7 Data Analysis

LEARNING OBJECTIVES

After reading this chapter, you will be able to:

- Understand the concept of data analysis.
- Understand the process of data analysis in Windows and UNIX system.
- Interpret and apply tools for data analysis.
- Distinguish different methods for data analysis.

Digital forensic is an exact science – not the procedures, but the results.

—Edewede Oriwoh

7.1 Preparation Steps for Forensic Analysis

In data analysis technique, we demonstrate how to find out the data and organize all of the pieces of computer media and integrate them. After integrations of all media and data, the data analysis phase takes place. In order to make the data usable, resides in forensic duplicates and qualified forensic duplicates of hard drives, additional planning may be required. In the next section, it has been explained how to restore duplicate image and how to start analysis phase for Linux and Windows operating systems.

7.1.1 Restoring a Forensic Duplicate

It can be tricky to restore forensic duplication. It is necessary that one should have a hard disk of greater capacity than the actual driver. Hard drive duplication is an important part of data acquisition process. Extracting files directly from a potential failing media is dangerous, because media can stop working any time. It is not only more preferable that the drive should be of equal capacity, but it is also necessary that the drive is from the same manufacturer. Due to this, the operator can transfer data quickly and easily from the original hard disk to the backup hard disk.

The Atola Insight Forensic is the industry's most efficient system for imaging hard disk, SSDs, and USB mass storage media quickly and safely (Fig. 7.1). The maximum imaging speed of system is MB/s.

Scanned by CamScanner

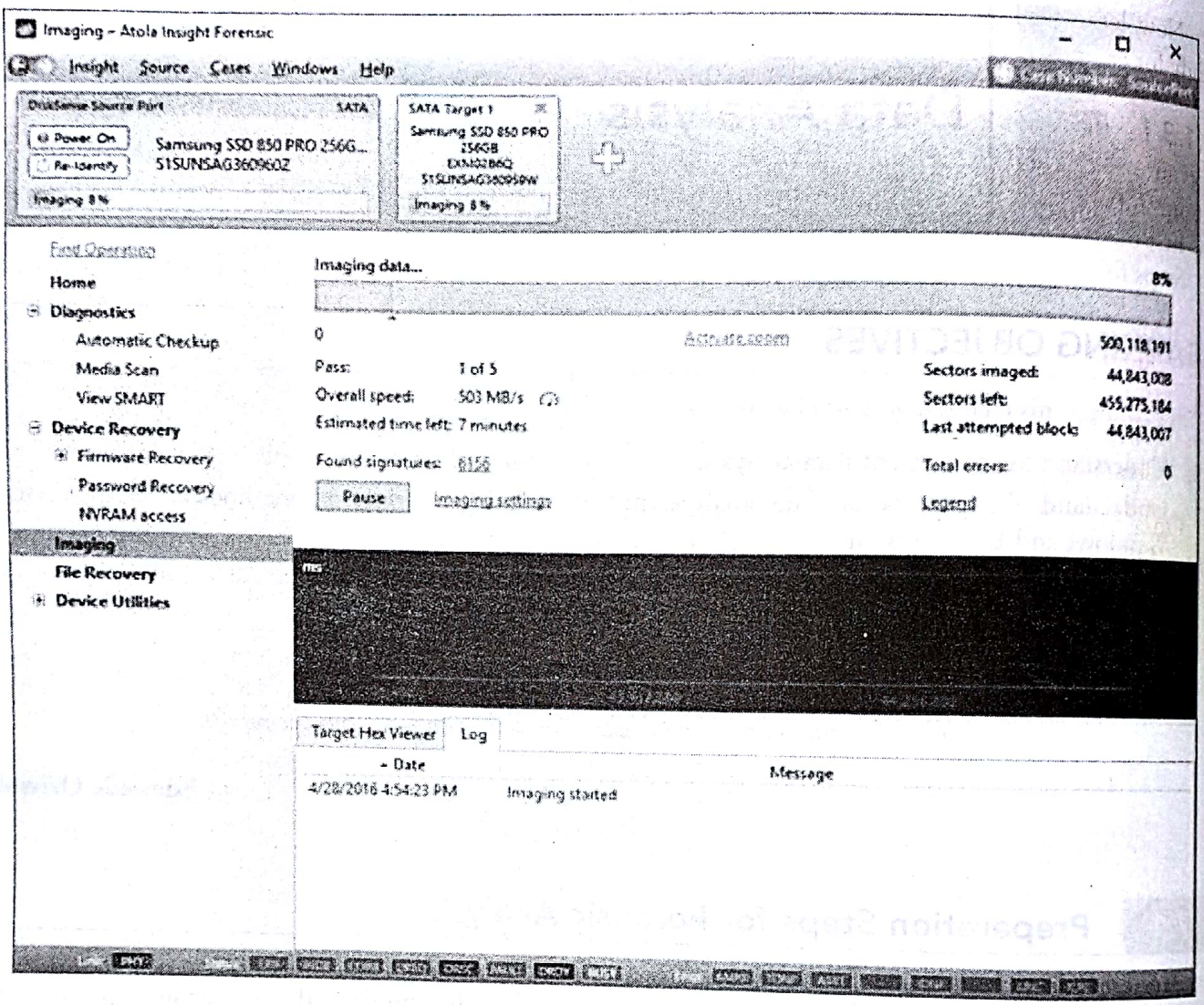

Figure 7.1 Imaging hard disk using Atola Insight Forensic.

7.1.2 Preparing a Forensic Duplication for Analysis in Linux

Linux is an ideal forensic duplication for analysis environment. The set of patches and tools provided by NASA Computer Crime Division (NCCD) can also be utilized. Large number of file systems and partition types can be interpreted by Linux. The user may need to enable number of option and recompile the kernel, if he/she wants to take advantage of its capabilities.

Red Hat can be used to perform analysis. The set of patches and tools provided by NCCD will be required in addition to the complete Red Hat version 8 and 7. This will allow the system to recognize multiple partitions by modifying kernel and loop playback mounting the code within a forensic duplication image. This allows you to identify any duplicate file without storing it on another hard disk drive.

7.1.3 Reviewing Image Files with Forensic Suites

It is basically a straightforward process. When a user is working with Encase or forensic toolkit (FTK), it is a strategic process while creating a new case and populating it with forensic. When a segment forensic duplicate image is being imported by a user, he/she might face various minor difficulties.

Scanned by CamScanner

Now, let us see how to initiate a case in these two surroundings and import the segmented replica to get ready for examination.

7.1.3.1 Reviewing Forensic Duplicates in Encase

It is an easy method to restore and analyze dd files, Safe Back files, and also Encase evidence files, with its strong suite of tools and easy-to-use interface. A new case must be created while acquiring an evidence for the first time.

Steps for creating Encase:

1. Download Encase
2. Choose a file
3. New
4. New case
5. "Create New" dialog box will appear

Once a new case is created, file can be added in that case by the user. Figure 7.2 shows adding a new dd image file to your case.

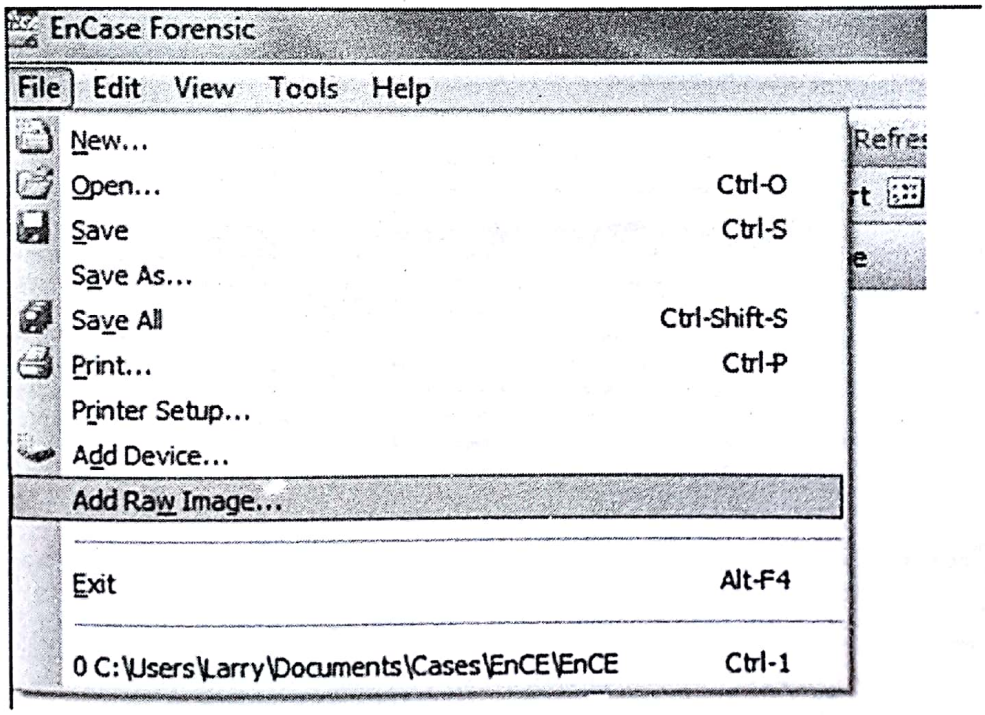

Figure 7.2 Selecting a raw image file to import into EnCase.

As we can see in Fig. 7.3, "an: Add Raw Image" dialog box is being displayed by Encase, when a user choose to dd a raw image. Here, the user needs to select the disk for dd image file that composes the raw image in proper order.

As seen in Figure 7.4, a powerful Window explorer-type interface, presented by Encase, displays all the content of raw image file once the dd files are added to the case successfully. From this stage onwards, user can use Encase suite of tools to perform almost all the preparation required to analyze the data in an effective and efficient manner.

Scanned by CamScanner

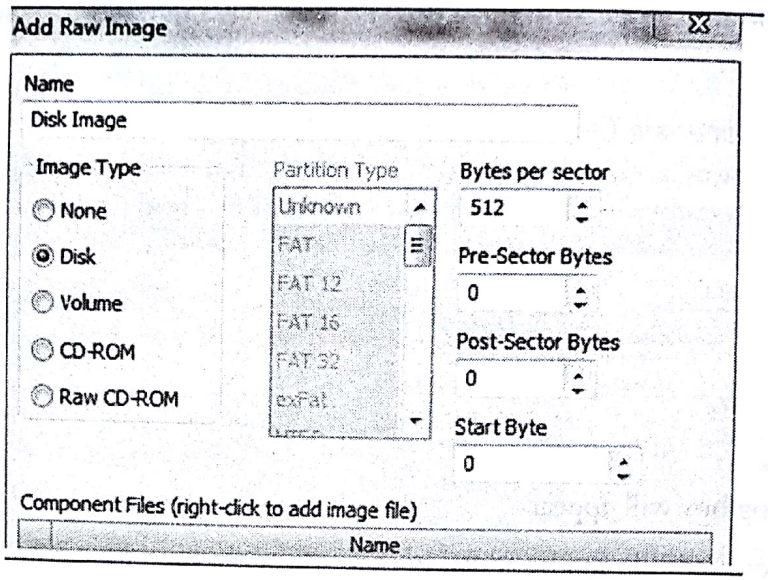

Figure 7.3 Selecting the appropriate dd image files.

