UNIT-III

FORENSICS ANALYSIS AND VALIDATION

Determining What Data to Collect and Analyze

Examining and analyzing digital evidence depend on the nature of the investigation and the amount of data to process. Criminal investigations are limited to finding data defined in the search warrant, and civil investigations are often limited by court orders for discovery. Corp.- rate investigators might be searching for company policy violations that require examining only specific items, such as e-mail. Therefore, investigations often involve locating and recovering a few specific items, which simplifies and speeds processing.

In the corporate environment, however, especially if litigation is involved, the company attar- nay often directs the investigator to recover as much information as possible. Satisfying this demand becomes a major undertaking with many hours of tedious work. These types of invest- ligations can also result in scope creep, in which an investigation expands beyond the original description because of unexpected evidence you find, prompting the attorney to ask you to examine other areas to recover more evidence. Scope creep increases the time and resources needed to extract, analyze, and present evidence. Be sure to document any requests for add- tonal investigation, in case you must explain why the investigation took longer than planned, why the scope widened during the course of the investigation, and so forth.

One reason scope creep has become more common is that criminal investigations increasingly require more detailed examination of evidence just before trial to help prosecutors fend off attacks from defense attorneys. Because defense attorneys typically have the right of full discovery of digital evidence used against their clients, it's possible for new evidence to come to light while complying with the defense request for full discovery. However, this new evidence often isn't revealed to the prosecution; instead, the defense uses it to defend the accused. For this reason, it's become more important for prosecution teams to ensure that they have analyzed the evidence exhaustively before trial. (It should be noted that the defense request for full discovery applies only to criminal cases in the however, depends on whether it's an internal corporate investigation or a civil or criminal investigation carried out by law enforcement. In an internal investigation, evidence collection tends to be fairly easy and straightforward because corporate investigators usually have ready access to the necessary records and files. In contrast, when investigating a criminal cyber- stalking case, you need to contact the ISP and e-mail service.

Some companies, such as AOL, have a system set up to handle these situations, but others do not. Many companies don't keep e-mail for longer than 90 days, and some keep it only two weeks.

An employee suspected of industrial espionage can require the most work. You might need to set up a small camera to monitor his or her physical activities in the office. You might also need to plant a software or hardware key logger (for capturing a suspect's keystrokes remotely), and you need to engage the network administrator's services to monitor Internet and network activities. In this situation, you might want to do a remote acquisition of the employee's drive, and then use another tool to determine what peripheral devices have been accessed.

1. For target drives, use only recently wiped media that have been reformatted and inspected for computer viruses. For example, use ProDiscover Secure Wipe Disk, Digital Intelligence PDWipe, or White Canyon Secure Clean to clean all data from the target drive you plan to use.

2. Inventory the hardware on the suspect's computer and note the condition of the computer when seized. Document all physical hardware components as part of your evidence acquisition process.

3. For static acquisitions, remove the original drive from the computer, if practical, and then check the date and time values in the system's CMOS.

4. Record how you acquired data from the suspect drive note, for example, that you created a bit-stream image and which tool you used. The tool you use should also create an MD5 or SHA-1 or better hash for validating the image.

5. When examining the image of the drive's contents, process the data methodically and logically. List all folders and files on the image or drive. For example, FTK can generate a Microsoft Access database listing all files and folders on a suspect drive. Note where specific evidence is found, and indicate how it's related to the investigation.

6. If possible, examine the contents of all data files in all folders, starting at the root directory of the volume partition. The exception is for civil cases, in which you look for only specific items in the investigation.

7. For all password-protected files that might be related to the investigation, make your best effort to recover file contents. You can use password recovery tools for this purpose, such as Access Data Password Recovery Toolkit (PRTK), NTI Password Recovery, or Pass ware Kit Enterprise

1. Identify the function of every executable (binary or .exe) file that doesn't match known hash values. Make note of any system files or folders, such as the System32 folder or its content, that are out of place. If you can't find information on an executable file by using a disk editor, examine the file to see what it does and how it works.

1. Maintain control of all evidence and findings, and document everything as you progress through your examination. ps to locate specific message Refining and Modifying the Investigation Plan In civil and criminal cases, the scope is often defined by search warrants or subpoenas, which specify what data you can recover. However, private sector cases, such as employee abuse investigations, might not spec- ify limitations in recovering data. For these cases, it's important to refine the investigation plan as much as possible by trying to determine what the case requires. Generally, you want the investigation to be broad enough to encompass all relevant evidence, yet not so wide-ranging that you waste time and resources analyzing data that's not going to help yourcase.

Of course, even if your initial plan is sound, at times you'll find that you need to deviate from the plan and follow where the evidence leads you. Even in these cases, having a plan that you deliberately revise along the way is much better than searching for evidence haphazardly.

Suppose, for example, an employee is accused of operating an Internet-based side business using company resources during normal business hours. You use this timeframe to narrow the set of data you're searching, and because you're looking for unauthorized Internet use, you focus the search on temporary Internet files, Internet history, and e-mail communicate- ion. Knowing the types of data you're looking for at the outset helps you make the best use of your time and prevents you from casting too wide a net. However, in the course of reviewing e-mails related to the case, you might find references to spreadsheets or Word documents containing financial information related to the side business. In this case, it makes sense to broaden the range of data you're looking for to include these types of files. Again, the key is to start with a plan but remain flexible in the face of new evidence.

