

Chapter | 14

Introduction to Forensics

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Understand basic forensics principles
- Make a forensic copy of a drive
- Use basic forensics tools

Introduction

In the preceding 13 chapters, you have been introduced to a variety of security topics: from concepts like the CIA triangle, to attacks such as session hijacking, to counter measures like IDS and honey pots. In this chapter, we are going to cover the basics of computer forensics. This is a very important topic for anyone involved in computer security or network administration. It is frequently the case that the first responder to a computer crime is the network administrator, not a law enforcement officer. And if you fail to handle the evidence properly, you may render it unusable in a court and ruin any chances of convicting the perpetrator.

Computer forensics is a comparatively new field. Widespread use of computers dates back to the 1970s and widespread computer crime to the 1990s. The field of computer forensics has evolved only in the past 20 to 25 years. The field of computer forensics, now often called cyber forensics, attempts to apply forensic science to computer devices.

CERT defines computer forensics in this manner:

“If you manage or administer information systems and networks, you should understand computer forensics. Forensics is the process of using scientific knowledge for collecting, analyzing, and presenting evidence to the courts. (The word *forensics* means “to bring to

the court.”) Forensics deals primarily with the recovery and analysis of latent evidence. Latent evidence can take many forms, from fingerprints left on a window to DNA evidence recovered from blood stains to the files on a hard drive.”¹

The goal of cyber forensics is to examine computer devices (laptops, servers, cell phones, tablets, and so on) using scientific methods to extract evidence in such a way that such evidence can be presented in a court. Now, there are certainly times when you will use forensics in scenarios that will never go to court. But the techniques were designed to satisfy the evidentiary requirements of courts.

It is important to keep in mind that a few jurisdictions have passed laws requiring that in order to extract the evidence, the investigator must be either a law enforcement officer or a licensed private investigator. This is a controversial law, given that normally private investigator training and licensing does not include computer forensics training. You should check with specifics in your state. However, many of those states will allow you to forensically examine a computer if you have the permission of the owner or if someone who is licensed seized the evidence. So this would not prohibit you from forensically examining computers in your company.

The purpose of this chapter is to give you a general introduction to the field of forensics. Clearly, each topic discussed in this chapter could be investigated in more depth.

General Guidelines

There are some general guidelines you should always follow in any forensic examination. You want to have as little impact on the evidence as possible. This means you want to examine it and not alter it. You want to have a clear document trail for everything that is done. And, of course, you want to secure your evidence.

Don't Touch the Suspect Drive

The first, and perhaps most important, precaution is to touch the system as little as possible. You do not want to make changes to the system in the process of examining it. Let's look at one possible way to make a forensically valid copy of a drive. Some of this depends on Linux commands, which you may or may not be familiar with. If you are not, I have had students with no Linux experience use these same commands and be able to accomplish the task of making a forensic copy of a drive. Later in this section I will show you how to image drives with other forensic tools, but first we will discuss how to do this without specialized tools.

You will need a bootable copy of Linux. Any Linux live CD will do. You will actually need two copies: one on the suspect machine and one on the target machine. Whichever version of Linux you use, the steps will be the same:

You have to completely wipe the target drive.

```
dd if=/dev/zero of=/dev/hdb1 bs=2048
```

1. CERT Forensics Definition: www.us-cert.gov/sites/default/files/publications/forensics.pdf

Now you need to set up that target forensics server to receive the copy of the suspected drive you wish to examine. The `Netcat` command helps with that. The specific syntax is as follows:

```
nc -l -p 8888 > evidence.dd
```

You are telling the machine to listen on port 8888 and put whatever it receives into `evidence.dd`.

On the suspect machine, you have to start sending the drive's information to the forensics server:

```
dd if=/dev/hda1 | nc 192.168.0.2 8888 -w 3
```

Of course, this assumes that the suspect drive is `hda1`. If not, then replace that part of the command with the partition you are using. This also assumes the server has an IP address of `192.168.0.2`. If not, replace it with whatever your forensics server IP address is.

You will also want to create a hash of the suspect drive. Later you can hash the drive you have been working with and compare that to the hash of the original drive and confirm that nothing has been altered. You can make a hash using Linux shell commands:

```
md5sum /dev/hda1 | nc 192.168.0.2 8888 -w 3
```

When you are done, you have a copy of the drive. It is often a good idea to make two copies: One you will work with, and another will simply be stored. But in no case do you do your forensic analysis on the suspect drive.

Image a Drive with Forensic Toolkit

AccessData is the maker of the Forensic Toolkit and the FTK Imager. The Forensic Toolkit is a commercial product that can be a bit expensive. The FTK Imager is a free download that can be used to make images of drives and to mount images that have been made. You begin by launching FTK Imager, as shown in Figure 14.1.

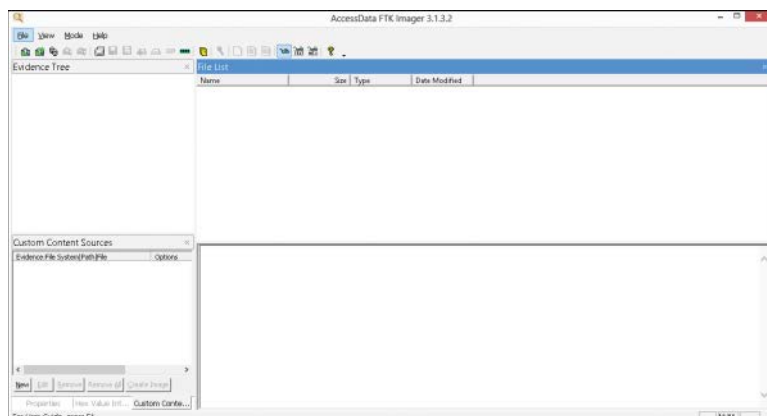


FIGURE 14.1 FTK Imager.

Choose File and select Create Disk Image, as you see in Figure 14.2.

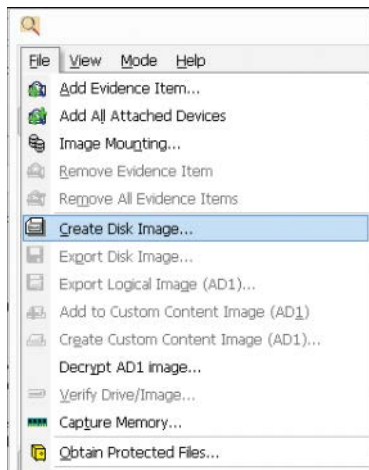


FIGURE 14.2 FTK Imager—Create Disk Image.

Next, you are prompted to select the type of drive you wish to image, as shown in Figure 14.3.

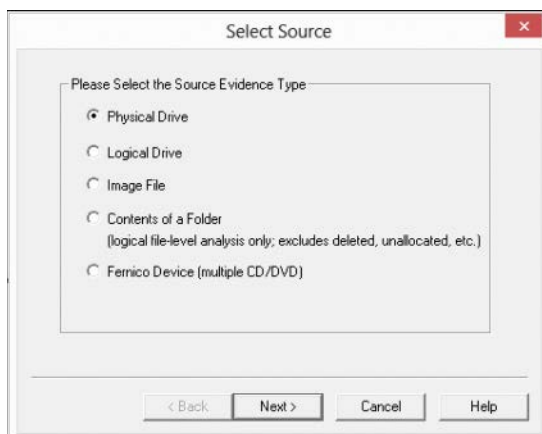


FIGURE 14.3 FTK Imager—Select Source.

Now, based on the source type you selected, you will need to make another choice. For example, if you selected Logical Drive, you now need to pick which logical drive, as shown in Figure 14.4.

