This chapter gives an overview of how to manage a computing investigation. You learn about the problems and challenges examiners face when preparing and processing investigations, including the ideas and questions they must consider. This chapter also introduces you to three software tools (one DOS based and two GUI based) and explains how to use them. Throughout this chapter, you examine the details and differences among software packages and learn how to use the software in different scenarios. You also explore standard problem-solving techniques.

As a basic computer user, you can solve most software problems by working with a graphical user interface (GUI). A forensics professional, however, needs to interact with primary levels of the OS that are more fundamental than a GUI. You should be comfortable working from the command line. In several instances, it’s your only alternative. Many computer forensics software tools involve working at the command line, and you should be prepared to learn how to use these tools.

In this chapter, you work with forensic disk images the size of floppy disks to perform the steps and projects in this chapter. After you know how to search for and find data on a small storage device, you can apply the same techniques to a large disk, such as a 40 GB or larger hard disk.
PREPARING A COMPUTER INVESTIGATION

Your role as a computer forensics professional is to gather evidence from a suspect’s computer and determine whether the suspect committed a crime or violated a company policy. If the evidence suggests that a crime or policy violation has been committed, you begin to prepare a case, which is a collection of evidence you can offer in court or at a corporate inquiry. To gather the evidence in a computer forensics case, you investigate the suspect’s computer and then preserve the evidence on a different computer. Before you begin investigating, however, you must follow an accepted procedure to prepare a case. By approaching each case methodically, you can evaluate the evidence thoroughly and document the chain of evidence, or chain of custody, which is the route the evidence takes from the time you find it until the case is closed or goes to court.

The following sections present two sample cases—one involving a computer crime and another involving a company policy violation. Each describes the typical steps of a forensics investigation, including gathering evidence, preparing a case, and preserving the evidence.

Examining a Computer Crime

Law enforcement often finds computers and computer components as they are investigating crimes, gathering other evidence, or making arrests. Computers can contain information that helps law enforcement determine the chain of events leading to a crime or information that provides evidence that’s more likely to lead to a conviction. For example, consider the following scenario in which computers were involved in a crime. The police raided a suspected drug dealer’s home and found a computer, several floppy disks, a personal digital assistant (PDA), a cell phone, and several thumb drives (also called “key-chain drives”) in a bedroom (see Figure 2-1). Two computers were “bagged and tagged,” meaning they were placed in evidence bags and then labeled with tags along with the storage media as part of the search and seizure. The lead detective on the case wants you to investigate the computer to find and organize data that could be evidence of a crime, such as files containing the names of the drug dealer’s contacts.

The acquisitions officer gives you documentation on items the investigating officers collected with the computer, including a list of the other storage media, such as removable disks, CDs, and DVDs. The acquisitions officer also notes that the computer is a Windows XP system and that the machine was running when they discovered it. Before shutting down the computer, officers photographed all the open windows on the Windows desktop, including one showing Windows Explorer. The acquisitions officer gives you digital photos of the desktop.

As a digital forensics investigator, you’re grateful that the officers followed proper procedure when acquiring the evidence. With digital evidence, it’s important to realize how easily key data, such as last accessed date, can be altered by an overeager investigator who is first on the scene. The U.S. Department of Justice (DoJ; www.usdoj.gov) has a document you can download that reviews proper acquisition of electronic evidence.
In your preliminary assessment, you assume that the floppy disks, hard disk, and other storage media include intact files, such as e-mail messages, deleted files, and hidden files. You have a range of software to use in your investigation. Your office owns Digital Intelligences DriveSpy and Image, Norton DiskEdit, Guidance Softwares EnCase, and AccessData’s Forensics Toolkit. This chapter introduces you to these tools. In Chapter 4 you learn the strengths and weaknesses of a multitude of software packages, including the ones introduced in this chapter.

Because some cases involve computers running legacy OSs, older versions of tools often need to be used in forensic investigations. For example, Norton Diskedit is an older tool, but you can still find it on the Norton SystemWorks 2004 CD.

After your preliminary assessment, you determine the risks in this case. Because drug dealers don’t usually make information about their accomplices readily available, the files on the disks you received are probably password protected. You might need to acquire password-cracking software or find an expert who can help you crack the passwords.

Now you’re ready to list the steps you need to take in the case, including how to address the risks and obstacles. Then you can begin the actual investigation and data retrieval.
Examining a Company Policy Violation

Companies often establish policies for computer use by employees. Employees surfing the Internet, sending personal e-mail, or otherwise using company computers for personal tasks during work hours can waste company time. Because lost time can cost companies millions of dollars, computer forensics specialists are often used to investigate policy violations. For example, consider the following scenario that involves a company policy violation.

George Montgomery has worked at a firm for several years and is now missing. Another employee, Martha, is also missing. No one knows where they are or has seen them in over a week, so Steve (George’s supervisor) asks the IT Department to confiscate George’s hard drive and all storage media in his work area.

Taking a Systematic Approach

When preparing a case, you can apply standard systems analysis steps to problem solving, which are explained in the following list. Later in this chapter, you apply these steps to cases.

- **Make an initial assessment about the type of case you are investigating**—To assess the type of case you’re handling, talk to others involved in the case and ask questions about the incident. Have law enforcement or company security officers already seized the computer, disks, and other components? Do you need to visit an office or other locale? Was the computer used to commit a crime, or does it contain evidence about another crime?

- **Determine a preliminary design or approach to the case**—Outline the general steps you need to follow to investigate the case. If the suspect is an employee and you need to acquire his or her system, determine whether you can seize the employee’s computer during working hours or if you have to wait until after office hours or the weekend. If you are preparing a criminal case, determine the information that law enforcement has already obtained.

- **Create a detailed design**—Refine the general outline by creating a detailed checklist of the steps you need to take and an estimated amount of time you need for each step. This outline helps you stay on track during the investigation.

- **Determine the resources you need**—Based on the OS of the computer you’re investigating, list the software you plan to use for the investigation, noting any other software or tools you might need.

- **Obtain and copy an evidence disk drive**—In some cases, you might be seizing multiple computers along with Zip disks, Jaz drives, CDs, thumb drives, PDAs, and other removable media. (For the examples in this chapter, you are using only floppy disks.) Make a forensic copy of the disk.
Identify the risks—List the problems you normally expect in the type of case you are handling. This list is known as a standard risk assessment. For example, if the suspect seems knowledgeable about computers, he or she might have set up a logon scheme that shuts down the computer or overwrites the data on the hard disk when someone tries to change the logon password.

Mitigate or minimize the risks—Identify how you can minimize the risks. For example, if you’re working with a computer on which convicted criminals or smart engineers have likely password protected the hard drive, you can make multiple copies of the original media before starting. Then if you destroy one or more copies during the process of retrieving information from the disk, you have additional copies.

Test the design—Review the decisions you’ve made and the steps you’ve already completed. If you have already copied the original media, a standard part of testing the design involves comparing hash signatures (discussed in Chapter 6) to ensure that you made a proper copy of the original media.

Analyze and recover the digital evidence—Using the software tools and other resources you’ve gathered, and overcoming the risks and obstacles you identified, examine the disk to find digital evidence. Later in this chapter, you recover data from a floppy disk.

Investigate the data you recover—View the information recovered from the disk, including existing files, deleted files, and e-mail, and organize the files to help prove the suspect’s guilt or innocence.

Complete the case report—Write a complete report detailing what you did and what you found.

Critique the case—Self-evaluation is a critical part of professional growth. After you complete a case, review it to identify successful decisions and actions and determine how you could have improved your participation.

The amount of time and effort you put into each step varies depending on the nature of the investigation. For example, in most casework, you need to create a simple investigation plan so that you don’t overlook any steps. However, if a case involves many computers with complex issues to identify and examine, a detailed plan with periodic review and updates is essential.

A systematic approach helps you discover the information you need for your case, and you should gather as much information as possible. “Never enough information” should be your credo when you start a computing investigation and begin hunting for a crucial piece of evidence. Eventually, however, you might feel that you have too much information, especially if it’s not logically organized. How do you process this information during a computer or network investigation? Where do you start gathering information? Moreover, what exactly are you looking for? These are some of the key questions you must answer during each phase of a computing investigation.
Assessing the Case

Recall that identifying case requirements involves determining the type of case you are investigating. Doing so means you should systematically outline the case details, including the nature of the case, the type of evidence available, and the location of the evidence.

In the previous company-policy violation case, suppose you have been asked to investigate George Montgomery, who is missing and suspected of conducting his own business using a company computer. Recall that Steve Billings, George’s supervisor, has confiscated all of George’s storage media that might contain evidence about George’s business and his whereabouts. By talking to George’s co-workers, Steve has learned the nature of George’s business. You can begin assessing this case as follows:

- **Situation**—Employee abuse case.
- **Nature of case**—Side business on the employer’s business computer.
- **Specs about the case**—The employee is reportedly conducting a side business on his assigned computer. The business involves registering domain names for clients and setting up their Web sites at local Internet service providers (ISPs).
- **Type of evidence**—Floppy disk.
- **Operating system**—Microsoft Windows XP.
- **Known disk format**—FAT12.
- **Location of evidence**—One 3½-inch floppy disk that a manager recovered from the employee’s assigned workstation. The manager has received complaints from the employee’s co-workers that he’s been spending too much time on his own business and not performing his assigned work duties. Company policy states that all company-owned computing assets are subject to inspection by company management at any time. Employees have no expectation of privacy when operating company computing systems.

Based on these details, you can determine the case requirements. You now know that the nature of the case involves employee abuse of computers, and you’re looking for evidence that an employee was conducting his own business using his employer’s computers. On the floppy disk Steve retrieved from the employee’s computer, you’re looking for any information related to Web sites, ISPs, or domain names. You know that the OS of the employee’s computer is Windows XP and that the floppy disk the manager retrieved uses the FAT12 file system. To duplicate the floppy disk and find deleted and hidden files, you need a reliable computer forensics tool, such as DriveSpy or Image Acquisition (also called Image), from Digital Intelligence. Because Image and DriveSpy run at the command line, you need to use a Windows 98 workstation to acquire the evidence from the floppy disk. Most computer forensics labs set up dual-boot machines or use forensic boot floppies on newer machines that allow you to boot to the MS-DOS prompt. You will also use two GUI-based tools—AccessData’s FTK Imager and Guidance Software’s EnCase—to create a forensics image and examine the evidence. (In Chapters 4 and 8, you discover that the OS of the...
forensics machine is independent of the OS of the suspect’s machine.) Because the manager already retrieved the floppy disk, you don’t need to obtain the disk yourself.

In Chapter 3 you see the advantages of using older OSs to acquire certain data.