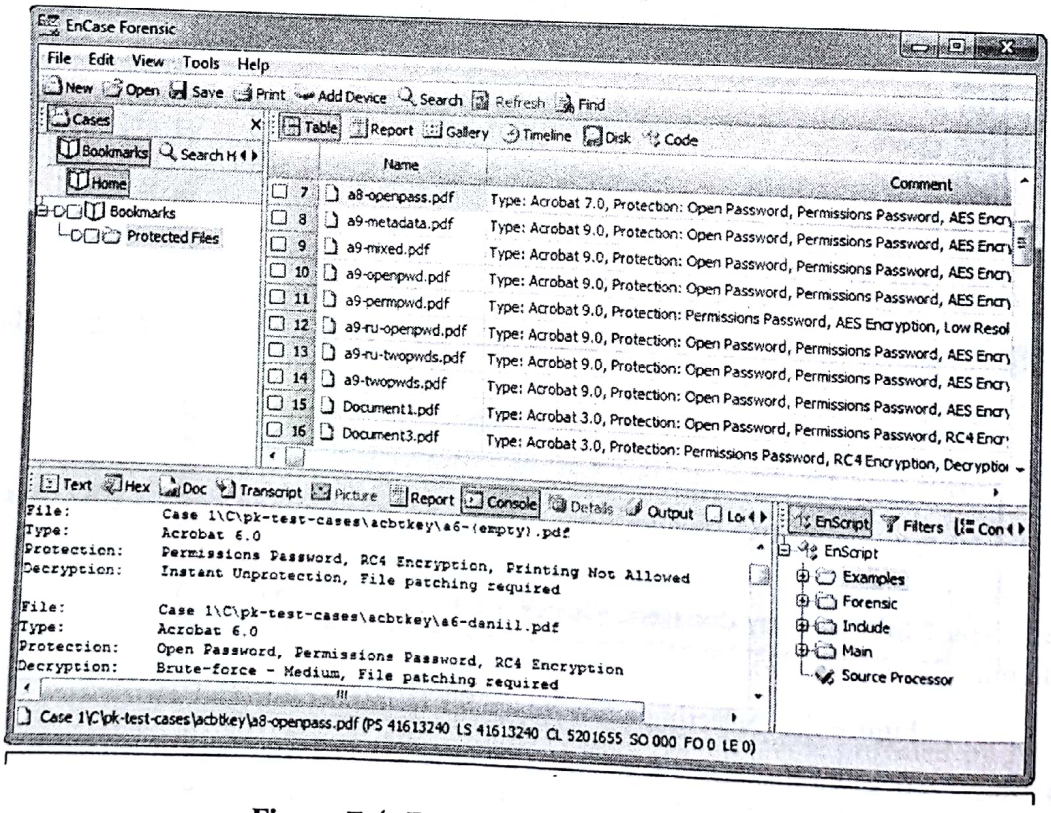

Figure 7.4 EnCase analysis environment.

1. Now, we look at Receiving Forensic Duplicates in FTK. Another powerful application in your toolkit is the FTK by Access Data. As compared to Encase, the interface and evidence import process are slightly more complicated; however, when dealing with e-mail store file and complex string, it can outperform Encase.
2. **How to begin a session:** When you start the application, a dialog box appears. Select "New case" option from it. Figure 7.5 shows case generation screen.

Scanned by CamScanner

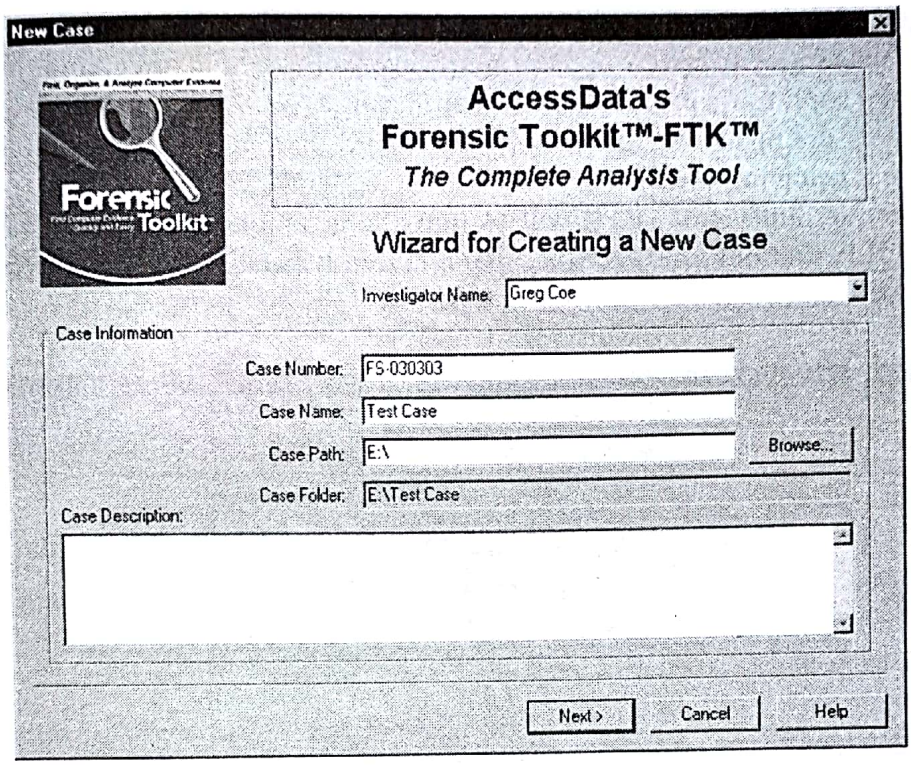

Figure 7.5 FTK case generation menu.

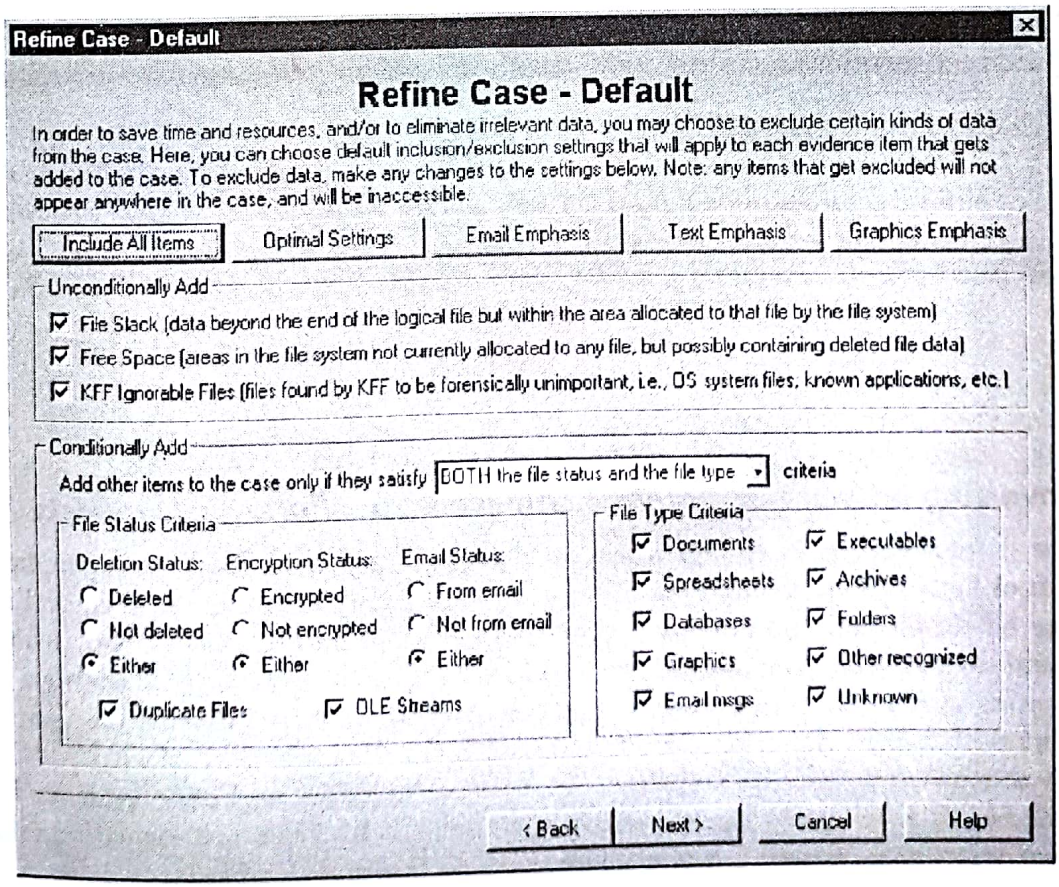

Figure 7.6 FTK refine case options..

Scanned by CamScanner

Now, you need to decide how you would like to view the data from evidence through the next several steps that appear. The best way to start is to select nearly every option, and not exclude any data, in order to get an idea of what the application is capable of. File from your ex-animation may be inadvertently executed if user is not careful and attentive. Figure 7.6 shows the case refining options that are available for execution while forensic image is being imported.

To import a forensic duplication, FTK will require a large amount of time. FTK's ability to handle complex files (viz., OLE, Outlook, and exchange file) is currently parallel. Figure 7.7 depicts the FTK interface with evidence loaded, sorted, and ready for analysis.

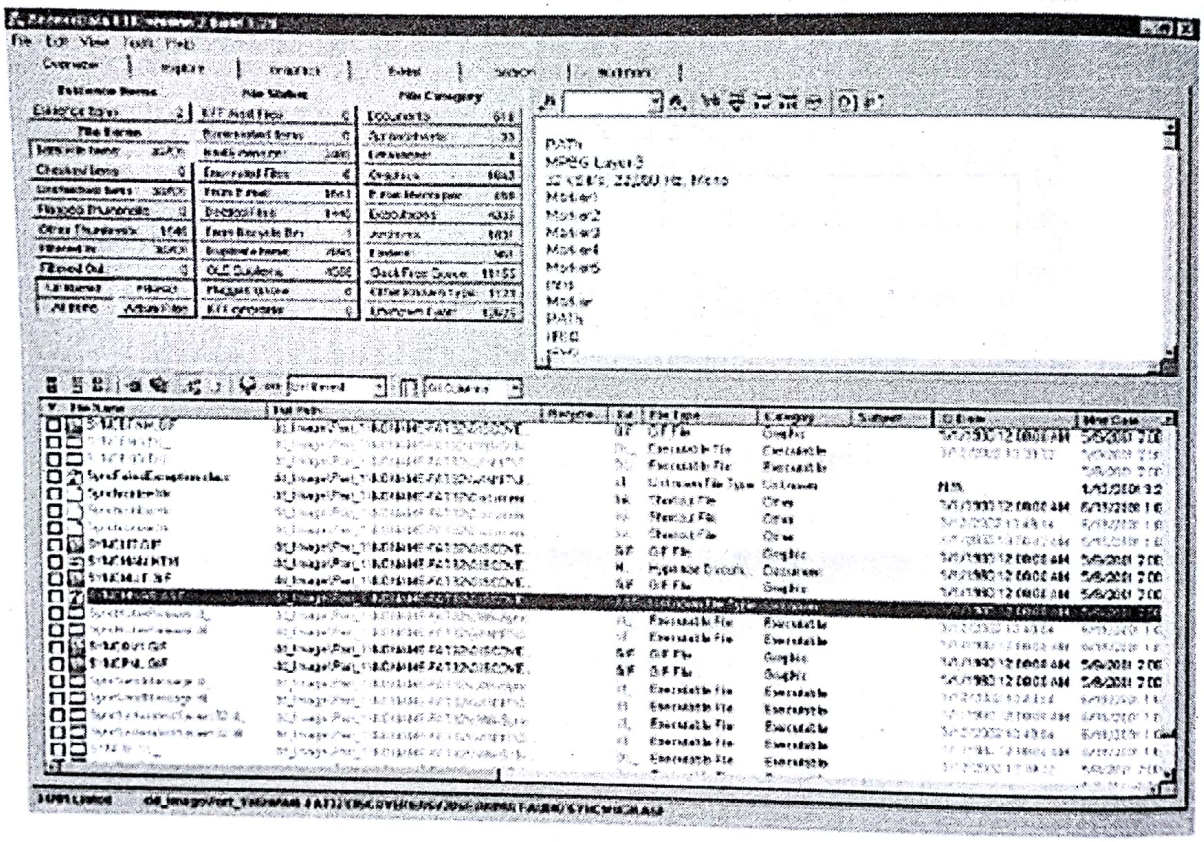

Figure 7.7 FTK analysis environment.

7.1.4 Converting a Qualified Forensic Duplicate to a Forensic Duplicate

What happens if something goes wrong, when you have collected qualified forensic duplicate? You are completely out of luck! The FTK will convert the qualified forensic duplicate executed by Encase or Safe book into true bit-for-bit duplicates of the original. The explorer program that allows an investigator to quickly load and examine duplicate image is provided by FTK software packages. Creating a new case file and building string search indices can prove to be more advantageous when the user does not have time to load a complete version of FTK.

Figure 7.8 shows Access Data FTK explorer. Here, we have loaded an Encase evidence file using the following steps: file, click on open image command, then right click on Encase evidence item that you want to export. Then, select item "Export Disk Image item."