Using Access Data Forensic Toolkit to Analyze Data

So far, you have used several different features of FTK; this section goes into more detail on its search and report functions. FTK can perform forensics analysis on the following file systems:

- Microsoft FAT12, FAT16, and FAT32

- Microsoft NTFS (for Windows NT, 2000, XP, and Vista)
- Linux Ext2fs and Ext3fs

FTK can analyze data from several sources, including image files from other vendors. It can also read entire evidence drives or subsets of data, allowing you to consolidate large volumes of data from many sources when conducting a computer forensics analysis. With FTK, you can store everything from image files to recovered server folders on one investigation drive.

FTK also produces a case log file, where you can maintain a detailed record of all activities during your examination, such as keyword searches and data extractions. This log is also handy for reporting errors to Access Data. At times, however, you might not want the log feature turned on. If you're following a hunch, for example, but aren't sure the evidence you recover is applicable to the investigation, you might not want opposing counsel to see a record of this information because he or she could use it to question your methods and perhaps discredit your testimony. (Chapter 15 covers testimony issues in more detail.) Look through the evidence first before enabling the log feature to record searches. This approach isn't meant to conceal evidence; it's a precaution to ensure that your testimony can be used in court.

FTK has two options for searching for keywords. One option is an indexed search, which catalogs all words on the evidence drive so that FTK can find them quickly. This option returns search results quickly, although it does have some shortcomings. For example, you can't search for hexadecimal string values, and depending on how data is stored on the eve- dense drive, indexing might not catalog every word. If you do use this feature, keep in mind that indexing an image file can take several hours, so it's best to run this process overnight.

The other option is a live search, which can locate items such as text hidden in unallocated space that might not turn up in an indexed search. You can also search for alphanumeric and hexadecimal values on the evidence drive and search for specific items, such as phone numbers, credit card numbers, and Social Security numbers. Figure 9-1 shows the hits found during a live search of an image of a suspected arsonist's laptop. You can right-click a search hit to add it to your bookmarks, which includes the result in your final report.

Validating Forensic Data

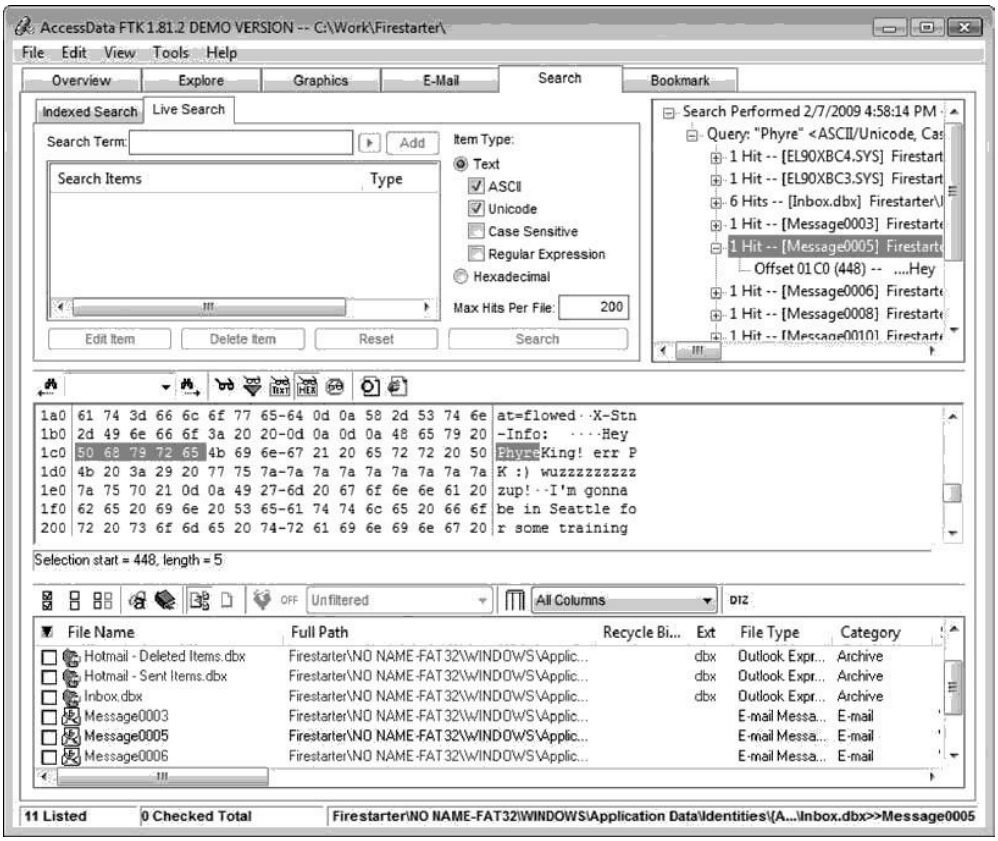

Fig: Validating Forensic Data

One of the most critical aspects of computer forensics is validating digital evidence because ensuring the integrity of data you collect is essential for presenting evidence in court. Chapter 5 introduced forensic hashing algorithms, and in this section, you learn more about validating an acquired image before you analyze it.

