Digital Forensics by Cyph3rRyx

Digital Forensics

Definition:

- Digital forensics is the process of recovering, analyzing, and preserving electronic data to investigate and prevent cybercrime.

Key Components:

1. **Identification:**
    - Involves pinpointing digital devices like computers, laptops, mobile phones, etc.
2. **Collection:**
    - Gathering electronic evidence from identified devices.
3. **Examination:**
    - In-depth analysis of the collected digital data.
4. **Preservation:**
    - Ensuring the integrity and secure storage of the digital evidence.

Objective:

- The primary goal is to uncover and interpret digital evidence in a manner admissible in a court of law.

Applications:

- Digital forensics is utilized to investigate a spectrum of criminal activities including hacking, fraud, embezzlement, cyberstalking, as well as for civil litigation and internal corporate investigations.

Process:

1. **Identification:**
    - Recognizing potential sources of digital evidence.
2. **Collection:**
    - Employing specialized tools to gather electronic data from various devices.
3. **Examination:**
    - Utilizing expertise in computer systems, networks, and digital storage media to analyze the collected evidence.
4. **Preservation:**
    - Ensuring the integrity and authenticity of digital evidence for legal proceedings.

Tools and Techniques:

- Involves the use of specialized tools and techniques to identify, extract, and analyze digital evidence.

Skillset:

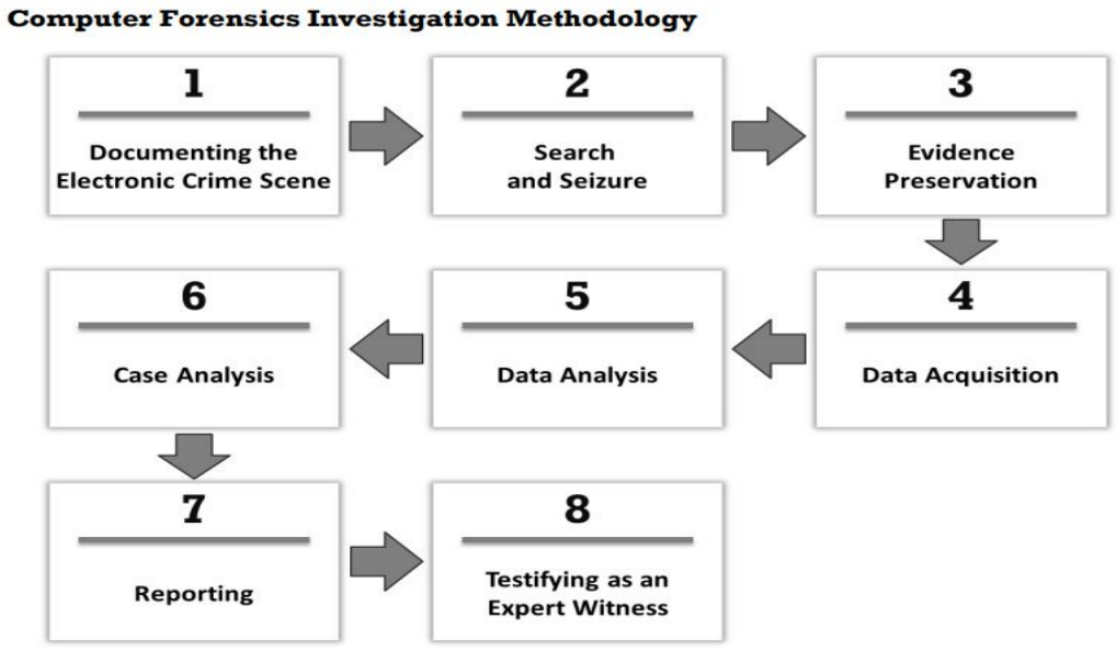
- Requires a thorough understanding of computer systems, networks, and digital storage media.

Scope:

- Encompasses investigating cybercrimes such as hacking and fraud, as well as supporting civil litigation and internal corporate investigations.

Legal Admissibility:

- Emphasis on presenting digital evidence in a way that is admissible in a court of law.



Documenting the Electronic Crime Scene

Purpose:

- Maintain a record of forensic investigation processes.

Details to Include:

1. Location of the crime.
2. Status of the system.
3. Connected network devices.
4. Storage media.
5. Smartphones, mobile phones, PDAs.
6. Internet and network access.

Traceability:

- Aid in tracing serial numbers or other identifiers of procured devices.

Documentation Elements:

1. Photographs.
2. Video.
3. Notes.

4. Sketches for scene recreation.

Search and Seizure

Objective:

- Maintain integrity of digital evidence.

Legal Approvals:

- Search and seizure orders.
- Preservation of evidence orders.

Execution:

- Use of surprise to capture digital devices.
- Data preservation for future legal proceedings.

Important Note:

- Individuals may face surprise seizure if they attempt unauthorized copying of files.

Evidence Preservation

Critical Steps:

1. **Device State:**
    - Do not change the current state of the device.
    - Call a forensics expert before any action.
2. **Power Down:**
    - Keep the device off if it's off.
    - For mobile phones, power down to prevent data wiping.
3. **Location Security:**
    - Avoid leaving the device unattended in open or unsecured areas.
    - Document device location, access, and movements.
4. **External Media:**
    - Do not plug any external storage media into the device.
5. **No Copying:**

- Do not copy anything to or from the device.

6. **Photograph Evidence:**
   - Take pictures from all sides to ensure no tampering.
7. **Login Credentials:**
   - Know and share device login credentials with forensic experts.
8. **No Opening Files:**
   - Avoid opening applications, files, or pictures on the device.
9. **Forensics Expertise:**
   - Only certified forensics experts should investigate or view files.
10. **Shutdown or Hibernate:**
    - If required, hibernate instead of shutting down to preserve volatile memory until the next boot.

Methods for Digital Forensics (DF) Experts

1. **Drive Imaging:**
   - *Definition:* Creating a bit-by-bit duplicate of the drive before analysis.
   - *Importance:* Ensures preservation of original data for examination.
   - *Process:* Forensic experts use specialized tools to create an exact copy of the drive.
2. **Hash Values:**
   - *Definition:* Cryptographic hash values (e.g., MD5, SHA1) generated during drive imaging.
   - *Purpose:*
     - Verify Authenticity and Integrity of the image as a replica.
     - Critical in court for evidence admission.
   - *Significance:* Even a minor alteration generates a completely new hash value.
   - *Usage:* Guarantees the integrity of evidence during forensic analysis and legal proceedings.

Chain of Custody (CoC)

Definition:

- Chain of Custody refers to the documented and chronological record of the possession, transfer, analysis, and disposition of physical or digital evidence during an investigation.

Key Elements:

1. **Collection:**
    - When evidence is initially gathered, it is documented, sealed, and labeled.
2. **Transfer:**
    - Records the movement of evidence from one person or location to another.
3. **Analysis:**
    - Documents any examination or testing conducted on the evidence.
4. **Storage:**
    - Tracks where and how the evidence is stored to maintain its integrity.
5. **Disposition:**
    - Records the final outcome or disposal of the evidence, whether it is returned, archived, or destroyed.

Purpose:

- Ensure the integrity and admissibility of evidence in legal proceedings by creating a transparent and unbroken trail of its handling.

Importance:

- Provides a clear and accountable history of the evidence, allowing for verification of its authenticity and reliability.

Significance:

- Chain of Custody is crucial in maintaining the credibility of evidence, preventing contamination, and addressing any challenges to its reliability during legal proceedings.

Data Acquisition:

Definition:

- Data acquisition is the process of gathering and recovering sensitive data during a digital forensic investigation, including accessing, recovering, and restoring data compromised in cybercrimes.

Objectives:

- Access, recover, and protect sensitive data.
- Produce forensic images from digital devices and other computer technologies.

Common Data Acquisition Methods

1. *Bit-stream Disk-to-Image Files:*
    - Creating a bit-for-bit duplicate image file of the original disk.
2. *Bit-stream Disk-to-Disk Files:*
    - Copying data directly from one disk to another.
3. *Logical Acquisition:*
    - Extracting logical storage objects (files, directories) from the file system.
4. *Sparse Acquisition:*
    - Collecting fragments of unallocated (deleted) data, useful when inspecting the entire drive is unnecessary.