You call this case the Domain Name case and determine that your task is to gather data from the storage media seized to confirm or deny the allegation that George is conducting his own business on company time. Remember that the employee is only suspected of abuse and the evidence you obtain might be exculpatory—meaning it tends to, or helps, prove his innocence. You must always maintain an unbiased perspective and be objective in all your fact-findings. If you are systematic and thorough, you’re more likely to produce consistently reliable results.

Planning Your Investigation

Now that you have identified the requirements of the Domain Name case, you can plan your investigation. You have already determined the kind of evidence you need; now you can identify the specific steps to gather the evidence, establish a chain of custody, and perform the forensic analysis. These steps become the basic plan for your investigation and indicate what you should do when. To investigate the Domain Name case, you should perform the following general steps. Most of these steps are explained in more detail in the following sections.

1. Acquire the floppy disk from George’s manager.
2. Complete an evidence form and establish a chain of custody.
3. Transport the evidence to your computer forensics lab.
4. Secure your evidence in an approved secure container.
5. Prepare your forensic workstation.
6. Obtain the evidence from the secure evidence container.
7. Make a forensic copy of the evidence floppy disk.
8. Return the evidence floppy disk to the secure evidence container.
9. Process the copied floppy disk with your computer forensics tools.

The approved secure container you need in Step 4 should be a locked, fireproof locker or cabinet that has limited access. Limited access means that only you and other authorized people can open the evidence container.
Chapter 2  Understanding Computer Investigations

The first rule for all investigations is to preserve the evidence, which means it should not be tampered with or contaminated. Because the IT Department members confiscated the storage media, you need to go to them for the evidence. When you talk to the IT Department manager, he confirms that the storage media has been locked in a secure cabinet since it was retrieved from George’s desk. Keep in mind that even though this is a corporate policy matter, many cases are thrown out because the chain of custody cannot be proved or has been broken. When this happens, there’s the possibility that the evidence has been compromised.

To document the evidence, you record details about the disk, including who recovered the evidence and when, and who possessed it and when. Use an evidence custody form, also called a chain-of-evidence form, which helps you document what has and has not been done with both the original evidence and forensic copies of the evidence.

Depending on whether you are working in law enforcement or private corporate security, you can create an evidence custody form to fit your environment. This form should be easy to read and use. It can contain information for one or several pieces of evidence. Consider creating a single-evidence form (which lists each piece of evidence on a separate page) and a multi-evidence form (see Figure 2–2), depending on the administrative needs of your investigation.

If necessary, document how to use your evidence custody form. Clear instructions help users remain consistent when completing the form. It also ensures that everyone uses the same definitions for collected items. Standardization helps maintain consistent quality for all investigations and avoid confusion and mistakes about the evidence you collect.

An evidence custody form usually contains the following information:

- **Case number**—The number assigned by your organization when an investigation is initiated.
- **Investigating organization**—The name of your organization. In large corporations with global facilities, several organizations might be conducting investigations in different geographic areas.
- **Investigator**—The name of the investigator assigned to this case. If many investigators are assigned, insert the lead investigator’s name.
- **Nature of case**—A short description of the case. For example, in the corporate environment, it might be “Data recovery for corporate litigation” or “Employee policy violation case.”
- **Location evidence was obtained**—The exact location the evidence was collected. If you are using a multi-evidence form, a new form should be created for each location.
- **Description of evidence**—Describes the evidence, such as “hard disk drive, 20 GB” or “one 3½-inch floppy disk, 1.44 MB.” On a multi-evidence form, write a description for each item of evidence you acquire.
- **Vendor name**—The name of the manufacturer of the computer evidence. List a 20 GB hard disk drive, for example, as a Maxtor, or list a floppy disk as a Floppy Disk Imation 2HD IBM Formatted 1.44MB, for instance. In later chapters, you see how differences among manufacturers can affect data recovery.

- **Model number or serial number**—List the model number or serial number (if available) of the computer component. Many computer components, including hard disk drives, memory chips, and expansion slot cards such as internal modems, have model numbers but not serial numbers.

- **Evidence recovered by**—The name of the investigator who recovered the evidence. The chain of custody for the evidence starts with this information. If you insert your name, for example, you are declaring that you have taken control of the evidence. It is now your responsibility to ensure that nothing damages the evidence and that no one tampers with it. The person placing his or her name here is responsible for preserving, transporting, and securing the evidence.

- **Date and time**—The date and time the evidence was taken into custody. This information establishes exactly when the chain of custody starts.

- **Evidence placed in locker**—Indicates which secure evidence container is used to sort your evidence and when the evidence was placed in the secure locker.

---

*Figure 2-2  A sample multi-evidence form used in a corporate environment*

```
<table>
<thead>
<tr>
<th>Case No.:</th>
<th>Investigating Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigator:</td>
<td></td>
</tr>
<tr>
<td>Location where evidence was obtained:</td>
<td></td>
</tr>
<tr>
<td>Description of evidence:</td>
<td>Vendor Name</td>
</tr>
<tr>
<td>Item 1</td>
<td></td>
</tr>
<tr>
<td>Item 2</td>
<td></td>
</tr>
<tr>
<td>Item 3</td>
<td></td>
</tr>
<tr>
<td>Item 4</td>
<td></td>
</tr>
<tr>
<td>Item 5</td>
<td></td>
</tr>
<tr>
<td>Item 6</td>
<td></td>
</tr>
<tr>
<td>Item 7</td>
<td></td>
</tr>
<tr>
<td>Item 8</td>
<td></td>
</tr>
<tr>
<td>Evidence Recovered by:</td>
<td>Date &amp; Time</td>
</tr>
<tr>
<td>Evidence Placed in Locker:</td>
<td>Date &amp; Time</td>
</tr>
<tr>
<td>Item 1 Evidence Processed by:</td>
<td>Disposition of Evidence</td>
</tr>
<tr>
<td>Item 2 Evidence Processed by:</td>
<td>Disposition of Evidence</td>
</tr>
<tr>
<td>Item 3 Evidence Processed by:</td>
<td>Disposition of Evidence</td>
</tr>
</tbody>
</table>
```

---

Copyright © 2005 by Course Technology. All rights reserved. This publication is protected by federal copyright law. No part of this publication may be reproduced without prior permission in writing from Course Technology. Some of the product names and company names have been used for identification purposes only and may be trademarks or registered trademarks of their respective manufacturers and sellers.
Chapter 2  Understanding Computer Investigations

- **Item #/Evidence processed by/Disposition of evidence/Date/Time**—When you or an authorized computing investigator obtain the evidence from the evidence locker for processing and analysis, list the specific item number and your name, and then describe what was done to the evidence.

- **Page**—The forms used to catalog all evidence for each location should have individual page numbers. List the page number, and indicate the total number of pages associated with this group of evidence. For example, if you collected 15 pieces of evidence at one location and your form has only 10 lines, you need to fill out two multi-evidence forms. The first form is filled in as “Page 1 of 2,” and the second page is filled in as “Page 2 of 2.”

Figure 2-3 shows a single-evidence form. The only major difference is that a single-evidence form lists only one piece of evidence per page. A single-evidence form gives you more flexibility in tracking individual pieces of evidence for your chain-of-custody log. Typically, it has more space for descriptive narrative, which is helpful when finalizing the investigation and creating a case report. Here you can accurately account for what was done to the evidence and what was found.

Use these forms as a reference to all actions taken for your investigative analysis.

<table>
<thead>
<tr>
<th>Metropolis Police Bureau</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-tech Investigations Unit</td>
</tr>
<tr>
<td>This form is to be used for only one piece of evidence. Fill out a separate form for each piece of evidence.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case No.</th>
<th>Unit No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigator:</td>
<td></td>
</tr>
<tr>
<td>Nature of Case:</td>
<td></td>
</tr>
<tr>
<td>Location where evidence was obtained:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item #</th>
<th>Description of evidence:</th>
<th>Vendor Name</th>
<th>Model No./Serial No.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Evidence Received by:</th>
<th>Date &amp; Time:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evidence Placed in Locker:</td>
<td>Date &amp; Time:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Evidence Processed by:</th>
<th>Disposition of Evidence</th>
<th>Date/Time</th>
</tr>
</thead>
</table>

![Figure 2-3 A single-evidence form](image-url)
You can use both multi-evidence and single-evidence forms in your investigation. By using two forms, you can keep the single-evidence form with the evidence and the multi-evidence form in your report file. Two forms also provide redundancy that can be used as a quality control for your evidence.

**Securing Your Evidence**

Computing investigations demand that you adjust your procedures to suit the case. For example, if the evidence for a case includes an entire computer system and associated media, such as floppy disks, Zip and Jaz cartridges, 4 mm DDS digital audio tape (DAT), and USB thumb drive storage devices, you must be flexible when you account for all the items. Some evidence is small enough to fit into an evidence bag. Other items, such as the CPU cabinet, monitor, keyboard, and printer, are too large.

To secure and catalog the evidence contained in large computer components, you can use large evidence bags, tape, tags, labels, and other products available from police supply vendors or office supply stores. When gathering products to secure your computer evidence, make sure they are safe and effective to use on computer components. Be cautious when handling any computer component to avoid damaging the component or coming into contact with static electricity, which can destroy digital data. When collecting computer evidence, make sure you use antistatic bags. (Consider using an antistatic pad with an attached wrist strap, too. Both help prevent damage to your computer evidence.)

Be sure to place computer evidence in a well-padded container. Padding prevents damage to the evidence as you transport it to your secure evidence locker, evidence room, or computer lab. Save discarded hard disk drive boxes, antistatic bags, and packing material for computer hardware when you or others acquire computer devices.

Because you might not have everything necessary to secure your evidence, you have to improvise. Securing evidence often requires you to build secure containers. If the computer component is large and contained in its own casing, such as a CPU cabinet, you can use evidence tape to seal all openings on the cabinet. Placing evidence tape over the floppy disk drive opening, power supply electrical cord insert, CD drive, and any other openings ensures the security of your evidence. As a standard practice, you should write your initials on the tape before applying it to the evidence. This practice makes it possible to prove later in court that the evidence hasn’t been tampered with because the case could not have been opened nor could power have been supplied to the closed case with this tape in place. If the tape hadn’t been replaced, your initials wouldn’t be present, which would indicate tampering. If you transport a CPU case, place a new floppy disk into the floppy disk drive to reduce possible damage to the drive while you’re moving it.

Computer components have specific temperature and humidity ranges. If it’s too cold, hot, or wet, computer components and magnetic media can be damaged. Even heated car seats can damage digital media, and placing a computer on top of a two-way car radio in the trunk...
can cause damage to magnetic media. When collecting computer evidence, make sure you have a safe environment for transporting and storing it until you reach a secure evidence container.

