iiNURTURE
Education Solutions
TOMORROW'S HERE

Chapter 3.1

Forensics Investigation Techniques

Aim

To equip students with the knowledge of various forensics investigation techniques used in computer forensics

Instructional Objectives

After completing this chapter, you should be able to:

- Explain forensic investigation
- Elaborate on forensics in regards to Windows platform
- Explain important factors of Linux forensic
- Explain the concept of mobile forensic

Forensic Investigation

Forensic Investigation

Forensic investigation is the technical analysis process of a crime scene using specialized knowledge and skills, policies and procedures, methods and tools to establish the facts that is acceptable to the court of law.

What is Computer Forensic Investigation?

Computer forensic investigation is the process of examination of all possible computer or data processing/storage devices using specialized means, methods and programs to establish the facts that is acceptable in a court of law.

- It is done in cases ranging from civil to criminal crime.
- Data storage devices based on the FAT and NTFS, data storage formats are analyzed in the process of investigation.

Computer forensic investigation process

Quiz / Assessment

1) What is Computer forensic investigation?

a) It is the process of scientific examination of data from computer storage media
b) It is the process of scientific examination of DNA found in the crime scene
c) It is the process of auditing of financial data found in the crime scene
d) It is the process of verification of all biological evidences

Quiz / Assessment

2) What type of evidence do computer forensic officers hope to acquire in a crime scene?

a) DNA evidence admissible in a court of law
b) Physical evidence admissible in a court of law
c) Digital evidence admissible in a court of law
d) Fingerprint evidence admissible in a court of law

Quiz / Assessment

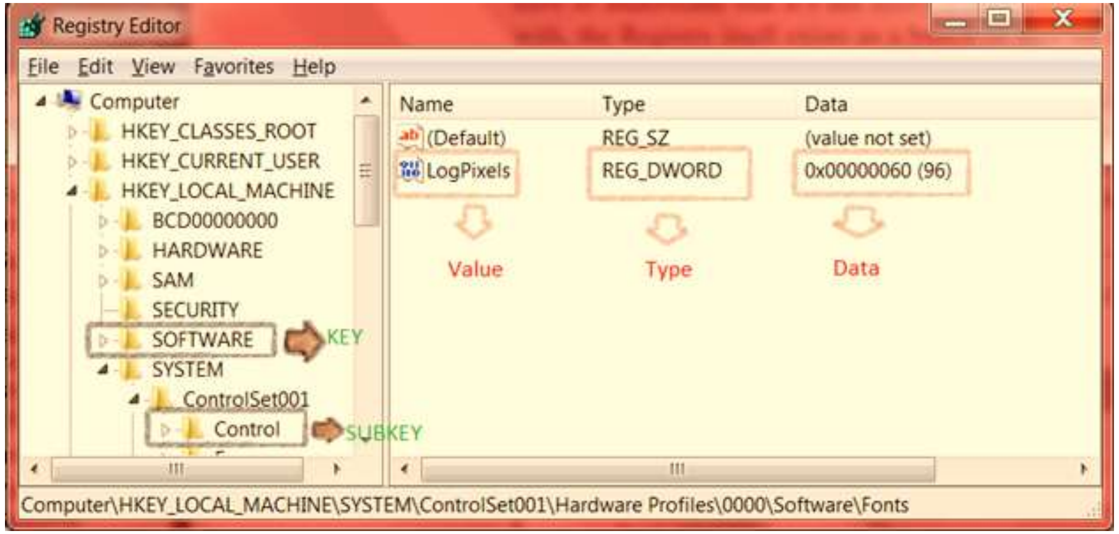
3) Data storage devices based on the FAT and NTFS, __________ formats are analyzed in the process of investigation.

a) Data storage
b) Data file
c) Data process
d) Data disc

Windows Forensics

Windows Forensics

The Windows operating system creates various artefacts during the operation. In Every artefact is unique and provides some form of evidence or action performed on the system, rendering the task of forensic investigation, an easy process.



