# Cyber Forensics

Vasudevan T V

# Module 1
# Introduction

- Cyber Forensics is a scientific method for extracting information from digital devices for use as evidence in criminal or civil cases
- Cyber forensics can do the following
- It can recover deleted files, chat logs, emails, etc.
- It can also get deleted SMS, Phone calls
- It can determine which user used which system and for how much time
- It can identify which user ran which program

# Types of Computer Forensics

- Memory Forensics
- It deals with collecting information from main memory, cache
- Disk Forensics
- It deals with recovering information from secondary storage media such as hard disks, pen drives, CD/DVD drives
- Database Forensics
- It deals with examining and analysing databases
- Email Forensics
- It deals with extracting information from Emails
- Network Forensics
- It deals with extracting information from various computer networks
- Mobile Phone Forensics
- It deals with extracting information from Mobile Phones

# Examples of Computer Crimes

- Hacking
- Accessing or stealing the information of an individual or a company without permission
- Copyright Violation
- Stealing or using copyrighted material without permission
- Cyber Terrorism
- Threatening or blackmailing a person or company
- Software Piracy
- Copying, distributing, or using software not purchased by the software user
- Computer Viruses
- The deliberate release of computer viruses that damage systems
- Financial Cyber Crimes
- Online banking frauds, credit card frauds, ATM frauds etc.

# Gathering Evidence

- To gather evidence from a digital device, you have to extract the exact copy from its storage medium
- This exact copy is called the bit stream copy (forensic copy) of the storage medium
- The process of extracting this copy is called acquiring an image or making an image of the storage medium
- This bit stream copy of all data in a disk is stored in a file called bit stream image
- The bit stream copy is different from the backup copy of a disk
- Backup software can copy only files that are stored in a folder or are of a known file type
- Backup software can't copy deleted files

# Storage Formats for Digital Evidence

- The gathered digital evidence (image file) is stored in different formats

1. raw format

- It is bit-by-bit copy of the data on the storage media without any additions and or deletions
- It does not contain any metadata
- It is an open source format
- advantage - fast data transfer
- disadvantage - It requires as much space as the original disk

# Storage Formats for Digital Evidence

- The gathered digital evidence (image file) is stored in different formats

2. proprietary format

- It is a vendor specific format for storing digital evidence
- It can only be read by the corresponding vendor software
- Example
- ILookIX image acquisition tool IXImager produces three proprietary formats—IDIF, IRBF and IEIF
- They can be read by IXImager only
- advantage - we can compress image files, add metadata such as date and time of data extraction, name of the investigator, comments, case details etc.
- disadvantage - It cannot be read by other software

# Storage Formats for Digital Evidence

- The gathered digital evidence (image file) is stored in different formats

3. Advanced Forensic Format (AFF)

- It is an open source format developed by Dr. Simson L. Garfinkel
- It is capable of producing compressed or uncompressed image files
- We can store metadata as part of image files

# Data Acquisition Methods

- There are 4 types of data acquisition methods

1. static acquisition

- It retrieves data from a non volatile source such as hard disk drive or USB drive

2. live acquisition

- It retrieves data from a volatile source such as RAM or a computer network

3. logical acquisition

- It captures only specific files of interest to the case or specific types of files

4. sparse acquisition

- It is a type of logical acquisition which also captures fragments of deleted data

# Data Acquisition Tools

- Accessing a disk drive directly can easily contaminate the evidence during forensics acquisition
- Hence it is accessed indirectly using boot CD/DVD/USB drives
- After booting using CD/DVD/USB Drives, the hard disk is write protected
- Mini-WinFE is one such boot utility for Windows
- Linux boot CD/DVD/USB can also be used for this purpose
- We can also use Linux live CD/DVD/USB drives for digital forensics analysis
- Using a boot CD/DVD/USB drive, we can access the hard disk, without having an OS
- Using a live CD/DVD/USB drive, we can start an OS

# Data Acquisition Tools

- The following Linux live CD/DVD/USB drives supports digital forensics analysis
- Penguin Sleuth Kit (`www.linux-forensics.com`)
- CAINE (`www.caine-live.net`)
- Deft (`www.deftlinux.net`)
- Kali Linux (`www.kali.org`)
- Knoppix (`www.knopper.net/knoppix/index-en.html`)
- SANS Investigate Forensic Toolkit (SIFT)(`http://computer-forensics.sans.org/community/downloads`)

# Digital Evidence Validation Methods

- We need to verify the integrity of data collected during the acquisition phase
- This process is called digital evidence validation
- Here we will be using a hashing algorithm utility
- This algorithm when applied on a data set such as file or disk drive, creates a binary or hexadecimal number, called a hash value
- This hash value is unique and is also referred to as digital fingerprint
- Making any alteration in one of the files — even changing one letter from uppercase to lowercase — produces a completely different hash value

# Digital Evidence Validation Tools

- Linux Validation Tools
- The linux shell commands dd and dcfldd, have several options that can be combined with other commands to validate data
- Current distributions of Linux include two hashing algorithm utilities: md5sum and sha1sum
- Both utilities can compute hashes of a single file, multiple files, individual or multiple disk partitions, or an entire disk drive