Scanned by CamScanner

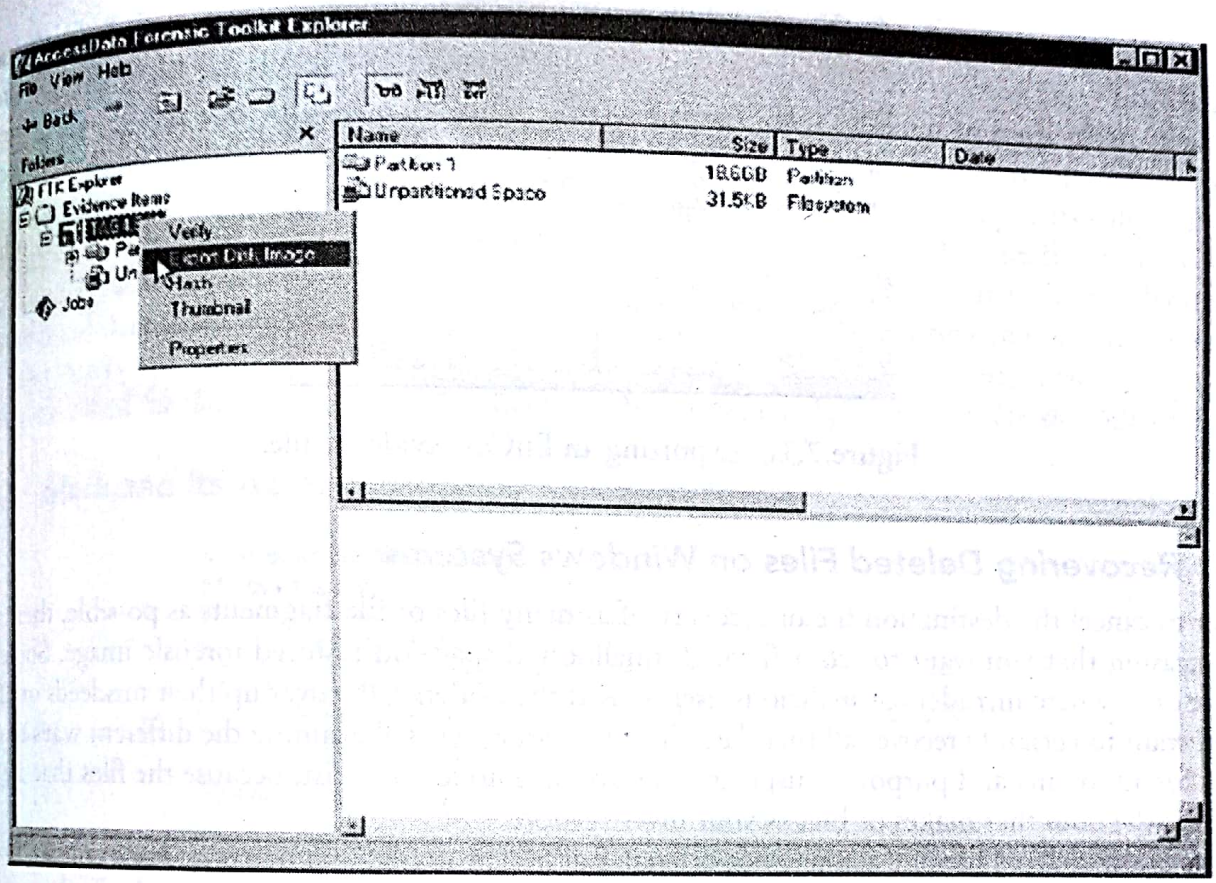

Figure 7.8 Selecting an evidence file for export.

Enable the option that will create MD5 of image (Fig. 7.9). The option is available here, that is, the files are split into chunks, when the user creates a duplicate image with dd. The image will be kept in single contagious file, if the destination file partition is larger enough.

Thus, we can say that this process is fast enough and that it takes approximately 12 min to convert 18GB Encase image to a true forensic duplicate (Fig. 7.10).

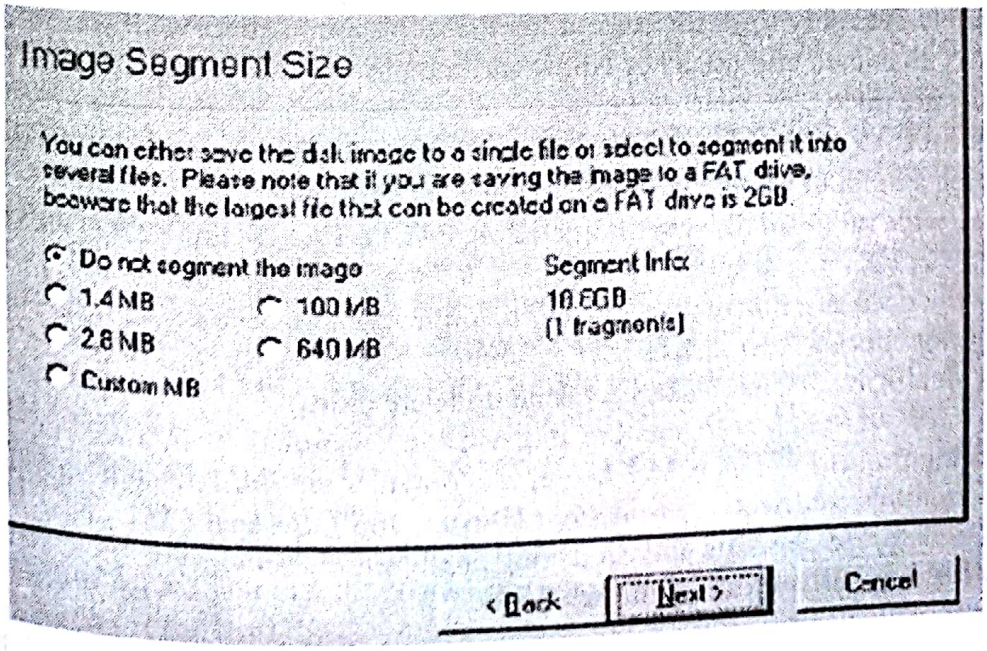

Figure 7.9 Selecting image segment size.

Scanned by CamScanner

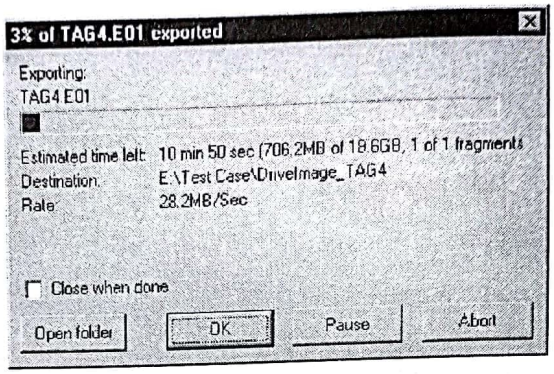

Figure 7.10 Exporting an EnCase evidence file.

7.1.5 *Recovering Deleted Files on Windows Systems*

In order to cancel the destination file or recovery of as many files or file fragments as possible, there would be an occasion that you want to scour through unallocated space on restored forensic image. Sometimes, there are cases where intruders or malicious users erased the evidence to cover up their misdeeds or identity and you want to certainly recover all that data. In this section, we will examine the different ways to obtain the files for all intents and purposes, suspects would believe no longer exist, because the files that are begin deleted are the ones that makes or breaks your investigation.

As we know, deleted files are actually not deleted, but merely marked for deletion. For example, from the FAT system, when a file or directory is deleted, the first letter of its file name is set to sigma character (Ó), or in hex, 0×E5. The deleted file located on a hard disk will remain intact until a new file or data. Special tools can find these "intact" deleted files and recover them for review. Remember, the sooner you attempt to recover a file, the better your chances of success. After a file has been marked for deletion, each hard drive I/O could overwrite the data you want to recover.

1. **Using Windows-based tools to recover files on FAT file systems:** To recover the files on FAT files system, we recommend the tools Encase and FTK. Both these tools have built-in capability to automatically recover any files. We have used the old Norton utilities and MS-DOS undeleted utilities; however, their use is rarely necessary since the current forensic tools are so effective. If you are interested, simply find the 0 × e5 character, and use a hex editor and rebuild the cluster chain (Dir/FAT/raw clusters) by hand. This is pure joy.
2. **Using Linux tools to recover files on FAT file systems:** The following capabilities should be provided by an operating system to value to a computer forensic examiner:
   (a) Supports a wide variety of file systems, including FAT12, FAT16, FAT32, NTFS, HPFS, Macintosh, OS/2, EXT2, EXT3, and UFS.
   (b) Recovers file slack and not allocate space. The improved loopback kernel makes it easy to recognize slack and not allocate drive space.
   (c) Provides an efficient, effective, and accurate undelete utility.
   (d) Delivers keyword search competences and performs all functions in a read-only state on the file system being processed. The NASA kernel also provides the read-only option to setup.
   (e) Handles compressed drives (DriveSpace, Dblspace, and DriveSpace 3).
   (f) Delivers widespread checking and cataloging of all forensic activities.
   (g) Delivers for data authentication and reliability.

Scanned by CamScanner

7.1.6 Recovering Unallocated Space, Free Space, and Slack Space

Once the forensic duplication of media and recovery of the entire possible file is done, there is still data left on evidence media that you will want to review. The remaining data is stored in slack place, unallocated space, and free space. So, to understand these terms, we must first review what an allocation unit or cluster is.

All the data stored on hard drive are arranged by the operating system into segments called allocation unit or clusters. For example, an operating system that uses 32k cluster reads and writes that from hard drive 32k at a time. It cannot read or write less than 32k at a time to hard drive. There are very few files that have exact amount of data to occupy an entire cluster or set of clusters. Therefore, when an operating system that writes 32k clusters to a hard drive is being asked to save a 20k Microsoft Word document, there is 12k of unused space called *file slack*. In our example, there may be remnants of previous files in this 12k of file slack.

7.1.6.1 Slack and Its Types

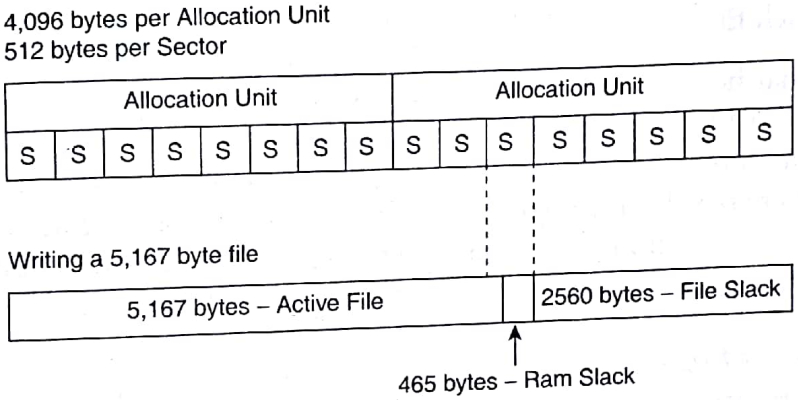

Figure 7.11 Illustration of slack space.

Most people refer to two different types of slack space, RAM slack and file slack. Figure 7.11 helps elucidate what we mean by these terms. The figure demonstrates how an operating system using 4k clusters would store a file that is 5,167 bytes in size.

Many people refer to two different types of slack space: file slack and RAM slack.

1. **File slack:** Everyone is aware that the file size varies, and that is ok! The fact is that many people are not aware that cluster is nothing but a place to store the files. The file system uses fixed sized containers or blocks of sectors, which the Microsoft operating system uses to assign disk storage space.
   Cluster and sector: Operating systems arrange all data stored on a hard drive into segments called allocation units or *clusters*.
   Example: A 5,000-byte file takes up 9 sectors; however, the operating system will allocate the file 2 clusters (16 sectors, 2 × 8 sectors), as it does not fit into 1 sector. Two Sectors is 8 kB (2 × 4 kB).
   A 2,500-byte file will fit into 5 sectors; however, the operating system will allocate the file 1 full cluster (8 sectors), which is 4 kB. A file which is 10,000 bytes will be allocated 12 kB – 3 sectors.
2. **RAM slack:** RAM slack is basically data between the end of a logical file and sector (NOT the cluster). It takes up to 512 bytes on a standard hard drive; if file takes up 400 bytes in the last logical sector, the remaining 112 bytes will be RAM slack. RAM slack contains a small portion of random data whose source is whatever contents of RAM that is chosen to fill that space. Ordinarily, it is a tiny fragment of some executable file in memory. File slack contains data from previously deleted files or from the factory conditioning of the hard drive.
   Note: RAM slack does not exist on trendy version of Windows and has not done for many times.