Name	Type	Data
(Default)	REG_SZ	(value not set)
LogPixels	REG_DWORD	0x00000060 (96)

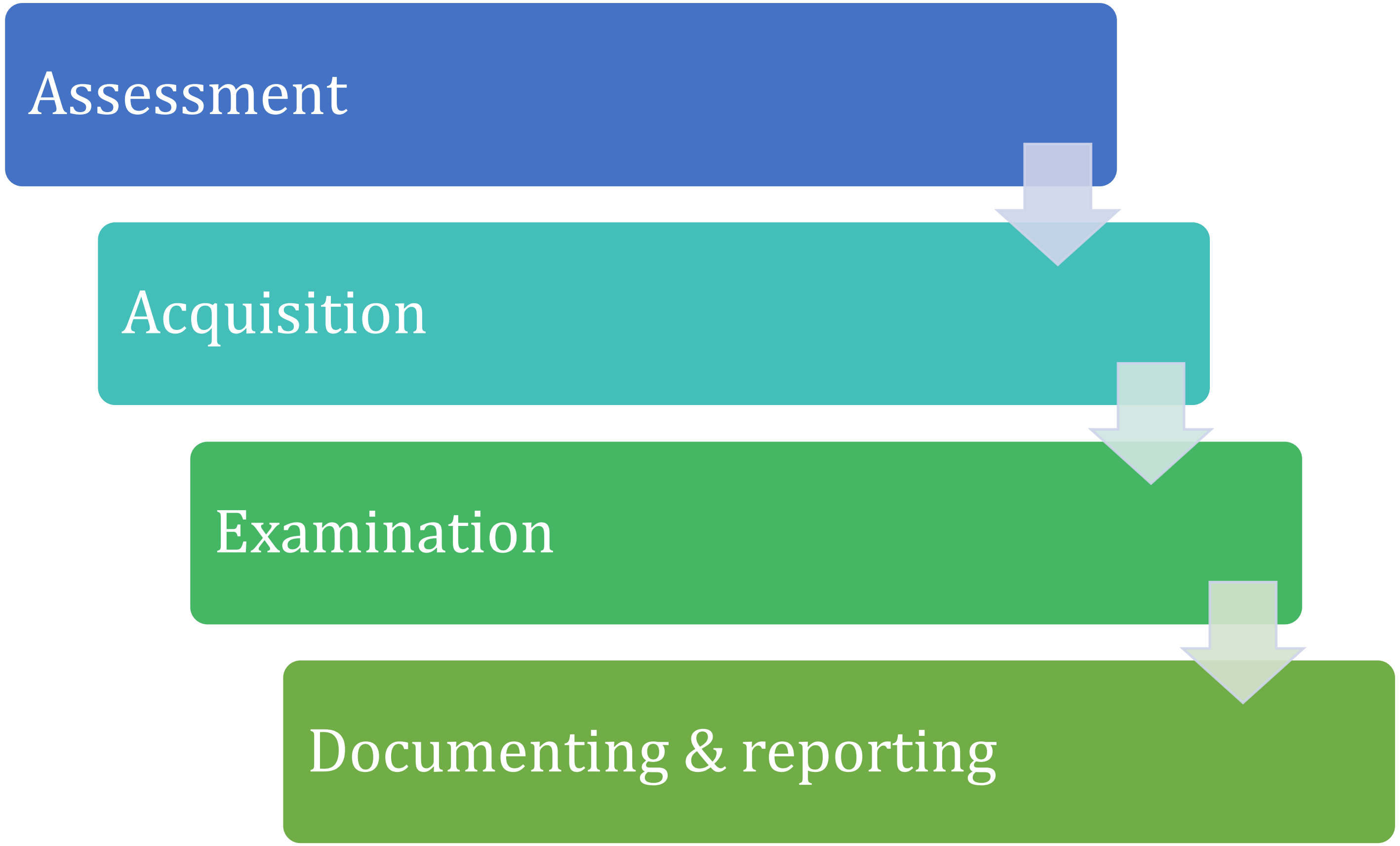
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Hardware Profiles\0000\Software\Fonts

Example of windows forensic

For Windows Forensics, it is Necessary to have:

- Good knowledge of the windows file system like FAT, NTFS etc.
- A good understanding of various windows artefact
- Understanding of various application and its functioning
- Hands on experience of various tools and techniques

Process of digital evidence



Assessment

Acquisition

Examination

Documenting & reporting

Windows File System

This system is used to store and retrieve files from a raw storage media.

