

**INVESTIGATING BY  
COMPUTER  
(SECOND EDITION)**

(No. 02-5411)

## CHAPTER 5

### DIGITAL FORENSICS

In most fraud cases these days, investigators gather a majority of their evidence from computers used by suspects. Sometimes information retrieval is as easy as obtaining a warrant and searching the hard drive of the target computer. But many computer crooks are able to anticipate their exposure soon enough to delete incriminating files from their machines. In these instances, you should know there are a variety of ways of recovering deleted or hidden data from a target computer and its peripherals.

It is absolutely vital for investigators to have a solid understanding of the suspect's level of sophistication. If insufficient information is available to make this assessment, then the suspect should be considered as an *expert* and it should be presumed that he has installed countermeasures against forensic techniques. Because of this fact, investigators should be extremely careful when working with computer equipment until the machine is shut down completely in order to prohibit the machine from modifying the drives.

If the equipment contains only a small amount of critical data on the hard drive, for example, software exists to wipe it permanently and quickly if a given action happens. It is straightforward to link this to the Microsoft Windows "shutdown" command. However, simply "pulling the plug" isn't always the correct answer either because information stored solely in RAM or on special peripherals may be permanently lost. Losing an encryption key stored solely in RAM, and possibly unknown even to the suspects themselves by virtue of having been automatically generated, may render a great deal of data on the hard drive(s) unusable, or at least extremely expensive and time-consuming to recover.

Electronic surveillance, using software or hardware recording devices, allows investigators to record a target computer's activity while the user works. These methods are described below as well.

#### **What is Deleted Data?**

Deletion is a widely misunderstood function in computing. That's because to delete is not the same thing as to destroy. Choosing the "Delete" option from a menu erases the file's reference from the table of contents but it does not erase the file.

The data of a deleted file stays on the hard drive. The files are just renamed and marked as deleted. In Windows or Macintosh system, deleted files are renamed and moved to a special folder. The data does not actually change, the computer just renames the file and stores it in the deletion folder.

***To delete  
is not the same thing as  
to destroy.***

Then, when the file is emptied out of the recycle bin or trash can, the file name is changed again and labeled as “free space,” available for overwriting. But the data still remains on the drive. In most computer operating systems, a deleted file has a character changed in its name (or some related identifying tag), so that the computer knows not to bring it up when asked to list its files. A word-processing document titled “scamfile.doc” might be renamed “\*%scamfile%\*.doc” and stored as “free space.”

Later, when the computer needs disk space, it might write over the document. For example, say you want to save a new file — the computer looks for “free” area, which includes files that have been marked as “deleted,” and writes over the old data with the new data. So your “newfile.doc” is inserted into the space occupied by “\*%scamfile%\*.doc.”

But until the old file is overwritten, it remains whole on the hard drive and is retrievable using any of the software packages described below. Even files that have been overwritten may be partially recoverable — the data may not all be overwritten, or some recoverable portions of the file may be dispersed across the machine’s “free” space.

Especially with the large hard drives available today (averaging 250 gigabytes of memory), deleted files may never be overwritten. The computer only writes over files marked for deletion if there is no other room available on the disk. As long as the disk has plenty of memory, the deleted file will never be touched because the computer continues to write in space that is truly free. If a target computer has not written over all its disk space, every file ever composed on that machine is intact and available for recovery.

Data recovery software can often identify details about the creation, revision, and deletion of data. So if a target has attempted to destroy files, the recovery process will reveal that action.

If the target computer has begun to overwrite deleted files, you may still recover portions of those files. Even when the deleted file has been completely overwritten by new material, the hard disk may contain a catalog of file names (every file ever named on the drive) and a history of which files have been saved and which ones have been deleted. A hard disk may also contain temporary files created while printing, copying, cutting and pasting, or sending the file as an e-mail attachment.

Copies of files may have been made without the user’s knowledge and saved in temporary directories by Windows and other applications. These temporary directories often go untouched by a perpetrator trying to erase his digital tracks because the person does not think to check the Temp directories.