**UNDERSTANDING DATA-RECOVERY WORKSTATIONS AND SOFTWARE**

Now you know what’s involved in acquiring and documenting the evidence. In Chapter 3, you examine a complete setup of a computer forensics lab, or the data-recovery lab, which is where you conduct your investigations and where most of your equipment and software are located, including the secure evidence locker. Be aware that some companies that perform computer investigations also do data recovery, which is the more well-known and lucrative side of the business.

Please note the difference between data recovery and computer forensics. In data recovery, you don’t necessarily need a sterile target drive when restoring the forensics image. Typically, the customer or your company just wants the data back. The other key difference is that in data recovery you usually know what you’re trying to retrieve. In computer forensics, you might have an idea of what you’re searching for, but not necessarily.

To conduct your investigation and analysis, you must have a specially configured personal computer (PC) known as a computer forensics workstation (or “forensic workstation”), which is a computer loaded with additional bays and forensics software. Depending on your needs, most computer forensics work can be performed on the following Microsoft OSs:

- MS-DOS 6.22
- Windows 95, 98, or Me
- Windows NT 3.5 or 4.0
- Windows 2000
- Windows XP

Chapters 3 and 4 cover the software resources you need and the forensic lab and workstation in detail. Visit www.digitalintel.com to examine the specifications of the Forensic Recovery of Evidence Device (F.R.E.D.) unit.

In addition to the Windows OSs listed, you can use Linux or UNIX to perform your analysis. Several open-source and freeware tools are available for this purpose. Note that Windows server software, such as Windows Server 2003 or Windows 2000 Server, isn’t generally used for forensics work.
If you start Windows while you are examining a hard disk, Windows alters the evidence disk by writing data to the Recycle Bin file and damages the quality and integrity of the evidence you’re trying to preserve. Chapter 7 covers which files Windows automatically updates at startup. Windows XP and 2000 systems also record the serial number of the hard drives and CPUs in a file, which can be difficult to recover.

Of all the Microsoft operating systems, the least intrusive (in terms of changing data) to floppy disks and hard disks is MS-DOS 6.22. Later in this chapter, you create a forensic boot floppy disk. This special bootable floppy disk doesn’t alter the data on a suspect’s computer disk. When you acquire data from a hard disk, you should start the system from a forensic boot floppy disk. The only exception is when you have installed a write-blocking device on the suspect’s hard disk. You can use one of several write-blockers that enable you to boot to Windows without writing any data to the evidence disk.

There are many hardware write-blockers on the market. Some are inserted between the disk controller and the hard disk; others connect to internal cables or other devices. One write-blocker is based on technology from ACARD (www.acard.com). ACARD has developed a circuit card that is inserted between the computer’s disk controller and the hard disk. Several ACARD models are based on the small computer system interface (SCSI). These SCSI-based devices enable you to connect and access Enhanced Integrated Drive Electronics (EIDE) disks. (See Chapters 7 and 8 for more information on hard disk types.) This special write-blocker circuit card prevents the OS from writing data to the connected disk drive. Other vendors sell write-blocker devices that connect to SCSI cards, FireWire, or USB 2.0 ports. Current vendors include Digital Intelligence with its SCSIBlock, FireBlock, and FireChief; Guidance Software, producer of FastBloc; and Intelligent Computer Solutions (www.icsforensic.com), which offers Image MaSSter Solo.

To avoid writing data to a disk, you set up your forensic workstation for Windows 98 so that it boots to MS-DOS rather than Windows 98. You need to use Windows 98 because Windows XP and 2000 can access only a DOS shell; they cannot boot directly to DOS. If you’re not already familiar with MS-DOS, the following section introduces you to common MS-DOS commands. MS-DOS is the baseline for all computer forensics analysis. Many computer forensics acquisition tools work in the MS-DOS environment. Although these tools can operate from an MS-DOS window in Windows 98 or from the command prompt in Windows 2000/XP, some of their functions are disabled or generate error messages.

Windows products are being developed that make performing disk forensics easier. However, because Windows has limitations when performing disk forensics, you must still become skilled in acquiring data in MS-DOS. At times, the only way you can recover data is with an MS-DOS tool. Remember that no single computer forensics tool can recover everything. Each has its own strengths and weaknesses. Develop skills with as many tools as possible to become an effective computing investigator.
Setting Up Your Workstation for Computer Forensics

To set up your Windows 98 workstation to boot into MS-DOS, you need to modify the Windows 98 file Msdos.sys. You can add commands to this file so that Windows displays a Startup menu listing options for starting your computer, including booting into MS-DOS.

The C: drive root directory for Windows 98 contains a system file named Msdos.sys. The properties for this file are usually set to Hidden and Read-only so that it can't be changed inadvertently. You can add two commands to this file so that it displays the Windows Startup menu, also called the Startup Boot menu. To add commands to the Msdos.sys file, follow these steps:

1. Start Windows 98, if necessary. Click Start, Run to open the Run dialog box.
2. In the Open text box, type msconfig and then click OK. The System Configuration Utility dialog box opens (see Figure 2-4).

3. On the General tab, you select startup settings. Configuring the Startup menu is an advanced setting, so click the Advanced button to open the Advanced Troubleshooting Settings dialog box (see Figure 2-5).
4. Click the Enable Startup Menu check box so that Windows displays the Startup menu when you start the computer.
5. Click OK to close the Advanced Troubleshooting Settings dialog box.
6. Click OK to close the System Configuration Utility dialog box. Windows modifies the Msdos.sys file by turning on the Boot Menu switch.
7. If a message appears asking whether you want to restart so that the changes can take effect, click Yes. Because the Startup menu has been enabled, ensure that Normal is selected for the boot option, and press Enter.

Now you can open the Msdos.sys file, examine its settings, and add a command to the file to extend the amount of time the Startup menu appears before it closes and Windows starts as usual. Before you can modify the Msdos.sys file, you must change its Read-only and Hidden properties. Follow these steps to change those properties and add a command to the Msdos.sys file:

1. If necessary, change the Windows view setting to show hidden files. To do this, double-click My Computer on the desktop, and then click View, Folder Options from the menu. In the Folder Options dialog box, click the View tab. Under the Hidden files folder, click the Show all files option button, and then click OK.

2. In the My Computer window, navigate to the root folder on your hard disk, which is usually C:. (If the drive where Windows is installed has a different drive letter, use that letter instead of C.) Right-click Msdos.sys, and then click Properties to open the Msdos.sys Properties dialog box.

3. In the Attributes section, click to clear the Read-only and Hidden check boxes. Click OK to close the Msdos.sys Properties dialog box.

4. Click Start, point to Programs, point to Accessories, and then click Notepad.

5. Click File, Open from the menu to open the Open dialog box. Navigate to the root drive, click All Files (*.*) if necessary, in the Files of type list box, and then double-click Msdos.sys. The Msdos.sys file opens in Notepad.
Chapter 2 Understanding Computer Investigations

Note that the BootMenu command is set to 1, which means it’s turned on. A setting of 0 means it’s turned off. (You might need to scroll to see the BootMenu command in this window.) If your Msdos.sys file contains a BootMenuDelay command, it’s also set to 5 seconds by default.

6. If your Msdos.sys file doesn’t include a BootMenuDelay line, press Enter at the end of the file to add a new line, and then type \BootMenuDelay=59, as shown in Figure 2-6. If your file does have a BootMenuDelay line, extend the amount of time the Startup menu is displayed by changing the BootMenuDelay setting to 59, which is the maximum setting for displaying the Startup menu.

7. Click File, Save from the menu. Close Notepad.

8. Now you need to restart your computer using the Normal boot option. If you’re working in a computer lab, check with your instructor or technical support person to make sure you have permission to restart your computer. Click Start, Shut Down, Restart, OK.

Next, you see how to install DriveSpy and Image on your computer. The CD that accompanies this book contains a 120-day license for your computer. You need to contact the vendor for a license key. Please note that the company might take several days for a response—it’s not an autoresponder.

1. Your computer should have rebooted to Windows 98. Use Windows Explorer to create folders named Chap02\Chapter and Tools in the work folder for this book.
In the “Read This Before You Begin” section of this book, you or your instructor created a folder on your system where you can store your work. This book calls this folder the “work folder,” which should be created on a drive that your instructor specifies. Create the Chap02\Chapter and Tools folders in your work folder.

2. Using Windows Explorer, copy the following Digital Intelligence files, after you have received them from Digital Intelligence, to the Tools folder in your work folder:
   - Drivespy.exe
   - Drivespy.hlp
   - Drivespy.ini
   - Image.exe
   - Image.ini

Your instructor will tell you where the files are located on the lab machines. For both Drivespy.exe and Image.exe, you must create a command-line batch file that appends an additional path defining the location for the Digital Intelligence tools so that you can use the forensic tools from any folder on your hard disk. To do so, follow these steps to create a text file in Notepad called Toolpath.bat:

1. To start Notepad, click Start, point to Programs, point to Accessories, and then click Notepad.
2. Type the command `SET PATH=%PATH%;C:\work folder\Tools` to define the path to your forensics tools. Replace `work folder` with the name of the work folder you’re using to store your files for this book. C:\ is the drive where your work folder is located.
3. Click File, Save As from the menu. In the Save As dialog box, click the Save in list arrow, and then navigate to C:\Windows. (If Windows is installed on a different drive, use that drive letter instead of C.) Click the Save as type list arrow, and then click All Files (*.*) in the File name text box, type Toolpath.bat. Click Save.
5. Shut down your computer by clicking Start, Shut Down, Restart, OK.
6. The Windows 98 Startup Menu appears, as shown in Figure 2-7. Use option 1 for a Normal boot to Windows 98 and option 5 for Command prompt only to boot to MS-DOS. You have approximately 59 seconds to respond to the menu. If you do not select one of the numbered mode options, the computer boots to Normal mode (Windows 98).
7. To boot your workstation into MS-DOS mode, at the Enter a choice prompt, type 5 to select Command prompt only and then press Enter.
Your workstation boots to the root level of your C:\ disk drive and displays a C:\> command prompt. You have now set up your workstation so that you can perform some basic computer forensics acquisitions and analysis at the DOS level.

**CONDUCTING AN INVESTIGATION**

Now you’re ready to return to the Domain Name case. You have created a plan for the investigation, set up your forensic workstation, and installed the software you need to examine the evidence. To begin conducting an investigation, you start by copying the evidence using a variety of methods. Recall that no single method retrieves all the data from a disk, so using several tools to retrieve and analyze data is a good idea.

Start by gathering the resources you identified in your investigation plan. You need the following items:

- Original storage media
- Evidence custody form
- Evidence container for the storage media, such as an evidence bag
- Bit-stream imaging tool; in this case, the Digital Intelligence Image utility
- Forensic workstation to copy and examine your evidence
- Secure evidence container
You use the Digital Intelligence Image utility to copy a floppy disk later in this chapter. For more information on this utility, visit the Digital Intelligence Web site at www.digitalintel.com. The PDF file included on the accompanying CD also explains the utility.