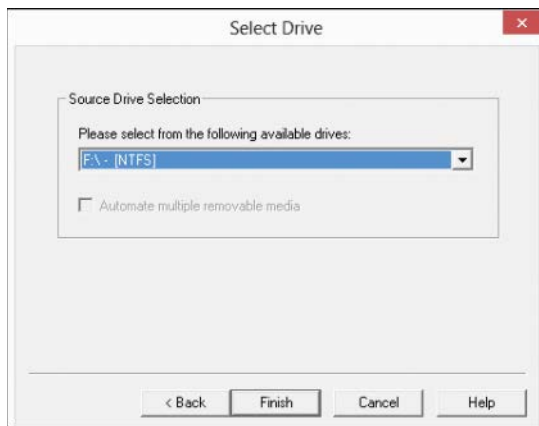


FIGURE 14.4 FTK Imager—Source Drive Selection.

Finally, select a destination for the image, as shown in Figure 14.5.

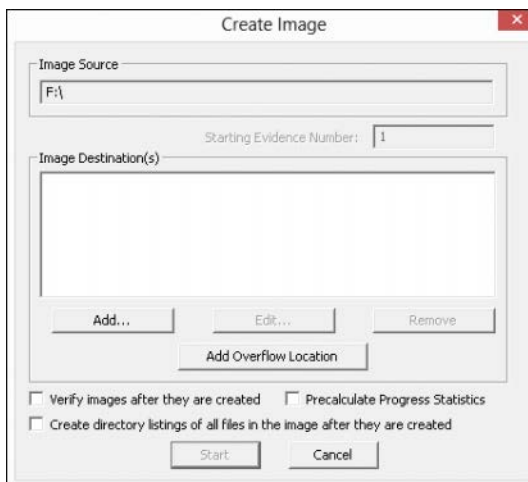


FIGURE 14.5 FTK Imager—Create Image.

The process for mounting an image is even easier. FTK Imager is well respected in the forensic community, easy to use, and free.

Can You Ever Conduct Forensics on a Live Machine?

We have emphasized, and rightfully so, that whenever possible you should always create an image of the drive and perform the analysis only on that image. For a long time this was considered the only

way to conduct computer forensics. However, the past few years have yielded some variation on that thinking. There are times when live forensics is possible or even desirable:

- When you find a machine running, you should conduct some analysis of running processes, memory, and so on before shutting it down.
- It may be necessary on clouds and clusters.
- When the machine has already been imaged, thus preserving evidence.
- When there is not a true forensic investigation, but rather asking a single question.
- Be careful shutting down; if the machine has drive encryption, then when you boot it back up you won't be able to retrieve data.

It is still important to keep in mind that imaging is the preferred method. The preceding list is just a list of suggested times when it may be possible to work with the live system. When doing live forensics, your report must explain why you did it, exactly what steps you did, and make sure the steps you take have the least impact on the system possible.

Document Trail

Beyond not touching the actual drive, the next issue is documentation. If you have never worked in an investigative capacity, the level of documentation may seem onerous to you. But the rule is simple: *Document everything.*

When you first discover a computer crime, you must document exactly what events occurred. Who was present, and what were they doing? What devices were attached to the computer, and what connections did it have over the network/Internet? What hardware was being used, and what operating system?

Then when you begin your actual forensic investigation you must document every step. Start with documenting the process you use to make a forensic copy. Then document every tool you use, every test you perform. You must be able to show in your documentation everything that was done.

Secure the Evidence

First and foremost, the computer must be taken offline to prevent further tampering. Now, there are some limited circumstances where a machine would be left online to trace down an active, ongoing attack. But the general rule is to take it offline immediately.

The next step is to limit access to the machine. No one who does not absolutely need access to the evidence should have it. Hard drives should be locked in a safe or secure cabinet. Analysis should be done in a room with limited access.

You must also be able to document who had access to the evidence, how they interacted with it, and where the evidence was stored. There must be no period of time that you cannot account for the evidence. This is called *chain of custody*.

Chain of Custody

The concept of chain of custody is one of the cornerstones of forensic science, whether that is cyber forensics or some other forensic discipline. Chain of custody refers to detailed documentation showing the status of evidence at every point in time from the moment of seizure to the moment the evidence is presented in court. Any break in that chain of custody will likely render that evidence inadmissible at trial.

According to the Scientific Working Group on Digital Evidence Model Standard Operation Procedures for Computer Forensics:

“The chain of custody must include a description of the evidence and a documented history of each evidence transfer”

This means that any time evidence is transferred from one location to another or from one person to another, that transfer must be documented. The first transfer is the seizure of evidence when the evidence is transferred to the investigator. Between that point in time and any trial, there may be any number of transfers.

Remember that it is almost impossible to over document. Detail what you do, what tools you use, who is present, who conducts what tests, and so on. I find it helpful to take frequent screenshots during my forensic analysis and to include those in my report.

FBI Forensics Guidelines

Beyond the general guidelines we have just discussed, the FBI gives some specific guidelines. In most cases, they will overlap with what we have discussed, but it is still useful to cover the FBI recommendations.

If an incident occurs, the FBI recommends that the first responder preserve the state of the computer at the time of the incident by making a backup copy of any logs, damaged or altered files, and of course any files left by the intruder. This last part is critical. Hackers frequently use various tools and may leave traces of their presence. Furthermore, the FBI warns that if the incident is in progress, activate any auditing or recording software you might have available. Collect as much data about the incident as you can. In other words, this might be a case where you do not take the machine offline but rather analyze the attack in progress.

Another important step is to document the specific losses suffered due to the attack. Losses typically include the following:

- Labor cost spent in response and recovery. (Multiply the number of participating staff by their hourly rates.)
- The cost of the equipment, if equipment was damaged.
- The value of the data if any was lost or stolen. How much did it cost to obtain that data, and how much will it cost to reconstruct it?

- Any lost revenue, including losses due to downtime, having to give customers credit due to inconvenience, or any other way in which revenue was lost.

Documenting the exact damages due to the attack is just as important as documenting the attack itself.

The FBI computer forensic guidelines stress the importance of securing evidence. The FBI also stresses that you should not limit your concept of *computer evidence* to PCs and laptops. *Computer evidence* can include the following:

- Logs (system, router, chat room, IDS, firewall)
- Portable storage devices (USB drives, external drives)
- Emails
- Devices capable of storing data, such as iPod, iPad, and tablets
- Cell phones

The FBI guidelines also stress making a forensic copy of the suspect drive/partition to work with and creating a hash of that drive.

U.S. Secret Service Forensics Guidelines

The United States Secret Service is another federal agency tasked with combating cybercrime and with computer forensics. It has a website devoted to computer forensics² that includes forensics courses. These courses are usually for law enforcement personnel.

The Secret Service also has released a guide for first responders to computer crime. It has listed its “golden rules” to begin the investigation:

- Secure the scene and make it safe.
- If you reasonably believe that the computer is involved in the crime you are investigating, take immediate steps to preserve the evidence.
- Determine whether you have a legal basis to seize this computer (plain view, search warrant, consent, and so on).
- Avoid accessing computer files. If the computer is off, leave it off.
- If the computer is on, do not start searching through it. If the computer is on, go to the appropriate sections in this guide on how to properly shut down the computer and prepare it for transportation as evidence.
- If you reasonably believe that the computer is destroying evidence, immediately shut down the computer by pulling the power cord from the back of the computer.

2. Secret Service Computer Forensics: www.ncfi.uss.gov/

- If a camera is available and the computer is on, take pictures of the computer screen. If the computer is off, take pictures of the computer, the location of the computer, and any electronic media attached.
- Determine whether special legal considerations apply (doctor, attorney, clergy, psychiatrist, newspapers, publishers, and so on).

These are all important first steps to both preserving the chain of custody and ensuring the integrity of the investigation.

EU Evidence Gathering

The Council of Europe Convention on Cybercrime, also called Budapest Convention on Cybercrime or simply Budapest Convention, refers to electronic evidence as evidence that can be collected in electronic form of a criminal offence.

The Electronic evidence guide is a basic guide for police officers, prosecutors, and judges.