Scanned by CamScanner

Example: With 512-byte of sector on NTFS drive and 8 sectors per cluster, the size of cluster is 4,096 bytes. This means that if the file is 5,100-byte long, if there are 3,092 bytes of slacks, this is broken down into 20 bytes of RAM slack and 3,072 bytes of file slack (or 6 slacks).

7.1.7 Generating File Lists

To create information file listings, one of the most critical yet overlooked steps in analyzing the content of hard drive should include the following information:

1. Full path of each file found on the evidence media.
2. Last written and modified time/date stamps for each file.
3. Creation time/date stamps, if they exist (Linux does not maintain a creation time/date stamp!).
4. Last access time/date stamps.
5. Logical size of each file.
6. An MD5 hash of each file.

An alternative way that helps reduce the workload of investigative step is to compare the MD5 hashes of investigative know-good files with all the files on evidence media. It is not uncommon to eliminate more than 50% of the files on a Windows system from your analysis, because the files have a known-good purpose. For example, there may be a file like the application file or operating system files that would probably not contribute to your case. Similarly, it is not uncommon to use the MD5 hashes of "known-bad" files in an effort to quickly locate files that are indicators of malicious intent.

7.1.7.1 Listing File Metadata

For rapid time/date stamp correlation, we have populated a database and have developed in-house script that takes directory output (Windows) or ls-al output (UNIX). When you simply perform live response and not do a forensic duplicate, these in-house tools are especially helpful. However, to assist you in listening the file data, we recommend you to use Encase environment or FTK.

As per our observation, we noticed that during most cases, we need to order every file involved in case by time/data stamps. Figure 7.12 illustrates how easy it is to display file data, when it comes to use Encase interface.

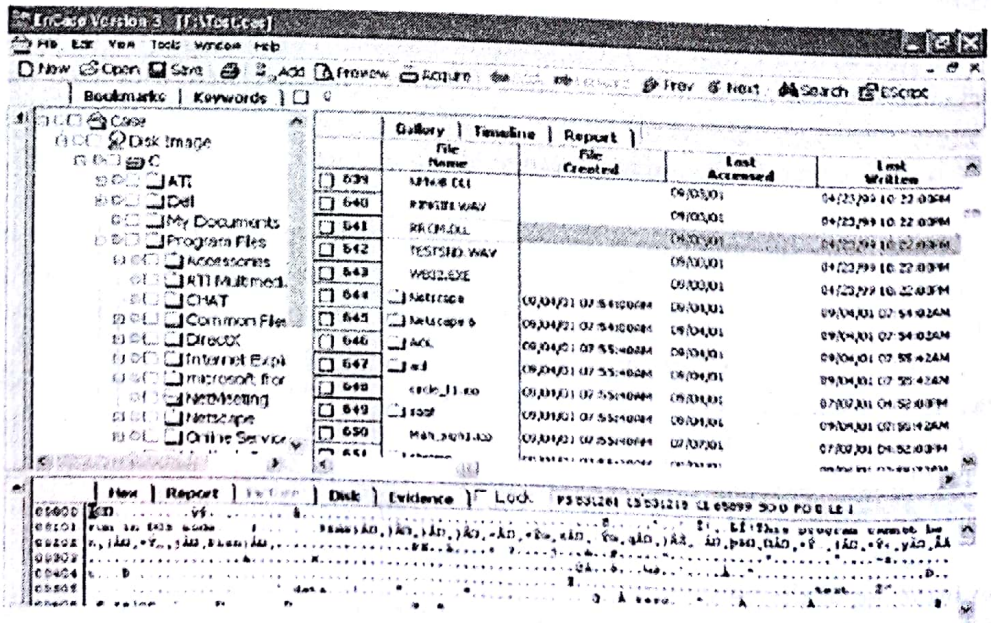

Figure 7.12 Reviewing time/date stamps in EnCase.

Scanned by CamScanner

In Figure 7.12, we order every file in the case in ascending order by file creation types. To view this three times/date stamp in adjacent columns, we have also adjusted columns in the file table that Encase has created.

For additional analysis and reporting, Encase has made it very easy to export file data to delimited text files that you can import from an application such as Microsoft Excel. The file that you can select to include in your export file is shown in Figure 7.13. You can also use Danny Mares CATALOG, a file list if you do not own Encase or FTK. The following command line works on as single partition drive (-p) and recursively lists all the files located on mount point/mnt/harddrive, creating an output file called filelisting.txt.

```
[root@localhost Mares]#./CATALOG -p /mnt/harddrive -o filelisting.txt
                                2>/dev/null
```

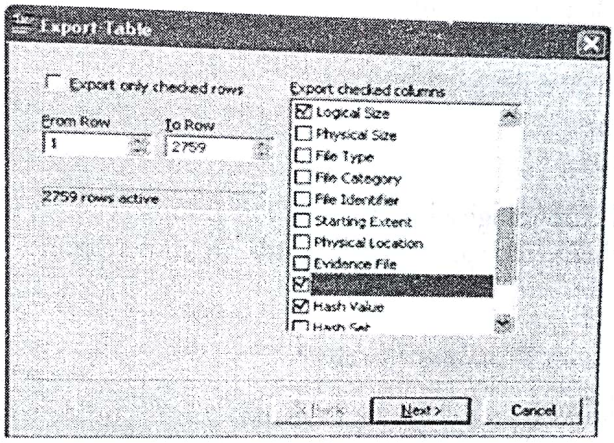

Figure 7.13 Selecting fields to be exported with the file lists.

7.1.8 *Preparing a Drive for String Searches*

When you perform computer forensic on hard drive, there are many different challenges. Perhaps, the most common challenge is that there is simply too much data to review on every hard drive, especially as the storage capacity of drive is commonly over 100 GB. Therefore, it is critical to reduce the amount of data that needs to be reviewed during analysis. Reviewing enormous amount of unallocated space or slack space is another challenge to be faced. We hope you will follow our guidance and perform string searches by minimizing the data you need to sift through. You have overcome the following challenges in order to properly string search media:

1. Frequent proprietary file formats endorse extra difficulty when trying to carry out string hunts on the matters of a hard drive. Files, such as Outlook's ".pst" and ".ost," Outlook Express's ".dbx," the Windows Registry files, the Windows event log files, the browser history files, and numerous other files, all need special tools for correct forensic examination.
2. Numerous compressed file formats render traditional string searching ineffective. Compressed files such as .tgz, .rar, .jar, .Z, .gz, .zip, arj, .lzh, packed files, and self-extracting archives are all foil traditional string searching utilities.
3. Encrypted files or password-protected files cannot be reviewed until unencrypted. Therefore, before you can conduct effective, complete string searches, you must:
   (a) Identify all compressed files and decompress them.
   (b) Identify all encrypted files and unencrypt them.
   (c) Identify all compressed files in e-mail stores and decompress them.

Scanned by CamScanner

7.2 Investigating Windows Systems

Once you have set up your forensic workstation with proper tools and recorded the low-level partition data from the target image, you are now set to conduct your investigation. For a formal examination of target system, following investigative steps are required:

1. Review all pertinent logs.
2. Perform keyword searches.
3. Review relevant files.
4. Identify unauthorized user accounts or groups.
5. Identify rogue processes and services.
6. Look for unusual or hidden files/directories.
7. Check for illegal entry points.
8. Inspect jobs run by the Scheduler service.
9. Analyze trust relationships.
10. Review security identifiers.

These steps are not filed chronologically or in order of importance. You may need to perform each of these steps or just a few of them. Your approach depends on your response plan and the circumstances of the incident.

Where Does Evidence Reside on Windows Systems?

It is important to know where we plan to look for evidence, before you dive into forensic analysis. The location will depend on specific cases, but in general evidence can be found in the following areas:

1. Volatile data in kernel structures
2. Slack space, where you can obtain information from previously deleted files that are unrecoverable
3. Free or unallocated space, where you can obtain previously deleted files, including damaged or inaccessible clusters
4. The logical file system
5. The event logs
6. The registry, which you should think of as an enormous log file
7. Application logs not managed by the Windows Event Log Service
8. The printer spool
9. Sent or received e-mail, such as the .pst files for Outlook mail

7.2.1 Reviewing All Pertinent Logs

The system log, application log, and security log are the three files that Windows NT, 2000, and XP operating system maintains. You will be able to obtain the following information by reviewing these logs:

1. Determine which users have been accessing specific files
2. Determine who has been successfully logging on to a system
3. Determine who has been trying unsuccessfully to log on to a system
4. Track usage of specific applications
5. Track alterations to the audit policy
6. Track changes to user permissions (such as increased access)

Scanned by CamScanner

System log records System processes and device driver activities. Windows includes device drivers that fail to start properly; hardware failures; duplicate IP addresses; and the starting, pausing, and stopping of services are audited by system events. The Application log is populated by Activities related to user programs and commercial off-the-shelf application. Application events that are audited by Windows include any errors or information that an application wants to report. The number of failed logons, amount of disk usage, and other important metrics can also be included by Application log. In the Security log, we find System auditing and the security processes used by Windows. Auditing done by Windows for Security events include changes in user privileges, changes in the audit policy, file and directory access, printer activity, and system logons and logoffs.

The Security log can be read by administrators only, but System logs and Applications can be viewed by any user. During an incident response, Security log is usually the most useful log. An investigator must be comfortable with viewing and filtering the output to these logs to recognize the evidence that they contain.

7.2.2 Performing Keyword Searches

It is important to perform string searches of the subject's hard drive during investigations into possession of intellectual property or proprietary information, sex offenses, and practically any case involving text-based communication. Many different keywords can be critical to an investigation, including user IDs, passwords, sensitive data (code words), known filenames, and subject-specific words (e.g., *marijuana*, *Mary Jane*, *bong*, and *dope*). To examine the contents of an entire drive, string searches can be conducted on the logical file structure or at the physical level to examine the contents of an entire drive.

Many keyword search utilities provide a "window" of information around the keyword or phrase. This allows the reviewer to determine its applicability to the investigation. However, on specialized cases involving privileged data, this window can present serious legal issues if the defense believes it leads to an excessive review of data. In such scenarios, plan your keyword searches carefully to minimize exposure while balancing the requirement for discovery of data relevant to your investigation.

Forensic software performs raw reads from the hard drive, conducting a physical-level string search of the drive. In most disk search tools that are marketed, you cannot physically read a drive that is running a Windows operating system, because various types of tools require that you boot the target system from a controlled boot floppy or other media (they cannot be run from active hard drives) and run the tool. Commonly used disk search utilities include dtSearch, offered by dtSearch Corp. Both utilities perform the search from a physical level. Encase has a string search capability that can be run against the evidence image file that it creates.

7.2.3 Reviewing Relevant Files

It can be a cumbersome and exciting task to determine the files that harbor evidence of an attack or misuse on Windows systems. To help in confirming or dispelling your suspicions, there is usually trace evidence somewhere on the system that helps to confirm or dispel your suspicions. The hard part may be finding it. Windows contains temp files, cache files, other countless locations where runtime data is stored, a Registry that keeps track of recently used files, and a Recycle Bin that maintains deleted files.

If possible, it is important to recognize files by their extensions as well as by their true file headers. At a minimum, you need to know what .doc, .tmp, .log, .txt, .wpd, .gif, .exe, and .jpg files are. Encase does not cover everything, although it provides viewing capability for many types of files. You may also need a comprehensive file viewer, such as Quickview Plus (by JASC Software), even if you are using this forensic utility. The name of a file does not "trick" the application because quick view and similar file viewers ignore the file extension.

Scanned by CamScanner

Popular third-party software can augment the monitoring and record keeping that a Windows system performs. You hit a jackpot every time your incidents occur on a system running a host-based firewall. Third-party firewall software provides fantastic audit trails for investigators to piece together incoming and outgoing network activity on a system.

Most personal firewall applications record every website a system visits, trap viruses, and provide an audit trail for every known attack on the system. This certainly makes reconstructing events easier.

7.2.4 Identifying Unauthorized User Accounts or Groups

To start rogue accounts on a system or to elevate their privileges is a common ploy by evildoers to start rogue accounts on a system to an unauthorized level, where they can get to data that they should not be able to access.