Gathering the Evidence

Now you’re ready to gather evidence for the Domain Name investigation. When you gather evidence, recall that you need antistatic bags and pads with wrist straps to ensure that you are grounded to prevent static electricity from damaging fragile electronic evidence. You also want to make forensic copies that are exact duplicates.

You need to acquire George Montgomery’s storage media from the IT Department and then secure the disk in an evidence bag. You perform the following steps to collect the evidence and transport it to your forensic facility:

1. Arrange to meet the IT manager so that you can interview him and pick up the storage media.
2. After interviewing the IT manager, fill out the evidence form, have him sign it, and then sign it yourself.
3. Store the storage media in an evidence bag, and then transport it to your forensic facility.
4. Carry the evidence to a secure container, such as a locker, cabinet, or safe.
5. Complete the evidence custody form. As mentioned earlier, if you’re using a multi-evidence form, you can store the form in the file folder for the case. If you’re also using single-evidence forms, store them in the secure container with the evidence. Reduce the risk of tampering by limiting access to the forms.
6. Secure your evidence by locking the container.

Understanding Bit-stream Copies

A bit-stream copy is a bit-by-bit copy of the original storage medium and is an exact duplicate of the original disk. Recall that the more exact the copy, the better chance you have of retrieving the evidence you need from the disk. A bit-stream copy is different from a simple backup copy of a disk. Backup software can only copy or compress files that are stored in a folder or are of a known file type. Backup software cannot copy deleted files or e-mail messages or recover file fragments.

Bit-streaming literally means that a disk is copied bit by bit, creating an exact image of the disk. A bit-stream image is the file that contains the bit-stream copy of all the data on a disk or disk partition. To create an exact image of an evidence disk, copying the bit-stream image to a target work disk that’s identical to the evidence disk is preferable (see Figure 2-8). The target disk’s manufacturer and model, in general, should be the same as the manufacturer and model of the original evidence disk. The size of both disks should also be the same,
although some software tools that create bit-stream images can accommodate a target disk that’s a different size than the original evidence disk is. These imaging tools are discussed in Chapter 9. As you’ll see, some of the latest versions of forensic tools enable you to work directly from the forensic image.

Occasionally, the track and sector maps on the original and target disks don’t match, even if you use disks of exactly the same size. Newer tools such as FTK Imager are available that adjust for the target-drive geometry.

**CREATING A FORENSIC BOOT FLOPPY DISK**

Recall that your goal when conducting a computer forensics examination is not to alter any portion of the original data on a disk when making a copy or examining the data. The preferred way to avoid modifying evidence data is to never examine the original evidence disk. Thus far, you have learned how to make a copy of a floppy disk so that you can re-create and then examine it. The same principle applies when examining hard disks—you must preserve the original disk and not alter its contents during your examination.

In the following section, you make a boot floppy disk to serve as your forensic boot floppy disk. Whenever a computer is started, it accesses files on the hard disk, even if the computer boots from a floppy disk that contains system files. When the boot process accesses files on the hard disk, it changes their date and time stamps, which can jeopardize an investigation, especially if a goal in the investigation is to determine when the computer was last used. By booting the computer without a specially configured floppy disk, you destroy information important to an investigation. Windows 9x can also alter other files, especially if DriveSpace is implemented on a FAT16 disk drive. The boot floppy disk you create is specially configured so that the boot process doesn’t alter any files on the hard disk when the computer is powered on, thus preserving the suspect’s disk drive. Having access to a software or hardware write-blocker for the suspect’s drive is always a good precaution.
Assembling the Tools for a Forensic Boot Floppy Disk

To make a boot floppy disk for forensics data acquisition, you need the following items:

- Disk editor, such as Norton Disk Edit or Hex Workshop, installed on your computer
- Floppy disk containing files you no longer need
- MS-DOS operating system, such as MS-DOS 6.22, Windows 95B (OSR2), or Windows 98 running on your computer, not Windows XP, 2000, Me, or NT
- Computer that can boot to a true MS-DOS level—that is, an MS-DOS 6.22, a Windows 95B (OSR2), or a Windows 98 computer
- Forensics acquisition tool, such as DriveSpy, EnCase, SafeBack, or SnapCopy
- Write-blocking tool to protect the evidence drive

The first task is to make the floppy disk bootable from the MS-DOS prompt, meaning that it contains the system files needed to boot the computer. The following steps use a Windows 98 computer to make the boot floppy disk. The process is similar for Windows 95.

1. Boot into DOS mode. Insert the floppy disk into your computer’s floppy disk drive, which is usually drive A.
2. At the C:\> prompt, format the floppy disk by typing `format a: /u /s`, pressing Enter, and then pressing Enter again when ready. When the system is done formatting, it prompts you for a volume name. Type in Bootdisk, and press Enter. Next, you’re asked if you want to format another disk. Type n for no, and press Enter.
3. At the DOS prompt, type `attrib -r -h -s a:*.*` and then press Enter to remove the Read-only and Hidden attributes for all files on the floppy disk.
4. On the A: drive, delete the Drvspace.bin file by typing `del a:\drvspace.bin` and pressing Enter.

To make the floppy disk bootable from Windows Explorer, follow these steps:

1. Boot into Windows 98. (Note: If your workstation’s BIOS is set to boot from the A: floppy drive first, remember to remove the bootable floppy disk from the drive before you start Windows.) Insert the floppy disk into your computer’s floppy disk drive, which is usually drive A.
2. Open Windows Explorer. Right-click the 3½ Floppy (A:) icon, and then click Format.
3. Click Full in the upper pane, and click to enable the Copy system files check box in the lower pane. Click Start. When you’re done, change the file attributes by right-clicking the files and clicking Properties. Click to clear the Hidden and Read-only check boxes, and click OK. Click Close in the Format Results dialog box, and then click Close in the Format dialog box.
4. Right-click the Drvspace.bin file, click Delete, and then click Yes in the Confirm File Delete message box.

After you create a bootable floppy disk, update the operating system files to remove any reference to the hard disk, which is usually the C: drive. This ensures that when you're acquiring a FAT16 or FAT32 evidence disk, your boot floppy disk does not contaminate it. You need to modify the Command.com and Io.sys files to make a forensic boot disk. The following steps show you how to use Hex Workshop for this task. Hex Workshop should already be installed on your computer before you perform these steps. If you're using Norton Disk Edit, first boot your workstation into MS-DOS mode. For further information on how to use Norton Disk Edit, refer to its online help.

1. If necessary, boot your workstation into Windows.
2. Insert the boot floppy disk you created in the previous set of steps into your computer's floppy disk drive.
3. The changes from this point can be done in Windows 98 or in Windows 2000. (Screen shots in these steps were taken using Windows 2000.) In Windows 2000, open Windows Explorer, and click Tools, Folder Options from the menu. Click the View tab, if necessary, and under the Advanced settings section, click Show Hidden files and folders, and then click OK. In Windows 98, click View, Folder Options from the Windows Explorer menu. Click the View tab. Under Hidden files, click the Show all files option button (if necessary), and click OK.
4. To start Hex Workshop, double-click the Hex Workshop icon on your desktop or click Start, point to Programs (All Programs in Windows XP), point to Hex Workshop, and then click Hex Workshop. The opening window shown in Figure 2-9 might differ slightly from your Hex Workshop window, depending on the version.
5. Click File, Open from the menu.
6. In the Open dialog box, navigate to the A: drive. Click Command.com, and then click Open.
7. To replace references to the hard disk (drive C:) in Command.com, start by clicking Edit, Replace from the menu.
8. In the Replace dialog box, click the Type list arrow under the Replace section. A list of data you can replace is displayed. Click Text String.
9. In the Find text box, type c:\ or the letter of your primary hard disk. In the Replace text box, type a:\ (see Figure 2-10).
10. Click OK. The Replace dialog box opens, which you use to search for and replace the specified text. Click the Replace All button, and then click OK.
11. Click File, Save from the bar to save the changes you made to Command.com on the floppy disk. If a message is displayed asking whether you want to make a backup of Command.com, click No.
In the following steps, you modify the Io.sys file to change all references to the C: drive and the DriveSpace utility. You don’t want to activate DriveSpace because it can corrupt data.

1. Click **File, Open** from the Hex Workshop menu.
2. In the Open dialog box, navigate to the A: drive, and then click **Io.sys**.
3. Click the **Open** button to open the file in Hex Workshop (see Figure 2-11).

**Figure 2-9** The opening window in Hex Workshop

**Figure 2-10** Specifying what text to replace in the Command.com file

In the following steps, you modify the Io.sys file to change all references to the C: drive and the DriveSpace utility. You don’t want to activate DriveSpace because it can corrupt data.

1. Click **File, Open** from the Hex Workshop menu.
2. In the Open dialog box, navigate to the A: drive, and then click **Io.sys**.
3. Click the **Open** button to open the file in Hex Workshop (see Figure 2-11).
4. Click **Edit, Replace** from the menu. In the Replace dialog box, click the **Type** list arrow, and then click **Text String**, if necessary. In the Find text box, type `c:\`. In the Replace text box, type `a:\`, and then click **OK**.

5. In the Replace dialog box, click the **Replace All** button, and then click **OK**.

6. Click **Edit, Replace** from the menu. In the Find text box, delete the current text, and then type `.bin`. In the Replace text box, type `.zzz` (see Figure 2-12). Replacing .bin with .zzz prevents Io.sys from referencing DriveSpace. Note that the .zzz extension isn’t associated with any program; it’s used here simply to change .bin to something else.

7. Click **OK**. In the Replace dialog box, click the **Replace All** button, and then click **OK**.

8. Click **File, Save** from the menu to save your changes to Io.sys on the floppy disk. If a message is displayed asking whether you want to make a backup of Io.sys, click **No**.

9. Click **File, Exit** from the menu to close Hex Workshop. Restart your machine with the forensic boot floppy disk to test it.

10. Store your forensic boot floppy disk in a safe place.
Now you can use the floppy disk to boot a suspect’s computer without contaminating evidence on the hard disk. Next, you add forensic software to the floppy disk so that you can use it to acquire an evidence disk. The specific forensics software you add to your forensic boot floppy disk depends on the tools you have available. In the following steps, you copy the Digital Intelligence software tools to the forensic boot floppy disk:

1. Access the command prompt on your computer.
2. Navigate to the Tools folder in your work folder.
3. Place your forensic boot floppy disk in the floppy disk drive. You need both DriveSpy and Image on the boot disk.
4. At the command prompt, type `copy *.* a:` and press Enter.
5. Verify that the files have been copied to the floppy disk by typing `dir a:` and pressing Enter.
6. Exit the command prompt.