Most computer forensic tools such as ProDiscover, X-Ways Forensics, FTK, and Encase provide automated hashing of image files. For example, when ProDiscover loads an image file, it runs a hash and compares that value to the original hash calculated when the image was first acquired. You might remember seeing this feature when the Auto Image Checksum Verification message box opens after you load an image file in ProDiscover. Computer foren- sics tools have some

limitations in performing hashing, however, so learning how to use advanced hexadecimal editors is necessary to ensure data integrity.

Validating with Hexadecimal Editors

Advanced hexadecimal editors offer many features not available in computer forensics tools, such as hashing specific files or sectors. Learning how to use these tools is important, especially when you need to find a particular file—for example, a known contraband image. With the hash value in hand, you can use a computer forensics tool to search for a suspicious file that might have had its name changed to look like an innocuous file. (Recall that two files with exactly the same content have the same hash value, even if they have different names.) Getting a hash value with a full-featured hexadecimal editor is much faster and easier than with a computer forensics tool.

Addressing Data-Hiding Techniques

Data hiding involves changing or manipulating a file to conceal information. Data-hiding techniques include hiding entire partitions, changing file extensions, setting file attributes to hidden, bit-shifting, using encryption, and setting up password protection. Some of these techniques are discussed in the following sections.

Hiding Partitions

One way to hide partitions is to create a partition and then use a disk editor, such as Norton Disk Edit, to delete any reference to it manually. To access the deleted partition, users can edit the partition table to re-create the links, and then the hidden partition reappears when the computer is restarted. Another way to hide partitions is with a disk-partitioning utility, such as G Disk, Partition Magic, System Commander, or Linux Grand Unified Boot loader (GRUB), which provides a startup menu where you can select an OS. The system then ignores other bootable partitions.

To circumvent these techniques, be sure to account for all disk space when you're examining an evidence drive. Analyze any disk areas containing space you can't account for so that you can determine whether they contain additional evidence. For example, in the following code, Disk Manager recognizes the extended partition (labeled EXT DOS) as being 5381.1 MB

(listed as Mbytes). The LOG DOS labels for partitions E through F indicate that they're logical partitions that make up the extended partition. However, if you add the sizes of drives E and F, the result is only 5271.3 MB, which is your first clue to examine the disk more closely. The remaining 109.8 MB could be a previously deleted partition or a hidden partition. For this example, the following code shows the letter ―H‖ to indicate a hidden partition. Disk Partitions Cylinders Heads Sectors Mbytes Sectors 2 5111661663 5495.8 11255328

Partition	Status	Type	Volume Label	Mbytes	System	Usage
D:	1		PRI DOS	109.8	FAT16	2%
	2		EXT DOS	5381.1		98%
E:	3		LOG DOS	109.8	FAT16	2%
	4	H	LOG DOS	109.8	FAT16	2%
F:	5		LOG DOS	5161.5	FAT32	94%

Windows creates a partition gap between partitions automatically; however, you might find a gap that's larger than it should be. For example, in Windows 2000/XP, the partition gap is only 63 sectors, so 109.8 MB is too large to be a standard partition gap. In Windows Vista, the gap is approximately 128 sectors.

In Figure, you can see a hidden partition in Disk Manager, which shows it as an unknown partition. In addition, the drive letters in the visible partitions are nonconsecutive (drive I is skipped), which can be another clue that a hidden partition exists. Most skilled users would make sure this anomaly doesn't occur, however.

Fig: Viewing a hidden partition in Disk Manager

In ProDiscover, a hidden partition appears as the highest available drive letter set in the BIOS. Figure 9-9 shows four partitions, similar to Figure 9-8, except the hidden partition shows as the drive letter Z. To carve (or salvage) data from the recovered partition gap, you can use other computer forensics tools, such as FTK or WinHex.

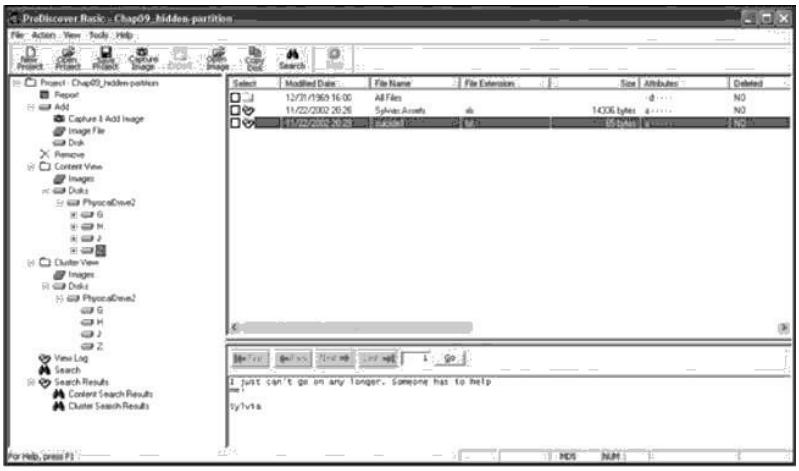

Fig: Viewing a hidden partition in ProDiscover

Marking Bad Clusters

Another data-hiding technique, more common in FAT file systems, is placing sensitive or incriminating data in free or slack space on disk partition clusters. This technique involves using a disk editor, such as Norton Disk Edit, to mark good clusters as bad clusters. The OS then considers these clusters unusable. The only way they can be accessed from the OS is by changing them to good clusters with a disk editor.