User accounts and user groups on a live system can be audited in several ways:

1. For unauthorized user accounts, Look in the User Manager (during a live system response).
2. To view all domain accounts on a domain controller and for suspicious entries, use usrstat from the NTRK.
3. Examine the Security log using Event Viewer, filtering for event ID 624 (addition of a new account), 626 (user account enabled), 636 (changing an account group), and 642 (user account changed).
4. Check the \%systemroot%\Profiles directories on the system. If the user account exists, but there is no corresponding \%systemroot%\Profiles*<user account>* directory, the user account has not been used to log in to the system yet. If that directory does exist, but the user account is no longer listed in the User Manager or Registry (at HKLM\SAM\Domains\Account\Users\Names), the user ID did exist at one time but no longer exists.

7.2.5 Identifying Rogue Processes

When reviewing a live system, Identifying rogue process is much simpler. For clear text user IDs and passwords, most rogue processes listen for network connections or sniff the network; these processes become easier to find when they are executing. PsList lists the name of the running process, List DLLs provides the full command line arguments for each running process, and Fport shows which processes are listening on which ports.

But now on a cold system, how can you find rogue processes? The easiest solution is to run the most up-to-date virus scanner on the whole logical volume of evidence. Make sure that the volume is mounted read-only, when you choose to run a virus-checking utility against the file system of the restored image. Without your knowledge, you would not want the tool to start moving and deleting files. PestPatrol is an excellent tool that identifies Trojans, backdoors, keystroke loggers, and other "malware."

7.2.6 Looking for Unusual or Hidden Files

There are no differences between bad guys who want to hide something and computer criminals. Once an attacker gains unlawful access to a Windows system, he/she needs to hide the files for later use. An insider may choose to make a few files "invisible," once he/she chooses to perform unauthorized or unacceptable deeds on his system. To hide data behind legitimate files, both these attackers can take advantage of the NTFS file streams. Unfortunately, how to stream files is common knowledge to the computer savvy.

To store multiple instances of file data under one file entry, Macintosh Hierarchical File System (HFS) originally developed a feature that NTFS contains. Because the Windows Explorer does not indicate the presence of the additional streams, the following multiple data streams may be used to hide data:

Scanned by CamScanner

1. Programming by JD Glaser - All Rights Reserved
2. Usage - sfind [path] /ns
3. [dirpath] Directory to search - none equals current
4. -ns Skip sub-directories
5. - or/either switch statement can be used
6. -? Help

Command prompt must have a minimum width of 80 characters.

7.2.7 Checking for Unauthorized Access Points

Windows NT does not allow remote command line-level access across a network without the use of external utilities; this is one of the biggest differences between Windows NT and UNIX systems. This changed dramatically with Windows 2000, which comes with a Telnet Server for remote command administration. An entry point to unwanted intruders could be provided by any service that allows some degree of remote Access. Such services could be provided by Trojans, in addition to built-in and third-party applications. These services include:

1. Terminal server
2. SQL/Oracle
3. Third-party telnet daemons on Windows NT
4. Windows 2000 Telnet Server
5. Third-party FTP daemons
6. Web servers (such as Apache and IIS)
7. Virtual network computing (TCP port 5800) and PC Anywhere (TCP port 5631)
8. Remote access services (PPP and PPTP)
9. X Servers

You must identify the access points to the system to determine how access was obtained, when responding to victim systems. For identifying the access points to a system, the Tools such as netstat and Fport are critical. They use API calls to read the contents of kernel and user space TCP and UDP connection tables. You need to allow the restored image to boot, if you intend to capture this information. If you performed this step during the live system review, before the system was shut down for imaging, compare the results of the two operations. Discrepancies may be indicative of an unauthorized daemon.

7.2.8 Examining Jobs Run by the Scheduler Service

A common trick by attackers is to have a scheduled event start backdoor programs for them and also change the audit policy, or perhaps even something more threatening such as a scheduled wiping of files.

Consider the following batch file running the NTRK tool remote to an NT system: remote /s "cmd.exe" batman5

If this command line were run at a specific time, someone could connect to the system using the following command line: remote /c <hostname> batman5.

The <hostname> is the NetBIOS name of the remote system and batman5 is the key phrase to connect. The person can now execute any commands desired using the *at* or *soon* utility. Malicious scheduled jobs are typically scheduled. The *at* command, with no command line arguments, will show any jobs that have been scheduled.

Scanned by CamScanner

7.2.9 Analyzing Trust Relationships

Trust relationships among domains can certainly increase the scope of a compromise, should a valid user ID and password be stolen by an attacker. Access to one machine may mean logical access to many others. Severity of the incident and scope of a compromise raise the trust relationships. Determining trust within UNIX environment is as simple as compared to determining trust within a Windows domain, which is difficult. *Non-transitive* or one-way trust is Windows NT. This means that access and services are provided in one direction only.

It does not need to trust your PDC, if your NT PDC trusts another domain. Therefore, users on the trusted domain can use services on your domain, but not vice versa. Windows 2000 can provide a two-way or *transitive* trust relationship. To communicate properly, Domains located within an Active Directory forest require two-way trusts. For example, in Windows 2000 Active Directory Services, if Domain A trusts Domain B and Domain B trusts Domain C, then Domain A trusts Domain C. This relationship is illustrated in Figure 7.14.

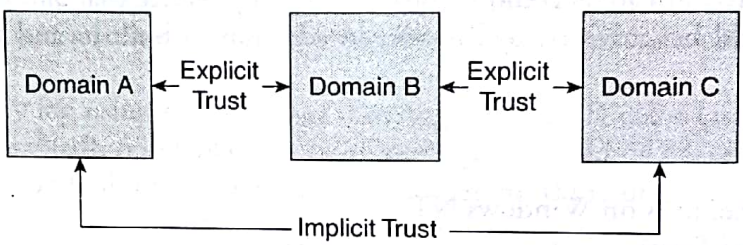

Figure 7.14 Windows 2000 trust relationships.

7.2.10 Reviewing Security Identifiers

You may need to compare security identifiers (SIDs) found on the victim machine with those at the central authentication authority, to establish the actions of a specific user ID. Here, we see how SIDs can contribute to incident response.

To identify a user or a group uniquely, SID is used. Each system has its own identifier, and each user has its own identifier on that system. To make the SID, computer identifier and the user identifier are combined. Thus, SIDs can uniquely identify user accounts. SIDs do not apply to share security.

For example, the following is a SID that belongs to the administrator account:

S-1-5-21-917267712-1342860078-1792151419-500

The S denotes the series of digits as a SID. The 1 is the revision level, the 5 is the identifier authority value, and 21-917267712-1342860078-1792151419 includes the subauthority values. The *500* is the relative identifier.

With help of usernames and passwords, Access to shares is accomplished. However, SIDs do apply when remote access to a domain is provided. A SID with the server's unique sequence of numbers is placed in the Registry of the workstation, after the first successful logon to that server. Therefore, SIDs can be the digital fingerprints that prove that a remote system was used to log on to a machine and access a domain.

7.3 Investigating UNIX Systems

The UNIX is powerful, flexible, and extremely functional. It has become essential for both UNIX users and forensic investigators, to investigate a compromised UNIX system and the ability to respond to a computer security incident. But UNIX does not have a decent standing for dependability or safety.

Scanned by CamScanner

Although UNIX does offer some effective safety features such as login and user accounts, which are stored in the **/etc/passwd**file, access control with a granularity of owner, cumentgroup, and world, and save record files-**usr/adm/lastlog, /var/adm/utmp, /var/adm/wtmp/, /var/adm/acct**. UNIX systems directly connected to the Internet are often subject to hacking attempts.

Some of the methods for UNIX investigation are:

1. Studying relevant logs
2. Carrying out keyword searches
3. Go through relevant files
4. Recognizing illegal user accounts or groups
5. Classifying rogue processes
6. Checking for illegal access points
7. Examining trust relationships
8. Noticing Trojan loadable kernel modules

These steps are not listed in order of importance or chronologically. For every incident, there is no need to take all of the steps. Your approach depends on the specific incident and the goals of your response. As you conduct your investigation, be aware that in the event of root compromise, anything can happen. An attacker with root access to a system can modify just about anything on the operating system, including the evidence that you are reviewing.

7.3.1 *Reviewing Pertinent Logs*

During incident response, UNIX operating systems have a variety of log files that can yield important clues. Not only are system activities, such as logons, startups, and shutdowns, logged, but also events associated with UNIX network services. Most log files are located in a common directory, usually /var/log. However, some flavors of Unix will use an alternate directory, such as /usr/adm or /var/adm. Some logs are placed in non-intuitive locations, such as /etc. You can consult operating system-specific documentation, when in doubt. However, not all log files are even on the system in question. You may find pertinent logs on a network server or security device such as a firewall or IDS.

7.3.2 *Performing Keyword Searches*

Ranging from e-mail harassment to remote network compromise cases, keyword searches are a critical part of almost every incident response investigation. Including an attacker's backdoor password, a username, a MAC address, or an IP address, the keywords can be a wide range of ASCII strings. Keyword searches can be performed on the logical file structure or at the physical level, examining the contents of an entire drive. Here, we focus on how to perform string searches using UNIX utilities.

7.3.2.1 *String Searches with Grep*

The grep command is a powerful and flexible command primarily tool for string searches. Use the grep command as follows, to perform a string search within a file:

```
[root@lucky]# grep root /etc/passwd
root:x:0:0:root:/root:/bin/bash
```

Notice that the line in the passwd file with the string root inside appears as output. The passwd file is a text file.

Now, let us try grep on a binary file:

```
[root@lucky]# grep PROMISC /sbin/ifconfig
```

Scanned by CamScanner

Binary file /sbin/ifconfig matches

This time, the string does not appear. Instead, you see a notification that a file of type binary has a matching entry. If you want to see the match, use the -aoption to handle binary files:

```
[root@lucky]# grep -a PROMISC /sbin/ifconfig
```

[NO FLAGS] UP BROADCAST DEBUG LOOPBACK POINTOPOINT NOTRAILERS RUNNING NOARP PROMISC ALLMULTI SLAVE MASTER MULTICAST DYNAMIC.

7.3.3 Reviewing Relevant Files

It is a safe bet that numerous files will port evidence connected to any given incident. However, your achievement in recognizing all the applicable files is much less certain. To help in identifying which files are likely to be relevant to any given incident, we use various techniques. These techniques include identifying relevant files by their time/date stamps and by the information gained during the initial response to UNIX. We also search configuration and system files commonly abused by attackers.

7.3.3.1 Incident Time and Time/Date Stamps

You must first know the time of the suspected incident, in order to search for files and directories that were accessed, modified, or created around the time of a suspected incident. The time frame may be very specific, such as when a network IDS discovered and logged the attack as it happened. The first step to make sure that the system time on the IDS matches that of the victim system is if you have a good record from an outside source (such as network IDS) of when the attack occurred.

To follow up on the relevant time windows that you have already determined is the goal in reviewing time/date stamps. All the files or directories accessed, modified, or created during this time are likely candidates as relevant items.

7.3.4 Identifying Unauthorized User Accounts or Groups

On victim systems, attackers will often modify account and group information. This modification can come in the form of additional accounts or escalations in privilege of current accounts. For future access, the goal is usually to create a backdoor. To validate that an attacker did not manipulate this information, you should audit user and group accounts on suspected victim systems. Auditing UNIX system account information is a straightforward process.

7.3.4.1 User Account Investigation

User information is stored in the /etc/passwd file. Using a variety of mechanisms, this is a text file that you can easily review through. Every user on a UNIX system has an entry in the /etc/passwd file. A typical entry looks like this:

```
lester:x:512:516:Lester Pace:/home/lester:/bin/bash
```

The entry consists of seven colon delimited fields: the username (lester), the password (shadowed in this case), the user ID (512), groupID (516), GECOS field (for comments; Lester Pace in this case), home directory, and default login shell.

7.3.4.2 Group Account Investigation

groupID shown in the /etc/passwd file as well as the/etc/groups files are used by Group accounts. A typical /etc/group file looks like this:

1. `$ cat /etc/group`

Scanned by CamScanner

2. `root::0:root,ashunn`
3. `bin::2:root,bin,daemon`
4. `sys::3:root,bin,sys,adm`
5. `adm::4:root,adm,daemon`
6. `uucp::5:root,uucp`

Along with the users, the file lists the groups that are associated with that group. It is important to note that an entry in the group file does not need to exist for a group to exist. Group membership is based on the group ID in the password file

7.3.5 Identifying Rogue Processes

When examining a live system, identifying rogue processes is much easier. You should record all listening ports and running processes.