Now you should make a backup copy of this floppy disk. You can use the MS-DOS Diskcopy command or you can make an image copy with the Digital Intelligence Image utility. You need your original forensic boot floppy disk and an extra blank floppy disk. To make a duplicate disk with Diskcopy, follow these steps:

1. Insert the original forensic boot floppy disk in the floppy disk drive (for example, drive A:).
2. Access a command prompt. Type `diskcopy a: a: /v` and then press Enter.

**Figure 2-12** Replacing the file extension

Now you can use the floppy disk to boot a suspect's computer without contaminating evidence on the hard disk. Next, you add forensic software to the floppy disk so that you can use it to acquire an evidence disk. The specific forensics software you add to your forensic boot floppy disk depends on the tools you have available. In the following steps, you copy the Digital Intelligence software tools to the forensic boot floppy disk:

1. Access the command prompt on your computer.
2. Navigate to the **Tools** folder in your work folder.
3. Place your forensic boot floppy disk in the floppy disk drive. You need both **DriveSpy** and **Image** on the boot disk.
4. At the command prompt, type `copy *.* a:` and press Enter.
5. Verify that the files have been copied to the floppy disk by typing `dir a:` and pressing Enter.
6. Exit the command prompt.

Now you should make a backup copy of this floppy disk. You can use the MS-DOS Diskcopy command or you can make an image copy with the Digital Intelligence Image utility. You need your original forensic boot floppy disk and an extra blank floppy disk. To make a duplicate disk with Diskcopy, follow these steps:

1. Insert the original forensic boot floppy disk in the floppy disk drive (for example, drive A:).
2. Access a command prompt. Type `diskcopy a: a: /v` and then press Enter.
3. Follow the prompts to make the duplicate copy, inserting the blank formatted floppy disk when requested.

Use these steps to make an image copy of the forensics disk with the Image utility:

1. Insert the original forensic boot floppy disk in the floppy disk drive (for example, drive A).

2. Access a command prompt and navigate to the Tools folder located in your work folder, which is where you originally installed the DriveSpy and Image programs.

3. With the forensic floppy disk in the drive, type `image a: for_boot.dat` and press Enter.

4. When the command prompt is displayed, remove the forensic boot floppy disk and place the blank disk in the drive.

5. Type `image for_boot.dat a:` and press Enter to transfer the files to the new disk. You now have a copy of your forensic boot floppy on a disk and on your hard disk.

Retrieving Evidence Data Using a Remote Network Connection

If you’re working on a LAN, you can retrieve bit-stream image copies of disks through a workstation’s network connections. An older product called SnapBack originally made it possible to boot a suspect’s workstation with a specially configured boot floppy disk that had the appropriate network drivers to connect to a remote server. Other tools, such as EnCase v4, now offer the same feature as SnapBack. RT-Tools also allows remote imaging of a drive. Acquiring a bit-stream image over a LAN can be time consuming, even with a 1000-Mb connection. However, if you have a direct NIC-to-NIC connection with a twisted-pair network cable, you can acquire a bit-stream copy through a network connection in a reasonable amount of time. This feature is available in Guidance Software’s EnCase v3 or later.

Copying the Evidence Disk

After you retrieve and secure the evidence, you’re ready to copy the evidence disk and analyze the data. The first rule of computer forensics is to preserve the original evidence. Conduct your analysis only on a forensic copy of the original media. A forensic copy is an exact duplicate of the original data. To make a forensic copy of a floppy disk, you must create a bit-stream data copy of the disk using an MS-DOS command or a specialized tool, such as the Digital Intelligence Image utility.
Making a Bit-stream Copy of a Floppy Disk Using MS-DOS

One method of making a duplicate copy of your evidence floppy disk is to use the MS-DOS command Diskcopy with the verification switch /v, which verifies that the data is copied correctly. This command copies one floppy disk to another floppy disk. Its only disadvantages are that it does not create a separate image file of the original floppy disk and does not generate a hash value. Use the Diskcopy command only if you have no other tools available to preserve the original data. The Image tool gives you a reliable backup of your floppy disk evidence. It generates a verifiable hash value, but Diskcopy does not generate a hash value that’s admissible in court as proof of nontampering. This topic is covered at length in Chapter 6.

To make a bit-stream copy of a floppy disk, retrieve the floppy disk (the storage medium) from your secure evidence container, and write the appropriate information on your evidence custody form. Then complete the following steps at the DOS prompt on your forensics workstation to make a bit-stream copy of a floppy disk using MS-DOS:

1. Because the evidence floppy disk you retrieved from the IT manager is the original storage medium, you must write-protect the floppy disk. Move the write-protect tab on the floppy disk to the open position. (When working with multiple disks, be sure to specify in your working notes, on which disks you moved the write-protect tab. Some judges have required investigators to return the evidence to the owner in exactly the same condition in which it was seized which includes correct repositioning of the write-protect tabs.)

2. If necessary, boot your forensic workstation to the MS-DOS prompt.

3. Insert the evidence floppy disk into your workstation’s floppy disk drive (usually the A: drive). The original disk is your source disk.

4. At the MS-DOS prompt, type the command diskcopy a: a: /v and press Enter. Recall that the /v switch verifies that the data is copied correctly. You might be prompted to insert the source disk; if you are, insert the disk and press Enter.

5. After the disk is copied, you are prompted to place a target disk in the A: drive. This is where you want to store the copy of the evidence disk. Remove the evidence disk and insert a blank unformatted or formatted disk into the floppy drive. The software automatically overwrites everything. Follow the on-screen instructions and proceed with the data copy.

6. As the data is being copied to the target floppy disk, place the original floppy disk into your secure evidence container. When asked whether you want to create another duplicate of the disk, type n for no. When asked whether you want to copy another disk, type n for no.

7. Place a label on the working copy of the floppy disk, if necessary, and then write Domain Name working copy #1 on the label.
Always remember to maintain your chain of custody for your evidence.

In a live investigation, you should place the original floppy disk into your secure evidence container as the data is being copied to the target floppy disk.

**Acquiring a Bit-stream Copy of a Floppy Disk Using Image**

You can also make a bit-stream copy of a floppy disk using Digital Intelligence’s Image utility. This tool creates a file that contains every byte of data on a floppy disk, creating an image of the floppy disk rather than just a copy. The unique feature of this tool is that it preserves your data in a compact data file (also called an image file) on your disk. After you have created an image file of the floppy disk, you can transfer the forensic image to another floppy disk.

Although newer tools on the market can read directly from the image file, with most computer forensics tools, recall that the image file must be restored to a medium of the same size and type to access the data. In this way, working with image files is similar to restoring a file from a true backup utility that does not merely copy files.

When you use Image, you first acquire a bit-stream copy of a floppy disk and store that copy in a file on your hard disk. You complete this task in the following steps. After that, you’ll copy the file from your hard disk to a blank floppy disk, as shown in the following section.

As described earlier, in a live investigation, you first retrieve the original floppy disk or storage medium from your secure evidence container, and then fill out your evidence custody form before performing the following steps at your forensic workstation. Because the image file for this case is in your student data files, you don’t need to perform these steps. You can, however, practice the steps using one of your own disks. To acquire a bit-stream copy of a floppy disk using Image, follow these steps:

1. Write-protect the original floppy disk by moving the write-protect tab to the open position.
2. If necessary, boot your computer to MS-DOS command mode.
3. Insert the original floppy disk into your computer’s floppy disk drive, which is usually the A: drive. This is the source disk.
4. Change to the Tools folder. Run the Toolpath.bat file by typing `toolpath` and pressing **Enter**. The system should respond by echoing the path, including the newly added Tools folder.
5. At the command prompt, change to the Chap02\Chapter folder in your work folder on the hard disk by typing `cd c:\work folder\Chap02\Chapter` and then pressing **Enter**. This command assumes that your work folder is in the root directory and the Chap02 folder is in the work folder. Substitute the names of the folders you’re using on your computer, if needed.
6. To acquire data from the original evidence floppy disk, you need to be in the directory you intend to save the image to. Next, type the command `image a: Test.img` and then press Enter. If your disk is in a floppy drive other than A:, substitute that drive letter in the command. Replace `work folder` with the name of the work folder on your hard disk. If the drive letter of your hard disk is not C, substitute that drive letter for C. This command generates the bit-stream copy and stores it in the `work folder\Chap02\Chapter` folder.

7. Remove the original evidence floppy disk. In a live investigation, you would return the original disk to your secure evidence container.

You have now acquired the bit-stream copy of your evidence and stored it on your hard disk in a file called `Test.img`. The next step is to transfer the image of your evidence to a target disk such as a floppy disk to create a working copy.

**Making a Bit-stream Copy of Evidence Using Image**

Now that you have created a bit-stream image copy of your original evidence floppy disk, you must create a working copy of the disk, one that you can analyze without contaminating the evidence. When you transfer the contents of the image file you created in the previous steps to a different disk, Image uncompresses the image file and creates an exact duplicate of the disk, including slack space and free space on the disk. Slack space is the disk area between the end of a file and the allotted space for that file, and free space is any space on the drive not currently assigned to an existing file. (Both terms are covered in detail in Chapters 7 and 8.)

1. If necessary, boot your computer to Windows.

2. Using Windows Explorer or My Computer, find the `C2Chap01.img` file in your student data files.

3. Copy the `C2Chap01.img` file from your student data files to the `Chap02\Chapter` folder in your work folder on your hard disk.

4. Reboot your computer to MS-DOS mode.

   ![TIP](image)

   You can also access the MS-DOS prompt in a window if you’re using Windows 98 or from the command line if you’re using Windows 2000 or XP.

5. Change to the Tools folder. Run the Toolpath.bat file by typing in `toolpath` and pressing Enter. The system should respond by telling you the Tools folder has been added to the path.

6. At the MS-DOS prompt, change to the `work folder\Chap02\Chapter` directory, if necessary, by typing the command `cd c:\work folder\Chap02\Chapter` and pressing Enter.
7. Place a blank formatted floppy disk into your computer’s floppy disk drive (usually drive A:).

8. At the MS-DOS prompt, type the command `image C2Chap01.img a:` and then press Enter.

9. Place a label on the working copy of the floppy disk, if necessary, and then write `Domain Name working copy #2` on the label.

You have now created a working bit-stream copy of your original evidence floppy disk, which contains the same evidence as the original. Next you can analyze the working bit-stream copy of your evidence.

Creating a Bit-stream Image with FTK Imager

There are GUI tools you can use to make a bit-stream or forensic-quality image. The first one you use in this book is AccessData’s FTK Imager. Later in this chapter, you see how FTK Imager can convert images to other formats for use with other forensics tools.