Data Analysis:

Process:

- After acquisition, data is analyzed for potential information.

Tools Used:

1. **Autopsy**
2. **Volatility**
3. **Redline**
4. **Wireshark**
5. **Stellar Data Recovery**

Case Analysis

Purpose:

- Answer key questions: Who, Why, When, What, How.

Reporting

Requirements:

- Report results to the Investigating Officer (IO).

Characteristics:

- Precision and accuracy in reporting are crucial.

Expert Testimony in Legal Proceedings

- *Definition:*
  - Presentation of expert testimony in court proceedings to assist the judge or jury in evaluating material facts.
- *Common Law Systems:*
  - Typically proffered by one of the parties involved.

Section 45 of IEA (Indian Evidence Act)

Fields Requiring Expert Opinion:

1. Foreign Law
2. Science & Art
3. Identity of Handwriting
4. Identity of Finger Impression
5. Electronic Evidence

Considered Expert Opinion:

- Relevant only in the mentioned fields.

Characteristics of Expert Opinion:

- Considered a relevant fact for the case.
- Based on superior knowledge and practical experience.

Forensics Readiness

Definition:

- Refers to an organization's ability to optimally use digital evidence within a limited time and with minimal investigation costs.

Components:

1. Technical and nontechnical actions.
2. Specific incident response procedures.
3. Designated trained personnel.

Benefits:

- Enables quick and efficient collection and preservation of digital evidence.
- Mitigates the risk of threats from employees and prepares preemptive measures.

Forensics Readiness Planning:

1. Identify potential evidence.
2. Determine the source of evidence.
3. Establish a policy for secure handling and storage.
4. Decide if the incident requires investigation.
5. Train staff to handle incidents and preserve evidence.
6. Create a documented procedure.
7. Establish a legal advisory board for guidance.

Role of Forensic Investigator:

Responsibilities:

1. Retrieve data from virtual and physical devices.
2. Collect and analyze network intrusion artifacts.
3. Reconstruct events leading to compromise or breach.
4. Process, analyze, and preserve digital evidence.
5. Extract and analyze metadata.
6. Collaborate with law enforcement, legal, compliance, and HR teams.
7. Ensure chain of custody of digital evidence.

8. Write technical reports documenting case findings.
9. Identify potential threats and provide security recommendations.
10. Provide testimony in legal proceedings.

Storage Device

Definition:

- A hardware device used for storing digital data and applications, such as images, videos, and audio. Examples include hard drives.

Storage Units Conversion:

- 4 bits = 1 nibble
- 8 bits = 1 byte
- 1024 bytes = 1 kilobyte
- 1024 kilobytes = 1 megabyte
- 1024 megabytes = 1 gigabyte
- 1024 gigabytes = 1 terabyte
- 1024 terabytes = 1 petabyte

RAM and ROM

Random Access Memory (RAM):

- Type of volatile computer memory used for temporarily storing data in current use or processing.
- Data is lost when power is turned off.
- Typically stores the operating system, application programs, and current data.

Read Only Memory (ROM):

- Type of non-volatile computer memory used for permanently storing data that doesn't need modification.
- Data is retained even when power is turned off.
- Typically stores computer's BIOS and firmware for hardware devices.

HDD (Hard Disk Drive)

Definition:

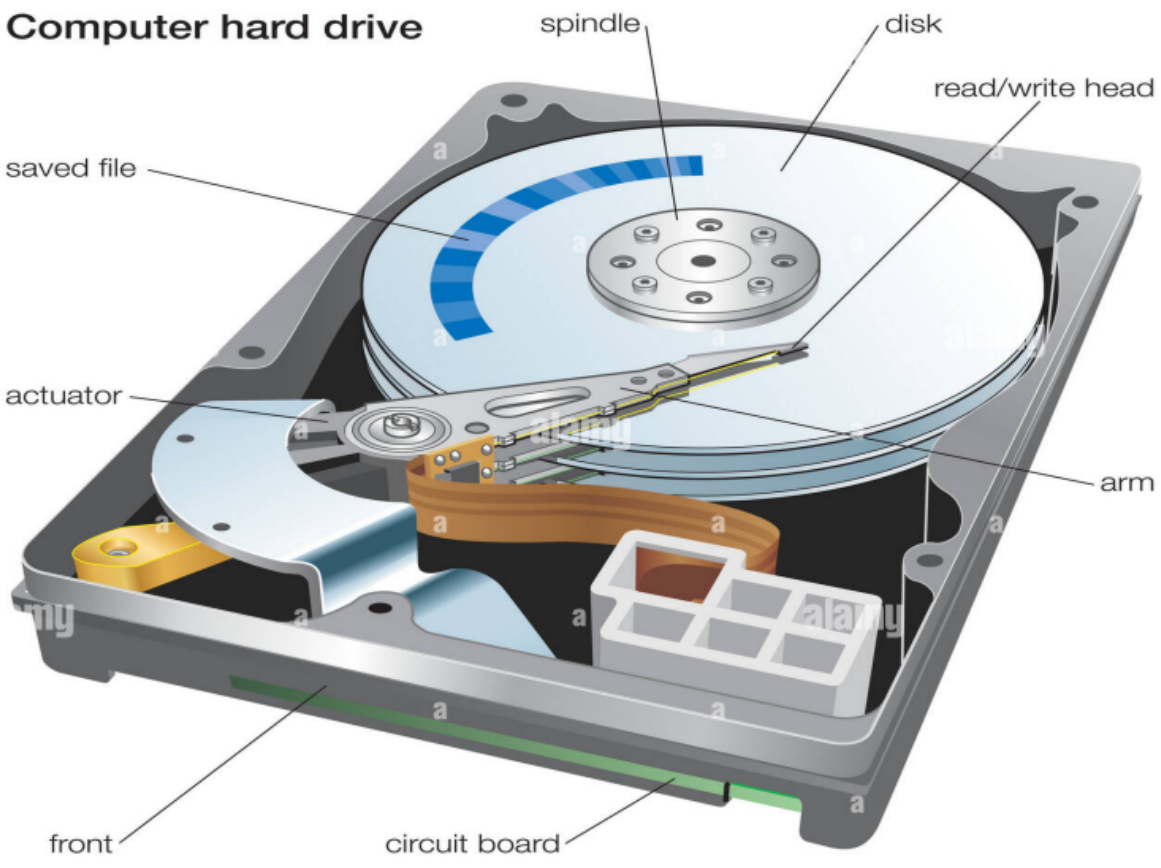
- Hard disk, also known as Hard Disk Drive, is a magnetic storage medium for computers.
- Consists of flat circular plates made of aluminum or glass coated with a magnetic material.
- Personal computer hard disks can store terabytes of information.
- Data is stored on surfaces in concentric tracks.
- Uses a magnetic head to write binary digits (1 or 0) and read them by detecting magnetization direction.