Some Temp directories contain files that were viewed from a CD-ROM — in these cases, you may be able to recover data that was never written on the target's hard drive, but which was viewed through some other device attached to the machine. *It is recommended that requests for deleted computer files should always be included in legal discovery demands.*

### Data Recovery Programs

Most computer operating systems come equipped with some form of recovery program. The Windows operating system employs a “Recycle Bin” program, usually positioned on the desktop and represented by an icon that looks like a small wastebasket, which stores a log of all deleted files. The Macintosh has a “Recover Files” option, and Novell NetWare has the “Salvage” command built in which will permit the user to reclaim deleted files.

For more advanced recovery work, programs such as EnCase, Undelete for Windows, Data-Sniffer, FTK, ProDiscover, Parabin, R-Tools, and Snap!Recovery are available. These programs recover deleted files locally or over a network. They are designed to search throughout a computer's disk space for files and portions of files.

These “undelete” programs search for entries starting with the special character for deleted files, and then recover those files. Undelete programs can potentially recover even parts of files, but the more the file's space has been overwritten, the harder recovery becomes.

A programming tool called a Sector Editor can bypass the file catalog displayed for users (the File Allocation Table, or FAT) and actually read the zeroes and ones on a hard drive. Whether software or hardware based, the Sector Editor searches the target disk, looking for information on files that were deleted but not permanently erased. As long as the file has not been overwritten, a sector editor can read it.

Other utilities such as *Lost and Found* or *Easy Recovery* can recover files from crashed or broken hard drives, even if the drive will no longer boot up. These software solutions claim that if the drive can spin, the data can be recovered.

If these software methods do not work, there are numerous services such as Datarec, Electronic Evidence Discovery, Inc., ActionFront, and DataBank that are dedicated to file recovery. Technicians at commercial services can retrieve data from hard drives that do not even spin. The cost of recovery can run from several hundred dollars to several thousand dollars for the recovery of the lost files.

### **Retrieving Data from Peripherals**

Electronic evidence can be collected from a variety of sources. Within a company's network, evidence will be found in any form of technology that can be used to transmit or store data. Evidence should be collected through three parts of a suspect's network: at the workstation of the suspect, on the mainframe accessed by the suspect, and on the network that connects the two. As data moves from peripheral devices into a computer and from the computer out to various devices, the data leaves evidence of itself, and sometimes leaves full copies of its contents. Below are some common peripherals and suggestions about recovering data from them.

#### **Laser Printers**

It is sometimes possible to recover an image of the last page printed on a laser printer. This technique requires planning because a data recovery expert must examine the printer before it has been moved. Other valuable evidence may be found manually by looking inside a laser printer, where paper from a paper jam has not been cleared away or other data-related materials may reside.

#### **Hard Disk Print Buffers**

Most laser printers have sixteen megabyte hard drives or larger that store each image before it prints, this information will stay on the drive until the printer runs out of memory space and writes over it. Most printers now have their own internal hard drives. Any information sent to and stored by a printer is recoverable unless the printer has overwritten the data.

#### **Print Spooler Device**

This device holds information to be printed. The spooler may be holding a print job if the printer was not ready to print when the print command was given (e.g., the printer was not turned on or was out of paper). This device should be handled at the scene since the information will be lost when power is disrupted.

#### **Keyboards**

Although they do not normally store information, some unusual keyboards are actually computer workstations and may contain an internal diskette drive. Keyboards may also have been fitted with a keystroke logging device prior to the seizure. (See below.)

#### **Hard Cards**

These appear to be a typical function board but they function like a hard disk drive and store information.

#### **Scanner**

Flatbed type scanners may have hard paper copy underneath the cover.

### **Fax Machines**

Although some kinds of stand-alone fax machines simply scan and send data without storing it, other models store the data (on an internal hard drive) before sending it. This data remains in the machine's memory until overwritten. Some fax machines contain two or more megabytes of memory — enough to hold hundreds of pages of information.