The EU also has five principles that establish a basis for all dealings with electronic evidence:

- **Principle 1: Data Integrity:** You must ensure that the data is valid and has not been corrupted.
- **Principle 2: Audit Trail:** Similar to the concept of chain of custody, you must be able to fully account for the evidence. That includes its location as well as what was done with it.
- **Principle 3: Specialist Support:** As needed, utilize specialists. For example, if you are a skilled forensic examiner but have limited experience with a Macintosh computer, get a Mac specialist should you need to examine a Mac.
- **Principle 4: Appropriate Training:** All forensic examiners and analysts should be fully trained and always expanding their knowledge base.
- **Principle 5: Legality:** Make certain all evidence is collected and handled in a manner consistent with all applicable laws.

Even if you don't work within the European Union, these guidelines, can be quite useful. Yes, they are rather broad, but they do provide guidance as to how to properly conduct a forensic examination.

Scientific Working Group on Digital Evidence

Scientific Working Group on Digital Evidence, or SWGDE (www.swgde.org), creates a number of standards for digital forensics. According to SWGDE Model Standard Operation Procedures for Computer Forensics, there are four steps of examination:

1. **Visual Inspection:** The purpose of this inspection is just to verify the type of evidence, its condition, and relevant information to conduct the examination. This is often done in the initial evidence seizure. For example, if a computer is being seized, you would want to document whether the machine is running, what its condition is, and what the general environment is like.

2. **Forensic Duplication:** This is the process of duplicating the media before examination. It is always preferred to work with a forensic copy and not the original.
3. **Media Examination:** This is the actual forensic testing of the application. By *media*, we mean hard drive, RAM, SIM card—some item that can contain digital data.
4. **Evidence Return:** Exhibit(s) are returned to the appropriate location—usually some locked or secured facility.

These particular steps provide an overview of how a cyber forensic examination should proceed. SWGDE has a number of useful documents on its website that you should consult to delve deeper into the nuances of a proper cyber forensics examination.

Locard's Principle of Transference

Dr. Edmond Locard was a forensic scientist who formulated what has become known as Locard's exchange principle or Locard's principle of transference.³ This principle was first applied to physical forensics, and it essentially states that you cannot interact in any environment without leaving something behind. For example, someone cannot break into a house and not leave something. That something could be a fingerprint, a hair, a foot print, and more. Now, a careful criminal will cover up some of this, such as by using gloves to keep from leaving fingerprints. But something will be left behind.

This applies to computer evidence as well and is one reason we prefer to work with a copy. Take Windows for an example. Anytime you log in, open a file, or do anything at all, you have changed registry settings, perhaps left temporary files, and left some traces. For a forensic examination, this is in fact critical. But it also means the investigator has to be careful not to leave traces behind.

Tools

We have previously discussed imaging a drive with either Linux commands or FTK disk imager. There are a variety of tools available for conducting forensic analysis and examination. In this section I will review a few of these for you. There are certainly other tools, but the ones listed here are very widely used.

FTK

We mentioned FTK previously, a brief description is also given here. The company AccessData is the creator of the Forensic Toolkit, better known as simply FTK. This is a robust computer forensics tool that allows you to recover deleted files, examine registry settings, and perform a variety of forensic examination tasks. The software itself can be cost-prohibitive but is quite popular with law enforcement.

AccessData has added additional features such as Known File Filtering for finding certain types of files. FTK can also search and detect files involved in child pornography. AccessData makes a phone forensics tool as well. You can learn more at <http://accessdata.com/>.

3. <http://www.forensichandbook.com/locards-exchange-principle/>

EnCase

This tool, made by Guidance Software, is quite popular with law enforcement and is a direct competitor with FTK. It allows you to image drives, recover deleted files, examine the registry, and other common tasks. It can also be cost-prohibitive for some organizations. You can learn more at <https://www2.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx>.

OSForensics

This is a newer tool, but one that has been well received in the forensic community. It is very low cost and easy to use. It is full featured, allowing you to recover deleted files, examine the registry, and search the drive. You can find out more and even download a fully working trial version at www.osforensics.com/.

Sleuth Kit

This is actually a suite of open source tools. The full suite of tools is full featured but more difficult to use. Each tool can require you to learn a set of command line (or shell) commands to execute. You can find out more at www.sleuthkit.org/.

Oxygen

This tool is specifically for phone forensics. It does a very good job of analyzing iPhones and a reasonably good job of analyzing modern Android. It is not (at least currently) as effective with older Androids or Windows phones. You can learn more at www.oxygen-forensic.com/en/.

Cellebrite

This is perhaps one of the most popular phone forensics tools, at least with law enforcement. It is very effective with a number of different phones. The only downside is that it is one of the most expensive phone forensics tools available. You can find out more at www.cellebrite.com/.

Finding Evidence on the PC

Once you have secured the evidence and made a forensic copy, it is time to start looking for evidence. That evidence can come in many forms. The tools mentioned in the preceding section can be used to extricate this evidence for you. However, in this section I will show you what it is these tools search for. It is important not to simply regurgitate what some automated tool tells you, but rather to understand what it is the tool is doing.

Finding Evidence in the Browser

The browser can be a source of both direct evidence and circumstantial or supporting evidence. Obviously in cases of child pornography, the browser might contain direct evidence of the specific crime.

You may also find direct evidence in the case of cyber stalking. However, if you suspect someone of creating a virus that infected a network, you would probably only find indirect evidence such as the person having searched virus creation/programming-related topics.

Even if the person erases his history, it is still possible to retrieve it. Windows stores a lot of information in a file called `index.dat` (information such as web addresses, search queries, and recently opened files).

Finding Evidence in System Logs

Regardless of what operating system you are using, the operating system has logs. Those logs can be critical in any forensic investigation, and you should retrieve them.

Windows Logs

Let's start with Windows 7/8/10. With all of these versions of Windows, you find the logs by clicking on the Start button in the lower-left corner of the desktop and then clicking the Control Panel. You then click on Administrative Tools and the Event Viewer. Here are the logs you would check for. (Note that not all appear in every version of Windows.)

Note: With all of these, you have to turn the logging on; otherwise, there will be nothing in these logs.

- **Security log:** This is probably the most important log from a forensics point of view. It has both successful and unsuccessful login events.
- **Application log:** This log contains various events logged by applications or programs. Many applications will record their errors here in the application log.
- **System log:** The System log contains events logged by Windows system components. This includes events like driver failures. This particular log is not as interesting from a forensics perspective as the other logs are.
- **ForwardedEvents log:** The ForwardedEvents log is used to store events collected from remote computers. This will only have data in it if event forwarding has been configured.
- **Applications and Services logs:** This log is used to store events from a single application or component rather than events that might have systemwide impact.

Windows servers will have similar logs. However, with Windows systems, you have an additional possible concern. It is possible that the attacker cleared the logs before leaving the system. There are tools that will allow one to wipe out a log. It is also possible to simply turn off logging before an attack and turn it back on when you are done. One such tool is `auditpol.exe`. `auditpol \\\ipaddress /disable` turns off logging. Then when the criminal exits, she can use `auditpol \\\ipaddress /enable` to turn it back on. There are also tools, like WinZapper, that allow you to selectively remove certain items from event logs in Windows.

Linux Logs

Obviously, Linux also has logs you can check. Depending on your Linux distribution and what services you have running on it (like MySQL), some of these logs may not be present on a particular machine:

- **/var/log/faillog:** This log file contains failed user logins. This can be very important when tracking attempts to crack into the system.
- **/var/log/kern.log:** This log file is used for messages from the operating system's kernel. This is not likely to be pertinent to most computer crime investigations.
- **/var/log/lpr.log:** This is the printer log and can give you a record of any items that have been printed from this machine. That can be useful in corporate espionage cases.
- **/var/log/mail.*:** This is the mail server log and can be very useful in any computer crime investigation. Emails can be a component in any computer crime and even in some noncomputer crimes such as fraud.
- **/var/log/mysql.*:** This log records activities related to the MySQL database server and will usually be of less interest to a computer crime investigation.
- **/var/log/apache2/*:** If this machine is running the Apache web server, then this log will show related activity. This can be very useful in tracking attempts to hack into the web server.
- **/var/log/lighttpd/*:** If this machine is running the Lighttpd web server, then this log will show related activity. This can be very useful in tracking attempts to hack into the web server.
- **/var/log/appopt.log:** This records application crashes. Sometimes these can reveal attempts to compromise the system or the presence of a virus or spyware.
- **/var/log/user.log:** These contain user activity logs and can be very important to a criminal investigation.