# Digital Evidence Validation Tools

- Windows Validation Tools
- Unlike Linux, Windows has no built-in validation tools
- The following third party programs can be installed in Windows
- X-Ways WinHex
- Breakpoint Software Hex Workshop
- OSForensics
- Autopsy
- EnCase
- FTK

# Storing Digital Evidence - Evidence Retention

- The following storage mediums can be used for digital evidence
- Magnetic Tapes
- Hard Disk Drives
- CD/DVD
- Pen Drives
- Cloud based systems
- If Evidence need to be retained for longer periods of time, the following storage mediums are suitable
- Magnetic Tapes
- Cloud based systems
- It is better to store digital evidence in multiple storage mediums to enhance security

# Module 2
# Understanding Digital Data and Storage Systems

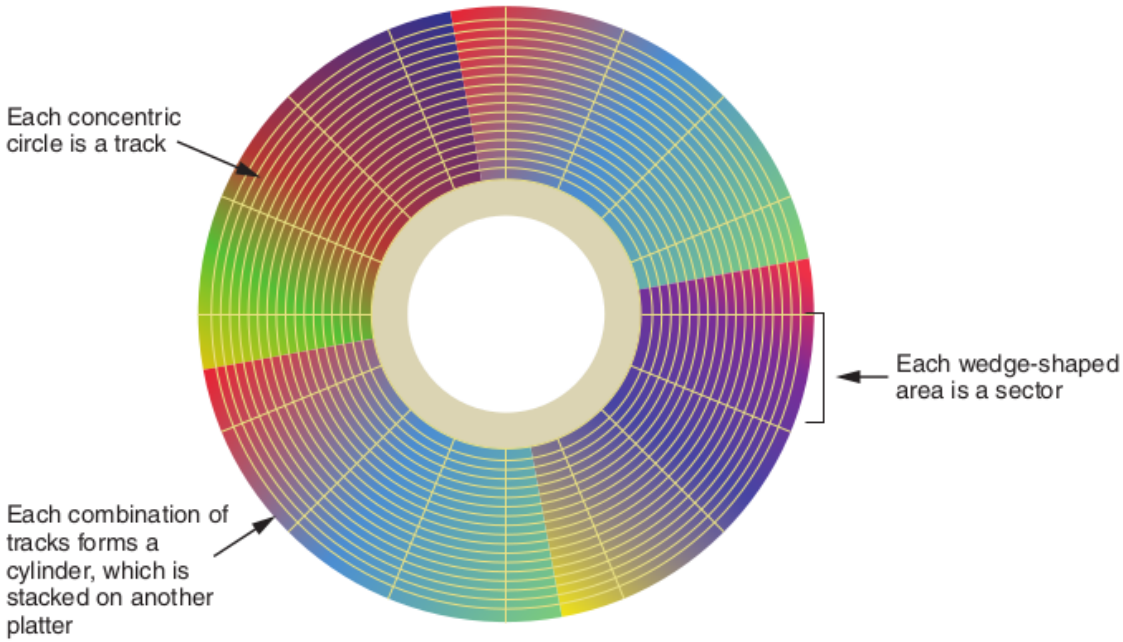
- To investigate digital evidence effectively, you must understand how the most commonly used OSs work and how they store files
- A file system on an OS determines how data is stored on the disk
- There are different types of file systems
- Here we will see what are the file systems used in Microsoft Windows

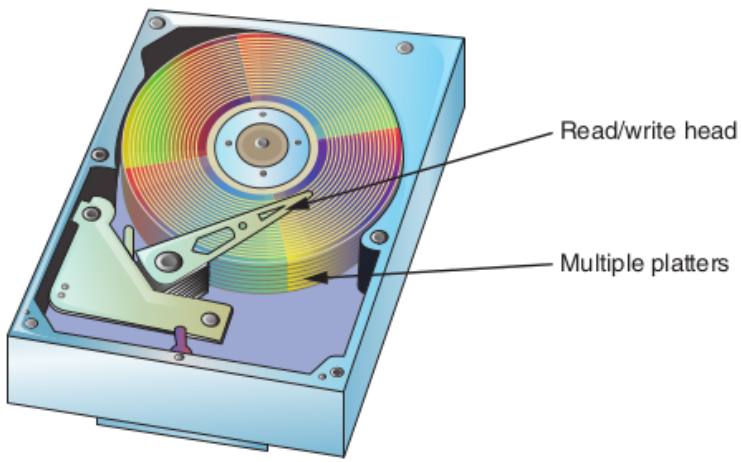
# Understanding Boot Sequence

- Booting is the process of starting a computer
- While starting the computer you are investigating, you have to make sure that it boots to a forensically configured CD, DVD, or USB drive
- Booting to the hard disk overwrites evidentiary data
- By default, the OS usually boots to the hard disk
- You can change the boot sequence so that the OS accesses the CD/DVD drive or USB drive, for example, before any other boot device
- The boot sequence is changed in the CMOS Setup Screen
- In many computers, the CMOS Setup Screen is accessed by pressing the delete key, while booting