### **Electronic Evidence Discovery**

Electronic discovery refers to discovery in civil litigation which deals with information in electronic form. Electronic information is different from paper information because of its intangible form, volume, and volatility. Documents stored in electronic format usually contain metadata (data about data), which is rarely found in paper documents.

E-discovery poses new challenges to the legal community, from attorneys to the courts, as electronic information is identified, preserved, reviewed and produced.

### **Electronic Documents**

Researchers at the University of California at Berkeley announced that 93% of all information created during 1999 was generated in electronic form. We can only image that the remaining 7% has shrunk since then. This does not say that paper documents have disappeared; it is simply produced using computer.

In order to better understand why e-discovery has become so important it is essential to understand the major differences between electronic documents and paper documents.

### ***Volume***

Computer hard drives are packed with electronic documents and, in many cases, duplicate copies of the same document. If the document was shared with colleagues, multiple copies of the same document could be found: local hard drives, network shares, backup tapes, e-mail attachments, and USB thumb drives. This simply goes to illustrate how a document can spread exponentially when sent to multiple recipients. It is important that any modification to the document itself (revisions, comments, etc.) make an entirely new document from an e-discovery perspective as even the most subtle changes could be important to the case at hand.

E-mail illustrates perfectly the sheer volume of documents. A simple example goes to show how many “documents” can be found in a user's inbox:

- An employee receives 25 e-mails/day.
- The employee works 240 days in the year.

- This generates 600,000 e-mails (or “documents”) to examine as part of the discovery process.

Furthermore, many users CC themselves on messages they send which leads to duplicate e-mails being stores in both the “Inbox” and the “Sent” folders. Using “Reply” and “Forward” functions will create multiple copies of the same e-mail on the computer network. As previously stated, a replied to e-mail is a distinct document from the original as it contains additional information.

### ***Location***

Another distinctive difference between paper and electronic documents is the number of locations which need to be searched when preparing disclosure or when complying with a production order or discovery request.

Paper documents will most often times be found in archive boxes, filing cabinets, or people’s desk. Electronic discovery makes this quite a bit more complicated as there is a multitude of locations where information can be stored:

- Desktops and laptops
- Network servers
- Mail servers
- Backup tapes
- Removable storage
- PDAs
- Cell phones

It may be necessary to search some or all of these locations in order to produce the requested information.

### ***Volatility***

Electronic documents are highly volatile since they are constantly changing: access times are changed when a user opens a file and backup tapes are overwritten as part of their normal cycles. Manipulating such volatile information requires proper training and procedures in order to ensure that no evidence is tainted or destroyed.

### ***Metadata***

Metadata is data about data and will most often times accompany documents as most programs which create documents will save metadata with the documents. This can include the name of the person who created the file, the name of the person who last edited the file, how many times the file has been

printed, and even how many revisions have been made on the file. Also included here are comments and revisions made to the document when “track changes” like functions are being used.

### ***Deleted and Hidden Documents***

Much like paper documents, electronic documents can be hidden from view, sometimes in plain sight.

### **Stages of the E-Discovery Process**

The stages of the e-discovery process do not themselves differ from those involved in traditional hard copy discovery. The significant variations are in concepts and terminology used throughout the process.

#### ***Identification***

The first step in the e-discovery process is to determine the scope, breadth, and depth of electronically stored information that might be pursued during discovery. Typically, organizations will manage large volumes of information as part of its ongoing operation. In most litigation, targeted individuals will be limited to those involved in the case at hand. This is not the case for the IT infrastructure as it supports the entire organization.

When identifying key players, this should be based upon department, job function, or other similar criteria. Once criterias have been established, it will be possible to identify which individuals should be targeted.

#### ***Preservation and Collection***

Here, information will be protected against alteration and destruction and then gathered from all the previously identified sources.