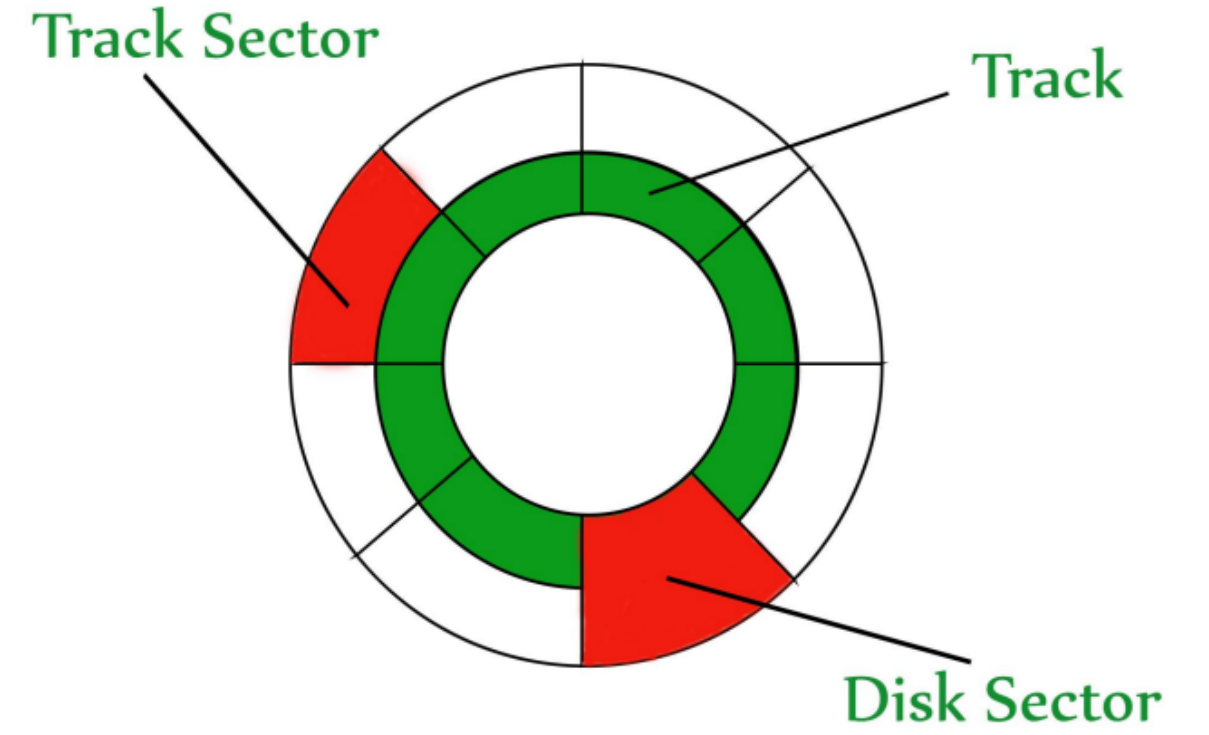
Components:

- Consists of several hard disks, read/write heads, a drive motor, and circuitry sealed in a metal case.

Function:

- Stores a computer's internal data storage.
- Some computers use solid-state drives (SSDs) based on flash memory chips instead of traditional hard disks for data storage.


Computer hard drive
spindle
disk
read/write head
saved file
actuator
arm
front
circuit board



How HDD Works?

1. **Data Storage in Binary Code:**
    - Data is stored in binary code, represented by 1s and 0s, on the magnetic layer of the hard drive.
2. **Read/Write Heads and Disk Rotation:**
    - Read/Write (R-W) heads are positioned above the surface of circular trays (disks).
    - These disks rotate rapidly, creating an air cushion that allows the R-W heads to float above the surface.
3. **Writing Mode:**
    - In writing mode, an electrical current passes through the R-W heads.
    - The electrical current modifies the magnetic surface, inscribing either a 0 or a 1, representing binary data.

4. **Reading Mode:**
    - In reading mode, the magnetic field on the disk transmits an electrical current to the R-W heads.
    - The electrical signal is then translated into a digital signal readable by the computer.

Components of HDD:

1. **Mechanical Component:**
    - Circular trays made of aluminum with a magnetic layer, known as platters.
    - Rotates around a spindle motor, with speeds typically ranging from 5,400 to 15,000 rotations per minute.
    - Read/Write heads are mobile components steered by an actuator.
    - An arm positions the heads to access information without direct contact with the magnetic surface.
2. **Electronic Component:**
    - Microprocessor and associative memory are located on a printed circuit board (PCB).
    - Signal processor handles the conversion of electric signals to digital signals.
    - Manages data transmission, processing, and commands between the motherboard and the hard drive.

Key Processes:

- **Seek Time:**
    - The time taken by the R-W head to move to the desired track from its current position.
- **Rotational Latency:**
    - The time taken by the sector to come under the R-W head.
- **Data Transfer Time:**
    - The time taken to transfer the required amount of data, influenced by the rotational speed of the disk.
- **Controller Time:**
    - The processing time taken by the controller.

- **Average Access Time:**
  - Seek time + Average Rotational latency + Data transfer time + Controller time.

Slack and Unallocated Space

- *Unallocated Space:*
  - Free space on a hard drive available for data storage, measured in clusters.
- *Slack Space:*
  - Unused space between the end of an actual file and the end of the cluster.
  - Important to note that read heads are never in direct contact with the magnetic surface, as even light friction or a speck of dust can damage the drive.

SSD (Solid State Drive)

- **Definition:**
  - SSD stands for Solid State Drive.
- **Composition:**
  - Contains NAND chips instead of moving platters or disks found in traditional HDDs.
- **Data Storage:**
  - Data is stored as charges in the NAND chips.
  - NAND chips can retain stored charge even without a power supply.
- **Binary Representation:**
  - Charged parts represent 1.
  - Non-charged parts represent 0.

Key Characteristics:

1. **No Moving Parts:**

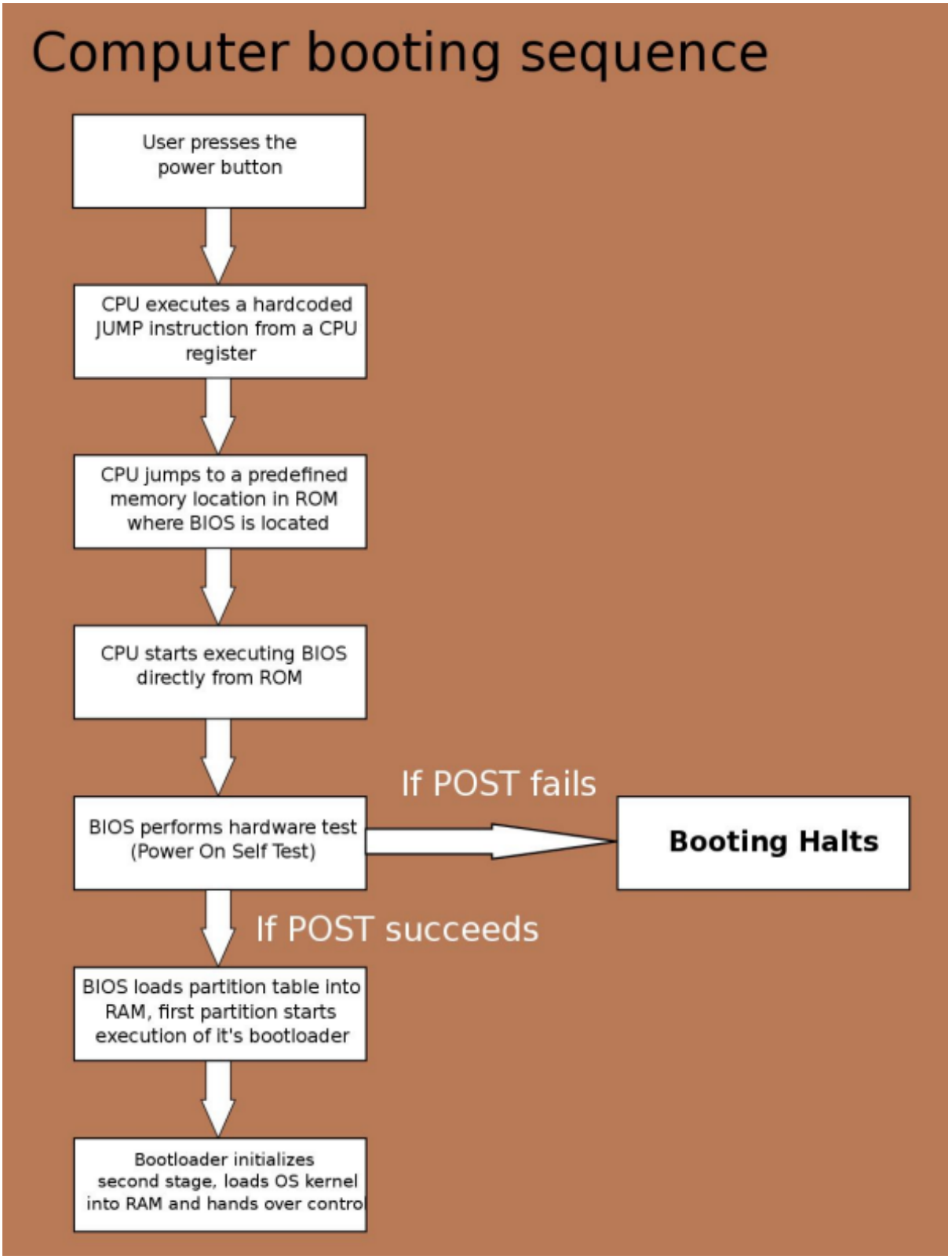
- Unlike traditional hard disk drives (HDDs), SSDs have no mechanical parts, contributing to faster data access.