# Understanding Disk Drives

- Components of a Disk Drive



# Understanding Disk Drives

- Disk drives are made up of one or more platters coated with magnetic material, and data is stored on platters in a particular way
- Each platter has two surfaces: top and bottom
- The following are the various disk drive components
- Geometry - Geometry refers to a disk's logical structure of platters, tracks, and sectors
- Head - The head is the device that reads and writes data to a drive. There are two heads per platter that read and write the top and bottom sides
- Tracks - Tracks are concentric circles on a disk platter where data is located
- Sector - A sector is a wedge shaped section on a track, usually made up of 512 bytes
- Cyllinder - The set of all tracks in the same position, for all platters, makes up a cylinder

# Solid State Storage Devices(SSDs)

- When data is deleted on a hard disk drive, only the references to it are removed, which leaves the original data in unallocated disk space
- Disk space which does not belong to any partition is called unallocated disk space
- No programs can write data to this space
- Deleted data can be recovered easily from unallocated space using forensic tools

# Solid State Storage Devices(SSDs)

- Solid State Storage(Flash Memory) is a type of non-volatile computer storage that stores and retrieves digital information using only electronic circuits, without any involvement of moving mechanical parts
- They are used in solid state storage devices such as memory cards, solid state drives, USB flash drives etc.
- Memory cells in solid state storage devices are designed to perform only 10,000 to 100,000 reads/writes, depending on the manufacturer's design
- After that they can no longer retain data
- All flash memory devices shift data from one memory cell to another, that have had fewer reads/writes, continuously
- This is to make sure that all memory cells wear evenly
- These properties make digital evidence recovery from solid state storage devices more difficult

# Microsoft File Systems

- Two commonly used file systems in Microsoft Windows are File Allocation Table(FAT) and New Technology File System(NTFS)
- In Microsoft File Systems, sectors are grouped to form clusters
- Combining sectors minimise the overhead of reading/writing to disks
- Clusters are usually of the size 512, 1024, 2048, 4096 or more bytes each
- The number of sectors in a cluster depends on the disk size
- A double sided floppy disk has one sector per cluster
- A hard disk has four or more sectors per cluster

# Disk Partitions

- Hard disks can be logically divided into 2 or more sections
- Each of these sections is called a disk partition
- The description about various partitions in a disk are stored in a table called partition table
- The partition table is stored in the Master Boot Record(MBR), located at the first sector of hard disk
- There are hexadecimal codes in a partition table for identifying the file systems in a disk
- Hexadecimal code 07 identifies NTFS
- Hexadecimal code 0B identifies DOS 32-bit FAT
- Hexadecimal code 81 identifies Linux File System

# Disk Partitions

- One can create large unused gaps between disk partitions called partition gaps
- These gaps can be used for hiding data
- All references to the partition gaps can be removed from the partition table
- Doing so will conceal them from the OS
- However, these hidden areas can be accessed using disk editors such as Norton DiskEdit, WinHex or Hex Workshop

# Understanding FAT

- File Allocation Table(FAT) is a file system originally developed for floppy disks
- It was later adapted for use in hard disks
- It was the default file system for MS-DOS and Windows 9x operating systems
- It was replaced by NTFS starting from Microsoft Windows XP
- However, it is still in use in USB flash drives and memory cards, because of its compatibility and ease of implementation

# Understanding FAT

- The following are its major variants
- FAT12
- It uses cluster addresses of 12 bit size
- It was used for floppy disk drives and small hard disks of size upto 16 MB
- FAT16
- It uses cluster addresses of 16 bit size
- It was used for hard disks of size upto 4 GB
- FAT32
- It uses cluster addresses of 32 bit size
- It was used for hard disks of size upto 16 TB

# Understanding FAT

- The following are its major variants
- exFAT
- It was developed for flash memory devices
- It can store large amount data that includes image, audio and video files
- VFAT(Virtual FAT)
- It can store file names of more than 8 characters and extensions of more than 3 characters

# Understanding NTFS

- New Technology File System(NTFS) was introduced by Microsoft in Windows NT operating system in 1993
- NTFS replaced FAT to become the default file system from Windows XP onwards
- It has several advantages over FAT file system
- It provides more information about a file
- It includes more security features
- NTFS has more control over files and folders than FAT
- It is a journaling file system
- In other words, it keeps track of all transactions in a file such as file saving, file deleting etc., before the system carries it out
- This information is stored in a data structure called journal
- When a power failure or system crash occurs, the system can complete the transaction or go back to the previous stable state, with the help of information from journal

# Understanding NTFS

- Partition Boot Sector is the first data set in NTFS
- It starts at sector[0] and can expand to 16 sectors
- Master File Table(MFT) is the first file in NTFS
- It comes immediately after Partition Boot Sector
- It consumes 12.5% of the disk when it is created
- It can expand upto 50% of the disk as data is added
- NTFS uses Unicode, an international data format that can represent all languages of the world
- Unicode replaced ASCII which could mainly represent text in English language only