In order to adequately preserve documents, organizations require a firm grasp of the information life-cycle in place within the organization. This addresses how, through normal business operations, the organization creates, stores, communicates, and destroys information. Modifications to the underlying processes will be required in order to prevent information from being altered or destroyed (such as backup tapes being overwritten as part of the normal cycle).

Collection addresses many other important issues with regards to the acquisition of electronic information marked as relevant as part of the identification phase. Although, collection is generally performed by the owner, strict physical security and the enforcement of chain of custody is essential. Principles of litigation generally require that electronic information be collected in a manner that is comprehensive, ensures the integrity of the content and of metadata, and preserves its form.

### ***Processing***

Once the collection process is completed, organizations are left with large volumes which may not be all relevant. The objective of the processing phase is to reduce the overall data (commonly known as “data culling”) which has been collected by setting aside duplicates, performing keyword searches for relevant information, and setting aside files which may not be relevant due to their type, origin, or date.

Electronic documents are then converted and stored from the form in which they were found to one that allows to conduct a more effective and efficient review.

Quality assurance is especially important during the processing phase as the amount of data being processed can be staggering which increases the potential for errors.

### ***Review and Analysis***

Review of electronic documents is used to separate relevant documents, which should be produced, from irrelevant documents, which need not be produced, and privileged documents, which should be withheld.

E-discovery will generate large amounts of data which can seem daunting. But advances in technology, specifically in data storage and search algorithms, has made reviewing these large amounts of information a much more efficient and effective process.

Once information has been reviewed, it should be analyzed. Here, the materials are evaluated in order to determine relevant summary information as a key topics, important people as well as “environmental” issues such as acronyms and corporate jargon.

Review and analysis are ongoing processes which are performed as new documents are collected and processed. Furthermore, as the case evolves and new information is uncovered, analysis criteria and objective may change.

### ***Production***

Here, the material is delivered to the parties involved on a variety of mediums which can range from CD/DVD to a Web-based hosting platform.

Again, technological evolution has helped to streamline the production process as many e-discovery products now include hosting platforms with Web-based connectivity which allow access to the uncovered documents. These platforms also include functionalities for searching, tagging, and commenting documents which greatly improve the efficiency of the e-discovery process.

### Securing Digital Forensics as Evidence

Because so much information is obtainable from a computer and its peripherals, investigators must treat these objects with care. Below are some recommendations for gathering computer materials as evidence. You should always consult an expert before attempting unfamiliar tasks with computers and computerized evidence.

The primary concern during the analysis of electronic evidence is to maintain the integrity of the evidence. This means that procedures must be developed to ensure that no allegations can be raised in litigation that the methodology used during the retrieval or analysis could have damaged or altered the hardware, media, or data that constitutes the evidence.

To effectively analyze the data stored within a computer the fraud examiner must have a practical understanding of the basic operations of a computer and how it stores information. The fraud examiner must also have the expertise to access the data at the most basic level. Without this knowledge, information could be hidden from view or stored within other files or locations not usually accessed by the computer.

Each new development in technology brings with it new concepts and a new vocabulary. The modern fraud examiner must become familiar with such terms as HEX and ASCII code, switches, feature groups, DNR, memory maps, GUIs, and interrupts.

Many times computers seized as evidence are only inventoried according to the information available on the outside of the CPU case — namely the make, model, and serial number of the particular unit. The components inside the CPU case are never examined. Fraud examiners must consider that there could literally be thousands of dollars of equipment inside this case. Inadequate inventories of computer equipment leave the organization (and possibly the fraud examiner) in a precarious liability position should any of this equipment be damaged or lost.

### Working with Digital Evidence

Due to the fragile nature of digital evidence, strict forensic procedures are required to handle and process digital evidence. The International Organization on Digital Evidence has set forth the following principles with regards to working with digital evidence:

- When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.

- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.

### **Search & Seizure**

As part of the investigative process, systems which may potentially contain digital evidence relevant to the case at hand will likely be identified. This will likely require the search and potentially the seizure of electronic media for further analysis.