2. **Durability:**
    - Resistant to physical shocks and vibrations due to the absence of moving components.
3. **Faster Data Access:**
    - SSDs provide quicker data access and transfer speeds compared to HDDs.
4. **Energy Efficiency:**
    - Consumes less power than HDDs as there are no moving parts.
5. **Silent Operation:**
    - Operates silently since there are no spinning disks or moving read/write heads.
6. **Compact Form Factor:**
    - Typically smaller and lighter than traditional HDDs, making them suitable for various devices.
7. **Reliability:**
    - Generally more reliable due to the absence of mechanical wear and tear.
8. **Longevity:**
    - Can endure a higher number of read and write cycles compared to traditional HDDs.

Booting of PC:

Definition:

- Booting is the process of starting the computer. It involves loading the operating system into the main memory, making the computer ready to accept user commands.



Initiation:

- Occurs when the CPU is first switched on with an empty memory.

Startup:

1. *Power On:*
    - The process begins when the computer is powered on or restarted.
2. *System BIOS Activation:*
    - The system BIOS (Basic Input/Output System) activates peripheral devices.

Types of Booting:

1. **Cold Booting (Hard Boot):**
    - *Description:*
        - The computer is started from its initial state by pressing the power button.
    - *Process:*
        - Instructions are read from the ROM, and the operating system is loaded into the main memory.
2. **Warm Booting (Soft Boot):**
    - *Description:*
        - The computer restarts without starting from the initial state.
    - *Trigger:*
        - Used when the system gets stuck or requires a restart while already ON.
        - Can be initiated using the restart button or CTRL+ALT+DELETE keys.

The Boot Process

1. **Power On:**
    - The boot process initiates when the computer is powered on or restarted.
2. **Basic Input/Output System (BIOS) Initialization:**
    - The system BIOS, a firmware embedded on the motherboard, activates and performs the Power On Self Test (POST).
    - POST checks essential hardware components, including the processor, memory, storage, and input/output devices.
    - If any issues are detected, the system may produce beep codes or display error messages.

3. **Bootstrap Loader Activation:**
    - After a successful POST, the BIOS locates and activates the bootstrap loader.
    - The bootstrap loader is a small program stored in the Master Boot Record (MBR) of the bootable device (usually the primary hard drive).
4. **Master Boot Record (MBR) and Boot Sector:**
    - The MBR contains the initial bootloader code.
    - The BIOS loads the MBR, which then accesses the boot sector of the active partition on the bootable device.
5. **Boot Sector Code Execution:**
    - The boot sector code, also known as the Volume Boot Record (VBR), is executed.
    - The VBR code is responsible for loading the core components of the operating system.
6. **Operating System Kernel Loading:**
    - The boot sector code loads the essential components of the operating system kernel into the computer's memory (RAM).
    - The kernel is the core part of the operating system that manages hardware resources and provides essential services.
7. **Device Drivers Loading:**
    - Once the kernel is loaded, the operating system loads necessary device drivers.
    - Device drivers are software components that enable communication between the operating system and hardware devices.
8. **Initialization and User Interface:**
    - The operating system initializes system settings, establishes user interfaces, and prepares for user interaction.
    - Graphical user interfaces (GUIs) or command-line interfaces (CLIs) are loaded, depending on the operating system.
9. **User Login:**

- If user authentication is required, the operating system prompts the user to log in by entering a username and password.

10. **User Desktop or Interface Display:**
    - Upon successful authentication, the user's desktop or interface is displayed, and the computer is ready for use.

In Short:

- The start-up
- Power On SelfTest
- Loading OS
- System Configuration
- Loading system utilities
- User authentication

Master Boot Record (MBR)

- **Definition:**
  - The Master Boot Record (MBR) is the information stored in the first sector of a hard disk or removable drive.
- **Purpose:**
  - Identifies how and where the system's operating system (OS) is located for the purpose of booting (loading) into the computer's main storage or random access memory (RAM).
- **Components:**
  - **Boot Code:**
    - The MBR includes a small program known as boot code.
    - This code is executed during the boot process and initiates the loading of the operating system.
  - **Partition Table:**

        - Contains information about the structure of the hard disk, including details about the partitions present.
        - Specifies the type and size of each partition.
- **Functionality:**
    - **OS Location:**
        - Identifies the location of the operating system on the storage device.
    - **Boot Sector Record Reading:**
        - Includes a program that reads the boot sector record of the partition containing the OS to be booted.
    - **Loading OS into RAM:**
        - The boot sector record, in turn, contains a program responsible for loading the rest of the operating system into RAM.
- **Key Role in Booting:**
    - During the boot process, the computer's BIOS or UEFI (Unified Extensible Firmware Interface) reads the MBR to find the bootable partition and initiate the OS loading process.
- **Limitation:**
    - MBR has limitations, such as supporting a maximum of four primary partitions or three primary partitions and one extended partition.
- **Legacy System Compatibility:**
    - MBR is a legacy partitioning scheme and is compatible with older systems.
- **Security Considerations:**
    - Vulnerable to certain types of malware attacks that can overwrite the MBR, affecting the boot process.
- **Evolution:**
    - Modern systems may use GUID Partition Table (GPT) as an alternative to MBR, offering benefits such as support for larger storage capacities and more partitions.

File System and Types

File System:

- A file system is a method used for storing and organizing computer files along with the data they contain, making it easy to locate and access them.
- It acts as a virtual filing cabinet, managing the organization, storage, and retrieval of files on various storage devices like hard disks, CDs, and flash drives.

Key Functions:

1. **Organization:** File systems organize data efficiently, resembling a hierarchical structure.
2. **Storage:** Manages the allocation and storage of data on physical media.
3. **Retrieval:** Facilitates easy retrieval of files when needed.
4. **Operations:** Handles tasks such as creating, deleting, and modifying files.

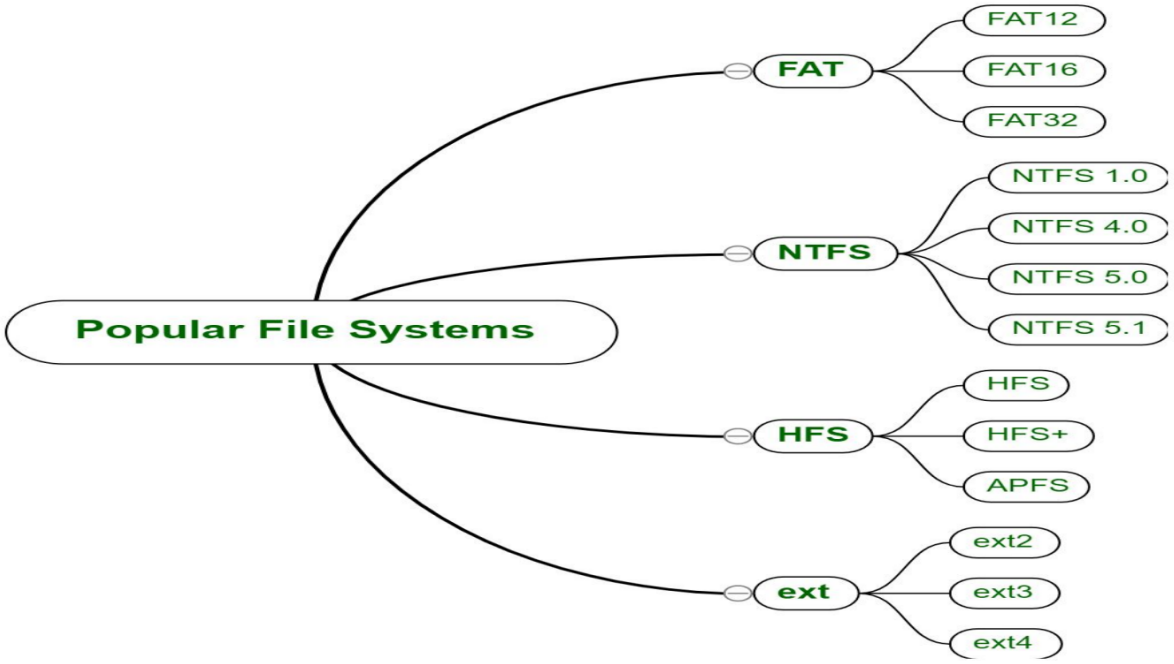
Common File Systems:

1. **FAT (File Allocation Table):**
    - *Usage:* Commonly used in removable storage devices and older Windows operating systems.
    - *Strengths:* Simplicity and compatibility.
    - *Limitation:* Limited in terms of maximum file size and partition size.
2. **NTFS (New Technology File System):**
    - *Usage:* Main file system for modern Windows operating systems.
    - *Strengths:* Security features, support for large file sizes, and advanced permissions.
    - *Limitation:* May not be as compatible with non-Windows systems.
3. **HFS+ (Hierarchical File System Plus):**
    - *Usage:* Used by macOS (prior to macOS Catalina, which uses APFS).
    - *Strengths:* Journaling for data integrity and support for large file sizes.
    - *Limitation:* Compatibility issues with non-Mac systems.
4. **ext4 (Fourth Extended File System):**

- *Usage:* Commonly used by Linux operating systems.
- *Strengths:* Journaling, support for large file systems, and backward compatibility with ext2 and ext3.
- *Limitation:* May not be as suitable for some specific use cases.

Unique Features and Characteristics:

- Each file system has its own set of features, strengths, and limitations.
- Examples include FAT's simplicity, NTFS's advanced security, HFS+'s journaling, and ext4's compatibility with older ext file systems.



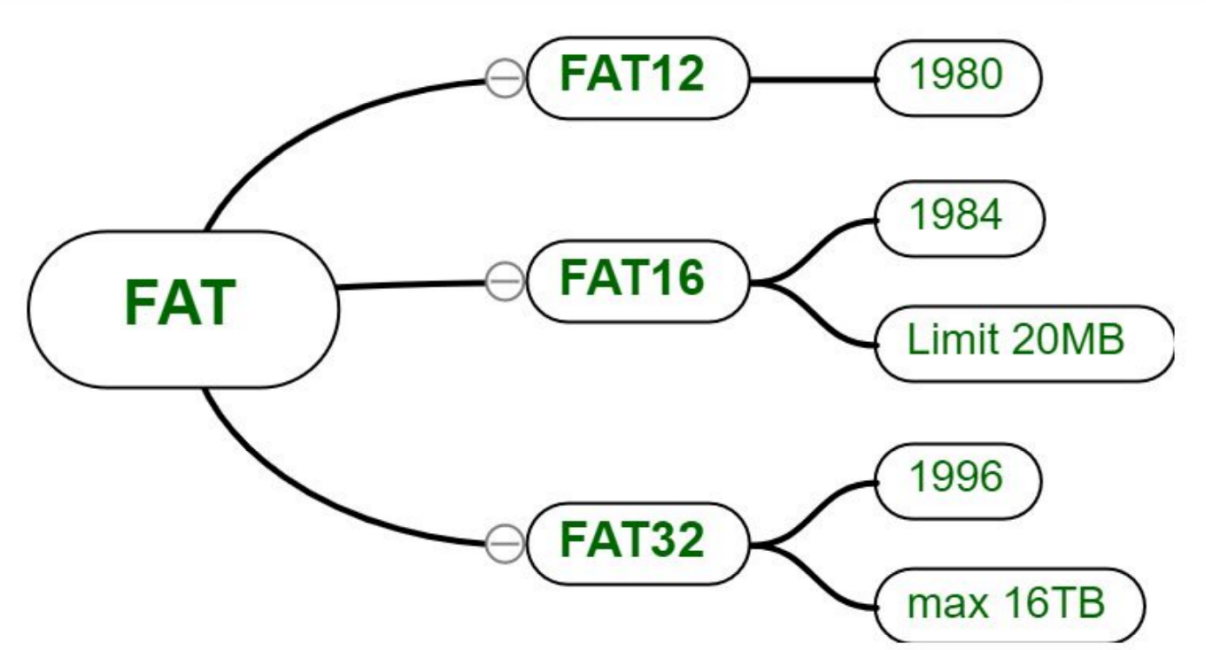
FAT (File Allocation Table)

- **Origin and Development:**
  - Originally developed by Microsoft for early versions of the MS-DOS operating system.
  - Widely adopted and still used in various devices, including flash drives, memory cards, and some older hard disk drives.
- **Allocation Method:**
  - Allocates file and folder storage using tables.

- **Variants:**
  - Three major variants:
    - FAT12 - 1980
    - FAT16 - 1984
    - FAT32 - 1996
- **Pros and Cons:**
  - **Pros:**
    - Simplicity and widespread support.
    - Readable and writable by multiple operating systems.
    - Suitable for smaller file systems and disks.
  - **Cons:**
    - File size limitations: 4GB in size.
    - Volume size limitations: Up to 2TB in size.
    - Poor performance, especially on large disks or files.
    - No journaling, potentially leading to data loss or corruption in the event of errors or crashes.
    - Limited support for file attributes like permissions and access control lists.
- **Usage and Compatibility:**
  - Often used in USB flash drives and pendrives due to its simplicity and wide support.
  - Compatible with Windows, Mac OS, and Linux, allowing the drive to be used across multiple platforms without compatibility issues.
- **Limitations of FAT32:**
  - Individual file size limited to 4GB.
  - Volume size limited to 2TB.
  - Performance can be slow, especially on large disks.
  - Lack of journaling can lead to data loss or corruption in case of errors or crashes.

- Limited support for file attributes.

- **Significance in USB Drives:**
  - Popular in pendrives due to simplicity, wide support, and compatibility with various operating systems.
  - File size limitations are not a significant concern for most pendrive users.
- **Comparison with NTFS:**
  - NTFS has higher theoretical limits in terms of file and volume size.
  - NTFS provides better performance and supports advanced features like journaling and file attributes.



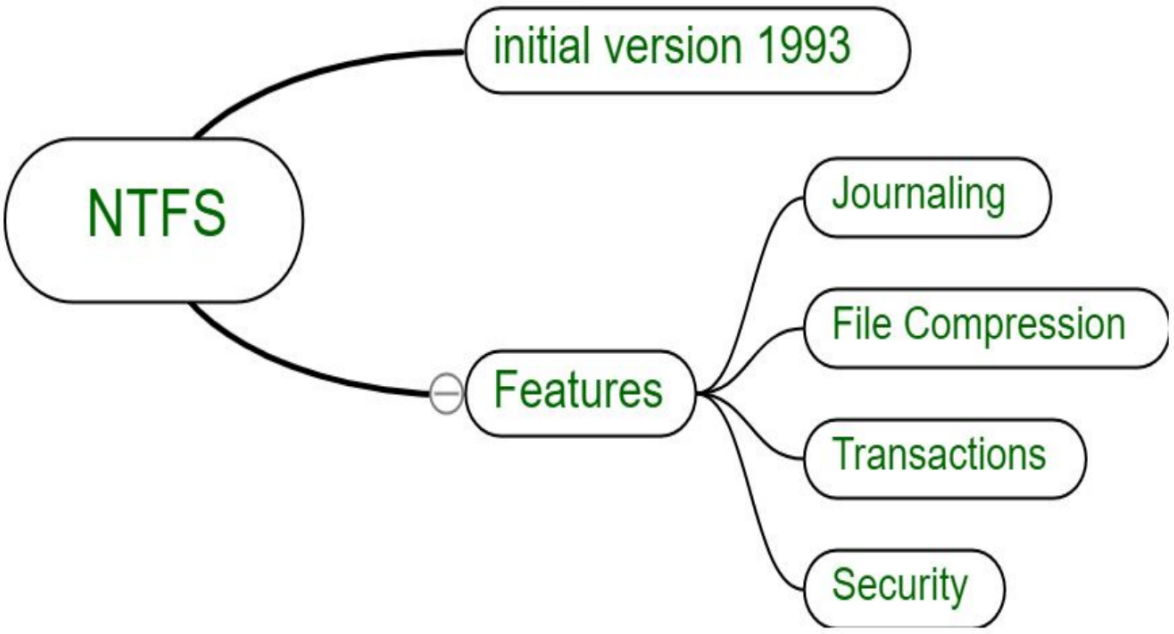
NTFS (New Technology File System)

- **Introduction:**
  - Introduced by Microsoft in 1993 with the Windows NT operating system.
  - Stands for New Technology File System.
  - An advanced and enhanced version compared to FAT systems.