Bit-Shifting

Some home computer users developed the skill of programming in the computer manufacturer's assembly language and learned how to create a low-level encryption program that changes the order of binary data, making the altered data unreadable when accessed with a text editor or word processor. These programs rearrange bits for each byte in a file. To secure a file containing sensitive or incriminating information, these users run an assembler program (also called a macro) on the file to scramble the bits. To access the file, they run another program that

restores the scrambled bits to their original order. Some of these pro- grams are still used today and can make it difficult for investigators to analyze data on a suspect drive.

Start Notepad, and in a text document, type TEST FILE. Test file is to see how shifting bits will alter the data in a file.

Save the file as Bit_shift.txt in your work folder, and exit Notepad.

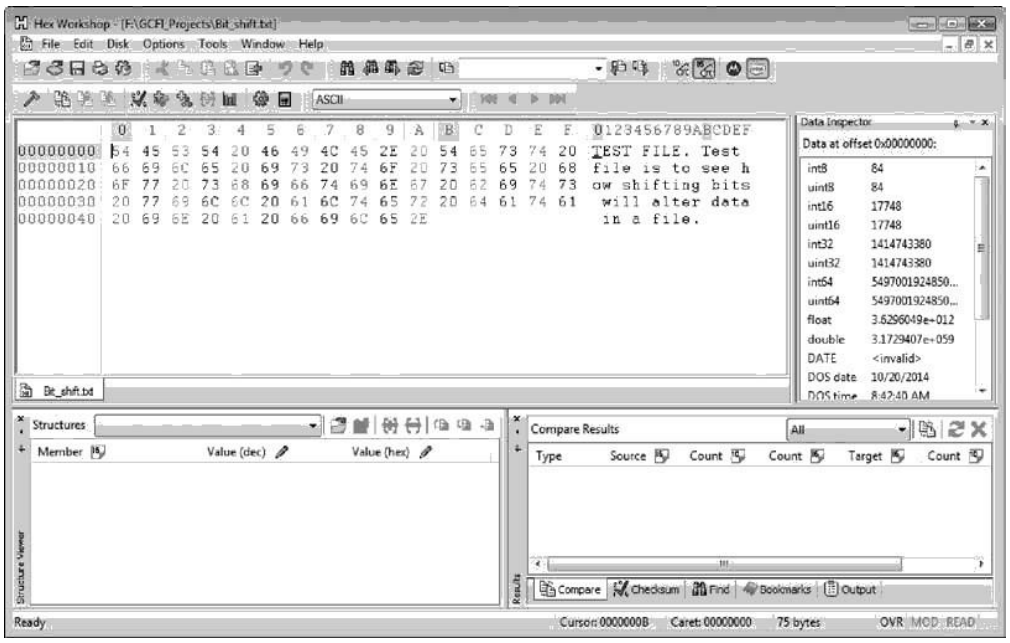

Fig: Hex workshop

Start Hex Workshop. Click File, Open from the menu. Navigate to your work folder, and then double-click Bit_shift.txt. Bit_shift.txt open in Hex Workshop.

To set up Hex Workshop for the bit-shifting exercise, click Options, Toolbars from the menu.

In the Customize dialog box, click the Data Operations check box, and then click OK.

Click the Shift Left button (<< icon) on the Data Operations toolbar. The Shift Left Operation dialog box opens, where you specify how you want to treat the data, the ordering scheme to use for bytes, and whether you shift bits for selected text or the entire file.

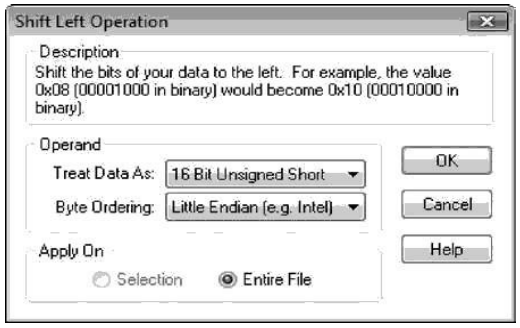

Fig: The Shift Left Operation dialog box

1. Click OK to accept the default settings and shift the bits in Bit_shift.txt to the left.

2.Save the file as Bit_shift_left.txt in your work folder. above Figure shows thefile in Hex Workshop, with the @ symbols indicating shifted bits.