To verify their validity, you should carefully examine the running processes. Also, review all binaries associated with listening services and running processes to ensure that they have not been modified.

7.3.5.1 What Can Happen?

You dutifully record listening ports and running processes. During your initial investigation, you notice an anomaly with FTP. During further examination:

```
[root@victim]# netstat -anp
tcp 0 0 0.0.0.0:23 0.0.0.0:* LISTEN 519/inetd
tcp 0 0 0.0.0.0:21 0.0.0.0:* LISTEN 519/ftpd
```

7.3.6 Checking for Unauthorized Access Points

UNIX is a fully functional, robust operating system. It has continually added functionality (network services are no exception) over the course of its long history. Along with the Network File System (NFS), telnet, finger, rlogin, and many others, a default installation of UNIX offers a dazzling array of network services. Any one of the networked services on UNIX systems can potentially allow some degree of remote access to unwanted intruders, as can a phone line connected to a modem.

X Servers, FTP, telnet, TFTP, DNS, send mail, finger, SNMP, IMAP, POP, HTTP, and HTTPS are some of the most common access points that we have seen intruders take advantage of. Unfortunately, this is just a partial list. As you conduct your investigation of the UNIX system, you will need to examine all network services as potential access points. Did you find anything suspicious from your investigation of configuration files, startup files, and listening sockets? What "normal" services were running on the system at the time of the suspected incident? How could an intruder access your system will help in answering all these questions. Examine every potential access point to ensure that it is configured securely and has the latest patches or software version.

7.3.7 Analyzing Trust Relationships

Include the most popular services like login, rsh, the Network Information Service (NIS and NIS+), NFS, and ssh. Trust can be established between UNIX systems with a variety of services. Trust relationships within UNIX systems were once a primary mechanism of attack. For system administrators and users, trust relationships can be convenient timesavers. If machine A trusts machine B, then the user on machine B can

Scanned by CamScanner

access machine A with no additional credentials. If you are a system administrator with dozens of systems to maintain, using this feature can be very enticing.

Investigate all possible trust relationships to determine if they played a part in the incident. Trust relationships are usually configured through files such as /etc/hosts.equiv orany .rhosts file in a user's home directory through shared keys and through NFS shares.

Trust relationships can be established with ssh. Nowadays, trust relationships seem to be less common. However, another type of trust is created through network topology. Common network segment must trust their peers that share networked computers.

7.3.8 Detecting Trojan Loadable Kernel Modules

On the various flavors of Linux, BSD and Solaris Loadable kernel modules (LKMs) or kernel extensions are found. They extend the capabilities of the base operating system kernel, typically to provide additional support within the operating system for device and file system drivers. LKMs run at the kernel level instead of at a normal user process level, when they are dynamically loaded by a user with root-level access.

Several intrusion-based LKMs have been developed, and once a malicious user obtains privileged access to your system, she/he can install one. Some common malicious LKMs include Adore, Knark, and Itf.

7.3.8.1 LKMs on Live Systems

It can become complicated to detect Trojan LKMs on a live system, because these tools actually intercept system calls (viz., ps or directory listing) to provide false information. They are specifically designed to prevent detection with traditional response methods. To detect anomalies or discrepancies, you can find them by combining externally executed commands with local commands, in many cases.

You are a system administrator with dozens of systems to maintain. Using this feature can be very enticing.

7.4 Investigating Applications

7.4.1 Web Browsers

Web browsers are used to execute different activities on the Internet by users (Figure 7.15). Browsers are used for many functions, such as information search, access to e-mail accounts, e-commerce, making the banking, instant messaging, online blogs, access to social networks. Web browser records many data associated with user activity. Information such as URLs visited by users, search terms, cookies, cache files, access time, and use time holds in memory on the system. In case of a different user to access the same computer, accessing to this data can be happen in a very easy way. Web browsers are significant tools on many of the crimes committed on digital resources. Examining the evidence which is the subject of criminal records is an important step examination of your browser. To reveal offender's profile and connections depends on web registry. The suspects can use web browsers for actions, such as to collect information, to hide the crime, to get in touch with crime partners. The evidence found by using the Web browser is a key factor for the forensic expert. Suspiciousness leaves a mark on his/her computer about every movement during the use of web browser. It is possible to examine evidence, such as history, cache, cookies, downloads list, entering URL addresses, access time of visit, frequency of visits from the suspect's computer. For conducting the analysis in a correct way, it is needed to probe registry of web browsers on image. The analysis of only a web browser is not sufficient to get the evidence.

Scanned by CamScanner

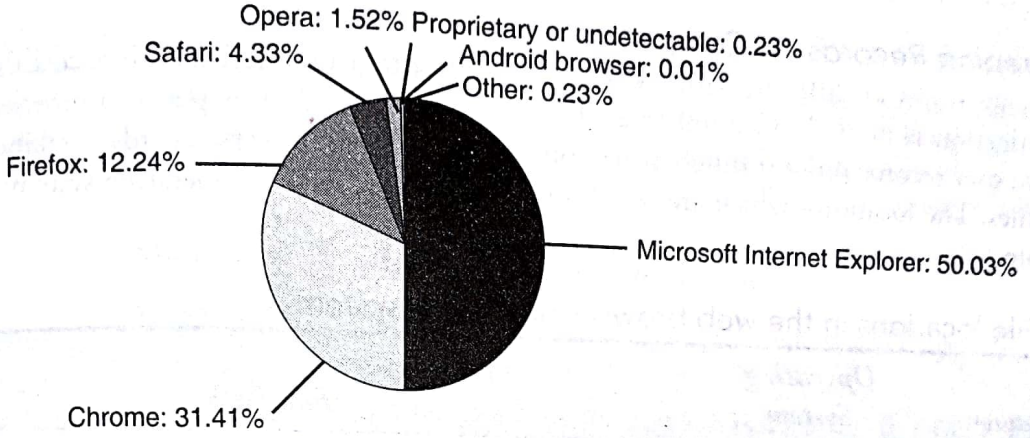

Figure 7.15 Utilization ratio of web browsers.

7.4.1.1 *Utilization Ratio of Web Browsers*

It is crucial to be able to examine evidence with different versions of browsers, such as Internet Explorer, Google Chrome, Firefox, Safari, and Opera for ensuring genuineness of the evidence. In this section, it is discussed how to get user web browser activities from image of an evidence. Usage of applications which are employed in this field are described and compared. Moreover, the processes of acquiring information, such as URL, visit date, visit count, web browser type, system user name, browser profile, URL size from web browser files are also discussed.

7.4.1.2 *Analyses of Web Browser Records*

Web browsers are the normally used applications in digital devices. Users perform their Internet activities with web browsers in various operating systems. Web browsers are used for several purposes, such as searching information, e-mail, e-commerce, news, e-banking, social media, and blog writing. Due to this reason, it is one of the most significant parts of evidence analysis. Information like which URLs were visited by the user, which words were searched, when these actions were made, are used by digital forensics experts to analyze the crime. Also, usage of different web browsers in the same period must be examined. A lot of open-source and licensed tools are there to perform analysis. Users often perform activities as specified in Table 7.1 in web browsers.

Table 7.1 User activity on web browsers

User Activity	*Word in URL*
Search	Search, word about search
E-mail	Mail, e-mail
Blog	Blog
Social Media	Facebook, Twitter, Instagram, vb.
News	News
Shopping	Shopping, shop, foni, vb.
Weather Condition	Weather
Game	Game
Video, Visual Content	Video
Music	Music, mp3
Banking	Bank, Credit

Scanned by CamScanner

7.4.1.3 Keeping Records on Computers

Web browsers are stores in different parts of the operating system user activity. To access the user information, investigation is needed in several areas. Furthermore, data varies as per web browsers type. Web browsers retain user records on four different sections: Cache records, history records, cookies registry, and downloaded files. The locations, which are web browsers that store data on operating systems, are demonstrated in Table 7.2.

Table 7.2 File locations in the web browser operating system

Web Browser	*Operating System*	*File Path*
Internet Explorer	Windows 95/98	C:\Temporary Internet Files\Content.ie5 C:\Cookies C:\History\History.ie5
	Windows 2000/XP	C:\Documents and Settings\%username%\Local Settings\Temporary Internet Files\Content.ie5 C:\Documents and Settings\%username%\Cookies C:\Documents and Settings\%username%\Local Settings\History\history.ie5
	Windows Vista, 7 and latest version	C:\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\ C:\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\
Firefox	Linux	/home/$USER/.mozilla/firefox/$PROFILE.default/places.sqlite
	MacOS-X	/Users/$USER/Library/Application Support/Firefox/Profiles/$PROFILE.default/places.sqlite
	Windows XP	C:\Documents and Settings\%username%\Application Data\Mozilla\Firefox\Profiles\%PROFILE%.default\places.sqlite
	Windows Vista, 7 and latest version	C:\Users\%USERNAME%\AppData\Roaming\Mozilla\Firefox\Profiles\ %PROFILE%.default\places.sqlite
Safari	MacOS-X	/Users/$USER/Library/Safari/ /Users/$USER/Library/Caches/com.apple.Safari/
	Windows XP	C:\Documents and Settings\%username%\Application Data\Apple Computer\Safari\ C:\Documents and Settings\%username%\Local Settings\Application Data\Apple Computer\Safari\
	Windows 7	C:\Users\%username%\AppData\Roaming \Apple Computer\Safari\ C:\Users\%username%\AppData\Local \Apple Computer\Safari\

(Continued)

Scanned by CamScanner

Table 7.2 (Continued)

Web Browser	Operating System	File Path
Opera	Linux	/home/$USER/.opera/
	MacOS-x	/Users/$USER/Library/Opera/
	Windows XP	C:\Documents and Settings\%username%\Application Data\Opera\Opera\
	Windows Vista, 7 and latest version	C:\Users\%username%\AppData\Roaming\ Opera\Opera\
Google Chrome	Linux	/home/$USER/.config/google-chrome/Default/Preferences
	MacOS-x	/Users/$USER/Library/Application Support/Google/Chrome/Default/Preferences
	Windows XP	C:\Documents and Settings\%username%\Local Settings\Application Data\Google\Chrome\User Data \Default\Preferences
	Windows Vista, 7 and latest version	C:\Users\%username%\AppData\Roaming\ Google\Chrome\User Data \Default\Preferences

As per web browsers, system stores data in various folders and locations. In the analysis process, it is essential to test data in various folders. Folders should be searched for in four different record types as mentioned in the previous section. Types storing of web browser are listed below. Internet Explorer is a web browser which computer users generally use. Internet activity records are stored for each user individually under the user profile folder. Data stores in Cookies, Cache, Download History, and History folders separately under the locations is showed in Table 7.2. Data stores under folders in index.dat or container. dat database files. Data is stored in binary format in this file. Safari stores web browser data in file which is named History.plist in binary format under the web browser data locations. It stores the information of URL addresses, date of visit, time, and the number of visits for each website. Firefox stores web browsers data in a file called places.sqlite. File uses the SQLite database format. Opera keeps data in different files with the extension .dat. These files are cookies4.dat, download.dat, global_history.dat, search_field_history. dat. Google Chrome stores data in the preferences file. There is separate file for each user. There is information about user policies, master preferences, and local locations data.

7.4.1.4 Time Formats Used by the Web Browser

It is essential to analyze the user behavior in a given time period for demonstrating crime in forensic examination. In order to find out the offender's activities, a time schedule should be made and followed. Thereby it can reveal about relationships with other related websites which are visited by the suspects in the same time. Time format which is used by web browsers is given in Table 7.3. The expert who examines must consider the time format that has been used by the web browser. Else, the time of suspect use cannot be determined. Therefore, the expert who examines must do time correction. The time format of the data obtained from the evidence must be consistent with the user's examination of his time format.