- **Installation and Usage:**
  - Commonly used for internal drives.
  - All Windows installations are typically done on NTFS-formatted storage.
  - No file size limits, no partition or volume limits.
  - Theoretically supports up to 16 exabytes for a single file.
- **Advantages of NTFS:**
  - **Security:**
    - Built-in security features include file and folder permissions, encryption, and access control.
    - Enables administrators to restrict access to sensitive data and protect it from unauthorized access.
  - **Performance:**
    - Better performance compared to FAT, particularly with large files or high volumes of data.
    - Faster access times, quicker file searches, and improved data transfer rates.
  - **Stability:**
    - More stable and reliable, especially with large volumes of data.
    - Can handle larger files and partitions, with built-in error detection and recovery mechanisms.
  - **Compatibility:**
    - While primarily used in Windows, NTFS is compatible with other operating systems like Linux and macOS.
    - Offers versatility for data storage and sharing.
- **Limitations of NTFS:**
  - **Compatibility:**
    - Not compatible with some older operating systems like MS-DOS and Windows 95.
  - **Fragmentation:**

- Like most file systems, NTFS can become fragmented over time, leading to potential performance issues.

- **Security:**
  - While robust, it may be vulnerable to attacks such as malware that can bypass security features.
- **File Size Limitations:**
  - While supporting large file sizes, there is a practical limit of around 16 exabytes.
- **Recovery:**
  - Recovery of data from NTFS can be more challenging in the event of system failure or corruption.
- **Lack of Portability:**
  - Primarily used on Windows systems and not easily transferable to macOS or Linux.
- **Compression:**
  - NTFS offers compression features but may negatively impact performance and may not be suitable for certain types of data.



HFS (Hierarchical File System)

- Stands for Hierarchical File System.
- Specifically designed for macOS by Apple.
- The advanced version available is HFS+ (Apple Hierarchical File System).
- Initially designed for media like floppy and HDD, and used to some extent on CD-ROM as read-only.

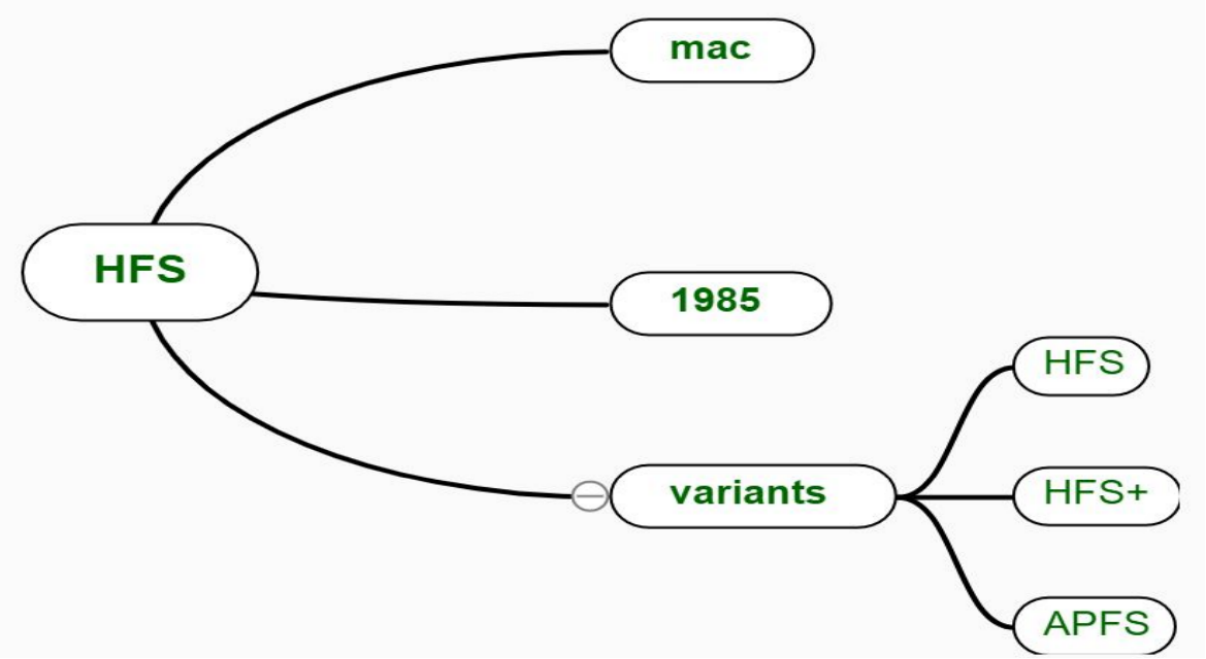
Why Mac uses HFS/HFS+:

- **Compatibility:**
  - Designed for the Mac operating system, ensuring maximum compatibility and efficiency.
- **Support for Mac-specific features:**
  - Supports features specific to Mac OS, such as resource forks, allowing storage of additional data related to a file.
- **Journaling:**
  - HFS+ introduced journaling, protecting against data loss in the event of a system failure or crash.
- **File size limitations:**
  - HFS+ supports larger file sizes than HFS, making it suitable for modern use cases.
- **Data integrity:**
  - Built-in data integrity checks to ensure file system stability and consistency.
- **Performance:**
  - Optimized for performance on Mac hardware, providing fast and efficient data access.
- **Seamless integration:**

- Tightly integrated into the Mac operating system for a seamless user experience.

Limitations of HFS:

- **Compatibility:**
  - Primarily designed for use on Mac systems, may not be compatible with other operating systems like Windows or Linux.
- **Fragmentation:**
  - Can become fragmented over time, potentially leading to slower performance.
- **Lack of support for modern features:**
  - May not support some modern features found in other file systems.
- **File size limitations:**
  - Although supporting larger file sizes than HFS, there is a practical limit of around 8 exabytes.
- **Journaling overhead:**
  - Journaling provides data protection benefits but may introduce some overhead.
- **Lack of support for case sensitivity:**
  - Not case-sensitive by default, causing issues when sharing files with case-sensitive systems.
- **Data recovery:**
  - Data recovery from HFS+ can be more challenging in the event of system failure or corruption.



EXT (Extended File System):

- Originally developed for UNIX and LINUX operating systems.
- First variant introduced in 1992.
- Overcame limitations like size of single file, volume size, and number of files in a folder.