### ***Expectation of Privacy***

The first question that should be asked in a computer fraud examination pertains to the expectation of privacy for any employee or outsider that might be involved in the incident.

For example, in one incident an employee was caught using a company computer for personal use. The company had never established computer use policies. The employee had never been formally notified that personal use of the computer was prohibited and that the company had the right to inspect the contents of the computer at any time. Therefore, when a supervisor discovered inappropriate personal files on the employee's computer, the employee protested the act as an invasion of his privacy.

This demonstrates that appropriate policies can be critical. In the above circumstances, the company might have created a situation where they would actually need to obtain a court order or a search warrant through a law enforcement agency just to examine the contents of their own computers.

Employees should be formally advised as to what their expectation of privacy includes and what is excluded as well. Consider a computer as a container of information. Unless otherwise informed, an employee may have an expectation of privacy with regard to the contents of his or her company workstation similar to their expectation of privacy for a purse or briefcase. Of course, if outsiders are involved in the case, cooperation from a law enforcement agency to obtain the appropriate search warrant might be required.

There is specific wording that should be used in the construction of a search warrant involving either computers or telecommunications equipment. How the equipment and magnetic media are described will be critical to the success of the court case.

### ***Pre-Search Preparation***

Obtaining as much intelligence as possible regarding the location of the potential evidence is extremely desirable before writing the search warrant affidavit. Questions that fraud examiners should consider might include:

- Determine the type of computer systems that will be involved in the search. What operating system is used? Are the computers networked together?
- Determine how many people will be needed to conduct the search. In one case, approximately 17 networked file servers were involved, with multiple routers and dial-up modems. A team of only two investigators would need at least four to six hours to complete a seizure of this magnitude.
- If expert witnesses with a specific expertise are required during the search, identify and clear them before the search is conducted. Depending on the circumstances, their credentials might need to be included in the warrant affidavit before they are approved by the magistrate issuing the search warrant. The time to discover that an “expert witness” has a criminal conviction is before the search warrant affidavit has even been written, not when the witness takes the stand to testify in litigation.
- Determine the resources that will be required to successfully conduct the search. If a great deal of equipment is to be seized, consider how the equipment will be transported from the location. Obtain sufficient boxes, labels, bags, and other supplies at this time.
- Consider the timing of the search. In another case, an assistant district attorney requested assistance in the execution of a search warrant. When detectives arrived, they discovered that the DA wanted them to seize more than 30 computers, including three file servers. This was at 3 p.m., and the DA then told the detectives that the authority to execute the search warrant expired at 5 p.m. The DA had made an error because the detectives physically could not properly conduct the seizure within that time frame. In this case, the evidence was lost. A better strategy would have been to time the execution of the search warrant for 5 p.m. on a Friday afternoon. This would give the entire weekend to conduct the search, if necessary.

### ***Where Can Evidence Be Found?***

Fraud examiners should consider the many different types of computer equipment, items with electronic memory, and types of storage media that might contain evidence. Items to be seized might contain any or all of the following, depending upon the nature of the fraud case:

- Computers
- Computer components
- Computer peripherals
- Word processing equipment
- Modems
- Monitors
- Printers
- Plotters

- Optical scanners
- Data storage devices
  - Magnetic
  - Laser
  - Optical
  - Tape
  - PCMCIA
  - ZIP or JAZZ drives
- Cables, wiring, cords
- Storage media
  - Floppy disks
  - Hard disks
  - Magnetic tape (reels)
  - PCMCIA RAM cards
  - CD-ROM
  - Magnetic/Optical disks
  - Digital Audio Tape (DAT)
  - Personal data managers
  - Flash RAM cards (consider digital camera storage)
- Computer programs
  - Operating systems
  - Application software
  - Utility programs
  - Compilers
  - Interpreters
- Documents
- Manuals
- Printouts
- File listings

All related documentation should be covered by the wording of the search warrant and seized along with the computer system. This documentation could be critical in the analysis of the system hardware and software. Documents could indicate changes that have been made to the system that will help the fraud examiner avoid damaging the system. The fact that access control products have been added to the system might be a helpful piece of information for the fraud examiner.

