these tools as a computer-aided magnetic microscope. The examiner can use tools like these to search for and find useful information, even when the precise nature of the original user's actions is unknown.

It is critical to maintain the physical integrity of the computers and media. To do so, identify and maintain the chain of custody of each piece of evidence obtained. Tag each item and identify what persons were involved with the preservation and transport of the data. Take pictures of the equipment if possible. Think of the relevant equipment as a weapon at a crime scene, and make every effort to document that it was handled in such a way as to preserve the integrity of the data contained in it. Don't, under any circumstances, turn on, boot up or even so much as look at any file in the ordinary manner. Otherwise, critical information about the files on the computer could be altered and lost.

When recovering a computer (or for that matter, any device containing magnetic media), be sure to pack and move these devices with care. Here are some best practices:

- Pack and move the items as if "fragile" cargo.
- Don't use plastic bags, peanuts or other materials that might generate static electricity.
- Avoid magnets, radio transmitters, x-ray machines or anything else that might disturb magnetic media.
- Create a second copy of the evidence and transport and maintain separately.

Best practices for documenting the gathering of evidence include annotation of:

- location of the device
- description, including make, model number, serial number and condition
- date and time collected
- by whom everything was collected.

After the evidence is documented and collected:

- Mark items with the case number, item number and initial.
- Package in antistatic wrapping to avoid loss of magnetic media.
- Seal to avoid tampering.

Consider legal requirements in each case:

- Should the data be collected under subpoena?
- Do you or your client have legal authority to gather the data?
- Must the data be collected by a licensed private investigator, and/or under some compulsory legal process?
- Will the scope of the search be limited to only relevant data?
- Are there Fifth Amendment or self-incrimination considerations?
- How will the chain of custody be maintained?
- Will the data be preserved using proper forensic tools?

V. Human Intelligence

Document exactly what you have collected and preserved. Know how it is customarily used. Find out who used what equipment and how they actually used it. For each item of electronic equipment, the computer forensic examiner needs to determine:

- what it is
- make and model

- external and internal magnetic media (disk drives)
- capacity of media
- BIOS (basic input output system) password
- relationship of equipment to other parts of the system
- owner of the computer
- user or users of the computer
- operating system
- applications
- location of files
- whether a network connection is required
- passwords.

Beyond understanding the equipment, the examiner must gain an understanding of the user:

- Is the user computer-literate?
- Does the user know or expect that the computers will be examined?
- Identify all computers to which the user had access.
- Ascertain the user's access rights to pertinent parts of the networks.
- Did the user have dedicated storage areas on the server?

VI. Forensic Examination Protocol

You don't have to know what these terms below mean, but be sure that your computer forensic examiner does. The examiner's protocol will include or consider the following steps:

- recovery of orphaned folders
- signature analysis
- hash analysis
- link file analysis
- initialization of case script

- NTUSER.dat file analysis
- recycler and INFO2 records
- Web-based e-mail
- temporary Internet files
- keyword search (the keyword search should be sufficiently "fuzzy" so that it will pick up misspelled words or partial numbers).

It is best if the forensic data review is performed in a laboratory environment. Qualified computer examiners should work with proper equipment and up-to-date software. Needless to say, they should know what they are doing. Before hiring an examiner, check to see whether they have any certifications, specialized training or significant work experience in the field. Prior testimonial experience is also helpful, as the credibility of the examination is often called into question by those whose bad actions have been uncovered by the forensic examiner.

One clue the examiner looks for is time stamps, which are located throughout the operational logs of a computer and indicate the data and time that a function occurred. Some fraudsters attempt to alter the time and date on a computer (like rolling back the odometer on a car) in order to cover their tracks, but they rarely do so successfully because of the numerous log files that a typical operating system contains. An examiner can determine whether time and date stamps have been intentionally altered by a user, and this can be invaluable evidence to a fraud investigation. It is hard to imagine an "innocent construction" of the fact that someone intentionally altered time and date stamps on a computer or some of its files without disclosure. The examiner can also look at file properties and metadata to determine when a file was created and when it was changed. Using sophisticated software, the examiner can create a detailed timeline on the computer and connect the timeline to files and other activities based on the time stamp for each file in its metadata.