Recovering deleted files

A file once deleted is not permanently 'removed' from the system.

Windows artefacts

During file operation windows system creates various related artefact on the system that includes but not limited to Windows File Systems (MFT) attributes, Windows Registry, Windows Event Logs, Prefetch/Superfetch Files, Shortcut & Link Files.

Quiz / Assessment

1) Why is the process of computer forensic investigation in Windows OS devices, an easy affair?

a) Because of the creation of 'artefacts' by the Windows OS system
b) Because Windows OS system retains all deleted files
c) Because Windows OS system prevents user from erasing vital files
d) Because Windows OS system is easy and user friendly

Quiz / Assessment

2) What is the full form of 'FAT'?

a) File Acquisition Table
b) File Allocation Table
c) File Application Table
d) File Assessment Table

Quiz / Assessment

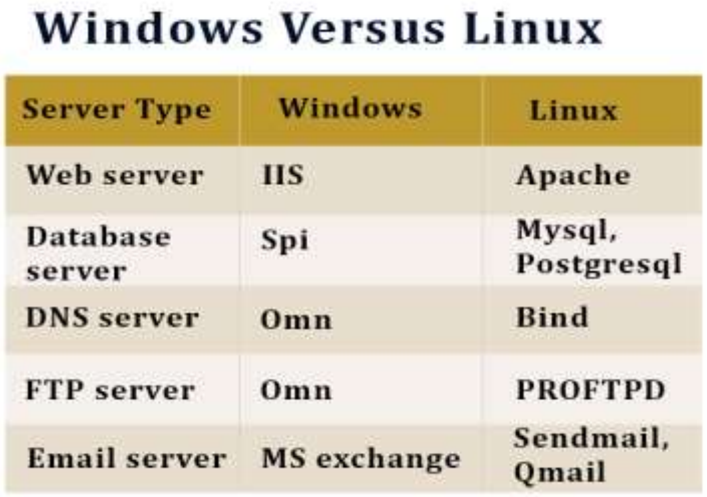
3) Where do deleted files go?

a) Into non being, as they are removed from the computer
b) They remain in the system as only the file information path is erased
c) Deleted files 'vanish' from the recycle bin and cannot be found there
d) Deleted files do not exist in the system as they are 'disappeared'

Important Factors of Linux Forensic

Introduction to Linux Forensics

It is commonly noticed in cases of cybercrime that intrusion evidences can be found in the file system in the form of some files or logs. Hence, knowing the file system functions and structure makes it easy to search, retrieve and analyse evidence.



Windows Versus Linux

Server Type	Windows	Linux
Web server	IIS	Apache
Database server	Spi	Mysql, Postgresql
DNS server	Omn	Bind
FTP server	Omn	PROFTPD
Email server	MS exchange	Sendmail, Qmail