In the previous exercise, you transferred the image for the in-chapter exercise to a floppy disk. This time you create a forensics disk image that other applications can read off this disk. Leaving the boot floppy disk in the drive, follow these steps:

1. Start FTK Imager by double-clicking the icon on your desktop.

2. Click File, Image Drive from the menu. Insert the floppy disk you labeled “Domain Name working copy #2.”

3. In the dialog box that opens, click the A: drive to select a local drive, and then click OK.

4. A wizard opens to walk you through the steps. Accept all the defaults. One of the steps asks you to specify the destination folder. If necessary, create a folder called Forensics Files. Name the file `Bootimage.1`.

   Note that FTK Imager creates two files: a Bootimage.1 file for the image and a Bootimage.txt file containing summary information for that file, including the MD5 hash value for verification.

5. Click Finish. After the image has been created, close FTK Imager.

Analyzing Your Digital Evidence

When you analyze digital evidence, your job is to recover the data. If users have deleted or overwritten files on a disk, the disk contains deleted files and file fragments in addition to complete files. Remember that as files are deleted, the space they occupied becomes free space—meaning it can be used for new files that a user saves. The files that were deleted are still on the disk until a new file is saved to the same physical location, overwriting the
original file. In the meantime, those files can still be retrieved. Most forensics tools can retrieve deleted files to be used as evidence.

To analyze digital evidence, in this chapter you use another MS-DOS tool from Digital Intelligence called DriveSpy, which is also a command-line tool. Then you use AccessData's Forensic Toolkit to read the image file directly. Note that in some instances you need to restore the forensic image to a physical drive to run software specific to the case, instead of generic software such as MS Office. (Be aware that applications such as the Forensic Toolkit start the associated programs. MS Office is considered a generic program in this instance because most people own it or StarOffice).

Overview of DriveSpy

DriveSpy is a powerful computer forensics tool compact enough to fit on a floppy disk. It recovers and analyzes data on FAT12, FAT16, and FAT32 disks, which are different formatting techniques Microsoft uses. DriveSpy logs all your actions and copies data from your forensic image disk. It searches for files that have been altered so that they appear to be a different format, and it searches for keywords of interest to your investigation. DriveSpy is designed to work from the DOS command prompt and has limited functionality from a Windows MS-DOS shell. It’s best to use DriveSpy from a workstation booted into MS-DOS. If you are running DriveSpy using MS-DOS version 6.22, DriveSpy can read disk drives larger than 8.4 GB and disk partitions larger than 2 GB. If you run DriveSpy in MS-DOS 7.0 or later, you can store recovered data in larger disk partitions. DriveSpy uses the following modes:

- **System mode**—DriveSpy operates at the workstation’s BIOS level and enables you to view and navigate to all disk drives connected to the computer.

- **Drive mode**—DriveSpy accesses the physical level of the disk drive. Use this mode when you need to examine a disk not formatted for MS-DOS or Windows 9x. Specifically, Drive mode lets you view the raw data on a disk. (Chapter 4 provides more details about DriveSpy Drive mode.)

- **Part (or Partition) mode**—DriveSpy refers to the logical level of the disk drive. At the logical level, you view the actual file structure of a disk—that is, the disk’s partition. In Part mode, DriveSpy can read MS-DOS and Windows 9x disks and shows the directory structures and files for FAT file systems. (FAT is covered in more detail in Chapter 7.)

DriveSpy extracts files and other raw data from a disk, including deleted files and fragments of deleted files that have been partially overwritten. DriveSpy can also generate an exact copy of a drive.

In this chapter, you have used Digital Intelligence’s Image, a special utility that creates an exact copy of a floppy disk. Image stores the data from a floppy disk in a compressed data file or a flat (noncompressed) file. Image also duplicates an evidence floppy disk on another floppy disk, which lets you preserve your original evidence. Recall that you should avoid working with the original medium. By creating a bit-by-bit copy, you can perform your
forensics examination on the duplicate floppy disk. Image is useless on large drives, however. As a result, there are several commands in the DriveSpy arsenal that can be used, such as the SavePart, SaveSect, and CopySect commands. The CopySect command enables you to save directly from one drive to another. (These commands are covered in Chapter 9.)

Using DriveSpy

Recall that you copied the DriveSpy files to the \Tools\folder earlier in this chapter. To start DriveSpy, the DriveSpy.exe file must be in the same folder as the DriveSpy.ini and DriveSpy.hlp files.

DriveSpy specifies drives by number, with the first drive being D0. Many systems have multiple partitions and multiple drives, which becomes important in your computer forensics lab where several drives might be connected to the same machine. Although DriveSpy identifies hard disks by number, it does not number the floppy disk and CD drives. With most versions of Windows (although Windows Me can present more challenges to use), you can start DriveSpy from Windows Explorer to access the DOS prompt. To prepare to analyze the bit-stream copy of your evidence disk, follow these steps:

1. Retrieve the forensic copy of your evidence disk (Domain Name working copy #2) from your evidence container, and write-protect the floppy disk by moving the tab to the open position.
2. Start your forensic workstation and boot into MS-DOS or to Windows 98.
3. Under the c:\work folder\Chap02\Chapter\ folder, use the DOS prompt or Windows Explorer to create two subfolders called copied and unerased.
4. To run the Toolpath.bat file created earlier, go to the \work folder\Tools folder (work folder is the name of your work folder); At the prompt, type toolpath.bat and press Enter. You return to a command prompt.
5. Insert the evidence disk you labeled “Domain Name working copy #2” into drive A: of your workstation.

Now you’re ready to start DriveSpy. To use DriveSpy to analyze the bit-stream copy of your evidence disk, leave the evidence disk in the floppy drive, and follow these steps:

1. At the MS-DOS prompt, type drivespy and then press Enter. The opening screen is shown in Figure 2-13. Note that DriveSpy provides a SYS prompt where you can type DriveSpy commands. You can use the DriveSpy Output command to log your actions, which you need for your final report for this examination. The log file keeps track of all the commands you use to obtain data from the forensic disk as well as all the output.
2. At the SYS> prompt, type the command outputc:\work folder\Chap02\Chapter\C2Chap01.log (substituting for work folder if needed) and then press Enter.
3. To access the floppy disk with DriveSpy, type drive a, and then press Enter.
4. DriveSpy changes to Disk mode and summarizes the disk information for the disk in drive A: (see Figure 2-14). Recall that Disk mode reads the physical level of the disk, and does not show file structures such as directories (or folders) and files.

5. To access Partition mode of the floppy disk, type `part 1` at the DA prompt, and then press Enter. Partition information is displayed, as shown in Figure 2-15, including the type of file system used on the disk, the number of sectors per cluster, the total sectors and clusters available in the partition, and its raw and formatted data storage capacity. The information also includes a useful map of where the start and end sectors are for the boot sector of the partition, the first and second FATs (FAT1 and FAT2), the root directory, and the data storage areas of the partition. Chapter 7 discusses these file structures in detail.
You have successfully explored the investigation disk that contains your evidence. Next, you can run basic commands to navigate to the DriveSpy folder and analyze and extract data from the evidence disk:

1. Restart DriveSpy by typing `drivespy` at the MS-DOS prompt and then pressing `Enter`.

2. At the DriveSpy SYS prompt (indicating System mode), create the log file where DriveSpy can record all the tasks you perform while working in DriveSpy. Type the command `outputc:\work folder\Chap02\Chapter\Ch2Chap02.log` and then press `Enter`, substituting the name of the work folder on your system if necessary.

3. At the DriveSpy SYS prompt, type `drive a` and press `Enter` to switch to Drive mode.

4. At the DA (Drive A) prompt, type `part 1` and press `Enter` to switch to Partition mode for the A: drive.

5. At the DAP1 (Drive A, Partition 1) prompt, type the command `dbexport c:\work folder\Chap02\Chapter\C2Chap01.txt` and then press `Enter`, substituting the name of the work folder on your system if necessary. The Dbexport command creates a text file with the name you specify, such as C2Chap01.txt. This text file contains all the entries of directories and files listed in the FAT and is useful in identifying what's on the evidence disk. You can also open this text file in a word processing, spreadsheet, or database program to sort and search for information.

Figure 2-15  Accessing the Partition mode of a disk

6. Type `q` and then press `Enter` to exit DriveSpy.

You have successfully explored the investigation disk that contains your evidence. Next, you can run basic commands to navigate to the DriveSpy folder and analyze and extract data from the evidence disk:

1. Restart DriveSpy by typing `drivespy` at the MS-DOS prompt and then pressing `Enter`.

2. At the DriveSpy SYS prompt (indicating System mode), create the log file where DriveSpy can record all the tasks you perform while working in DriveSpy. Type the command `outputc:\work folder\Chap02\Chapter\Ch2Chap02.log` and then press `Enter`, substituting the name of the work folder on your system if necessary.

3. At the DriveSpy SYS prompt, type `drive a` and press `Enter` to switch to Drive mode.

4. At the DA (Drive A) prompt, type `part 1` and press `Enter` to switch to Partition mode for the A: drive.

5. At the DAP1 (Drive A, Partition 1) prompt, type the command `dbexport c:\work folder\Chap02\Chapter\C2Chap01.txt` and then press `Enter`, substituting the name of the work folder on your system if necessary. The Dbexport command creates a text file with the name you specify, such as C2Chap01.txt. This text file contains all the entries of directories and files listed in the FAT and is useful in identifying what's on the evidence disk. You can also open this text file in a word processing, spreadsheet, or database program to sort and search for information.
6. Next, you copy all the allocated data from the evidence disk. Allocated data is data not deleted from the disk. At the DriveSpy prompt, enter the command `copy *.* /s c:\work folder\Chap02\Chapter\copied` (replacing the italicized text if necessary), and then press Enter. The recursive `/s` switch copies all the allocated files in any subdirectories that might exist on the evidence disk to the Chap02 folder in your work folder. If a message appears asking whether you want to view the results in page mode because they might be lengthy, press Y. (Note: Do not press Enter because it generates an error message.)

7. To copy all deleted files from the evidence disk, type the command `unerase *.* /s c:\work folder\Chap02\Chapter\unered` (replacing the italicized text if necessary), and then press Enter. If a message appears asking whether you want to view the results in Page mode because they might be lengthy, press Y. (Note: Do not press Enter because it generates an error message.)