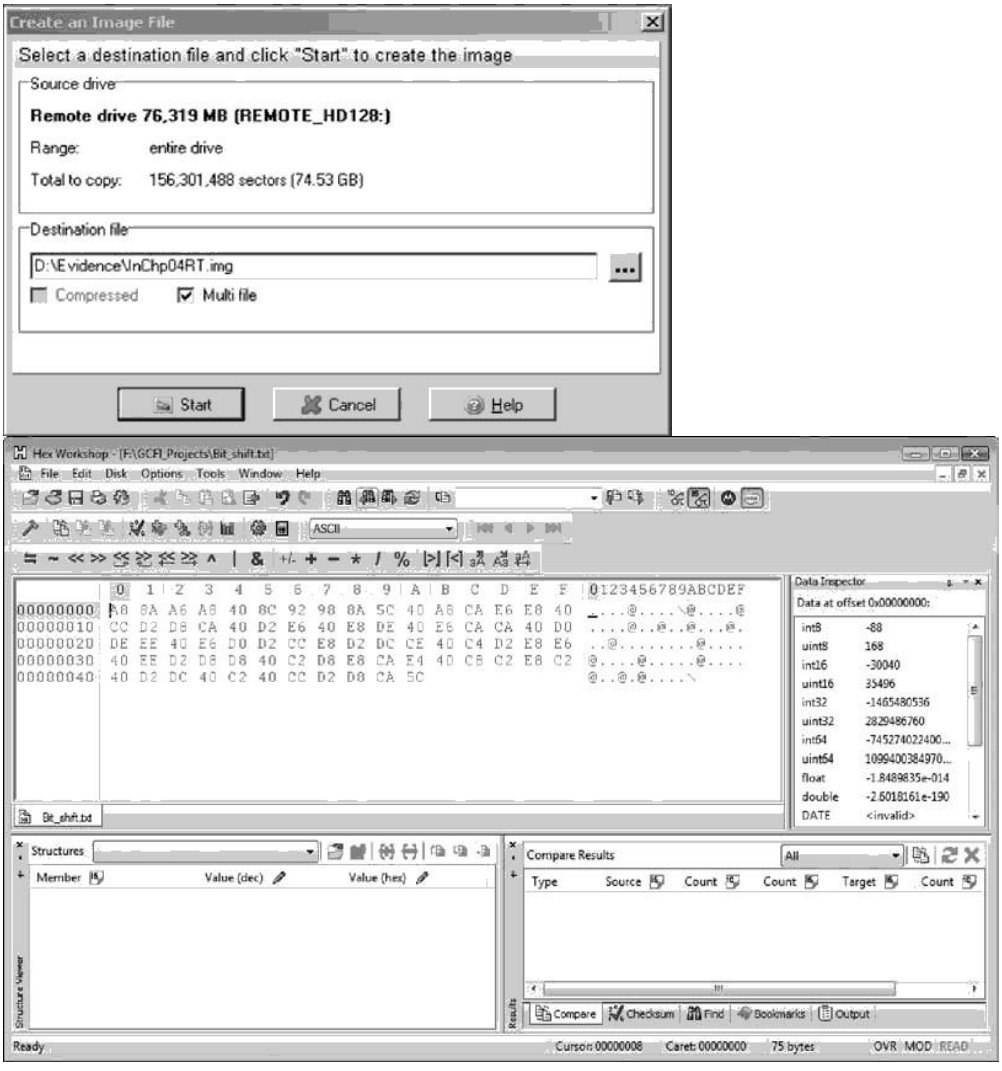

Fig:Viewing the shifted bits

1. To return the file to its original configuration, shift the bits back to the right by clicking the Shift Right button (>> icon) on the Data Operations toolbar. Click Ok to accept the default settings in the Shift Right Operation dialog box. The file is displayed in its original format.

2. Save the file as Bit_shift_right.txt in your work folder, and leave Hex Workshop open for the next activity. Now you can use Hex Workshop to find the MD5 hash values for these three files and determine whether Bit_shift.txt is different from Bit_shift_right.txt and Bit_shift_left.txt. (You could also use FTK or ProDiscover to find the MD5 hash values.) To check the MD5 values in Hex Workshop, follow thesesteps:

1. With Bit_shift_right.txt open in Hex Workshop, click File, Open to open Bit_shift.txt, and then repeat to open Bit_shift_left.txt.

2. Click the Bit_shift.txt tab in the upper pane to make it the active file.

3. Click Tools, Generate Checksum from the menu to open the Generate Checksum dialog box. In the Select Algorithms list box, click MD5, and then click the Generate button. Copy the MD5 hash value of Bit_shift.txt, shown in the lower-right pane, and paste it in a new text document in Notepad.

4. Repeat Steps 2 and 3 for Bit_shift_left.txt and Bit_shift_right.txt, pasting their hash values in the same text file in Notepad.

5. Compare the MD5 hash values to determine whether the files are different. When you're finished, exit Notepad and Hex Workshop.

Typically, antivirus tools run hashes on potential malware files, but some advanced malware uses bit-shifting as a way to hide its malicious code from antivirus tools. With the bit-shifting functions in Hex Workshop, however, you can inspect potential malicious code manually. In addition, some malware that attacks Microsoft Office files consists of executable code that's embedded at the end of document files, such as Word documents, and hidden with bit- shifting. When an Office document is opened, the malware reverses the bit-shifting on the executable code and then runs it.

Performing Remote Acquisitions

Remote acquisitions are handy when you need to image the drive of a computer far away from your location or when you don't want a suspect to be aware of an ongoing investiga- tion. This method can save time and money, too. Many tools are available for remote acquisi- tions; in the following sections, you use Runtime Software to learn how remote acquisitions are made.