Windows versus Linux

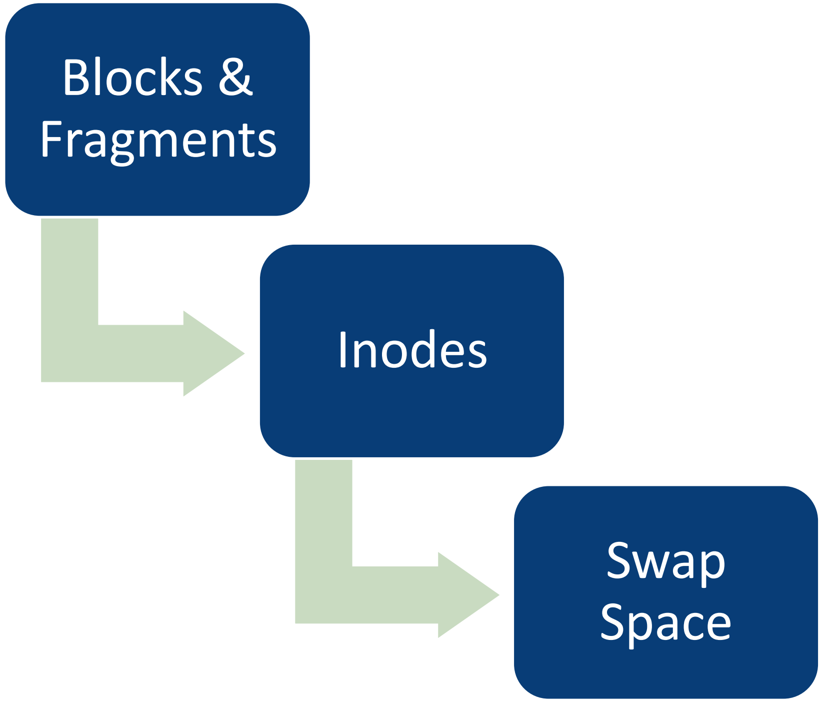
Important Factors of Linux Forensic

Forensics investigation on a Linux system is completely different from Windows forensics.

In Linux operating system, everything is treated as a file. It uses **ext (Extended File System)** file system most of the time.

SWAP is not a file system but actually a swap space just like a page files in windows for faster performance.

Fundamentals of individual building blocks of EXTn file system

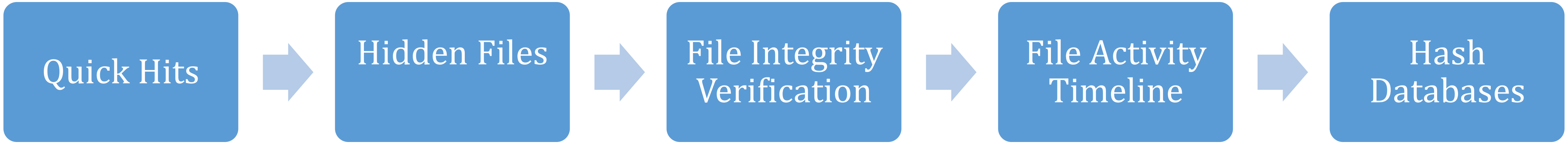


Linux File System

In Linux operating system, everything is treated as a file. It uses **ext** (Extended File System) file system most of the time.

Linux Analysis

There are numerous methods in Linux to dissect the information. Four methods are available in Linux analysis. They are:



Quick Hits

Hidden Files

File Integrity Verification

File Activity Timeline

Hash Databases

Quiz / Assessment

1) What is called as a 'swap space'?

a) A swap space is a major building block of the Linux system
b) It is a mechanism which can be used to 'swap' files
c) It is a mechanism by which windows files can be turned to Linux files
d) It is a mechanism which oversees replacement activities

Quiz / Assessment

2) Who discovered the 'EXT3' File system?