Getting Back Deleted Files

It is a fact that criminals frequently attempt to destroy evidence. This is also true with computer crimes. The criminals may delete files. However, there are a variety of tools you can use to recover such files, particularly in Windows. DiskDigger is a free tool that can be used to recover Windows files. This is a very easy-to-use tool. There are more robust tools, but the fact that this is free and easy to use makes it perfect for students learning forensics. Let's walk through its basic operation. It should be noted that all the aforementioned forensics tools will recover deleted files for you. It must also be noted that there are many file recovery tools available on the Internet. DiskDigger is simply shown as an example of what is available.

On the first screen, shown in Figure 14.6, you select the drive/partition you wish to recover files from.

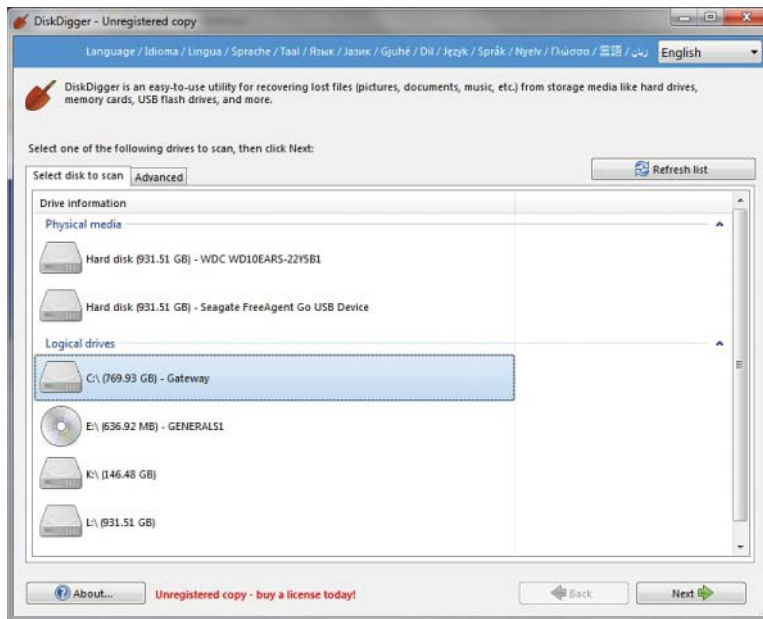


FIGURE 14.6 Add a new scan.

On the next screen, you select the level of scan you want to do. This is shown in Figure 14.7. Obviously, the deeper the scan, the longer it can take.

Then you will get a list of the files that were recovered. You can see this in Figure 14.8.

You can see the file and the file header. You can also choose to recover the file if you wish. Obviously, it is possible that DiskDigger will only recover a file fragment. But that can be enough for forensics.

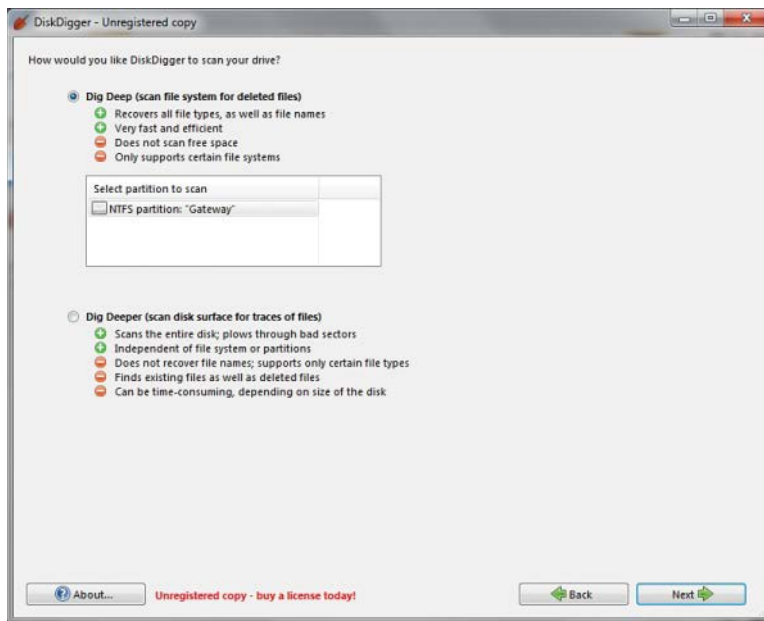


FIGURE 14.7 Select depth of scan.

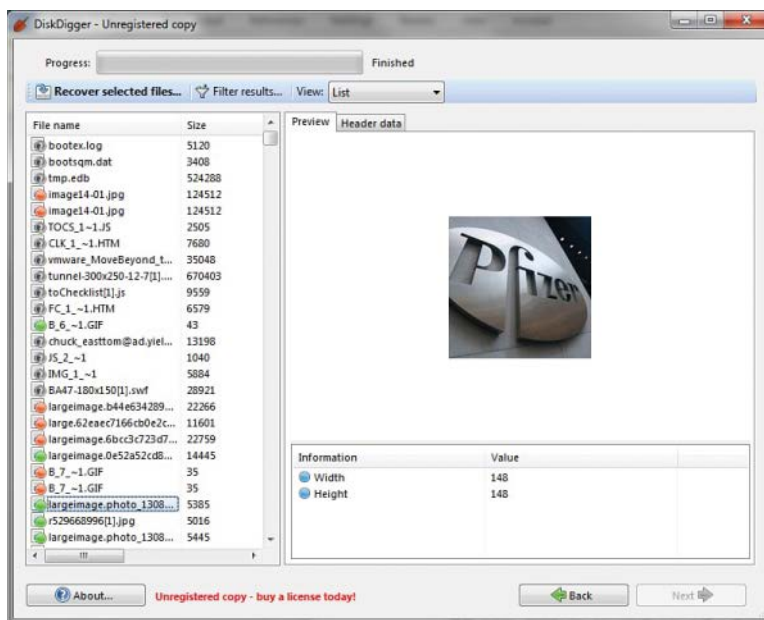


FIGURE 14.8 Recovered files.

NOTE

In addition to deleted files, it is important to check slack space. When a file is saved, the entire cluster is allocated whether it is needed or not. Consider this example: You have a computer with a cluster size of 10 sectors. You save a file that takes only up 3 sectors. As far as the operating system and file system are concerned, all 10 sectors are in use. That leaves 7 sectors unaccounted for. This space is slack space. It is possible to hide data in slack space.

Operating System Utilities

There are a number of utilities built in to the operating system that can be useful in gathering some forensic data. Given that Windows is the most commonly used operating system, we will focus on those utilities that work from the Windows command line. However, one of the key issues in conducting forensics work is to be very familiar with the target operating system. You should also note that many of these commands are most useful on a live running system to catch attacks in progress.

Net Sessions

This command lists any active sessions connected to the computer you run it on. This can be very important if you think an attack is live and ongoing. If there are no active sessions, the utility will report that, as shown in Figure 14.9.