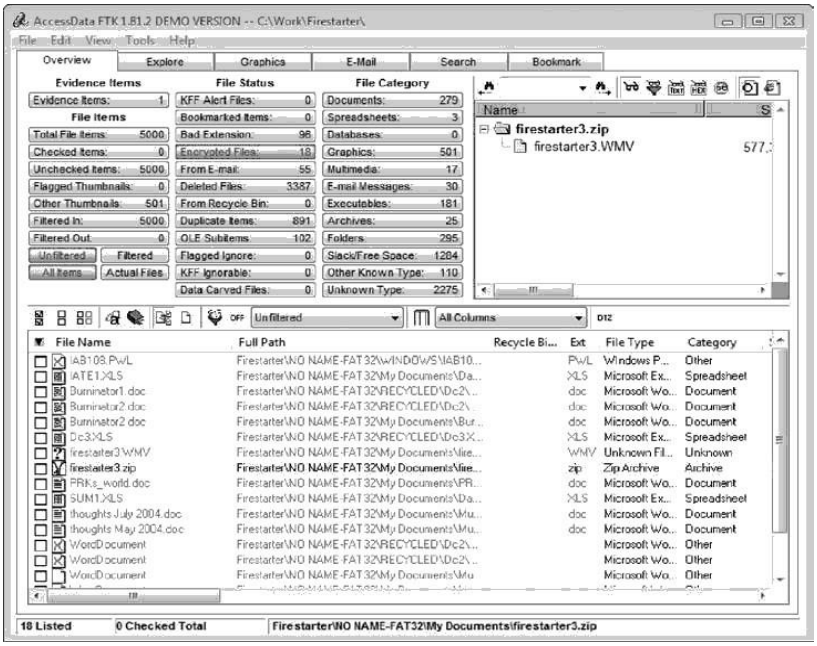

Fig: FTK displaying encrypted files

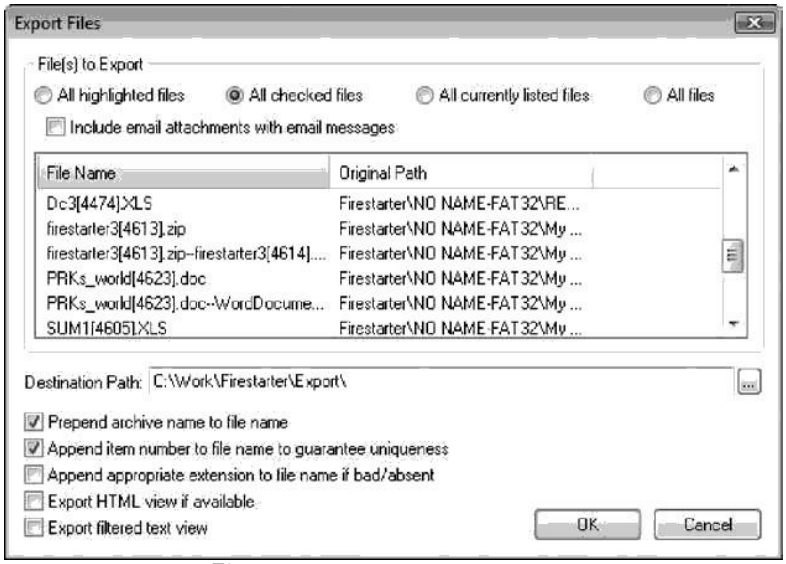

Fig: Exporting encrypted files

Remote Acquisitions with Runtime Software

Runtime Software (*www.runtime.org*) offers the following shareware programs for remote acquisitions:

DiskExplorer for FAT

- DiskExplorer for NTFS
- HDHOST

Chapter 4 introduced these tools; remember that they're designed to be file system specific, so there are DiskExplorer versions for both FAT and NTFS that you can use to create raw format image files or segmented image files for archiving purposes.

HDHOST is a remote access program for communication between two computers. The connection is established by using the DiskExplorer program (FAT or NTFS) corresponding to the suspect (remote) computer's file system. The following sections show how to make a live remote acquisition of another computer over a network. To use these tools, it's best to have computers connected on the same local hub or router with minimal network traffic.

Network Forensics Overview

Network forensics is the process of collecting and analyzing raw network data and tracking network traffic systematically to ascertain how an attack was carried out or how an event occurred on a network. Because network attacks are on the rise, there's more focus on this field and an increasing demand for skilled technicians. Labor forecasts predict a shortfall of 50,000 network forensics specialists in law enforcement, legal firms, corporations, and universities.

Network forensics can also help you determine whether a network is truly under attack or a user has inadvertently installed an untested patch or custom program, for example. A lot of time and resources can be wasted determining that a bug in a custom program or an untested open-source program caused the –attack.

Network forensics examiners must establish standard procedures for how to acquire dataafter an attack or intrusion incident. Typically, network administrators want to find compromised.

Securing a Network

Network forensics is used to determine how a security breach occurred; however, steps must be taken to harden networks before a security breach happens, particularly with recent increases in network attacks, viruses, and other security incidents. Hardening includes a range of tasks, from applying the latest patches to using a layered network defense strategy, which sets up layers of protection to hide the most valuable data at the innermost part of the network. It also ensures that the deeper into the network an attacker gets, the more difficult access becomes and the more safeguards are in place. The National Security Agency (NSA) developed a similar approach, called the defense in depth (DiD) strategy. DiD have three modes of protection:

- People
- Technology
- Operations

If one mode of protection fails, the others can be used to thwart the attack. Listing people as a mode of protection means organizations must hire well-qualified people and treat them well so that they have no reason to seek revenge. In addition, organizations should make sure employees are trained adequately in security procedures and are familiar with the organize- tion's security policy. Physical and personnel security measures are included in this mode of protection. The technology mode includes choosing strong network architecture and using tested tools, such as intrusion detection systems (IDSs) and firewalls. Regular penetration testing coupled with risk assessment can help improve network security, too. Having systems in place that allow quick and thorough analysis when a security breach occurs is also part of the technology mode of protection.