Scanned by CamScanner

Table 7.3 Time format used by web browser

Web Browser	*Time Format*
Internet Explorer	FILETIME: 100-ns(10-9) Since January 1, 1601 00:00:00 (UTC)
Firefox	PRTime:microsecond (10-6) Since January 1, 1970 00:00:00 (UTC)
Google Chrome	WEBKIT Time: microsecond (10-6) Since January 1, 1601 00:00:00 (UTC)
Safari	CG Absolute Time: second Since January 1, 2001 00:00:00 (UTC)
Opera	UNIX Time: second Since January 1, 1970 00:00:00 (UTC)

7.4.1.5 Clearing the Web Browser History

The analysis process of web browsers record, suspicious could have deleted browsers data. Many web browsers offer options to delete cache, cookies, history, download files to users. When this information is deleted, users will destroy what can be obtained in the examination by using function of browser. There are two ways of deleting records: (i) by overwriting the existing data with the launch of applications, the old data is lost and (ii) by deleting data from the browser menu or the index by users voluntarily. After the first method, accessing old data is very hard. But, after the second method, accessing data is possible by recovering and disk scratching actions. Choice and access roads allowing the deletion of records by users of the browser is given in Table 7.4.

Table 7.4 Locations of deleting data according to the type of browser

Web Browser	*Delete Options Path*
Internet Explorer	Settings/Internet Options//Deletes
Firefox	Settings/Privacy/History about:preferences#privacy
Google Chrome	Settings/History/Search Data chrome:// settings/clearBrowserData
Safari	Settings/Privacy/Delete All Web Site Data Settings/History
Opera	Settings/History/Privacy and Security/ Delete All Search Data Opera://settings/clearBrowserData

7.4.1.6 Tools for Analysis

WEFA, NetAnalaysis, Browser History Examiner, FTK, and Encase are the softwares that are commonly used for analyzing web browsers in digital forensics examinations. In this chapter, features of specified web browser analyze tools are also presented.

Scanned by CamScanner

IEF (Internet Evidence Finder): IEF is a software with license fee produced by Magnet forensics company. Personal computers are used in the process of examinations of smart phones and tablets by experts. With its different models, it presents the characteristics, such as examining internet TV series, analysis of traces obtained from mobile applications. It is used on Windows and MacOs operating systems.

WEFA: WEFA is a free, web browser analyze tool. It runs on Windows NT and later versions. It supports Internet Explorer (~11), Mozilla Firefox, Apple Safari, Opera, Chromium, Google Chrome, Google Chrome Canary, Comodo Dragon, CoolNovo (ChromePlus), Swing browsers. For these browsers, WEFA offers various methods to perform analysis from an active system or an image disk. These methods include gathering the web browser's cache, cookies, internet history, download history, session data, temporary internet files, and the timesheet data information. The obtained data can be displayed in timeline view, HTML view or URL parameters view searches.

NetAnalysis: NetAnalysis is a licensed tool developed by Digital Detective company for digital examining of web browsers. It supports Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari, and Opera bowsers. It allows the examination of Internet history, cache, cookies and other components. It has also an effective reporting feature that allows quickly gathering evidence according to user behavior. Moreover, this software has effective analytical tools for decoding and understanding data. At the same time, it has ability to use SQL queries to identify related evidence. This software can also be used to recover deleted web browser components.

Browser History Examiner: Browser History Examiner is a licensed tool developed by Foxton Forensics Company and it extracts and analyzes web history. It supports Chrome, Firefox, Internet Explorer, and Edge web browsers. And it can analyze a lot of data type as downloads, cache data, and visited URL files. Internet activities in a specific timeline can be traced with web site timeline feature. Data can be analyzed by using various filters like key word list and time–date range with advanced filtering feature. Image files saved in the browser cache can be easily shown in thumbnail galleries with cache image viewer feature. Web sites stored in browser cache can be reconstructed and analyzed with cache web page viewer feature. Different time zone conversions can be performed with Time Zone and DST Configuration feature and all obtained data from these features are reported.

FTK: FTK is one of the tools developed to analyze systems entirely. It enables to analyze web browser data with its features. Web browser history is virtualized in detail. Internet Explorer, Firefox, Chrome, Safari, and Opera browsers are supported. Also, deleted web browser data can be recovered by FTK. This software also has a feature to report analysis results.

Encase: Encase system is an analysis tool developed to examine systems entirely. It enables to examine web browser data with its features. With the help of a simple script, all browser history, cookies, and cache files are copied into a file by using third-party software. Internet explorer, Firefox, Chrome/Chromium, Opera and Safari are supported in Windows, UNIX and Mac operating systems. Also, it enables to recover deleted internet components. Obtained data can be analyzed by filtering according to key word and time parameters. WEFA, NetAnalysis, and History Examiner are developed especially for performing digital analysis of web browsers. But, FTK and EnCase applications are developed to examine files and systems. This software also has features as analyzing web history and holistic analysis.

7.4.2 E-mail

E-mail has emerged as one of the most widely used communication application, used for exchange of data and to carry out data transactions. Due to an increased use of e-mails in the present scenario, its security has also become a major issue. Nowadays, e-mails are being used as the prime weapon to conduct a crime. E-mail phishing, frauds, sexual predation, sending spam e-mails, and injection of viruses through e-mails are among the major crimes that the culprits carry out with the help of e-mails. Also, different types of data theft through e-mails may adversely affect an organization's operation or workaround of an individual itself.

Scanned by CamScanner

Whenever a digital or cybercrime comes into existence, the first step taken is consulting data investigators. Digital investigators collect, preserve, and analyze e-mails to investigate a crime. For an efficient and deep investigation of e-mails, a wide variety of tools and particular procedures are used. In the upcoming section, we will shed some light on the procedures and various techniques that are employed for an efficient investigation of e-mails in a particular crime.

7.4.2.1 Procedure to Investigate an E-mail

In e-mail forensics, the source and content of e-mails is considered as evidence. The process includes identifying the actual sender, recipient, date, time and location of mail transaction, intention of the sender, etc. It also involves investigation of metadata, keyword searching, port scanning, etc. Various techniques that are used for e-mail investigation are as follows:

1. **Header Analysis of e-mails:** While investigating e-mails, we usually start from the scratch and analyze the headers of the mails. Headers contain information about the senders of the e-mails and also information about the path through which the e-mails have travelled. During the time of a crime, the e-mail headers are spoofed in order to hide the identity of the sender. If the messages passing through SMTP server do not possess SMTP idiosyncrasies, then they are faked.
2. **Link Aanalysis:** Link analysis is a graphical data analysis method to evaluate e-mails exchanged between users. Since a crime can involve multiple suspects, link analysis is used in order to examine the link between the suspects. Since there can be thousands of mails that are linked between suspects, therefore it becomes a time-consuming task that defeats the purpose of e-mail investigation.
3. **Bait Tactics:** The basic aim of the bait tactics is to extract the IP address of the culprit. In this technique, an e-mail with http:<img src>tag which has some image source at a computer that is monitored by investigators is sent to the e-mail address that is under investigation. Now the recipient is the one who originally was sender during the crime. When the e-mail is opened, a log entry which contains the IP address of the recipient is recorded on the server which is hosting the image and the recipient is tracked. In a case when the recipient is using a proxy server, then the IP address of the proxy server is recorded by the investigators. The log of the proxy server is used to track the culprit. In case, the logs of the proxy server are not available, then a tactic e-mail is sent to the culprit. The tactic e-mail can either be an HTML page or an Embedded Java Applet.
4. **Investigation of Server:** In the server investigation, server logs and copies of delivered messages between sender and receiver are investigated. The e-mails from the sender and receiver, which are not recoverable, are received or extracted from proxy or ISP servers, as the servers store a copy of all the e-mails after their respective delivery. In addition, SMTP servers, which store the details like credit card number and other data associated with a particular user, may be used to identify the owner of the particular e-mail address.
5. **Investigating Network Device:** The source of an e-mail message can also be investigated with the help of logs maintained by network devices, such as routers, firewalls, and switches. Owing to its complexity, this technique is only deployed in the absence of logs of ISP or proxy servers. Unavailability of server logs may occur due to various reasons, such as absence of chain of evidences.
6. **Fingerprints of Sender Mailers:** The received header field proves to be helpful in the identification of software which handles e-mail at server. Also, different set of headers, such as "X-Mailers" can be used for the identification of the software, which handles e-mail at the client. These headers describe information about the applications and their servers used by the client to send e-mails.
7. **Software-embedded identifiers:** The information about the creator of e-mails may be included in the custom headers or in form of MIME contents as a TNEF. The investigation may reveal names of PST files, MAC address, etc., of the computer, which was used to send e-mails.

Scanned by CamScanner

E-mail forensics talk about the study of source and content of e-mail as evidence to identify the actual sender and receiver of a message, data/time of transmission, thorough record of e-mail transaction, intending to the sender, and so on. This learning includes examination of metadata, keyword searching, port scanning, and more for authorship acknowledgment and credentials of email scams. Various methods that are used for e-mail forensic are briefly described in the following sections.

7.4.2.2 Header Analysis

Metadata in the e-mail message is the method of governing information, that is, envelope and headers together with headers in the message body comprise information about the sender and/or the track along which the message has traversed. Some of these may be tricked to cover the identity of the source. A thorough examination of these headers and their association is done in header analysis.

7.4.2.3 Bait Tactics

In bait tactic exploration, an e-mail with http: "Error! Filename not specified." Label-devising image source at some computer observed and supervised by the detectives is sent to the source of e-mail under examination comprising real (genuine) e-mail address. When the e-mail is read or opened, a log entry comprising the IP address of the recipient (source of the e-mail under examination) is recorded on the http server holding the image, and thus sender is tracked. However, if the recipient (source of the e-mail under examination) is using a proxy server, then IP address of the proxy server is logged. The log on proxy server can be used to track the source of the e-mail under examination. If the proxy server's log is inaccessible due to some reason, then detectives may send the tactic e-mail containing:

1. embedded Java Applet that runs on receiver's computer or
2. HTML page with Active X Object, both targeting to extract IP address of the receiver's computer and e-mail it to the investigators.

7.4.2.4 Server Investigation

In this research, duplicates of distributed e-mails and server logs are examined to classify source of an e-mail message. E-mails purged from the clients (senders or receivers) whose recovery is impossible may be requested from servers (proxy or ISP), as most of them store a copy of all e-mails after their deliveries. Further, logs preserved by servers can be studied to track the address of the computer accountable for making the e-mail transaction. However, servers store the copies of e-mail and server logs only for restricted amount of time and some may not cooperate with the investigators. Further, SMTP servers, which store data like credit card numbers and other data relating to the owner of a mailbox, can be used to identify the person behind an e-mail address.

7.4.2.5 Network Device Investigation

In this form of e-mail investigation, logs preserved by the network devices such as routers, firewalls, and switches are used to examine the source of an e-mail message. This form of examination is difficult and is used only when the logs of servers (proxy or ISP) are inaccessible due to some cause (e.g., when ISP or proxy does not preserve a log or absence of collaboration by ISPs or failure to preserve chain of evidence).

7.4.2.6 Software Embedded Identifiers

Some information about the owner of the e-mail, attached files, or documents may be included with the message by the e-mail software used by the sender for composing e-mail. This information may be included in the form of custom headers or in the form of MIME text as a Transport Neutral Encapsulation Format (TNEF). Examining the e-mail for these particulars may reveal some important information about the

Scanned by CamScanner

source e-mail preferences and choices that could assist client-side proof collecting. The examination can disclose PST file names, Windows logon username, MAC address, and more of the client computer used to send e-mail message.

7.4.2.7 Sender Mailer Fingerprints

Credentials of software handling e-mail at server can be revealed from the received header field and credentials of software handling e-mail at client can be determined by means of diverse set of headers like "X-Mailer" or equivalent. These headers describe applications and their versions used at the clients to send e-mail. This information regarding the client computer of the sender can be used to help investigators formulate an operative plan, and thus prove to be very useful.

7.4.3 Mail Forensic Tools

There are numerous tools which may contribute in the study of sender and text of e-mail message, so that an attack or the mischievous motive of the invasions may be examined. These tools, while giving easy-to-use browser setup, computer-generated reports, and other features, help to recognize the origin and destination of the message, track the route pass through by the message, recognize spam and phishing networks, and so on. This section presents some of these tools.

7.4.3.1 eMailTrackerPro

eMailTrackerPro examines the headers of an e-mail to sense the IP address of the computer that directed the message, so that the source can be chased down. It can track numerous e-mails at the same time. The geographical position of an IP address is important and crucial evidence for defining the risk level or legitimacy of an e-mail message. This tool can locate the city that the e-mail most probably came from. It recognizes the network provider (or ISP) of the source and offer contact information for further examination. The real path to the source's IP address is stated in a routing table, offering additional position information to help find out the source's correct and accurate position. The misuse reporting feature in it can be used to make additional examination stress free. It checks the mail against DNS blacklists, like Spamcop, to additionally defend against junk and mischievous e-mails. It supports Japanese, Russian, and Chinese language junk filters in addition to the English language. A main feature of this tool is misuse reporting that can generate a report that can be sent to the ISP of source. The ISP can then take steps to take legal action against the account holder and help put a stop to junk.