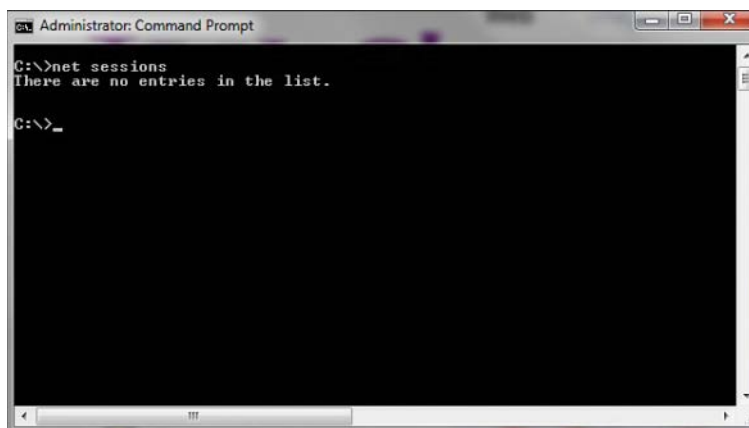
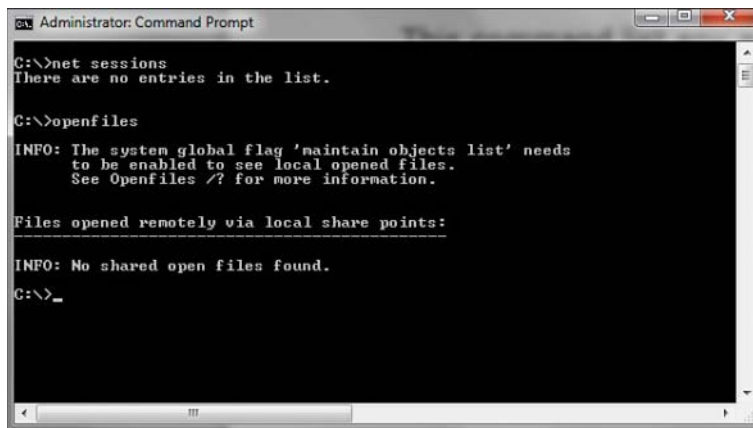


FIGURE 14.9 Net sessions.

Openfiles

This is another command useful for finding live attacks ongoing. This command will list any shared files that are currently open. You can see this utility in Figure 14.10.



```
Administrator: Command Prompt
C:\>net sessions
There are no entries in the list.

C:\>openfiles
INFO: The system global flag 'maintain objects list' needs
to be enabled to see local opened files.
See 'Openfiles /?' for more information.

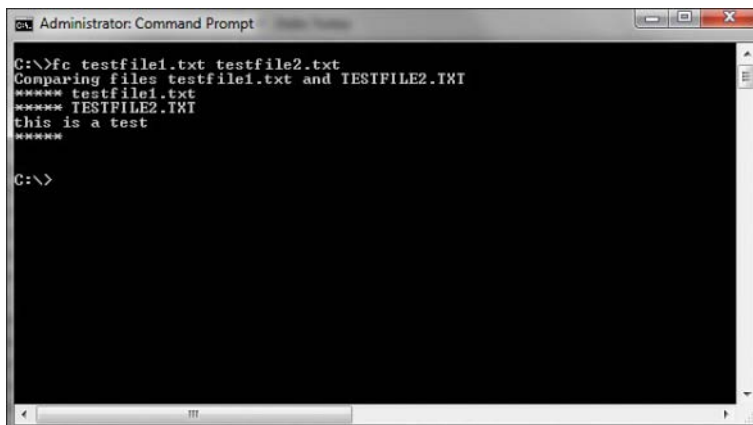
Files opened remotely via local share points:
-----

INFO: No shared open files found.
C:\>_
```

FIGURE 14.10 Openfiles.

Fc

Fc is a command you can use with a forensic copy of a machine. It compares two files and shows the differences. If you think a configuration file has been altered, you can compare it to a known good backup. You can see this utility in Figure 14.11.



```
Administrator: Command Prompt
C:\>fc testfile1.txt testfile2.txt
Comparing files testfile1.txt and TESTFILE2.TXT
**** testfile1.txt
**** TESTFILE2.TXT
this is a test
****

C:\>
```

FIGURE 14.11 Fc.

Netstat

This command is also used to detect ongoing attacks. It lists all current network connections—not just inbound, but outbound as well. You can see this utility in Figure 14.12.

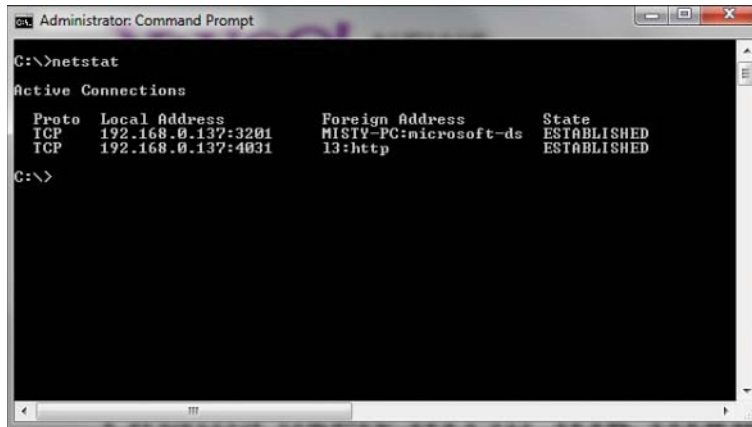


FIGURE 14.12 Netstat.

The Windows Registry

The Windows Registry is an incredible repository of potential valuable forensics information. It is the heart of the Windows machine. There are a number of interesting pieces of data you can find here. It is beyond the scope of this chapter to make you an expert in the Windows Registry, but it is hoped that you will continue on and learn more. Microsoft describes the Registry as follows:

“A central hierarchical database used in the Microsoft Windows family of Operating Systems to store information necessary to configure the system for one or more users, applications and hardware devices.

The registry contains information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents that each can create, property sheet settings for folders and application icons, what hardware exists on the system and the ports that are being used.”⁴

The Registry is organized into five sections referred to as *hives*. Each of these sections contains specific information that can be useful to you. The five hives are described here:

1. **HKEY_CLASSES_ROOT (HKCR):** This hive stores information about drag and drop rules, program shortcuts, the user interface, and related items.
2. **HKEY_CURRENT_USER (HKCU):** This will be very important to any forensic investigation. It stores information about the currently logged-on user, including desktop settings and user folders.
3. **HKEY_LOCAL_MACHINE (HKLM):** This can also be important to a forensic investigation. It contains those settings common to the entire machine, regardless of the individual user.

4. Microsoft Computer Dictionary, Fifth Edition

4. **HKEY_USERS (HKU):** This hive is very critical to forensics investigations. It has profiles for all the users, including their settings.
5. **HKEY_CURRENT_CONFIG (HCU):** This hive contains the current system configuration. This might also prove useful in your forensic examinations.

You can see the Registry and these five hives in Figure 14.13.

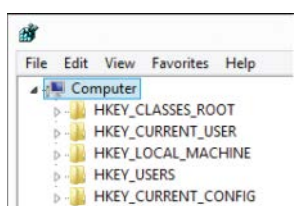


FIGURE 14.13 Windows registry.

Most people use the `regedit` tool to interact with the Registry. In Windows 7 and Server 2008, you select Start, Run and then type in `regedit`. In Windows 8 and 10, you will have to go to the applications list, select All Apps, and then find Regedit or use the Windows+R key and type in `regedit`. Most forensics tools provide a means for examining the Registry as well.

All Registry keys contain a value associated with them called `LastWriteTime`. This value indicates when this registry value was last changed. Rather than be a standard date/time, this value is stored as a `FILETIME` structure. A `FILETIME` structure represents the number of 100-nanosecond intervals since January 1, 1601. Clearly, this is important forensically.

It is also interesting to note that Microsoft rarely uses strong encryption to hide items in the Registry. If an item is encrypted, it is likely encrypted with some simple algorithm such as ROT 13.

Most internal text strings are stored and processed as 16-bit Unicode characters. Unicode is an international character set standard that defines unique 2-byte values (maximum 65,536 characters) for most of the world's known character sets.

You can export a specific key from the command line with

```
reg export HKEY_LOCAL_MACHINE\System\ControlSet\Enum\UBSTOR
```

or within `regedit`, you can right-click on a key and select Export.