8. At the command prompt, type `q` to exit DriveSpy, and type `exit` to close the command-prompt window.

DriveSpy locates all the deleted files on the evidence disk that have not been overwritten. That is, it searches the FAT for all files in which the filename starts with the MS-DOS delete symbol of a lowercase sigma (σ). Then DriveSpy copies the contents of the deleted files to the specified location, such as the Chap02 folder in your work folder. To analyze the data, follow these steps:

1. Reboot your machine to Windows mode.
2. Use Windows Explorer or My Computer to open the floppy disk, and note how many files it contains.
3. Right-click the first file and then click Properties. In the General tab of the Properties dialog box for the file, note the Created, Modified, and Accessed dates and times. List the filename and properties in a separate document or sheet of paper. Put an asterisk next to any times that are during George’s working hours (8 a.m. to 5 p.m.). Then close the Properties dialog box. Note the properties for each file on the disk.
4. Open each file. In a separate document or on a sheet of paper, note what each file contains, and then close any open windows.
5. Use Windows Explorer or My Computer to open the `work folder\Chap02\Chapter` folder and examine the contents. You should see several files in addition to the log and text files. These are the deleted files DriveSpy retrieved.
6. In Notepad, open `C2Chap01.txt` and examine the contents. Depending on your system, you might see the sigma symbol (σ) to represent deleted files or a question mark (?) at the beginning of the filename. Close Notepad.
7. Examine the contents of the deleted files. Determine whether they contain information about George’s own business and his whereabouts.
8. In Windows Explorer or My Computer, right-click each file and examine the Created, Modified, and Accessed dates and times in the file’s Properties dialog box. Record your findings in a separate document or sheet of paper.

You should find evidence that proves George was working on his own business during company work hours.

Overview of Forensic Toolkit

AccessData’s Forensic Toolkit (FTK) is an easy-to-use GUI application, even for first-time users. FTK is part of a suite of tools that includes FTK Imager, the Registry Viewer, and the Password Recovery Toolkit. With this arsenal, you can usually solve most cases. FTK reads FAT12, FAT16, FAT32, and NTFS files.

Using Forensic Toolkit

FTK (either the demo or licensed version) should be loaded on your lab machine. Earlier you created an image of the boot floppy disk. In this exercise, you use it to become acquainted with FTK. To analyze the data, follow these steps:

1. Start FTK. You should see the opening window shown in Figure 2-16.

   ![Figure 2-16 The opening window for FTK](image)

2. Click **Start a new case**, and then press **Enter** or click **OK**.

3. In the New Case dialog box (see Figure 2-17), type your name in the Investigator Name text box.

4. In the Case Number text box, type **C2-3**, and in the Case Name text box, type **Boot**.

5. Click the **Browse** button next to the Case Path text box, and select your Chapter 2 work folder. Notice that FTK adds your case name to the end of the location and creates that subfolder for you.

6. Click **Next** in all the remaining dialog boxes until you arrive at the Add Evidence dialog box (see Figure 2-18).

7. Click the **Add Evidence** button, and then verify that the Acquired Image of Drive option button is selected (see Figure 2-19). Click the **Continue** button.
Figure 2-17  The New Case dialog box

Figure 2-18  The Add Evidence dialog box
8. Click to select **Bootimage.1** and click **Open**. In the Evidence Information dialog box, click **OK**.

9. Click **Next** to get to the Case Summary dialog box shown in Figure 2-20, and then click **Finish**.

10. When FTK finishes, explore some of the buttons in this dialog box, such as **Executables and Total File Items** (see Figure 2-21).

11. Close FTK.
After you analyze a disk, you can retrieve deleted files and e-mail, items that have been purposefully hidden, and much more, which you do later in this book. The files on George’s floppy disk indicate that he was doing outside work on the company’s machine.

Now that you have retrieved and analyzed the evidence, you need to find the answers to the following questions to write the final report:

- How did George’s manager acquire the disk?
- Did George perform the work on a laptop, which is his own property? If so, did he perform his business transactions on his break or during his lunch hour?
- At what times of the day was George using the non-work-related files? How did you retrieve that information?
- Which company policies apply?
- Are there any other items that need to be considered?

When you write your report, state what you did and what you found. The log file DriveSpy generates gives you a historical account of all the steps you have taken. As part of your report, depending on guidance you have from your management or legal counsel, include the DriveSpy log file to document your work. In any computing investigation, you should be able to repeat your steps and achieve the same results. Without this ability, your work product has no value as evidence.
Keep a written journal of everything you do. Your notes can be used in court, so be mindful of what you write or e-mail, even to a fellow investigator. Often these journals start out as handwritten notes, but you can transcribe the notes to electronic format periodically.

Basic report writing involves answering the six Ws: who, what, when, where, why, and how. In addition to these basic facts, you must also explain computer and network processes. Typically, your reader will be a senior personnel manager, a lawyer, or, on rare occasions, a judge and might have little computer knowledge. Identify your reader and write the report for that person. Provide explanations for processes, the inner workings of systems and their components, and how they work.

Your organization might have predefined templates to use when writing reports. Depending on your organization’s needs and requirements, your report must describe the findings from your analysis. The log file generated by DriveSpy lists all your activity in the order you performed your examination and data recovery. Integrating a computer forensics log report will augment your formal report. Consider writing your narrative first and then placing the log output at the end of the report, using references to the log report on your fact-findings. Writing technical reports for your investigations is covered in more detail in Chapter 14.

In the Domain Name case, you would want to show conclusive evidence that George had his own business that registered other people’s domain names and would provide the names of his clients and his income from this business. You would also want to show letters he wrote to clients about their accounts. The time and date stamps on the files are during work hours. As the investigator, you eventually hand the evidence file to your supervisor or to Steve, George’s boss. They then decide on a course of action.

CRITIQUING THE CASE

After you close the case and make your final report, you need to meet with your department or a group of fellow investigators and critique the case. Ask yourself critical questions such as the following:

- How could you improve your participation in the case?
- Did you expect the results you found? Did the case develop in ways you did not expect?
- Was the documentation as thorough as it could have been?
- What feedback has been received from the requesting source?
- Did you discover any new problems? If so, what are they?
- Did you use new techniques during the case or during research?

Make notes to yourself in your journal about techniques or processes that might need to be changed or addressed in future investigations. Then store your journal in a secure place.
CHAPTER SUMMARY

- Always use a systematic approach to your investigations. Determine the type of problem you are dealing with, create a preliminary plan, choose your resources, perform a risk analysis, and then implement the plan.

- When planning a case, take into account the nature of the case, the instructions from the requester, what additional tools and expertise you might need, and how you will acquire the evidence.

- Criminal cases and corporate-policy violations should be handled in much the same manner to ensure that quality evidence is presented. Both criminal cases and corporate-policy violations can go to court.

- When you begin a case, apply standard problem-solving techniques, such as defining the problem, designing a solution, and carrying out that solution.

- You should create a standard evidence custody form to track the chain of custody of the evidence related to your case. There are two types of forms—a multi-evidence form and a single-evidence form.

- Always maintain a journal to make notes on exactly what you did when handling evidence.

- An image file is a bit-by-bit duplicate of the original disk. You should use the duplicate whenever possible.

- DriveSpy and Image are command-line forensic tools that can retrieve existing files, deleted files, and file fragments.

- You can create bit-stream copies of files by using the Diskcopy DOS utility or the Image tool.

- In completing a case, describe what you did, how you did it, and what you found.

- You should always critique your own work to determine what improvements you made during each case, what could have been done differently, and how to apply those lessons to future cases.

KEY TERMS

allocated data — Data on a drive that has not been deleted or written over.

approved secure container — A fireproof container that is locked by key or combination.

bit-stream copy — A bit-by-bit copy of the data on the original storage medium.

bit-stream image — The file used to store the bit-stream copy.

chain of custody — The route evidence takes from the time the investigator obtains it until the case is closed or goes to court.
Computer forensics workstation — A workstation set up to allow copying of forensic evidence, whether on a hard drive, floppy, CD, or Zip disk. It usually has various software preloaded and ready to use.

Data recovery lab — An alternate name for a computer forensics lab.

Evidence bag — A nonstatic bag used to transport floppy disks, hard drives, and other computer components.

Evidence custody form — A printed form indicating who has signed out and been in physical possession of evidence.

Evidence floppy disk — The original disk on which electronic evidence was found.

Forensic copy — An exact copy of an evidence disk used during the actual investigation.

Free space — Space on a drive that is not reserved for saved files.

Image file — A file created by the Image tool from Digital Intelligence.

Multi-evidence form — An evidence custody form used to list all items associated with a case. See also single-evidence form.

Password-cracking software — Software used to match the hash patterns of passwords or simply guess the words by using common combinations or standard algorithms.

Password protected — Files and areas of any storage media can have limited access by requiring a password to prevent unintentional use.

Personal digital assistant (PDA) — One of several pocket-sized computers that store addresses, notes, and calendars. One popular brand is Palm.

Single-evidence form — A form that dedicates a page for each item retrieved for a case. It allows the investigator to add more detail about exactly what was done to the evidence each time it was taken from the storage locker. See also multi-evidence form.

Slack space — Space on a disk between the end of a file and the allotted space for that file.

Review Questions

1. List the five standard steps of computer investigations.
2. Digital Intelligence’s Image tool is:
   a. a GUI tool
   b. a command-line tool
   c. a Linux tool
   d. none of the above
3. A bit-stream image is the same as a backup copy. True or False?
4. List three items that should be on an evidence custody form.
5. What is involved in planning an investigation?
6. You should always prove the allegations made by the person who hired you. True or False?
7. An evidence bag is typically made of nonstatic material. True or False?
8. What is the command you use in Digital Intelligence’s Image to copy an image of a disk from your hard drive to a working forensic floppy disk?

9. Who should have access to a secure container?
   a. only the primary investigator
   b. only the investigators in the group
   c. everyone on the floor
   d. only senior-level management

10. Typically, the Image tool creates a file with what extension?

11. Why should your evidence disk be write-protected?

12. Why should you be familiar with command-line software?

13. What does the Drive A (DA) command in DriveSpy do?
   a. accesses the hard drive
   b. accesses the CD-ROM
   c. accesses the floppy disk drive
   d. accesses the secondary hard drive

14. List three items that should be in your case report.

15. Why should you critique your case after it is done?

16. The Image utility is developed by:
   a. Microsoft
   b. Digital Intelligence
   c. Norton
   d. Symantec

17. Diskcopy is:
   a. a utility by AccessData
   b. a standard MS-DOS command
   c. a Digital Intelligence utility
   d. none of the above

18. To access Partition mode information in DriveSpy, you type:
   a. D1
   b. Part 1
   c. Drive A
   d. Partition1
Chapter 2  Understanding Computer Investigations

19. The Unerase command in DriveSpy does which of the following?
   a. retrieves allocated files
   b. retrieves partial files
   c. retrieves deleted files that have not been written over
   d. is not a valid command

20. What do you call a list of the people who have had physical possession of the evidence?

H A N D S - O N  P R O J E C T S

In the following Hands-on Projects, continue to work at the workstation you set up in this chapter.