Performing Live Acquisitions

The problem investigators face is the order of volatility (OOV), meaning how long a piece of information lasts on a system. Data such as RAM and running processes might exist for only milliseconds; other data, such as files stored on the hard drive, might last for years. The following steps show the general procedure for a live acquisition, although investigators differ on exact steps:

- Create or download a bootable forensic CD, and test it before using it on a suspect drive. If the suspect system is on your network and you can access it remotely, add the appropriate network forensics tools to your workstation. If not, insert the bootable forensics CD in the suspect system.
- Make sure you keep a log of all your actions; documenting your actions and reasons for these actions is critical.
- A network drive is ideal as a place to send the information you collect. If you don't have one available, connect a USB thumb drive to the suspect system for collecting data. Be sure to note this step in your log.
- Next, copy the physical memory (RAM). Microsoft has built-in tools for this task, or you can use available freeware tools, such as mem fetch (*www.freshports.org/sysutils/ memfetch*) and Back Track (discussed in the following section).
- The next step varies, depending on the incident you're investigating. With an intrusion, for example, you might want to see whether a rootkit is present by using a tool such as Root Kit Revealer (*www.microsoft.com/technet/sysinternals/Utilities/ RootkitRevealer.mspx*). You can also access the system's firmware to see whether it has changed, create an image of the drive over the network, or shut the system down and make a static acquisition later.
- Be sure to get a forensically sound digital hash value of all files you recover during the live acquisition to make sure they aren't altered later.

Performing a Live Acquisition in Windows

Live acquisitions are becoming more necessary, and several tools are available for capturing RAM. ManTech Memory DD (*www.mantech.com/msma/MDD.asp*) can access up to 4 GB RAM in standard did format. Another freeware tool, Win32dd (*http://win32dd.msuiche.net*), runs from the command line to perform a memory dump in Windows. In addition, comer- coal tools, such as Guidance Software Winen.exe, can be used.

Another popular tool is Backtrack (*www.remote-exploit.org/backtrack.html*), which com- bines tools from the White Hat Hackers CD and The Auditor CD (see Figure 11-3). More than 300 tools are available, including password crackers, network sniffers, and freeware for- entices tools. Backtrack has become popular with penetration testers and is used at the annual Collegiate Cyber Defense Competitions.

Fig:Some of the tools available in BackTrack

Developing Standard Procedures for Network Forensics

Network forensics is a long, tedious process, and unfortunately, the trail can go cold quickly. A standard procedure often used in network forensics is as follows:

- Always use a standard installation image for systems on a network. This image isn't a bit-stream image but an image containing all the standard applications used. You should also have the MD5 and SHA-1 hash values of all application and OS files.
- When an intrusion incident happens, make sure the vulnerability has been fixed to prevent other attacks from taking advantage of the opening.
- Attempt to retrieve all volatile data, such as RAM and running processes, by doing a live acquisition before turning the system off.
- Acquire the compromised drive and make a forensic image of it.

- Compare files on the forensic image to the original installation image. Compare hash values of common files, such as Win.exe and standard DLLs, and ascertain whether they have changed.

In computer forensics, you can work from the image to find most of the deleted or hidden files and partitions. Sometimes you restore the image to a physical drive so that you can run programs on the drive. In network forensics, you have to restore the drive to see how mal- ware attackers have installed on the system works. For example, intruders might have trans- mitted a Trojan program that gives them access to the system and then installed a root kit, which is a collection of tools that can perform network reconnaissance tasks (using the ls or net stat command to collect information, for instance), key logging, and other actions.

Using Network Tools

A variety of tools are available for network administrators to perform remote shutdowns, monitor device use, and more. The tools covered in this chapter are freeware and work in Windows and UNIX. Sysinternals (*www.microsoft.com/technet/sysinternals/*) is a collection of free tools for examining Windows products. They were created by Mark Russinovich and Bryce Cogs well and acquired by Microsoft.

Fig: Opening page of Sysinternals

As you can see in above Figure, you can choose from file and system, networking, process, and security tools, among others. The following list describes a few examples of the powerful Windows tools available at Sysinternals:

- RegMon shows all Registry data in real time.
- Process Explorer shows what files, Registry keys, and dynamic link libraries (DLLs) are loaded at a specific time.
- Handle shows what files are open and which processes are using these files.
- Filemon shows file system activity.

Far too many tools are available to list here, but you should take some time to explore the site and see what's available. One in particular that's worth investigating is PsTools, a suite created by Sysinternals that includes the following tools:

- *PsExec*—Runs processes remotely
- *PsGetSid*—Displays the security identifier (SID) of a computer or user
- *PsKill*—Kills processes by name or process ID
- *PsList*—Lists detailed information about processes
- *PsLoggedOn*—Displays who's logged on locally
- *PsPasswd*—Allows you to change account passwords
- *PsService*—Enables you to view and control services
- *PsShutdown*—Shuts down and optionally restarts a computer
- *PsSuspend*—Allows you to suspend processes

Understanding Rules of Evidence

Consistent practices help verify your work and enhance your credibility, so you must handle all evidence consistently. Apply the same security and accountability controls for evidence in a civil lawsuit as in a major crime to comply with your state's rules of evidence or with the Federal Rules of Evidence. Also, keep in mind that evidence admitted in a criminal case might also be used in a civil suit, and vice versa. For example, suppose someone is charged with murder and acquitted at

the criminal trial because the jury isn't convinced beyond a reasonable doubt of the person's guilt. If enough evidence shows that the accused's negligence contributed to a wrongful death, however, the victim's relatives can use the evidence in a civil lawsuit to recover damages.