# MFT and File Attributes

- Each record in MFT contains file or folder information
- Each record is divided into several record fields
- A record field is also referred to as an attribute Id
- Each record field contains metadata about the file or folder, file's data or links to the file's data
- For small files of size upto 512 bytes, all file metadata and data are stored in the MFT record
- This type of record is called resident
- Files having size greater than 512 bytes are stored outside the MFT
- Here the MFT record contains cluster addresses(data runs) where the file is stored in the disk drive
- This type of record is called non resident

# MFT and File Data

- The following are some important file data are stored in a MFT record
- MFT Header
- It is the first section in an MFT record
- It contains the size of the MFT record
- It also indicates the starting position of the first attribute
- Attribute 0x10: Standard Information
- 0x10 is the attribute id of the Standard Information attribute
- It contains the date and time of file creation
- It contains the date and time of last access of file
- It contains the date and time of last modification of file
- Attribute 0x20: Attribute List
- Attributes that don't fit in MFT(non resident attributes) are listed here along with their locations

# MFT and File Data

- Attribute 0x30: File_Name
- The file names are contained here
- File names upto 8 characters are stored in one attribute
- File names having more than 8 characters are stored in 2 attributes
- Attribute 0x40: Object_ID
- This attribute contains file ownership and access control information
- Attribute 0x80: Data
- It contains data of resident files
- It contains data runs to non resident files

# NTFS Compressed Files

- For improving data storage, NTFS provides compression as in FAT
- In FAT16, one can compress only a disk volume (partition)
- NTFS provides compression at file, folder or volume level
- Most Forensic tools can decompress and analyse compressed data
- They can easily handle data compressed using WinZip, GNU gzip and PKZip

# NTFS Encrypting File System(EFS)

- There is a built-in encryption facility in NTFS starting from Windows 2000
- It is called Encrypting File System(EFS)
- EFS can encrypt files, folders or disk volumes
- EFS uses public key cryptography
- Here public key is used for encryption and private key is used for decryption
- Here there is a mechanism for recovering encrypted files, if there is any problem with the private key
- For this a recovery key can be generated

# Deleting NTFS Files

- When a file is deleted, it is moved to recycle bin
- The original path to it are stored in the file Info2
- This information is used when we restore the file from the recycle bin
- When the file is removed from recycle bin, the references to the file in the MFT are removed so that the file cannot be accessed now
- The original space of the file can now be used for storing new file
- We can also delete a file using the MS-DOS command delete
- Here the file is not moved to the recycle bin and its references are removed immediately

# Resilient File System(ReFS)

- ReFS is a new file system that can be used in Windows 8 and Windows Server 2012
- This uses B+ Tree sorting method which provides fast access from large data sets
- In this file system, all the updates to files are stored to new locations
- In other words, the files are not overwritten immediately
- This ensures that original data can be recovered easily, if any failure occurs during the update operation

# Whole Disk Encryption

- Nowadays there are software tools that can be used for encrypting the entire disk drive
- These tools encrypt each sector of a drive separately
- They also use advanced encryption algorithms such as AES and IDEA
- To examine an encrypted drive we need to decrypt it first
- Here we need to to decrypt each sector of a drive
- The larger the drive, the longer the decryption takes
- After decryption, we can use standard acquisition methods to retrieve the data

# Microsoft BitLocker

- BitLocker is a Microsoft utility for whole disk encryption
- It is available starting from the version Windows Vista
- It can encrypt NTFS drives only
- If we want to encrypt FAT drives, you have to use other tools
- It uses Advanced Encryption Standard(AES) encryption algorithm
- For decrypting using BitLocker, correct password is needed
- If password is lost, the system remains in the encrypted state

# Understanding Windows Registry

- Windows Registry is a hierarchical database containing system and user information
- It contains information about installed hardware and software
- It contains the security settings of the computer
- It contains the desktop configuration settings
- It contains information regarding the most recently used files
- It contains usernames and passwords for various users
- It contains information regarding the currently logged in user

# Understanding Windows Registry

- For investigative purposes, Windows Registry contains valuable information
- For viewing and modifying its contents, registry editors are used
- Regedit is the built-in editor for Windows9x
- Regedt32 is the built-in editor for Windows 2000, Windows XP and Windows Vista
- Both Regedit and Regedt32 can be used in Windows 7 and Windows 8
- Some forensics tools, such as X-Ways Forensics, OSForensics, Forensic Explorer, and FTK, have built-in Registry viewers

# Microsoft Windows Startup Tasks

- Here we will learn what files are accessed when Windows starts
- This will be useful while examining a suspect's computer
- Startup in Windows 7, Windows 8 and Windows 10
- Here a BCD Registry file in the \Boot\Bcd folder is maintained to control the boot process
- To access this file, you use the BCD Editor
- To access the Advanced Boot Options menu, press F8 or F12, while booting
- To modify the boot priority order, press F2 or Delete while booting