Project 2-1

In this project, the case involves a murder investigation. You use the Image tool to copy an image file to a blank floppy disk. Assume that the image is a verified copy of a data disk. You now need to copy it to a blank target disk, using the following steps:

1. In Windows Explorer, navigate to the Chap02 folder in your work folder. Create a new subfolder called Projects.
2. In the student data files, find the file named C2Prj01.img in the Chap02\Projects folder. Copy the file to the Chap02\Projects folder in your work folder.
3. Insert a blank, formatted floppy disk in the floppy disk drive.
4. Open a command-prompt window by clicking Start, pointing to Programs, and then clicking MS-DOS Prompt.
5. Navigate to the Chap02\Projects folder in your work folder.
6. Type image C2Prj01.img a: and press Enter. This command copies an exact image of a disk contained in the C2Prj01.img file to the disk in drive A. If Image does not start, you might need to run the Toolpath.bat file created earlier in the chapter.
7. Type exit to close the command-prompt window.
8. Use Windows Explorer to view the files you copied to the floppy disk. In a separate document or on a sheet of paper, list these files.
9. Start DriveSpy.
10. Type drive a and press Enter to access the floppy disk. To capture the screen, press the PrtScr key to save a copy of the screen to the Clipboard. (Your PrtScr key...
might have a different name, such as Print Screen.) Open a word processing pro-
gram, such as WordPad, open a new document, and then press Ctrl+V to paste the
screen image into the document. Print the document and give it to your instructor.

11. In the command-prompt window, type part 1 and press Enter to access the Parti-
tion mode. Capture the screen and print a copy of it, as in Step 10.

12. Type q to exit DriveSpy.

13. List four items or terms you saw and write their definitions in a separate document
or on a sheet of paper. Refer to the Digital Intelligence Web site at www.digitalintel.
com, if necessary.

14. Examine the files you retrieved from the image. In what way could they be con-

ected to a murder? What other information would you need?

15. Write one to two paragraphs summarizing how you would approach this case.

**Project 2-2**

In this project, you practice making and restoring image files. You restore the image to a
floppy disk, create an image of the disk, and then restore it to another disk. Follow these steps
to use DriveSpy to compare two disks:

1. Copy C2Prj02a.img from the student data files to the Chap02\Projects folder in
your work folder.

2. Open a command-prompt window by clicking Start, pointing to Programs, and
then clicking MS-DOS Prompt.

3. If you have not run Toolpath.bat during this session at the computer, change to the
Tools folder by typing cd c:\work folder\tools from the root and then pressing
Enter. Type toolpath.bat and press Enter to make the Image program available in
your current directory. Then change to the Chap02\Projects folder in your work
folder.

4. Label a blank, formatted floppy disk Project 2-2 Disk1 and insert it in the floppy
disk drive.

5. At the DOS command prompt, type image C2Prj02a.img a: and press Enter.
This places the files sector by sector on the floppy disk.

6. Start Windows Explorer, navigate to the Chap02\Projects folder in your work folder,
and note the files that are listed.

7. With the same floppy disk in the drive, at the command prompt, create a new image
by typing image a: C2Prj02b.img and pressing Enter.

8. Label a blank, formatted floppy disk Project 2-2 Disk2 and insert the second disk
in the floppy disk drive.

9. At the DOS command prompt, type image C2Prj02b.img a: and press Enter.

10. Create two subfolders in the Projects folder called Disk1 and Disk2.
11. Leaving the second floppy disk in the drive, start DriveSpy by typing `drivespy` in the C:\`work folder\Chap02\Projects area of your work folder and pressing Enter. Type `drive a` and press Enter, then type `part 1` and press Enter to access the DAP1> prompt.

12. Create a log file for Disk2 by typing the command `outputc:\work folder\Chap02\Projects\Disk2\C2Prj02.log` and then pressing Enter.

13. Next, use the Dbexport command by typing the command `dbexport c:\work folder\Chap02\Projects\Disk2\C2Prj02.txt` and then pressing Enter.

14. Copy all the allocated files to the Disk2 folder by typing the command `copy *.* /S c:\work folder\Chap02\Projects\Disk2` and then pressing Enter. If prompted to disable Page mode, press Y, but don’t press Enter afterward because it generates an error message.

15. Type the command `unerase *.* /S c:\work folder\Chap02\Projects\Disk2`, and then press Enter to retrieve all deleted files. If prompted to disable Page mode, press Y.

16. Replace Disk2 with Disk1 and repeat Steps 12 to 15 for Disk1.

17. When you finish, type q to exit DriveSpy and exit to close the command-prompt window.

18. Use Windows Explorer to compare the two folders and their files. In a word processing document or on a sheet of paper, list the files each folder contains and note any discrepancies.

**Project 2-3**

In this project, you see the problems of using DriveSpy in a DOS shell, or command-prompt window, by attempting to use the Wipe command to overwrite unallocated space on a specified drive with zeroes. This helps ensure that data on a disk does not change during transportation, analysis, or storage. For this project, use a floppy disk that contains files you no longer need and follow these steps in a command-prompt window:

1. In the floppy disk drive, insert a formatted floppy disk containing files you no longer need.

2. Open a command-prompt window.

3. If necessary, navigate to the `work folder\Tools folder`.

4. To start DriveSpy, type `drivespy` and press Enter.

5. Type `drive a` and press Enter, and then type `part 1` and press Enter to access the Partition mode of the floppy disk in your drive.

6. Type `wipe /free` and press Enter. You use the /free switch to specify that DriveSpy should overwrite unallocated disk space with zeroes. An error message is displayed stating that “Windows is running; the Wipe command has been disabled.”
7. Exit DriveSpy, and then close the command-prompt window.
8. Reboot your machine to MS-DOS mode.
9. If necessary, navigate to the work folder\Tools folder, and start DriveSpy.
10. At the SYS> prompt, type drive a and then press Enter. Type part 1 and then press Enter to access the Partition mode of the disk.
11. Type wipe /free and press Enter. When asked if you are sure you want to wipe the disk, type Y. Wipe displays the number of unallocated sectors on the floppy disk and then wipes the disk (in other words, fills the unallocated sectors with zeros so that the sectors can’t contain any other data).
12. Exit DriveSpy, and then reboot to Windows.

**Project 2-4**

In this project, you explore the Drivespy.ini file, which is a critical file for using the program.

1. Start Notepad.
2. Click File, Open from the menu. In the Open dialog box, navigate to the work folder\Tools folder.
3. Click the Files of type list arrow, and then click All Files (*.*).
4. Double-click the DriveSpy.ini file to open it.
5. Click File, Print from the menu. Make sure you are connected to a printer, and then click OK to print the file. Refer to the printed copy of this file as you write a report in the following steps.
6. In a separate Notepad document, list the parts of the DriveSpy.ini file—those areas that are in square brackets, such as [License].
7. In the [File Headers] section, select six file types with which you are unfamiliar. In your report, answer the following questions:
   - Is the application still in use today?
   - If so, what version?
   - If not, what applications can still open the file type? For example, WordStar documents can be opened in Microsoft Word.
   - If you needed more information about the application, who in your area would know? Which user groups could you ask?
Project 2-5

In this project, you take an image created with Digital Intelligences Image utility, restore it to a floppy disk, and then use FTK Imager to create a *.1 file for use in FTK.

1. Obtain a blank floppy disk, and then open a DOS prompt on your machine.
2. Change to the Tools folder and run Toolpath.bat.
3. Change to the directory containing the files for this chapter, such as C:\Chap02. You should have a file from your student data disk called C2prj05.img. If you don’t, copy it from your data disk to this location.
4. Restore the image to the blank floppy disk by typing image C2Prj05.img a: and pressing Enter. After it has finished, close the command-prompt window.
5. Restart, if necessary, to get to the area where FTK and FTK Imager are located.
7. Click File, Image Drive from the menu to open a dialog box listing the local drives. Click the A: drive and then click OK.
8. Make sure the destination folder is C:\Chap02 and the filename is C2Prj05. Keep all the default settings until you reach the final window, and then click Finish. When the process is finished, close FTK Imager.
9. Start FTK, and click the Start a new case option button.
10. In the New Case dialog box, type in your name as the investigator. Type C2-5 for the case number and test conversion for the case name. Click OK.
11. Click Next, leaving all the defaults until you reach the Add Evidence dialog box. Click the Add Evidence button, click the Acquired Image of Drive option button, and then click Continue. In the dialog box that opens, click the file you just generated.
12. Click Next again to continue to the Case Summary dialog box, and then click Finish.
13. When FTK has finished, try exploring the files. After you’re done, close FTK.

Project 2-6

In this project, you use FTK to examine a forensic disk image and look for existing and deleted files.

1. Start FTK.
2. Start a new case.
3. Type your name as the investigator.
4. Assign a case number of C2-6 and a case name of Shakespeare.
5. Click Next in all the dialog boxes, accepting the default settings.
6. In the Add Evidence to Case dialog box, click the Add Evidence button, click the Individual File option button, and click to select the C2Prj06.1 file from your student data files.

7. Click Open, click OK, and click Next to get to the Case Summary dialog box, and click Finish.

8. After FTK has finished, click the Documents button under File Category. Notice in the lower pane that two of the documents have a red X next to them. They are files that have been deleted.

9. You can click each file and see a preview of it. In Chapter 7, you see how to start the associated programs, such as Microsoft Word, for each file.

10. Close FTK.

Case Projects

Case Project 2-1
An insurance company has assigned your firm to review a case for an arson investigation. The suspected arsonist has already been arrested, but the insurance company wants to determine whether there’s any contributory negligence on the part of the victims. Review the synopsis of the case (refer to the ArsonMemo.doc file in your student data files), and decide what course of action your firm needs to take. Write an outline for how your firm should approach the case.

Case Project 2-2
A young girl is missing after having an argument with her parents. They call the police on May 28. A police investigator shows up the next day to interview them. The officer finds out that the daughter had spent a lot of time on the Internet. The parents agree to let him take her laptop. What should happen next?

Case Project 2-3
Jonathan Simpson owns a construction company. One day a subcontractor calls him, saying that he needs a replacement check for the job he completed at 1437 West Maple Avenue. Jonathan looks up the job on his accounting program and agrees to reissue the check for $12,750.00. The subcontractor says that the original check was for only $10,750.00. Jonathan looks around the office and cannot find the company checkbook or ledger. Only one other person has access to the accounting program. Jonathan calls you to investigate. How would you proceed? Write a one-page report detailing the steps Jonathan needs to take to obtain the necessary evidence and protect his company.
Case Project 2-4

You are the computer forensics investigator for a law firm. The firm acquired a new client, a young woman who was discharged from her job for inappropriate material discovered on her computer. She swears she never accessed that material. What questions should you ask and how should you proceed? Write a one to two-page report detailing the computer the new client could access, who else had access to it, and any other relevant facts that should be investigated.

Case Project 2-5

A desperate employee calls because she has accidentally deleted crucial files from her hard drive and cannot retrieve them from the Recycle Bin. What are your options? Write one to two pages in response that explain your capabilities and list the questions you need to ask her about her system.