### Processing Evidence for Removal

The search for and seizure of technical equipment requires new and very specific procedures that must be followed by fraud examiners to guarantee the integrity of the evidence, and to protect both the organization and the individual fraud examiner from civil litigation. How should a computer system be confiscated? Consideration should be given to generating written guidelines in the event that the computer system might actually be seized by someone who is not computer-literate.

***Being computer-literate is not the same thing as being computer investigations literate.***

People who believe themselves to be computer-literate might be a bigger problem than someone who knows nothing at all. These people might wish to exhibit their knowledge by displaying directories of disks, or even by executing programs. If they have not received the proper training their actions might contaminate the potential evidence contained in the system or on the magnetic media. The chain of custody for the evidence also can be destroyed in this manner. In one case, a computer that had been seized by a law enforcement agency contained a game program that was found to have been played while in police custody.

Basic computer procedures are essential when processing this type of evidence. These precautions must be followed explicitly when working with computers:

- *Do not* eat, drink, or smoke close to the computer system or near any of the storage media. Crumbs, liquid, and/or smoke particles could all potentially damage the equipment or stored data. If this happens, it becomes very difficult, if not impossible, to recover the data (and evidence).
- *Do not* fold or bend disks, or touch the magnetic media inside the disk cover.
- *Do not* write on a disk, on a label of a disk, or on a bag that contains a disk. Write on a label and then place the label on the disk. If it is necessary to write on a disk, use a soft felt-tip pen.
- *Do not* place magnetic media near magnetic fields, as this could cause damage. Magnetic fields strong enough to damage data are more common than you might think.
- *Do not* expose magnetic media to either extreme heat or cold. Temperatures outside of the range from 40-90 degrees Fahrenheit can damage the data.
- *Do not* fingerprint magnetic media. The particles of fingerprint powder are almost impossible to remove from the media surface, and the drive will not be able to read the data contained on the media. Permanent damage to the drive equipment could also result.

### Evidence Storage

After a computer system and/or storage media has been seized for analysis there are special storage requirements that must be addressed until the items are either submitted as evidence in a possible litigation or until they are no longer required by the fraud examiner.

The storage environment should be in a location that is:

- Relatively dust-free
- Both temperature and humidity controlled
- Free of magnetic and electronic fields

### ***Possible Threats to Magnetic Media***

- Telephones
- Radio speakers
- Radio transmitters
- Xerox machine
- Plastic garbage or sandwich bags
- Degaussing equipment
- Electric fans
- Under-shelf lighting (heat)
- Leaving media in vehicle trunk during extreme temperatures (either hot or cold)
- Magnets
- Proximity to a radiator or an open heating vent

There are certain issues that must be considered when preserving computer evidence. These areas should be considered regardless of whether the incident will be processed as a criminal offense for prosecution or for possible civil litigation. Even if the organization decides to take no action at all, how a computer fraud examination is conducted might have potential civil liability implications for both the organization and/or the fraud examiner.

Should the fraud examiner discover evidence on a computer system, he or she must be able to state unequivocally that the evidence was not changed in any way by their actions. This requires that strict forensic methodologies be followed to satisfy the stringent evidentiary standards to ensure the integrity of the evidence for possible court presentation.

### **Bit-Stream Image Copies**

If possible, the fraud examiner should make an exact duplicate, or “mirror” copy, of any media that is to be analyzed. This will ensure that no changes or damage occurs to the original evidence. This will not be possible in all cases due to a lack of equipment or other resources, but should be considered as the “ideal” procedure.

When there is no alternative but to analyze the original of the seized evidence, consideration should be given to using utility software to “lock” the disk so that no information can be written to the disk. This will protect the integrity of the original evidence, and prevent inadvertent alteration of the original data.