A computer generates a substantial body of evidence concerning its use. Temporary Internet files essentially save or cache pages visited by the user, allowing the pages to load more quickly for subsequent visits. This data can help ascertain what files were opened, what Web sites were visited, what the user searched for and with whom was she communicating (possibly co-conspirators outside of the walls of the company network). Many people do their banking or stock trading online, so finding the temporary Internet files can lead you to where they bank, where they have investments, and other critical information to asset-tracing or flow-of-fund analysis. Other forms of metadata include dates and times a Web site was visited,

Web-based e-mail records, Google or other search-engine searches, files accessed across a network or files accessed through an external USB (universal serial bus) device. Search-engine history can also be invaluable. Many criminal cases have turned on the nature of the searches conducted by the user. Googling "opening an offshore account," "where to buy cyanide" or "file-shredding software" can be a big tip-off.

VII. E-mail

With more than 1.3 billion e-mail users worldwide, more than 210 billion messages are sent worldwide every day. E-mail is the primary source of office communication. Without access to e-mail, one can't know what was being said in commerce. People think that e-mail can be recovered only if a record of the e-mail remains on the company's e-mail server. Not so.

Web-based e-mail like Gmail, AOL, Yahoo, MSN and others are often readily discoverable and carefully preserved. Don't hesitate to ask the service providers for this information, and be prepared to serve a subpoena.

VIII. Some Objects of a Computer Forensic Examination

A. Link Files

The fraud investigator doesn't need to know how these are created, but she does need to know to ask about them. These files could include shortcuts, recently used files, or other files that might have been removed from the main directory but that remain available in places like the "recently used" folder of the user's account. Often, deleted documents are found in these link files.

B. Metadata

The term metadata refers to information about the nature and history of the data itself. Metadata describes the data and is contained within the data. For example, an image may include metadata that describes how large the picture is, the image resolution and when it was created. The metadata contained in a Word document or Excel spreadsheet would include the length of the document, who the author is and when the document was created and modified. It is important to note that metadata can be altered (*i.e.,* author names changed, dates amended), and it can also be stripped from a document, usually by creating an image of the document through the use of a PDF program like Adobe Acrobat. Many people are unaware that metadata exists. A computer forensic examiner is trained to examine metadata for clues relevant to a fraud examination, and she can often identify significant and perhaps damning evidence.[30] Common examples are e-mails, letters or contracts that were actually created *after* the date contained on the document itself.

Metadata is not limited to information that might be found in a file. System metadata is also maintained and available. System metadata includes:

- date the file was created
- date the last time something was written to the file
- date the last time the file was accessed
- volume label and name of device
- type of media
- volume and serial number
- based path for the file
- working directory for the file.

C. The Registry

Many computer users have heard of the "registry" but don't have a clue what it is or what it means. They may know enough to know not to disturb it for fear that doing so would ruin the computer. The computer's registry contains logging and

30 An outstanding publication entitled "Understanding Metadata" published by the National Information Standards Organization can be found at www.niso.org/publications/press/UnderstandingMetadata.pdf.

operational files that are associated with each computer user's account. Files and "artifacts" in the registry can often be a reliable indicator of who did what and when on a particular computer.

Registry data can determine what programs were used or "executed," how frequently and the last date and time the program was used. The registry can also identify different devices connected to a computer through the USB ports. This is often a critical piece of evidence. It is the registry file that shows whether a thumb drive was connected to the computer and data was copied or deleted from a program on the thumb drive. The registry can also identify whether some other mass-storage device was connected to the computer and data was inappropriately downloaded.