# Microsoft Windows Startup Tasks

- Startup in Windows Vista
- Here the following boot utilities are used

1. Bootmgr.exe

- This controls boot flow and allows booting multiple OSs, such as booting Vista along with XP

2. Winload.exe

- This installs the kernel

3. Winresume.exe

- This restarts Vista from hibernation mode

# Microsoft Windows Startup Tasks

- Startup in Windows XP
- Here the following boot utilities are used

1. NT Loader (Ntldr)

- This loads the OS

2. Boot.ini

- This will display a boot menu

3. BootSect.dos

- This will contain the address of each OS in the computer

4. Ntoskrnl.exe

- This is the Windows XP kernel located in systemroot\Windows\System32 folder

# Module 3
# Linux File Structures

- Linux is a family of open source operating systems based on the linux kernel
- Linux kernel was developed by Linus Torvalds in 1991
- He still maintains the official kernel
- All other tools, graphical interfaces, and so forth are maintained and developed by others
- Many of these tools are provided by the GNU Project
- The most widely used distributions include Ubuntu, CentOS, Mint, Fedora, and Gentoo

# Linux File Structures

- The following are some important system files in Linux containing information about users and their activities
- /var/log/lastlog
- Contains user's last logon information
- /var/log/wtmp
- Contains logon and logoff history information
- /var/run/utmp
- Current user's logon information
- /etc/shadow
- Master password file, containing hashed passwords for the local system
- /etc/passwd
- Contains account information for the local system

# Linux File Structures

- The core top level directories in Linux are given below
- /usr
- Most applications and commands are in this directory or its sub directories
- /etc
- Most system configuration files are stored in this directory
- /home
- The home directories for all users, usually named after their usernames
- /root
- The home directory for the root user(superuser)
- /dev
- Contains files that represent devices that are attached to the local system
- /var
- Contains variable data such as temporary files

# File Structures in Ext4

- The extended file system (Ext), implemented in 1992 was the first file system to be used for the Linux kernel
- It was succeeded by the second extended file system(Ext2)
- It was followed by the third extended file system(Ext3)
- Ext3 is a journaling file system, having a built-in recovery mechanism after a crash
- A few years later, Fourth Extended File System (Ext4) was introduced
- Ext4 added support for partitions larger than 16 TB
- It supports management of large files also
- In Linux everything is considered a file including disk drives, monitors, system memory, directories etc.
- A file, like an object in an object-oriented programming language, has properties and methods that can be performed on it

# File Structures in Ext4

- A block is the smallest unit in the Linux file system
- There are 4 types of blocks in the Linux file system

1. boot block

- It contains the bootstrap code - instructions for startup

2. super block

- It contains vital metadata about the file system such as type, size, status(mounted or not) etc.

3. Inode block

- It contains information about inodes
- Inodes contain metadata about files and directories in the system such as type, links to a file or directory, size, last access time and last modified time etc.