a) Stephen Cowey
b) Stephen Hawking
c) Stephen Tweedie
d) Stephen Curry

Quiz / Assessment

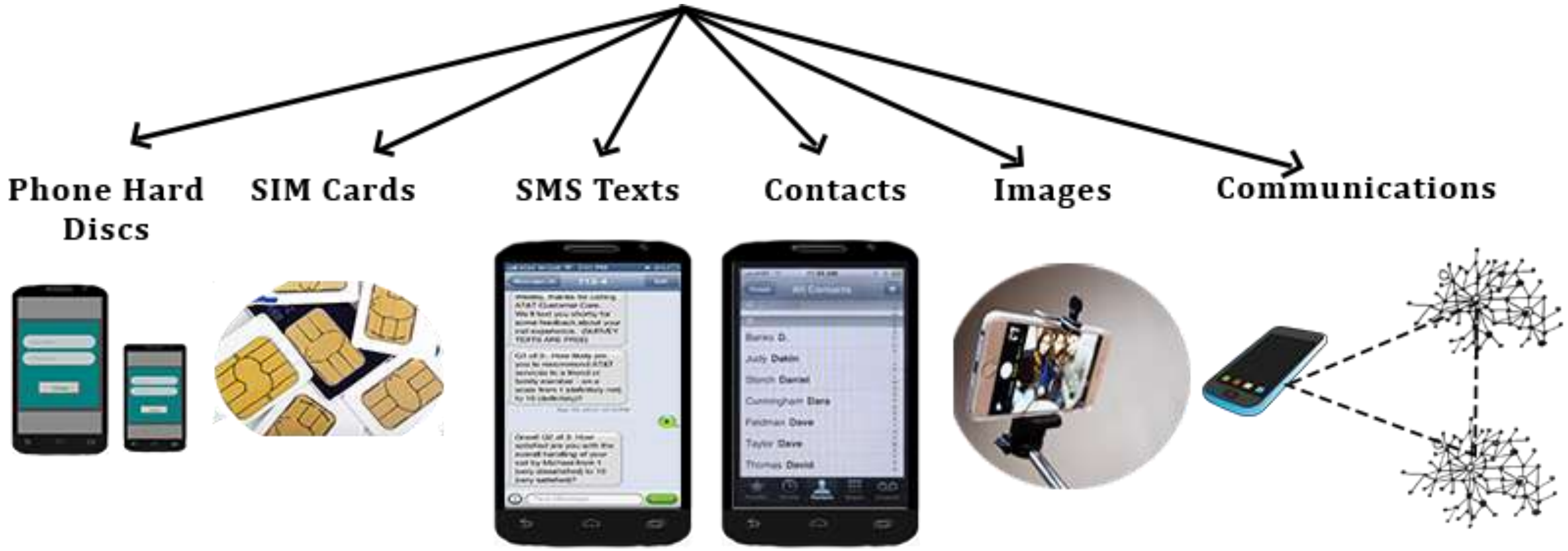
3) Identify which one of the following is a forensic analysis tool.

a) RegEdit
b) RegLookup
c) RegReveal
d) RegFind

Mobile Forensics

What is Mobile Forensics?

‘Mobile Forensics’ is a branch of computer forensics dealing primarily with the task of recovering digital data and evidence from mobile devices in forensically sound conditions.



Mobile Forensics

Mobile Forensics

Mobile Forensics the most advanced and new branch of computer forensics and is quite challenging because of the availability of various operating and daily new applications announcements

Mobile forensics analysis is not at all an easy task. There is various mobile devices forensics hardware and software's have been developed and available commercially and freeware but, still we don't have fit for all kind of tools in the market.