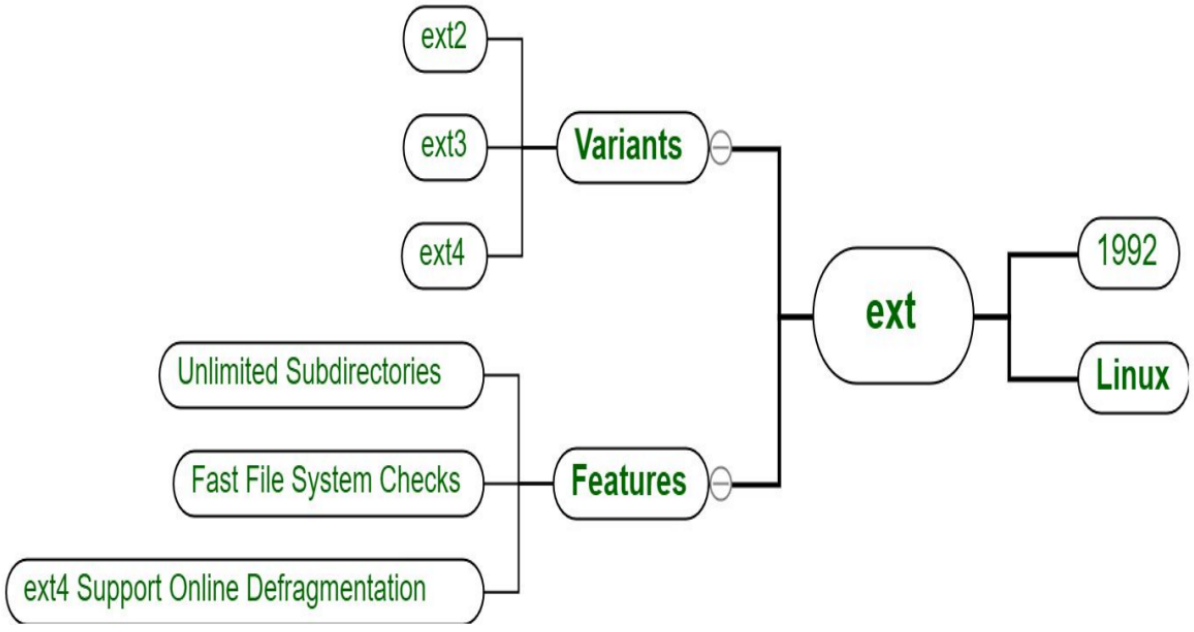
Why Linux systems use EXT:

- **Performance:**
  - Faster and more efficient than FAT or NTFS file systems, using fewer system resources.
- **Stability and reliability:**
  - Designed specifically for use with Linux, making them more stable and reliable.
- **Compatibility:**
  - Fully compatible with Linux, reducing limitations and potential compatibility issues.

- **Features:**
  - Offers advanced features like journaling for data loss prevention.

Limitations of EXT:

- **Fragmentation:**
  - Can suffer from fragmentation, potentially impacting system performance.
- **Compatibility:**
  - Designed specifically for Linux, may not be compatible with other operating systems.
- **Lack of built-in encryption:**
  - No built-in support for encryption, requiring third-party tools for sensitive data.
- **Limited file size:**
  - Depending on the version, there may be limits on the size of individual files.
- **Complexity:**
  - More complex and challenging to manage, especially for novice users.



Fragmentation:

- **Definition:**
  - Fragmentation occurs when information is deleted from storage media, leaving behind small gaps or free spaces.
  - As new data is saved, it is placed into these gaps or free spaces.
- **Process:**
  - When data is deleted, the space it occupied becomes available for new data.
  - If the gaps left by the deleted data are small, the new data may be stored in multiple available gaps.
- **Causes:**
  - Deletion of files or data.
  - Continuous saving and deletion of data over time.
- **Types of Fragmentation:**
  1. **External Fragmentation:**
     - Free spaces or gaps are scattered throughout the storage medium.
     - New data may be stored in non-contiguous blocks, leading to inefficient use of space.
  2. **Internal Fragmentation:**
     - Free space exists within allocated blocks or clusters.
     - Inefficient use of space within individual storage units.

Booting Process: Overview

1. **General Booting Process:**
   - The computer loads the operating system (OS) into its memory (RAM) during the booting process.

- Initialization begins by switching on the BIOS (Basic Input/Output System), loading it onto the RAM.

2. **BIOS and Power-On Self-Test (POST):**
    - BIOS stores the first instruction, initiating the Power-On Self-Test (POST).
    - POST checks the BIOS chip and CMOS RAM, ensuring hardware integrity.
    - If POST detects no battery failure, it proceeds to check hardware devices and secondary storage.

3. **Windows Booting:**
    - Windows XP, Vista, and 7 use the conventional BIOS-MBR method.
    - Windows 8 and later versions offer a choice between conventional BIOS-MBR and UEFI-GPT methods.

4. **CPU and BIOS Firmware:**
    - When the user switches ON the system, the CPU sends a Power Good signal to the motherboard.
    - BIOS starts the POST, checking hardware and loading firmware settings from non-volatile memory.

5. **Add-On Adapters and System Integration:**
    - If POST is successful, add-on adapters perform a self-test for integration with the system.

6. **Pre-Boot Process and System Boot Disk:**
    - Pre-boot process completes with POST, detecting a valid system boot disk.
    - Computer's firmware scans the boot disk and loads the Master Boot Record (MBR).

7. **MBR, Boot Configuration Data (BCD), and Bootmgr.exe:**

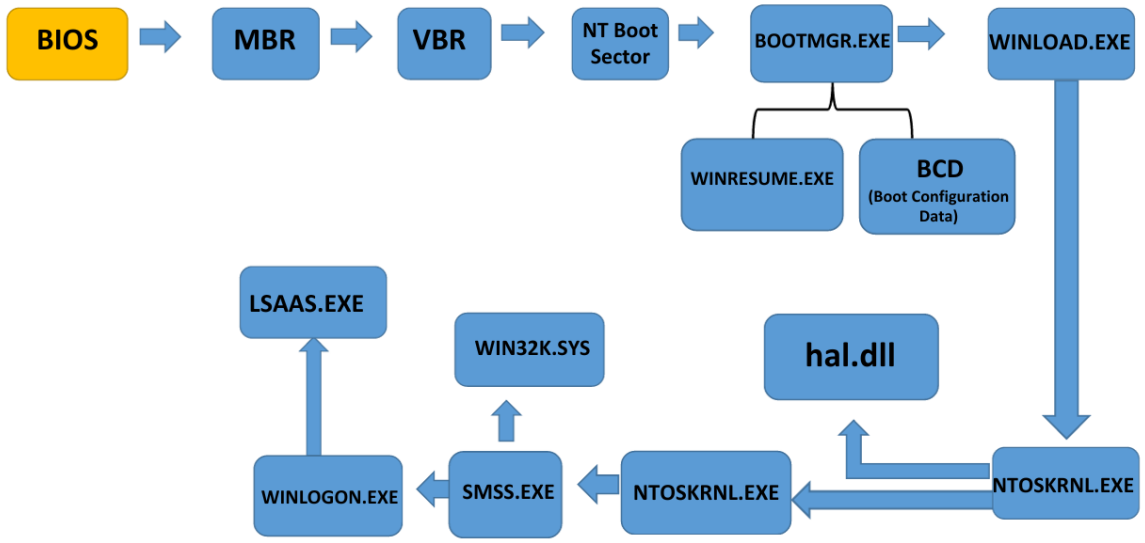
- MBR triggers Bootmgr.exe, which locates Winload.exe on the Windows boot partition.
- MBR searches for basic boot information in Boot Configuration Data (BCD).

8. **Windows Loader and OS Kernel Loading:**
    - Windows loader (Winload.exe) loads the OS kernel ntoskrnl.exe.
    - Kernel starts running, loading hal.dll, BOOT_START drivers, and SYSTEM registry hive into memory.

9. **Control Handover to Session Manager Process (SMSS.exe):**
    - Kernel passes control to the Session Manager Process (SMSS.exe).
    - SMSS.exe loads other registry hives and drivers needed for configuring the Win32 subsystem.

10. **User Authorization and Session Initialization:**
    - Session Manager Process triggers Winlogon.exe.
    - Winlogon.exe presents the user login screen for authorization.
    - SMSS.exe initiates the Service Control Manager, starting services, non-essential drivers, LSASS.EXE, and Group Policy scripts.

11. **User Session Creation and Desktop Initialization:**
    - Once the user logs in, Windows creates a session for the user.
    - Service Control Manager starts explorer.exe and initiates the Desktop Window Manager (DMW) process.
    - DMW initializes the desktop for the user, completing the booting process.



Windows Forensics: Collecting Volatile Information

Definition:

- Volatile information is data lost when the system powers off, primarily residing in RAM (Random Access Memory).

Significance:

- Includes artifacts like logged-on users, command history, network-related data.
- Vital for understanding the current state of the system during an incident.

Contrast with Non-Volatile Information:

- Non-volatile data persists even when the system is off.
- Includes data in internal/external storage, Windows registry, and file systems.

Collection Process:

- Live data acquisition captures volatile information while the system is running.