As part of your professional growth, keep current on the latest rulings and directives on col- lecting, processing, storing, and admitting digital evidence. The following sections discuss some key concepts of digital evidence. You can find additional information at the U.S. Department of Justice Web site (*www.usdoj.gov*) and by searching the Internet for –digital evidence,| –best evidence rule,| –hearsay,| and other relevant keywords. Consult with your prosecuting attorney, Crown attorney, corporate general counsel, or the attorney who retained you to learn more about managing evidence for your investigation. DVD to your work folder. The work folder path shown in screenshots might differ slightly from yours.

- Start Microsoft Word, and in a new document, type By creating a file, you can identify the author with file metadata. Save it in your work folder as InChp05-01. doc, and then exit Microsoft Word.
- To start FTK, click Start, point to All Programs, point to Access Data, point to Forensic Toolkit, and click Forensic Toolkit. If you're prompted with a warning dialog box and/or notification, click OK to continue, and click OK, if necessary, in the message box thanking you for evaluating the program.
- Click Go directly to working in program, and then click OK. Click File, Add Evidence from the menu.
- In the Add Evidence dialog box, enter your name as the investigator, and then click Next. In the Evidence Processing Options dialog box, accept the default setting, and then click Next.
- In the main Add Evidence to Case dialog box, click the Add Evidence button. In the next Add Evidence to Case dialog box, click the Individual File option button, and then click Continue.
- In the Browse for Folder dialog box, navigate to your work folder, click

- InChp05-01.doc, click Open, and then click OK. Click Next, and then click Finish.
- In the main window, click the Overview tab, if necessary. Under the File Category heading, click the Documents button. Click to select the InChp05-01.doc file in the bottom pane; its contents are then displayed in the upper-right pane. Figure shows an example (although the filename in this figure is different).

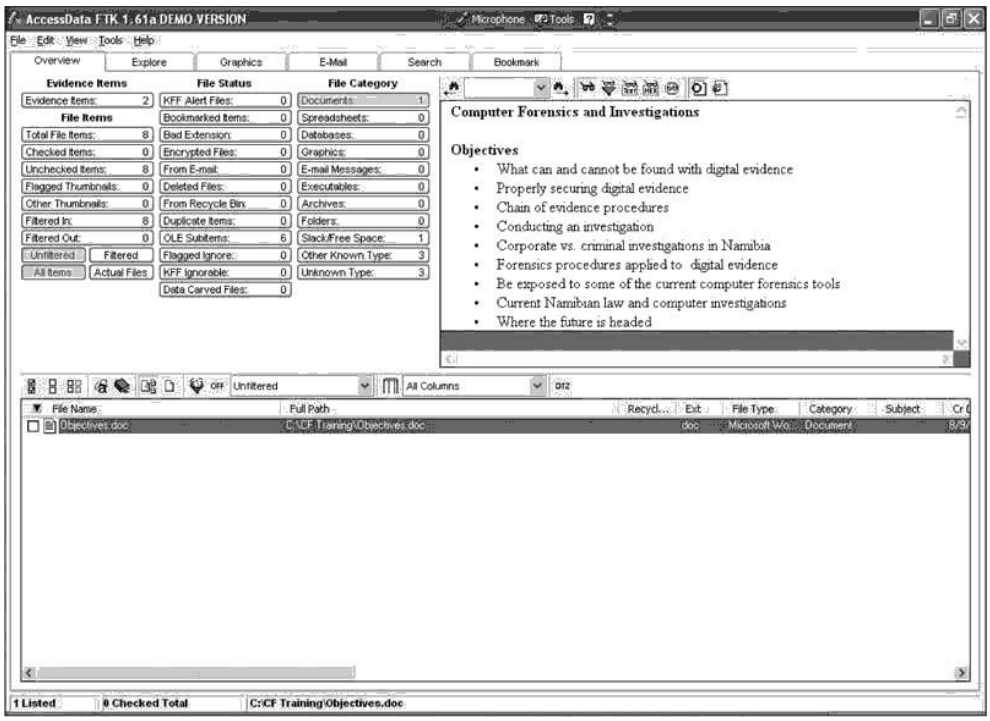

Fig: Selecting a document

- On the File List toolbar at the upper right, click the View files in native format button, if the button isn't already selected. (*Hint*: Hover your mouse over buttons to see their names displayed.)
- Next, click the View files in filtered text format button. If you entered your username and organization when you installed Word, that information is displayed (see Figure 5-2).

10. Exit FTK, clicking No if prompted to back up your work.

11. In addition to revealing the author, computer-stored records must be proved authentic, which is the most difficult requirement to prove when you're trying to qualify evidence as an exception to the hearsay rule. The process of establishing digital evidence's trustworthiness originated with written documents and the best evidence rule, which states that to prove the content of a written document, recording, or photograph, ordinarily the original writing, recording, or photograph is required (see Federal Rules of Evidence, 1002). In other words, the original of a document is preferred to a duplicate. The best evidence, therefore, is the document created and saved on a computer's hard disk.