Specific Entries

Now that you have a basic working knowledge of the Registry, it is important to look at some specific Registry information you may find.

USB Information

One of the first things most forensic analysts learn about the Windows Registry is that they can find out what USB devices have been connected to the suspect machine. The Registry key `HKEY_LOCAL_MACHINE\System\ControlSet\Enum\USBSTOR` lists USB devices that have been connected to the machine. It is often the case that a criminal will move evidence to an external device and take it with him. This could indicate to you that there are devices you need to find and examine. This registry setting will tell you about the external drives that have been connected to this system. You can see this in Figure 14.14.

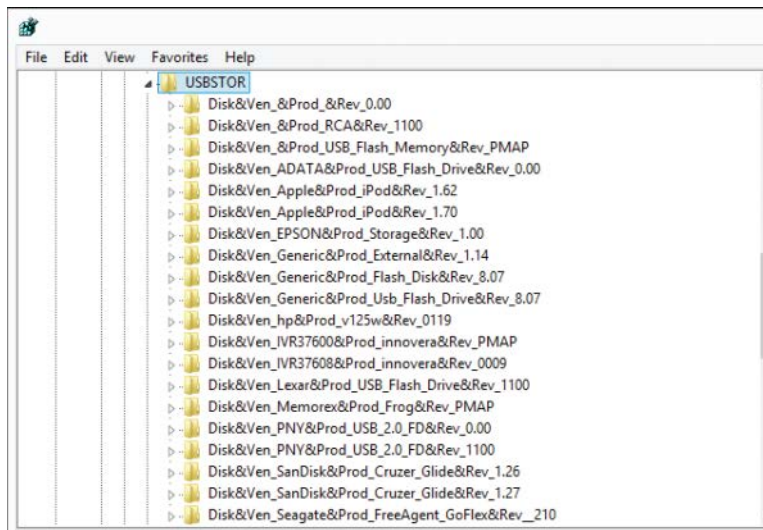


FIGURE 14.14 Windows Registry—USBSTOR.

However, this does not give the complete picture. Some related keys are quite useful:

`SYSTEM\MountedDevices` allows investigators to match the serial number to a given drive letter or volume that was mounted when the USB device was inserted. Incidentally, this particular Registry key is not limited to USB devices.

What user was using the USB device can be found here:

`\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2`

The vendor and product ID can be found here:

`SYSTEM\CurrentControlSet\Enum\USB`

All of these related USB Registry keys should be examined in order to get a complete and accurate picture of what happened regarding specific USB devices.

Autostart Locations

This key is frequently used by malware to remain persistent on the target system. It shows those programs that are configured to start automatically when Windows starts.

Example: `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`

Obviously, you should expect to see legitimate programs in this Registry key. However, if there is anything you cannot account for, it could indicate malware.

Last Visited

`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU`

This key will show recent sites that have been visited. The data is in hex format, but you can see the text translation when using regedit, and you will probably be able to make out the site visited just by looking at regedit.

Recent Documents

Recent documents can be found at the following key:

`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs`

This can be quite forensically important, particularly in cases involving financial data or intellectual property. This key allows you to determine what documents have been accessed on that computer.

As you can see, this key is first divided into document types. Then, once you select the type, you can see the recent documents of that type that have been accessed.

Uninstalled Software

`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall`

This is a very important registry key for any forensic examination. An intruder who breaks into a computer might install software on that computer for various purposes such as recovering deleted files or creating a backdoor. He will then, most likely, delete the software he used. It is also possible that an employee who is stealing data might install steganography software so he can hide the data. He will subsequently uninstall that software. This key lets you see all the software that has been uninstalled from this machine.

There are certainly other keys of interest. And the aforementioned forensics tools will pull this information (and more) for you. If you are going to be working with forensics, particularly with Windows machines, it is critical that you learn the Windows Registry.

Mobile Forensics: Cell Phone Concepts

There are some basic devices and terminology you will need to know before we delve into cell phones. Some of these, such as SIM, are probably at least somewhat familiar to you.

Cell Concepts Module

The following sections are the parts of a phone.

Subscriber Identity Module

A subscriber identity module, or SIM, is the heart of the phone. It is a circuit, usually a removable chip. The SIM is how you identify a phone. It stores the international mobile subscriber identity (IMSI). The IMSI, which we will discuss in detail in just a moment, uniquely identifies a phone. So if you change the SIM, you effectively change the IMSI and thus change the phone's identity. This SIM will also usually have network information, services the user has access to, and two passwords. Those passwords are the personal identification number (PIN) and the personal unblocking code (PUK). The PUK is a code used to reset a forgotten PIN. However, using the code wipes the phone and resets it to its factory state, thus destroying any forensic evidence. If the code is entered incorrectly 10 times in a row, the device becomes permanently blocked and unrecoverable.

International Mobile Subscriber Identity

The international mobile subscriber identity (IMSI) is usually a 15-digit number but can be shorter in some cases. (Some countries use a shorter number.) It is used to uniquely identify a phone. The first three digits are a mobile country code (MCC), and the next digits represent the mobile network code. In North America that is three digits; in Europe it is two digits. The remaining digits are the mobile subscription identifier number (MSIN) that identifies the phone within a given network. To prevent tracking and cloning, the IMSI is only sent rarely. Instead, a temporary value or TMSI is generated and sent.

Integrated Circuit Card Identification

While the integrated circuit card identification (IMSI) is used to identify the phone, the SIM chip itself is identified by the ICCID. The ICCID is engraved on the SIM during manufacturing, so it cannot be removed. The first seven digits identify the country and issuer, and are called the Issuer Identification Number (IIN). After that is a variable length number that identifies this chip/SIM, then a check digit.

International Mobile Equipment Identity

The International Mobile Equipment Identity (IMEI) number is a unique identifier used to identify GSM, UMTS, LTE, and satellite phones. It is printed on the phone, often inside the battery compartment. You can display it on most phones by entering #06# on the dial pad. Using this number, a phone can be blacklisted or prevented from connecting to a network. This works even if the user changes the SIM card.

Cellular Networks

In addition to understanding the cell phones themselves, it is necessary to understand the networks. All cell phone networks are based on radio towers. The strength of that radio signal is purposefully regulated to limit its range. Each cell tower base station consists of an antenna and radio equipment. Following is a brief description of the different types of networks.

Global System for Mobile Communications

Global System for Mobile Communications (GSM) is an older technology, what is commonly called 2G. This is a standard developed by the European Telecommunications Standards Institute (ETSI). Originally, GSM was developed just for digital voice, but it was expanded to include data. GSM operates at many different frequencies, but the most common are 900MHz and 1800MHz. In Europe, most 3G networks use the 2100MHz frequency.

Enhanced Data Rates for GSM Evolution

Many consider Enhanced Data Rates for GSM Evolution (EDGE) a level between 2G and 3G. It is technically considered pre-3G but was an improvement on GSM (2G). It was specifically designed to deliver media such as television over the cellular network.

Universal Mobile Telecommunications Systems

The Universal Mobile Telecommunications Systems (UMTS) is 3G and is essentially an upgrade to GSM (2G). It provides text, voice, video, and multimedia at data rates up to and possibly higher than 2 megabits per second.

Long Term Evolution

Long Term Evolution (LTE) is what is commonly called 4G. It provides broadband Internet, multimedia, and voice. LTE is based on the GSM/EDGE technology. It can theoretically support speeds of 300 Megabits per second (Mbps). Unlike GSM and GSM-based networks, LTE is based in IP just like a typical computer network.

Integrated Digitally Enhanced Network

Integrated Digitally Enhanced Network (iDEN) is a GSM-based architecture that combines cell phone, two-way radio, pager, and modem into a single network. It operates on 800MHz, 900MHz, or 1.5GHz frequencies and was devised by Motorola.

Understanding the networks that cell phones work on is important to understanding cell phone forensics. Today you are most likely encountering LTE, though 3G networks/phones still exist.