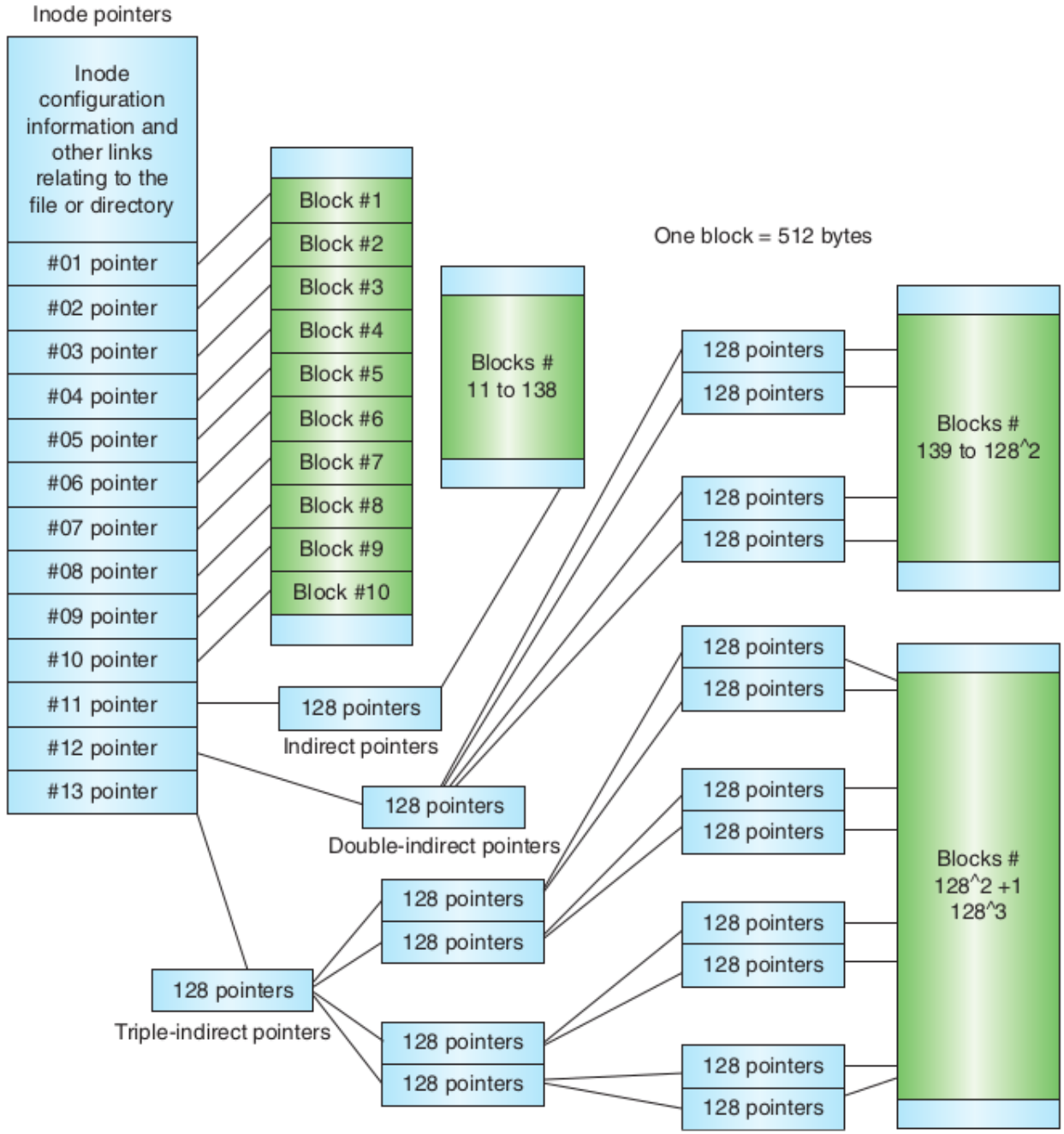
4. data block

- It contains the files and directories

# File Structures in Ext4

- Corresponding to each file or directory, there will be an Inode
- An Inode has 13 pointers
- The first 10 pointers are called direct pointers
- Each of them directly refer to a data block
- The eleventh pointer is an indirect pointer, which links to 128 pointers
- Each of these 128 pointers directly refer to a data block
- The twelfth pointer is a double indirect pointer, which links to 128 pointers
- Each of these 128 pointers links to another 128 pointers in the second layer, which directly refer to a data block
- The thirteenth pointer is a triple indirect pointer, which links to 128 pointers, each pointing to another 128 pointers, and each pointer in the second layer pointing to another 128 pointers in the third layer, which directly refer to a data block

# File Structures in Ext4



# Module 4
# Understanding Mobile Device Forensics

- It deals with extracting information from mobile phones to use as evidence in criminal or civil cases
- Depending on your phone's model, the following information might be stored on it
- Incoming, outgoing, and missed calls
- Multimedia Message Service (MMS) and Short Message Service (SMS) messages
- E-mail accounts
- Web pages
- Photos, videos, and music files
- Calendars and address books
- Social media account information
- GPS data
- Voice recordings and voicemail
- Bank account logins

# Mobile Phone Basics

- The digital networks used in the mobile phone industry are given below
- Code Division Multiple Access (CDMA)
- It uses the spread spectrum technology
- It enables each user to transfer the data over the entire frequency spectrum at any time
- Global System for Mobile Communications (GSM)
- This uses Time Division Multiple Access (TDMA)
- This enables many users share the same frequency channel at different times
- Time Division Multiple Access (TDMA)
- In this digital network, different users share the same frequency channel at different times

# Mobile Phone Basics

- Integrated Digital Enhanced Network (iDEN)
- This digital network is used by Motorola
- This provides phone and data services
- Digital Advanced Mobile Phone Service (D-AMPS)
- This network is a digital version of the original analog standard for cell phones
- Enhanced Data GSM Environment (EDGE)
- This digital network, a faster version of GSM, is designed to deliver data
- Orthogonal Frequency Division Multiplexing (OFDM)
- This technology for 4G networks uses energy more efficiently than 3G networks and is more immune to interference

# SIM Cards

- We need SIM (Subscriber Identity Module) Cards for a mobile equipment to work
- It is a memory card with a microprocessor inside it
- The following are the important functions of a SIM card
- It identifies the subscriber to the mobile network
- It stores mobile service related information
- It can be used to back up the device
- SIM card comes in 3 sizes: standard, micro and nano
- The main advantage of a SIM card is portability

# Acquisition Procedures for Mobile Devices

- When you seize a mobile for investigation, it can be in on or off state
- If it is in off state, leave it like that, and find the associated charger
- If it is in on state, isolate the device from incoming signals using any of the given below methods

1. Place the device in airplane mode, if this feature is available
2. Place the device in a paint can, preferably one that previously contained radio wave-blocking paint
3. Use a Faraday bag that conforms to Faraday wire cage standards
4. Turn off the device

- After reaching the forensic lab, you can retrieve information from SIM cards, Internal Memory and External Memory Card

# Mobile Phone Forensics Tools and Methods

- Mobile Phone Forensics Tools
- In android devices, AccessData FTK Imager tool can be used
- In iPhone, MacLockPick tool can be used
- Mobile Phone Forensics Methods

