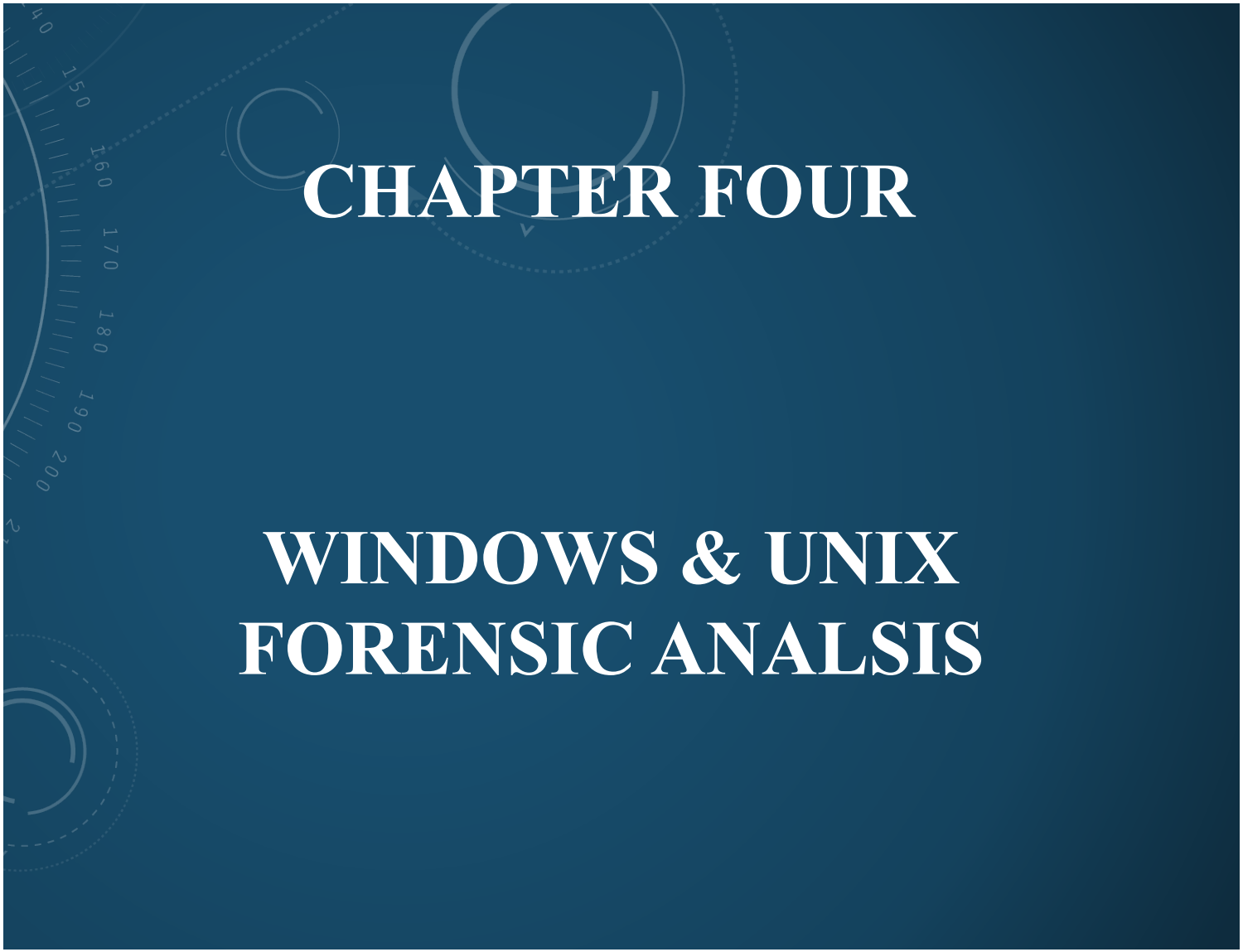

4.0 Preparation Steps for Forensic Analysis

4.1 Investigating Windows Systems

4.2 Investigating UNIX Systems

4.3 Investigating Applications

4.0 Preparation Steps for Forensic Analysis

4.1 Investigating Windows Systems

4.2 Investigating UNIX Systems

4.3 Investigating Applications

Preparation Steps for Forensic Analysis :

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.

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.

4.0 Preparation Steps for Forensic Analysis

4.1 Investigating Windows Systems

4.2 Investigating UNIX Systems

4.3 Investigating Applications

Preparation Steps for Forensic Analysis :

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.

a. 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.

4. Converting a Qualified Forensic Duplicate to a Forensic Duplicate :

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.

5. Recovering Deleted Files on Windows Systems :

a. 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.

4.0 Preparation Steps for Forensic Analysis

4.1 Investigating Windows Systems

4.2 Investigating UNIX Systems

4.3 Investigating Applications

Preparation Steps for Forensic Analysis :

5. Recovering Deleted Files on Windows Systems :

b. 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:

(1) Supports a wide variety of file systems, including FAT12, FAT16, FAT32, NTFS, HPFS, Macintosh, OS/2, EXT2, EXT3, and UFS.

(2) Recovers file slack and not allocate space. The improved loopback kernel makes it easy to recognize
slack and not allocate drive space.

(3) Provides an efficient, effective, and accurate undelete utility.

(4) 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.

(5) Handles compressed drives (DriveSpace, Dblspace, and DriveSpace 3).

(6) Delivers widespread checking and cataloging of all forensic activities.

(7) Delivers for data authentication and reliability.

4.0 Preparation Steps for Forensic Analysis

4.1 Investigating Windows Systems

4.2 Investigating UNIX Systems

4.3 Investigating Applications

Preparation Steps for Forensic Analysis :

6. Recovering Unallocated Space, Free Space, and Slack Space :

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.

Slack and Its Types :

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

a. 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.
Cluster and sector: Operating systems arrange all data stored on a hard drive into segments called allocation units or clusters.

b. 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.

4.0 Preparation Steps for Forensic Analysis

4.1 Investigating Windows Systems

4.2 Investigating UNIX Systems

4.3 Investigating Applications

Preparation Steps for Forensic Analysis :

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:

- **a.** Full path of each file found on the evidence media.
- **b.** Last written and modified time/date stamps for each file.
- **c.** Creation time/date stamps, if they exist (Linux does not maintain a creation time/date stamp!).
- **d.** Last access time/date stamps.
- **e.** Logical size of each file.
- **f.** An MD5 hash of each file.

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.

4.0 Preparation Steps for Forensic Analysis

4.1 Investigating Windows Systems

4.2 Investigating UNIX Systems

4.3 Investigating Applications

Investigating Windows Systems :

Refer Word File for this topic Module 4.1

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.

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.

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.

4.0 Preparation Steps for Forensic Analysis

4.1 Investigating Windows Systems

4.2 Investigating UNIX Systems

4.3 Investigating Applications

Investigating Unix Systems :

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.

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.

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.

6. Checking for Unauthorized Access Points :

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.

4.0 Preparation Steps for Forensic Analysis

4.1 Investigating Windows Systems

4.2 Investigating UNIX Systems

4.3 Investigating Applications

Investigating Unix Systems :

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.

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.

Investigating Applications :

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.

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.

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.

a. *eMailTrackerPro*
b. *EmailTracer*
c. *Adcomplain*
d. *Aid4Mail Forensic*
e. *AbusePipe*
f. *AccessData's FTK*
g. *EnCase Forensic*
h. *FINALeMAIL*
i. *Forensics Investigation Toolkit*