Remember that a modern cell phone or tablet is actually a computer. A few short years ago, this was not the case. However, modern mobile devices are, in every respect, full-fledged computers. This means they have hardware, operating systems, and applications (often called *apps*). It is important

to have at least a working knowledge of the operating systems used on mobile devices in order to successfully perform forensic analysis.

iOS

Apple's iPhone, iPod, and iPad are very common, and all run on the same operating system, iOS. The iOS operating system was originally released for the iPhone and iPod in 2007 and later expanded to include the iPad. It is based on a touch interface, wherein the user will perform gestures such as swiping, dragging, pinching, and tapping on the screen. The iOS is based on the OS X for Macintosh but is heavily modified.

The iOS is divided into four layers. The first is the Core OS layer, which is the heart of the operating system. This is a layer that users and applications don't directly interact with. Instead, applications interact with the Core Services layer, the second layer. The third layer, or Media layer, is responsible for music, video, and more. Finally, there is the Cocoa Touch layer, which responds to user gestures.

The iOS uses the HFS+ file system. HFS+ was created by Apple as a replacement for the Hierarchical File System (HFS) and is used in both iOS and OSX. iOS can use FAT32 when communicating with Windows machines (such as when synchronizing an iPhone with a Windows PC).

The iOS divides its data partition as follows:

- Calendar entries
- Contact entries
- Note entries
- iPod_control directory (this directory is hidden)
- iTunes configuration
- iTunes music

Clearly, the calendar and contact entries can be of interest in any forensic investigation. However, some of the data hidden in the iPod_control directory is also very important. Of particular interest to forensics investigation is the folder iPod_control\device\sysinfo. This folder contains two very important pieces of information:

- iPod model number
- ipod Serial number

Android

The Android is the single largest alternative to iOS. It is based on Linux—in fact, it is a modified Linux distribution, and it is open source. That means that if you have the programming and operating system knowledge to follow it, you can download and read the Android source code for yourself at

<http://source.android.com/>. It should be noted that proprietary Android phones often make their own modifications or additions to the open source Android source code.

The Android OS was first released in 2003 and is the creation of Rich Miner, Andy Rubin, and Nick Sears; however, Google acquired Android in 2005. The versions of Android have been named after deserts/sweets:

- Version 1.5 Cupcake released April 2009
- Version 1.6 Donut released September 2009
- Version 2.0–2.1 Éclair released October 2009
- Version 2.2 Froyo released May 2010
- Version 2.3 Gingerbread released December 2010
- Version 3.1–3.2 Honeycomb released February 2011
- Version 4.0 Ice Cream Sandwich released October 2011
- Version 4.1–4.2 Jelly Bean released June 2012
- Version 4.4 KitKat released September 2013
- Version 5.0 Lollipop released November 2014
- Version 6.0 Marshmallow released October 2015

The differences from version to version usually involve adding new features, not a radical change to the operating system. They are all Linux-based, and the core functionality, even from Cupcake to KitKat, is remarkably similar. This means that if you are comfortable with any version of Android, you should be able to perform a forensic analysis with all versions of Android.

Windows

Microsoft has produced several variations of Windows aimed at the mobile market. The company's first foray into the mobile operating system market was Windows CE. That operating system was also released as the Pocket PC 2000, which was based on Windows CE version 3. In 2008, Windows Phone was released. It had a major drawback in that it was not compatible with many of the previous Windows Mobile apps. In 2010, Microsoft released Windows Phone 7.

With the advent of Windows 8, Microsoft is moving all of its devices to the same operating system. This means that PCs, phones, and tablets will use the same Windows—namely, Windows 8. This simplifies forensic analysis. Windows 10 follows the same process of having the same operating system on the phone, tablet, and PC.

What You Should Look For

What are general principles that help you determine what to look for in a cell phone or other mobile device? Items you should attempt to recover from a mobile device include the following:

- Details of the phone itself
- Call history
- Photos and video
- GPS information
- Network information

Information about the phone should be one of the first things you document in your investigation. Just as you would document the specifics of a PC (model, operating system, and so on) you were examining, you should also document the phone or tablet specifics. This will include model number, serial number of the SIM card, operating system, and more. The more descriptive information you can document, the better.

The call history will let you know who the user has spoken to and for how long. Obviously, call records by themselves are not sufficient to prove most crimes. With the exception of stalking or breaking a restraining order, just showing that one person called another is not enough to prove a crime. However, it can begin to build a circumstantial case.

Photos and video can provide direct evidence of a crime. In the case of child pornography, the relevance is obvious. However, it may surprise you to know that it is not uncommon for some criminals to actually photograph or videotape themselves committing serious crimes. This is particularly true of young criminals conducting unplanned crimes or conducting crimes under the influence of drugs or alcohol. There are numerous cases of perpetrators filming or photographing themselves performing crimes ranging from vandalism to burglary and rape.

GPS information has become increasingly important in a variety of cases. So many individuals have devices with GPS enabled that it would seem negligent for a forensic analyst to not retrieve this information. GPS cannot confirm that a suspect committed a crime, but it can show that the suspect was at a location where a crime was committed. Of course, GPS can also help to exonerate someone. If a person is suspected of committing a crime but his vehicle and cell phone GPS are shown to be many miles away at the time of the crime, this can help establish an alibi.

Network information is also important. What Wi-Fi networks does the phone recognize? This might indicate where the phone has been. If a phone has connected to a coffee shop that is near the scene of a crime, it at least shows the perpetrator was in the area. It is also possible that traditional computer crimes, such as denial of service (DoS) and SQL injection, might trace back to a public Wi-Fi point, and the perpetrator was clever enough to mask his computer's identity. If you can show his cell phone GPS was connected to that Wi-Fi, it will help establish he had the opportunity to commit the crime.

The Need for Forensic Certification

Why certifications? This question has been bandied about the information technology field for years. Various pundits come down upon one extreme or the other. Some claim certifications are invaluable, and others claim they are worthless. Also, some subindustries within IT have different attitudes about certifications. In the Cisco world, certifications are king. In the Linux community, certifications have negligible value. So what is the worth of certifications in forensics?

First, you must examine the purpose of certifications. What does it mean to be certified? Frequently, people who have a dim view of certifications have that view because they have encountered someone with a certification who was not very competent. This denotes a misunderstanding of what any certification is. Certification is supposed to indicate that the holder of that certification has met a minimum standard. It does not mean that the person in question is the master of that topic, but rather she is competent. Similarly, a medical degree does not guarantee the person is a great doctor, merely that she has obtained a minimum competency in medicine.

However, it is possible to pass a certification and not be very good at the topic. But the same is true of any field and any educational endeavor. There are certainly some medical doctors (thankfully few) who are incompetent. But if you suddenly have chest pains, I bet you would prefer someone call you a medical doctor rather than a plumber. The odds of a medical doctor having the requisite skill are much higher than that of a plumber. The same is true for IT certifications. While it is certainly possible that someone could be certified and not be competent, the odds that a certified person is competent are much higher. That is why employers frequently require or prefer certifications. It makes the job of filtering through applicants much easier.

Any IT certification can be one valuable indicator of a job applicant's skill. It is not the only indicator and certainly should not be the only thing considered, but it is one factor. This brings us to forensic certifications. Is there a need for another one? First look at what cyber forensics certifications are currently available. All forensics certifications come in one of two types. The first type is vendor certifications. These usually are focused only on the product (or products) that vendor sells. The second type is conceptual certifications. These tests are not about a specific tool, but rather forensic concepts.

AccessData, the creators of the Forensic Toolkit, has multiple certifications for its product. So does Guidance Software, the creators of EnCase. Both of those vendor certifications are quite good. However, they are both vendor certifications. The emphasis is on the particular proprietary suite of tools rather than a general coverage of cyber forensics. If you are going to work with either tool, it is a very good idea to get the appropriate vendor certification, but that is not the same thing as a broad-based cyber forensics course/test.