The process of the mobile device forensic includes following phases

1.Seizure

2.Acquisition

3.Manual

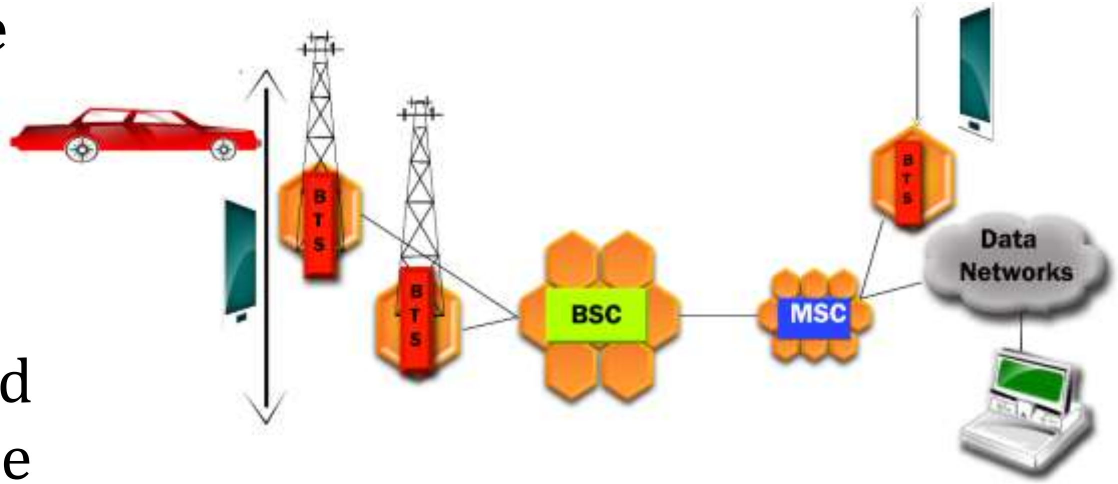
4.Logical

5.Physical

6.Examination and Analysis

Cellular Network

The process of transmission and reception of phone calls and other data on mobile and smartphones is made possible by the communication network.



Example of Cellular Network

Handset Specification

In smart phone there are many pre-defined applications and ability of storing customize applications.

Mobile Operating System

A mobile operating system is an operating system for smartphones, tablets, PDAs, or other mobile devices. It allows smartphones, tablet PCs and other devices to run applications and programs. A mobile OS typically starts up when a device powers on.

Four main Mobile OS

Procedures for Handling Handset Evidence

- Securing and Evaluating the Scene
- Documenting the Scene
- Isolation
- Packaging
- Transporting
- Storing Evidence
- Triage/On-Site Processing
- Triage Decision Making

Quiz / Assessment

1) What does 'mobile forensics' deal with?

a) Cellular, mobile and smartphones
b) Laptops and micro PC's
c) Microcomputers
d) Microprocessors

Quiz / Assessment

2) What is the purpose of an 'IMEI' number?

a) It helps in ensuring that phone calls are not dropped
b) It plays a role in sending and receiving of SMS's
c) It helps Forensic investigators in properly identifying a mobile phone
d) It helps in identifying cellular nodes

Quiz / Assessment

3) What record framework is the most used part on NAND memory?

a) FAA record framework
b) FAN record framework
c) FAV record framework
d) FAT record framework

Activity

Offline Activity

Offline Activity (15 min)

- List the challenges faced by investigators in obtaining information from mobile devices to use in criminal investigations

Note: Refer Table of Content for the activities

Summary

✓ When a file is permanently deleted from a file system, it can be retrieved using data recovery tools such as Data Recovery Wizard Professional, Recuva (Windows), PhotoRec (Windows/Mac/Linux), Undelete Plus (Windows), TestDisk (Windows/Mac/Linux), etc.

✓ During Forensics investigation collecting data is an important process. Windows by default collects and stores various artefacts related to user activity, internet activist, logon events and various applications related activities. This is very useful for collecting data.

✓ Mobile Forensics is the most advanced and new branch of computer forensics and is quite challenging. Various mobile devices forensics hardware and software's are used in mobile forensic analysis.

e-References

- What information appears in event logs? (Event Viewer) - Windows Help. (2016). windows.microsoft.com. Retrieved 22 June 2016, from http://windows.microsoft.com/en-in/windows/what-information-event-logs-event-viewer#1TC=windows-vista

- 152 NTFS. (2016). Cse.scu.edu. Retrieved 22 June 2016, from http://www.cse.scu.edu/~tschwarz/coen252_07Fall/Lectures/NTFS.html

- Forensic Analysis of Prefetch files in Windows - Magnet Forensics Inc.. (2014). Magnet Forensics Inc.. Retrieved 22 June 2016, from https://www.magnetforensics.com/computer-forensics/forensic-analysis-of-prefetch-files-in-windows

External Resources

- Hayes, D. D. *A Practical Guide to Computer Forensics Investigations.* US: Pearson Education, Inc. 2005

- Nelson, B., Phillips, A., & Steuart, C. *Guide to Computer Forensics and Investigations, Fourth Edition*. USA: Cengage Learning. 2010

- Philipp, A., Cowen, D., & Davis, C. *Hacking Exposed Computer Forensics, Second Edition*. New York: McGraw-Hill. 2010