1. Manual extraction

- This method involves looking at the device's content page by page and taking pictures. It's used if investigators can't do a logical or physical extraction

2. Logical extraction

- The mobile device is connected to a forensic workstation via a wired (USB cable, for example) or wireless (such as Bluetooth) connection, and then the file system information is extracted

# Mobile Phone Forensics Tools and Methods

3. Physical extraction

- Similar to logical extraction; But here deleted files can also be retrieved

4. Hex dumping and Joint Test Action Group (JTAG) extraction

- This method gets information from the processor, RAM, flash memory, or other physical components

5. Chip-off

- This method involves physically removing flash memory chip and gathering information at the binary level

6. Micro read

- This method looks at logic gates with an electron microscope and can be used even when data has been overwritten on magnetic media. It's very expensive,so it's typically used only in cases involving national security

# Securing a Network

- The following strategies are used for securing a network

1. Layered Network Defence Strategy

- This sets up multiple layers of protection to hide the most valuable data at the innermost part of the network. It also ensures that the deeper into the network an attacker gets, the more difficult access becomes, since more safeguards are in place.

2. Defence in Depth (DiD) Strategy

- This is used by National Security Agency(NSA)
- This has 3 modes of protection
- People - Use well qualified and well trained personnel
- Technology - Choose a strong network architecture having intrusion detection systems (IDSs) and firewalls
- Operations - Updating software, antivirus software, and OSs
- If one mode of protection fails, the others can be used to thwart the attack

# Developing Procedures for Network Forensics

- A standard procedure often used in network forensics is as follows

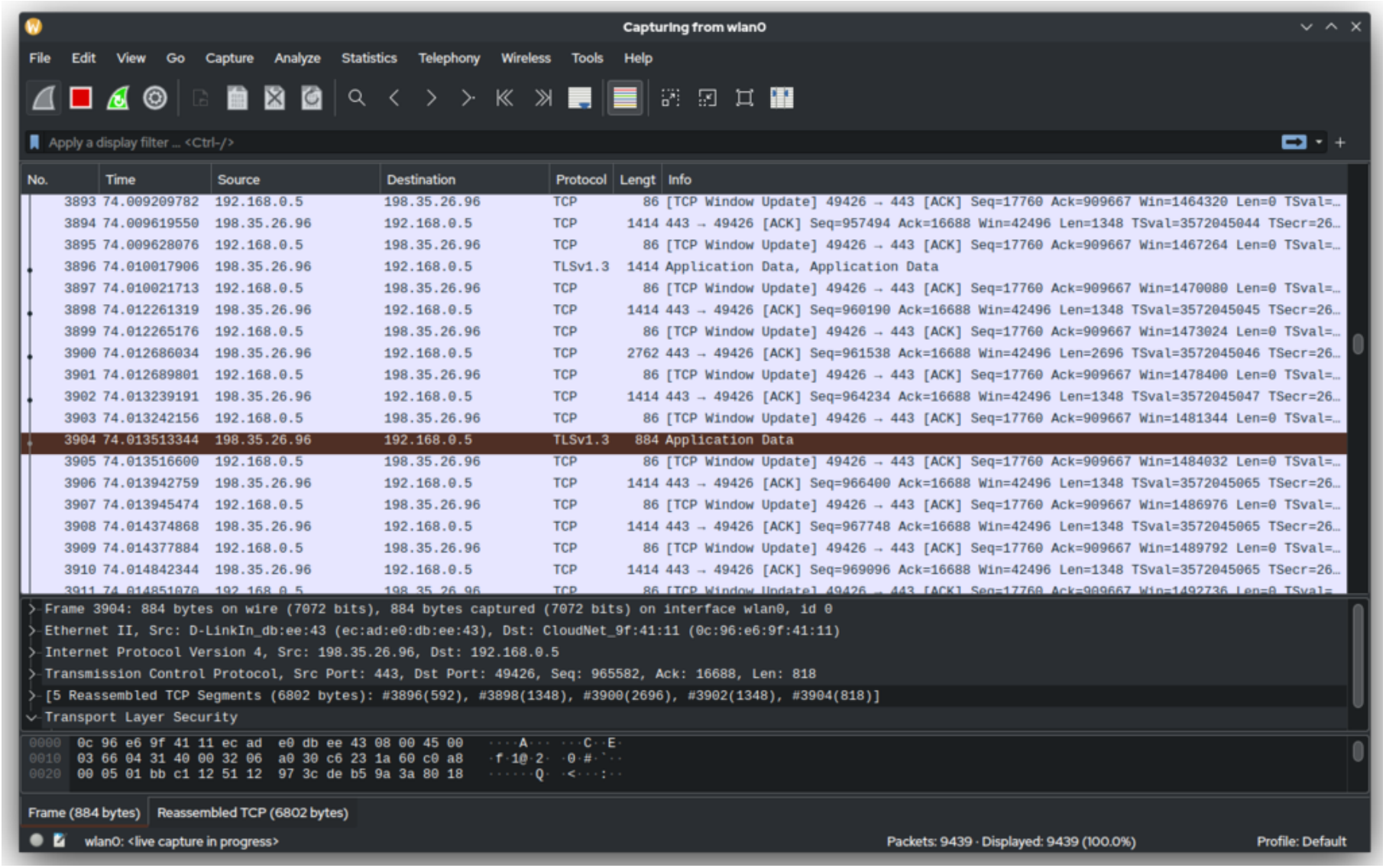
1. Use a standard installation image for systems on a network, containing all the applications. You should also have MD5 and SHA-1 hash values of all applications and files
2. When an intrusion incident happens, make sure the vulnerability has been fixed to prevent further attacks
3. Attempt to retrieve all volatile data, such as RAM and running processes, by doing a live acquisition before turning the system off
4. Acquire the compromised drive and make a forensic image of it
5. Compare files on the forensic image with the original installation image. Compare hash values of files to determine whether they have changed