The EC-Council has its Certified Hacking Forensics Investigator test, and it has been somewhat popular. However, as the name suggests, it has an emphasis on hacking and counter hacking. The EC-Council's primary focus has always been hacking.

This brings us to the topic of ISC2's Certified Cyber Forensics Investigator. Is this certification test worth taking? The first thing to realize is that ISC2 has a long history of well-respected certification

courses/tests, starting with the CISSP, which is the oldest and most well-known computer security certification. This means the CCFP is backed by a strong support organizations. The content of the course/test is also very good. The domains covered include forensic science, application forensics, investigatory procedures, law, and ethics. It is just the sort of broad coverage of cyber forensics that is needed.

The SANS Institute offers a number of certifications, including the Certified Forensics Analyst (GCFA) and Certified Forensics Examiner (GCFE). Both of these are well respected in the industry. The only issue with either one is the cost. SANS courses and their certification tests are among the most expensive in the industry.

Expert Witnesses

At some point, any forensic examiner might be called to testify in court. Being an expert witness is very different from being a witness of fact. To begin with, an expert witness is allowed to testify about things he did not see or hear. Second, an expert witness is allowed to make inferences and formulate theories.

However, there are definite limits to and requirements for expert testimony. You cannot simply get on the stand and essentially state, “Well, I am an expert and this is true because I say so.” There are some rules. The following sections give a brief overview of some of those rules.

Federal Rule 702

Federal rule 702 defines what an expert witness is and the rules concerning when she can testify and what she can testify to. Essentially, rule 702 states the following⁵:

- A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
 - a. the expert’s scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
 - b. the testimony is based on sufficient facts or data;
 - c. the testimony is the product of reliable principles and methods; and
 - d. the expert has reliably applied the principles and methods to the facts of the case.

What this means is that, first and foremost, the expert must be an expert in that specific topic or field. That person’s testimony must be useful to the judge or jury in understanding technical or specialized facts in the case. But just as important, the expert must base her opinions on reliable scientific methods.

5. https://www.law.cornell.edu/rules/fre/rule_702

Daubert

The Daubert standard is used in U.S. federal courts to determine whether or not an expert's scientific testimony is based on reasoning or methodology that is scientifically valid and can properly be applied to the facts at issue. Under this standard, the factors that may be considered in determining whether the methodology is valid are: (1) whether the theory or technique in question can be and has been tested; (2) whether it has been subjected to peer review and publication; (3) its known or potential error rate; (4) the existence and maintenance of standards controlling its operation; and (5) whether it has attracted widespread acceptance within a relevant scientific community. The Daubert standard is the test currently used in the federal courts and some state courts. This is very similar to Federal Rule 702.

Additional Types of Forensics

Digital forensics is a growing field. Computer and phone forensics are the most widely encountered types of digital forensics, but not the only areas of digital forensics. In this section, you will see a brief overview of some other subdisciplines of digital forensics.

Network Forensics

The first, must fundamental thing to learn about network forensics is packet analysis. Before we continue, you may wish to review the material from Chapter 2, "Networks and the Internet," and ensure you are comfortable with basic networking.

Essentially, network forensics involves capturing the network packets traversing the network and examining them for evidence. Many things can be determined from network forensics: where the packet came from, what protocol it is using, what port it is using, and if it is encrypted or not.

The following are some other popular tools for network analysis:

- **Wireshark:** See www.wireshark.org
- **CommView:** See www.tamos.com/products/commview/
- **Softperfect Network Protocol Analyzer:** See www.softperfect.com
- **HTTP Sniffer:** See www.elfetech.com/sniffer/
- **ngrep:** See <http://sourceforge.net/projects/ngrep/>

Any of these tools can work for network analysis.

Virtual Forensics

Virtualization is a broad term that encompasses many technologies. It is a way to provide various IT resources that are independent of the physical machinery of the user. The virtualization makes a logical IT resource that can operate independent of the end user's operating system as well as hardware. The

most basic issue for forensics is the situation where a suspect machine has a virtual machine running on it. There are also issues with getting data from cloud servers.

Virtual Machines

A virtual machine is an interesting concept and was the precursor of more broad-based virtual systems that we will discuss later in this chapter. A virtual machine essentially sets aside a certain portion of a computer's hard drive and RAM (when executing) to run in complete isolation from the rest of the operating system. It is much like you are running an entirely separate computer; it simply shares the resources of the host computer. It is, quite simply, a virtual computer—thus, the name virtual machine.

Each vendor stores data in a slightly different manner, but the next lists show the most interesting files (forensically interesting) for three of the most widely used virtual machine vendors.

■ VMware Workstation:

- **.log files:** This is simply a log of activity for a virtual machine.
- **.vmdk:** This is the actual virtual hard drive for the virtual guest operating system. Virtual hard drives can be fixed or dynamic. Fixed virtual hard drives remain the same size. Dynamic virtual hard drives expand as needed.
- **.vmem:** This is a backup of the virtual machine's paging file/swap file. This can be very important to a forensic investigation.
- **.vmsn:** These are VMware snapshot files, named by the name of the snapshot. A VMSN file stores the state of the virtual machine when the snapshot was created.
- **.vmsd:** A VMSD file contains the metadata about the snapshot.

■ Oracle Virtual Box:

- **.vdi:** These are VirtualBox disk images called virtual disk images.
- **/.config/VirtualBox:** This is a hidden file that contains configuration data.
- **.vbox:** This is the machine settings file extension. Prior to version 4.0, it was .xml.

■ Virtual PC:

- **.vhx:** These are the actual virtual hard disks. They are obviously quite important to a forensic examination.
- **.bin files:** These contain the memory of the virtual machine, so these absolutely must be examined.
- **.xml files:** These files contain the virtual machine configuration details. There is one of these for each virtual machine and for each snapshot of a virtual machine. These files are always named with the GUID used to internally identify the virtual machine in question.

Cloud

A cloud has been defined as “a pool of virtualized computer resources.”⁶

People often speak of the cloud as if there were only one cloud, or at least one type of cloud. This impression is inaccurate. There are multiple clouds and multiple types of clouds. Any organization with the appropriate resources can establish a cloud, and it may establish it for diverse reasons, leading to different types of clouds.

Public clouds are defined by the NIST as those clouds that offer their infrastructure or services to either the general public or at least a large industry group.

Private clouds are those used specifically by a single organization without offering the services to an outside party.⁷ There are, of course, hybrid clouds that combine the elements of a private and public cloud. These are essentially private clouds that have some limited public access.

Community clouds are a midway point between private and public. These are systems wherein several organizations share a cloud for specific community needs. For example, several computer companies might join to create a cloud devoted to common security issues.

A cloud system depends on several parts. Each of these could be a location for evidence.

- **Virtual storage:** The virtual servers are hosted on one or more actual/physical servers. The hard drive space and RAM of those physical servers is partitioned for the various virtual servers' usage.
- **Audit monitor:** There is usually an audit monitor that monitors usage of the resource pool. This monitor will also ensure that one virtual server does not/cannot access data of another virtual server.
- **Hypervisor:** The hypervisor mechanism is the process that provides the virtual servers with access to resources.
- **Logical network perimeter:** Since the cloud consists of virtual servers, not physical ones, there is a need for a logical network and a logical network perimeter. This perimeter isolates resource pools from each other.

Individual cloud implementations might have additional utilities, such as administration consoles that allow a network administrator to monitor, configure, and administer the cloud.

There are two issues with cloud forensics. The first is jurisdictional. Often cloud data is replicated across servers in different countries, each with its own laws. Then there is the technical issue of getting the data. It is very unlikely that you would be able to image the entire cloud in question. So you will probably have to perform a logical copy of the data in question or even a live analysis.

6. <http://www.ijcit.com/archives/volume1/issue2/Paper010225.pdf>

7. http://www.ijarcse.com/docs/papers/Volume_3/3_March2013/V3I3-0320.pdf