D. Swap Files

Data may exist on a computer hard drive temporarily. There are sectors on a disk drive called "swap files" where the hard drive is used as virtual memory to speed along computer operations. These "swap files" may contain bits and pieces of e-mail, spreadsheets, word processing documents and information relating to recent Internet activity. This data may be destroyed if the computer is turned back on, so one must leave the computer off and resist the temptation to fire it up and start poking around for interesting e-mails or documents while waiting for the forensic examiner to pick up the machine. Instead, permit the computer forensic examiner to create a bit-by-bit image of all hard drives on a computer without booting the system. That way, the image of the disk can be examined without compromising the integrity of the data on the disk drives in any way.

E. Audit Trails and Computer Logs

Computer networks keep track of activity on the network. For example the network will record information about when, where and who accessed a computer system, including the exact date and time. Log-ins and passwords facilitate detailed record-keeping about a computer system. Not only does the network record access, it also will contain security-related information, including unauthorized attempts to gain access. The network will remember and identify documents created, stored, accessed or deleted on a system.

F. Cookies

There's a famous *New Yorker* cartoon that shows a dog typing at a computer. The caption reads: "On the Internet, no one knows you're a dog." While that may be true, many people continue to think that that when they access the Internet, they can do so anonymously. That is very rarely the case. Those who invite users to visit their Web sites often have a subtle string attached. They require the user to accept a "cookie" in their computer hard drive. The cookie accomplishes several things for the Web site sponsor. It identifies the computer user as a visitor to the site. It also allows the web site sponsor to gather information concerning the characteristics of that user, particularly if he or she has "subscribed" to the site. Cookies can and often do reside on a computer for some time. The identity of the computer user is often known by the sites that are visited by the user. Furthermore, the identity of the owner of an e-mail account is usually known by the user's service providers. Subpoenas and forensic tools can often be deployed to determine the identity of an "anonymous" poster.

Cookies that load onto a user's machine contain a great deal of useful information about the user. Cookies can reside as test files or can also be found in the "browser history." The Web sites visited by a person committing fraud may include banks where otherwise undisclosed deposits are maintained, or perhaps Web sites for places where undisclosed properties or assets are located (Cayman Islands, anyone?). Evidence of other crimes, such as pornography, is also often located via cookies. Cookies may also help to uncover undisclosed assets (maybe, for example, expensive automobiles, jewelry, aircraft, etc.). Most Web browsers allow for the enablement or disablement of cookies as a security measure. However, in the interest of speed and efficiency, many users will work around their Web browsers' security. More importantly, certain sites, particularly financial sites such as bank or securities firms, simply won't allow a user to visit without a cookie authenticating the user's rights to visit.

IX. Embedded Information

An example of embedded information can be found in virtually any PC file. See for yourself. The following example is taken from Windows 7. Select a file in a folder. Right click on it. You'll see a box with a cornucopia of information. Tabs will include "General," "Security," "Statistics," "Contents" and "Custom."

The "General" tab in an Excel spreadsheet will inform you of the following:

- document name
- document type
- program that opens the document
- location
- size
- size on disk
- dates created, modified and accessed.

The "Security" tab will provide the following additional information:

- object name
- group and users
- permissions.

The "Custom" tab will contain additional data:

- name
- type
- value.

The "Details" tab can be particularly revealing, affording the following data, among other things:

- title
- subject
- tags
- categories
- comments
- author
- last saved by
- revision number

- version number
- program name
- company
- manager
- content created date
- date last saved
- date last printed
- date created
- date modified.

X. Devices Other than Computers

Personal-information managers, iPhones, BlackBerries and the like afford excellent computer forensic opportunities. Here are several reasons why:

- They synchronize with desktop software.
- They send e-mail messages making the sender appear to be in the office.
- The have Internet access, browsers and cookies.
- They have camera capability.
- Data storage capabilities have exploded, making a phone almost the equivalent to a computer hard drive.

XI. Conclusion

Evidence contained on a computer or other device can make or break a fraud case. Preserving, collecting and analyzing that evidence is not a job for amateurs. In fact, examination of computer forensic evidence by untrained personnel can corrupt and destroy critical information and ruin an investigation. Find qualified forensic professionals and work with them using a team approach. Employ the knowledge you have gained here, and you will obtain satisfactory—and sometimes spectacular—results.