7.4.3.2 EmailTracer

EmailTracer is an Indian effort in cyber forensics by the Resource Centre for Cyber Forensics (RCCF), a leading center for cyber forensics in India. It develops cyber forensic tools grounded on the necessities of law enforcement agencies. Among numerous other digital forensic tools, it has established an e-mail tracer tool named EmailTracer. This tool tracks the initiating IP address and other particulars from e-mail header, produces thorough HTML report of e-mail header analysis, discovers the city-level particulars of the source, plots path traced by the mail, and show the initiating geographic position of the e-mail. In addition to these, it has keyword searching ability on e-mail content together with attachment for its classification.

7.4.3.3 Adcomplain

Adcomplain is a tool for reporting unsuitable marketable e-mails and make use of net postings, along with chain letters and "make money fast" postings. It robotically examines the message, composes a misuse report, and mails the report to the offender's internet service provider by carrying out an effective header examination. The report shows the support preceding the U.S. Federal Trade Commission. Adcomplain can be taken back from the command line or robotically from numerous news and mail readers.

Scanned by CamScanner

7.4.3.4 Aid4Mail Forensic

Aid4Mail Forensic is an e-mail investigation software for forensic analysis, e-discovery, and court case proceedings support. It is an e-mail relocation and translation tool, which supports various mail formats together with Outlook (PST, MSG files), Windows Live Mail, Eudora, Thunderbird, and MBOX. It can explore through mail by date, header content, and by message body content. Mail folders and files can be managed even when disconnected from their e-mail client, together with those stored on CD, DVD, USB drives, flash drives, floppies, portable HDDs, and so on. Aid4Mail Forensic can hunt PST files and all maintained mail formats by date range and by keywords in the message body or in the headers. Extraordinary Boolean operations are maintained. It is capable to recover the deleted e-mail from MBOX files and can bring back deleted e-mail during exportation.

7.4.3.5 AbusePipe

AbusePipe examines abuse objection e-mails and regulates which of ESP's clients are distributing spam grounded on the material in e-mailed objections. It robotically creates reports recording clients disrespecting ESP's suitable user policy, so that action to close them down can be taken instantaneously. AbusePipe can be configured to robotically answer to individuals reporting abuse. It can support in meeting authorized responsibilities like reporting on the clients linked to a given IP address at a specified date and time.

7.4.3.6 AccessData's FTK

AccessData's FTK is typically court-validated digital investigations platform computer forensics software, passing on computer forensic analysis, decryption, and password cracking within a spontaneous and personable interface. It has rapidity, analytics, and enterprise class scalability. It is recognized for its instinctive interface, e-mail study, customizable data views, and solidity. It maintains popular encryption technologies, like Credant, SafeBoot, Utimaco, EFS, PGP, Guardian Edge, Sophos Enterprise, and S/MIME. Its present maintained e-mail types are Lotus Notes NSF, Outlook PST/OST, Exchange EDB, Outlook Express DBX, Eudora, Microsoft Internet Mail, Earthlink, Thunderbird, Quickmail, Netscape, AOL, and RFC 833.

7.4.3.7 EnCase Forensic

EnCaseForensic is computer forensic application that offers detectives the capability to copy a drive and reserve it in a forensic way by means of the EnCase evidence file format, a digital evidence container examined by courts universally. It comprises a full set of enquiries, bookmarking, and reporting features. Guidance software and third-party vendors offer support for extendedabilities to make sure that forensic inspectors have the most complete set of services. Together with many other network forensics researches, it also supports Internet and e-mail examination. It comprised Instant Messenger toolkit for Microsoft Internet Explorer, Mozilla Firefox, Opera, and Apple Safari. The e-mail support contains for Outlook PSTs/OSTs, Microsoft Exchange EDB Parser, Outlook Express DBXs, Lotus Notes, Hotmail, AOL, Netscape Mail, Yahoo, and MBOX records.

7.4.3.8 FINALeMAIL

FINALeMAIL can bring back the e-mail database file and finds lost e-mails that do not have data position information related with them. FINALeMAIL has the ability of reestablishing lost e-mails to their source state, reobtain full e-mail database files even when such files are criticized by viruses or spoiled by unintentional layout. It can recover e-mail messages and attachments emptied from the "Deleted Items Folder" in Netscape Mail, Microsoft Outlook Express, and Eudora.

7.4.3.9 Forensics Investigation Toolkit

Forensics Investigation Toolkit (FIT) is content forensics toolkit to read and examine the content of the Internet raw data in Packet CAPture (PCAP) format. FIT offers auditors, security administrative officers,

Scanned by CamScanner

fraud, and forensic detectives along with legal prosecution officers the power to carry out content analysis and rebuilding on precaptured Internet raw data from wired or wireless networks. All protocols and services examined and rebuilt are shown in readable presentation to the users. The other individuality of the FIT is that the imported raw data files can be directly described and rebuilt. It supports case management functions, thorough information together with Date-Time, Destination IP, Source IP, Source MAC, WhoIS, and Google Map integration purposes. Examining and rebuilding of various Internet traffic types which comprises e-mail (POP3, SMTP, IMAP), IM or Chat (MSN, ICQ, Yahoo, QQ, Skype Voice Call Log, UT Chat Room, Gtalk, IRC Chat Room), Webmail (read and sent), File Transfer (FTP, P2P), Telnet, HTTP (Content, Upload/Download, Video Streaming, Request), and Others (SSL) can be achieved using this toolkit.

7.5 Malware Handling

Malware analysis is a process to perform analysis of malware and how to study the components and behavior of malware. In this section, it will use two methods of malware analysis: (i) static analysis and (ii) dynamic analysis. Static analysis is a method of malware analysis which is done without running the malware, while dynamic analysis is a method of malware analysis, which the malware runs in a secure system. Malware analysis is important, since many malwares at this day are not detectable by antivirus. Now viruses are made with special ability to avoid detection from antivirus. On this research, we will focus on implementation of malware analysis using static analysis and dynamic analysis method.

Static analysis is a method of analysis of malware that is done without running the malware, and analysis using this method is much more secure than using the method of dynamic analysis. Malware analysis using the method of static analysis can be further divided into two stages: (i) basic static analysis and (ii) advanced static analysis. Dynamic malware analysis is a method of analysis of malware by running the malware. To make it more secure, malware will run inside a virtual machine, so the malware will not damage your computer system. Malware analysis using the method of dynamic analysis can be divided into two stages: (i) basic dynamic analysis and (ii) advanced dynamic analysis. Malware analysis method can be seen in Fig. 7.16.

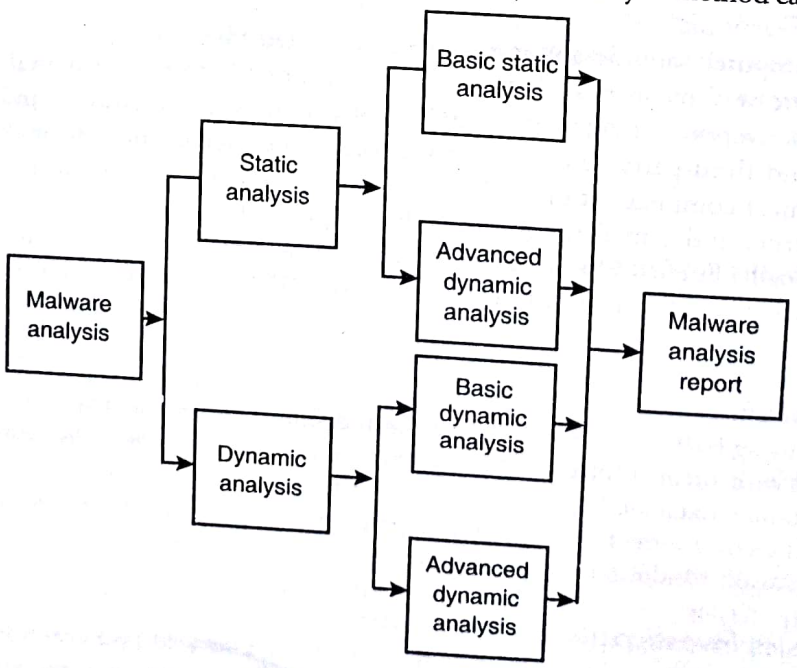

Figure 7.16 Malware analysis method.

Scanned by CamScanner

7.5.1 Basic Static Analysis

The basic method in static analysis, carried out testing against a program which is called as malware with doing the scanning using antivirus, moreover also doing hashing, and detection of packed or obfuscated at the program. As well as conducting an analysis of the structure of portable executable which is owned by the program.

7.5.2 Advanced Static Analysis

In the advanced method of static analysis, further analysis will be undertaken of the method of static analysis with analysis against the strings, linked libraries and function as well as using IDA disassembler.

7.5.3 Basic Dynamic Analysis

The basic method in dynamic analysis, will be build a virtual machine that will be used as a place to do a malware analysis. In addition, malware will be analysis using malware sandbox and monitoring process of malware and analysis packets data made by malware.

7.5.4 Advanced Dynamic Analysis

In the advanced method of dynamic analysis, further analysis will be undertaken of dynamic analysis methods with debugging on malware, analysis the registry and do an analysis on a windows system.

7.5.5 Malware Analysis Report

From the results of malware analysis using static analysis and dynamic analysis method, we will obtain a report of information on the characteristics of malware.

Summary

Examining and analyzing digital evidence depend on the nature of the investigation and the amount of data to process. You begin a computer forensics case by creating an investigation plan that defines the investigation's goal and scope, the materials needed, and the tasks to perform. Depending on the evidence you find, you might have to modify your investigation plan at some point.

Key Terms

- **Bit shifting:** The process of shifting one or more digits in a binary number to the left or right to produce a different value.
- **Key escrow:** A technology designed to recover encrypted data if users forget their passphrases or if the user key is corrupted after a system failure.
- **Known File Filter (KFF):** A database containing the hash values of known legitimate and suspicious files. It is used to identify files for evidence or eliminate them from the investigation if they are legitimate files.
- **Scope creep:** The result of an investigation expanding beyond its original description, because the discovery of unexpected evidence increases the amount of work required.

Scanned by CamScanner

- **Steganography:** A cryptographic technique for embedding information in another file for the purpose of hiding that information from casual observers.
- **Client/server architecture:** A network architecture in which each computer or process on the network is a client or server. Clients request services from a server, and a server processes requests from clients.
- **Enhanced Simple Mail Transfer Protocol (ESMTP):** An enhancement of SMTP for sending and receiving e-mail messages. ESMTP generates a unique, non-repeatable number that is added to a transmitted e-mail. No two messages transmitted from an e-mail server have the same ESMTP value.
- **Mbox:** A method of storing e-mail messages in a flat plaintext file.
- **Messaging Application Programming Interface (MAPI):** The Microsoft system that enables other e-mail applications to work with each other.
- **Multipurpose Internet Mail Extensions (MIME):** A specification for formatting non-ASCII messages, such as graphics, audio, and video, for transmission over the Internet.
- **Phishing:** A type of e-mail scam that is typically sent as spam soliciting personal identity information that fraudsters can use for identity theft.
- **Post Office Protocol Version 3 (POP3):** A protocol for retrieving e-mail messages from an e-mail server.
- **Simple Mail Transfer Protocol (SMTP):** A protocol for sending e-mail messages between servers.
- **Spoofing:** Transmitting an e-mail message with its header information altered so that its point of origin appears to be from a different sender. Spoofed e-mails are also referred to as forged e-mail. Spoofing is typically used in phishing and spamming to hide the sender's identity.

Review Questions

1. What is hacker? Explain hacker tools concept.
2. Write a short note on steps of UNIX system investigation.
3. Name different log files used during Windows investigation.
4. Describe the basic investigative steps for formal examination of Windows System.
5. Explain the process of restoring the forensic duplication.
6. Describe the basic investigative steps for formal examination of Unix System.
7. What do you mean by data analysis?

Scanned by CamScanner