# Wireshark Packet Analyser

- It is a free and open source software for retrieving and analysing information from computer networks
- It is an important tool for network forensics
- It is a cross-platform application
- It can be used in GUI and command line modes
- It is written in C, C++ and Lua
- It was released in 1998
- Using this, live data can be read from different types of networks
- Captured data in the form of packets can be analysed using this tool

# Wireshark Packet Analyser

- Wireshark GUI



# Module 5
# Types of Forensics Reports

1. Verbal Report

- It is a preliminary report and addresses areas of investigation yet to be completed
- It is given to an Attorney

2. Written Report

- It is a detailed report usually in the form of an affidavit or a declaration
- It is also given to an Attorney

3. Examination Plan

- It is a document used by the attorney to examine the forensic report given by the forensic examiner

# Types of Forensics Reports

- It includes the following items
- Name of the forensic examiner
- Academic Qualification
- Experience
- Professional Society Memberships
- Publications
- Questionnaire regarding the forensic examination
- Length of the forensic examination
- Fee of the forensic examination

# Guidelines for Writing Report

- A report usually includes the sections shown in the following list
- Abstract (or summary)
- Table of contents
- Body of report
- Conclusion
- References
- Glossary
- Acknowledgments
- Appendixes

# Guidelines for Writing Report

- For writing reports clearly, use the following criteria

1. Communicative quality

- Make the document easy to read

2. Ideas and organisation

- Specify all the relevant details in an organised manner

3. Grammar and vocabulary

- Keep the grammar simple
- Technical terms should be used consistently

4. Punctuation and spelling

- Make them accurate and consistent

# Guidelines for Writing Report

- Provide Supporting Material
- Use supporting material such as figures, tables, data, and equations
- Format Consistently
- Indent all paragraphs
- Use fonts consistently
- Use consistent heading styles throughout
- Explain Examination and Data Collection Methods

# Generating reports with Autopsy

- Steps

1. Create a New Case

- Click on "New Case" to create a new case
- Provide relevant case information such as Case Name, Case Number and Case Description
- Choose a location on your system to store the case files and evidence

2. Add Evidence

- Click "Add Data Source" to add evidence
- You can add various data sources, such as a hard drive, disk image, or a folder

# Generating reports with Autopsy

3. Processing the Evidence

- After adding the evidence, Autopsy will begin processing it
- Depending on the size of the evidence, this process may take some time

4. Analyzing the Case

- Once processing is complete, you'll be able to analyse the case
- Keyword Search
- You can search specific keywords or phrases within the evidence
- Timeline Analysis
- This presents a chronological view of events related with the case
- File Analysis
- You can view files based on categories such as images, documents, videos, etc.
- Generating Reports
- You can generate comprehensive reports summarising your findings

# Ethics and Codes of Expert Witnesses

- Ethics are moral principles that are to be followed by an expert witness while conducting a forensic examination
- Maintain integrity
- Conduct unbiased analysis
- Codes are standards that are formulated by external bodies such as professional forensic organisations
- Maintain utmost objectivity in all forensic examinations and present findings accurately
- Conduct examinations based on established, validated principles

# Considerations in disqualification

- Courts have used the following factors to disqualify an expert
- Whether the attorney informed the expert that their discussions were confidential
- Whether the expert reviewed materials marked as confidential
- Whether the expert was asked to sign a confidentiality agreement
- Whether the expert provided the attorney with confidential information
- Whether the expert was requested to perform services for the attorney
- Whether the attorney compensated the expert

# Ethical Responsibilities of a Forensic Examiner

- Maintain utmost objectivity in all forensic examinations and present findings accurately
- Conduct examinations based on established, validated principles
- Testify truthfully in all matters before any board, court, or proceeding
- Avoid any action that would appear to be a conflict of interest
- Never reveal any confidential matters or knowledge learned in an examination without an order from a court of competent jurisdiction or the client's express permission
- Not withhold any findings, that would cause the facts of a case to be misrepresented or distorted

# References


1. Bill Nelson, Amelia Phillips, Christopher Steuart, “Guide to Computer Forensics and Investigations”, Cengage Learning, 6th Edition.
2. https://www.geeksforgeeks.org/cyber-forensics/