- Careful tool selection to avoid modifying memory contents.

Potential Artifacts:

- User(s) logged on, timeline of incidents.
- Programs and libraries in use.
- Files accessed and shared during attacks.
- Network information, connections, and status.
- Open files, processes, command history.
- Process memory, shared resources, clipboard contents.

Use Cases:

- Malware analysis.
- Examination of log and cache files.
- Active password determination.
- Investigation of network connections.

Tool Impact Awareness:

- Running tools for volatile data collection may alter memory contents.

Examples of Volatile Information:

- User sessions.
- Active network connections.
- Loaded processes and their memory.
- Clipboard content.
- Open files and shared resources.

Windows Forensics: Utility Tools and Data Collection

Utility Tools:

1. **PSTools:**
    - Provides a set of command-line utilities for system management.
2. `net session` **command:**
    - Displays computer and usernames, open files, and session durations.
3. `net file` **Command:**
    - Displays details of open shared files on a server, including name, ID, and file locks.
4. **NetworkOpenedFiles.exe:**
    - Windows utility tool showing files currently opened by other computers.

Collecting Network Information:

- **NetBIOS Name Table Cache:**
    - Maintains connections to other systems via NetBIOS.
    - Use `nbtstat` command to view NetBIOS name table cache.
- `netstat` **Command:**
    - Displays active network connections and listening ports.
    - Options:
        - `a`: Show all sockets (listening and non-listening).
        - `at`: List all TCP ports.
        - `au`: List all UDP ports.
        - `l`: List only listening ports.
        - `an | grep ':80'`: Identify process using a specific port (Linux).

Process Information:

Investigate running processes on a system for forensics purposes:

- **Information to Collect:**
    - Full path to the executable image (.exe file).

    - Command line used to launch the process.
    - Time the process has been running.
    - Security/user context in which the process is running.
    - Modules loaded by the process.
    - Memory contents of the process.
- **Windows Utility Tools:**
    - **Task Manager:**
        - Displays running programs, processes, and services.
    - **Tasklist:**
        - Lists applications and services with Process ID (PID) locally or remotely.
    - **PSTools.exe:**
        - Set of command-line utilities for detailed system management.

Process to Port Mapping:

- **netstat Commands:**
    - `netstat -a -all`: Show all sockets (listening and non-listening).
    - `netstat -at`: List all TCP ports.
    - `netstat -au`: List all UDP ports.
    - `netstat -l`: List only listening ports.
    - `netstat -an | grep ':80'`: Identify process using a specific port (Linux).

Examining Process Memory:

- **Purpose:**
    - Identify suspicious or malicious processes.
- **Tools:**
    1. **Process Explorer:**
        - Windows utility tool with VirusTotal support.
        - Checks if a running process is malicious.

2. **ProcDump:**
    - Command-line utility to dump the memory of a running process.

Collecting Network Status:

- **Information to Collect:**
    - Network Interface Cards (NICs) details.
    - Connection status (wired/wireless).
    - Assigned IP addresses.
- **Tools and Commands:**
    1. **Ipconfig/ifconfig:**
        - Displays NIC configuration and IP details.
    2. **Promiscdetect Tool:**
        - Checks if the network adapter is in promiscuous mode (possible sniffer indication).
    3. **Promqry Tool:**
        - Assesses the status of network interfaces.

Network Forensics Overview

Definition:

Network forensics is a subset of digital forensics focused on monitoring and analyzing computer network traffic. It aims to gather information, establish legal evidence, and detect intrusions.

Characteristics:

- **Real-time and Dynamic:**
    - Involves monitoring live network traffic.
    - Deals with volatile and dynamic information.
- **Pro-active Investigation:**

    - Requires a proactive approach due to the transient nature of network traffic.
- **Purpose:**
    - Discover the source of security attacks.
    - Investigate problem incidents within a network.

Steps in Collecting and Analyzing Network-Based Evidences:

1. **Identification:**
    - Recognize and define the scope of network evidence.
2. **Preservation:**
    - Ensure forensically sound preservation of evidence.
3. **Collection:**
    - Gather relevant network traffic data.
4. **Examination:**
    - Analyze data for patterns, anomalies, or indicators of compromise.
5. **Analysis:**
    - Interpret findings to reconstruct events and identify threats.
6. **Presentation:**
    - Present analyzed information in a clear format for legal or investigative purposes.

Network Components and Their Forensic Importance

1. Host

- Definition: A computer or device connected to a network.
- Characteristics:
    - Offers information resources, services, and applications.
    - Identified by a host address at the network layer.
- Importance:

    - Holds valuable artifacts.
    - Categorized as server or client systems.
    - Essential for understanding user activities.

2. Node

- Definition: A physical network node in data communication.
- Characteristics:
    - Can be data communication equipment (DCE) or data terminal equipment (DTE).
    - Has a MAC address if at least a data link layer device.
- Importance:
    - All hosts are physical network nodes.
    - Nodes of a distributed system include clients, servers, or peers.

3. Router

- Definition: Networking device responsible for directing data packets between computer networks.
- Characteristics:
    - Routes data packets based on destination address information.
    - Connects two or more data lines from various networks.
- Importance:
    - Handles traffic directing duties.
    - Differentiates between home routers and enterprise routers.

4. Switch

- Definition: Computer networking device using packet switching to connect devices on a network.
- Characteristics:
    - Forwards data only to devices that need it.
    - Controls traffic flow by identifying devices using MAC addresses.

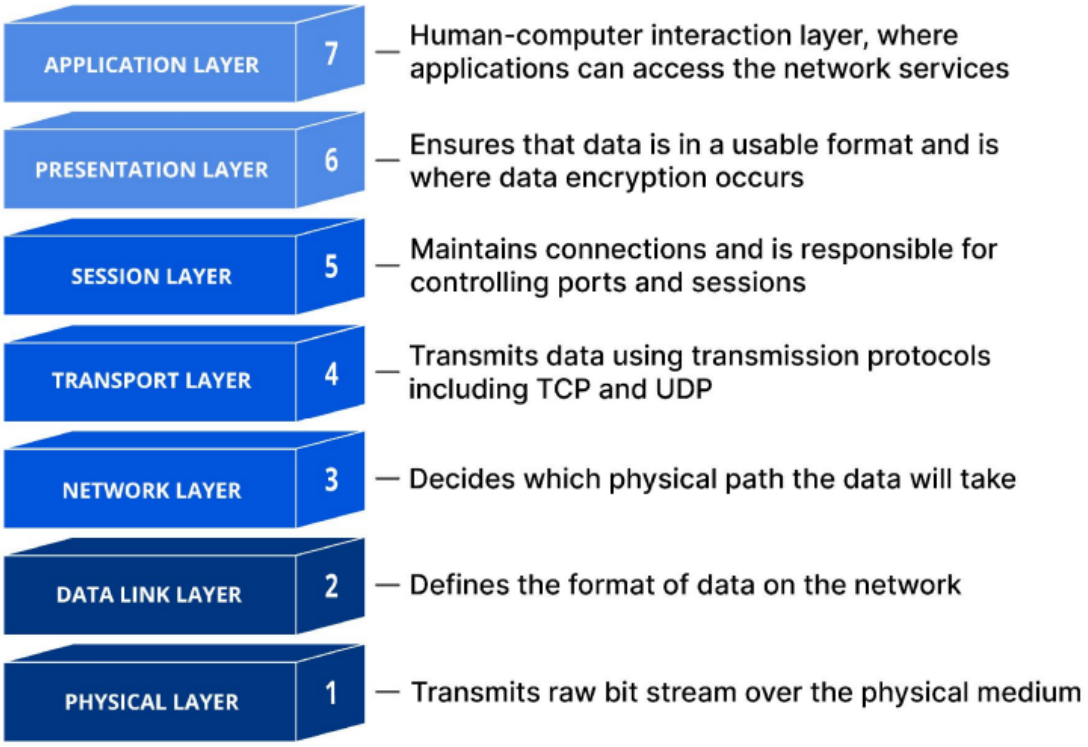
- Importance:
  - Enhances network security and efficiency.
  - Replaced less sophisticated network hubs.

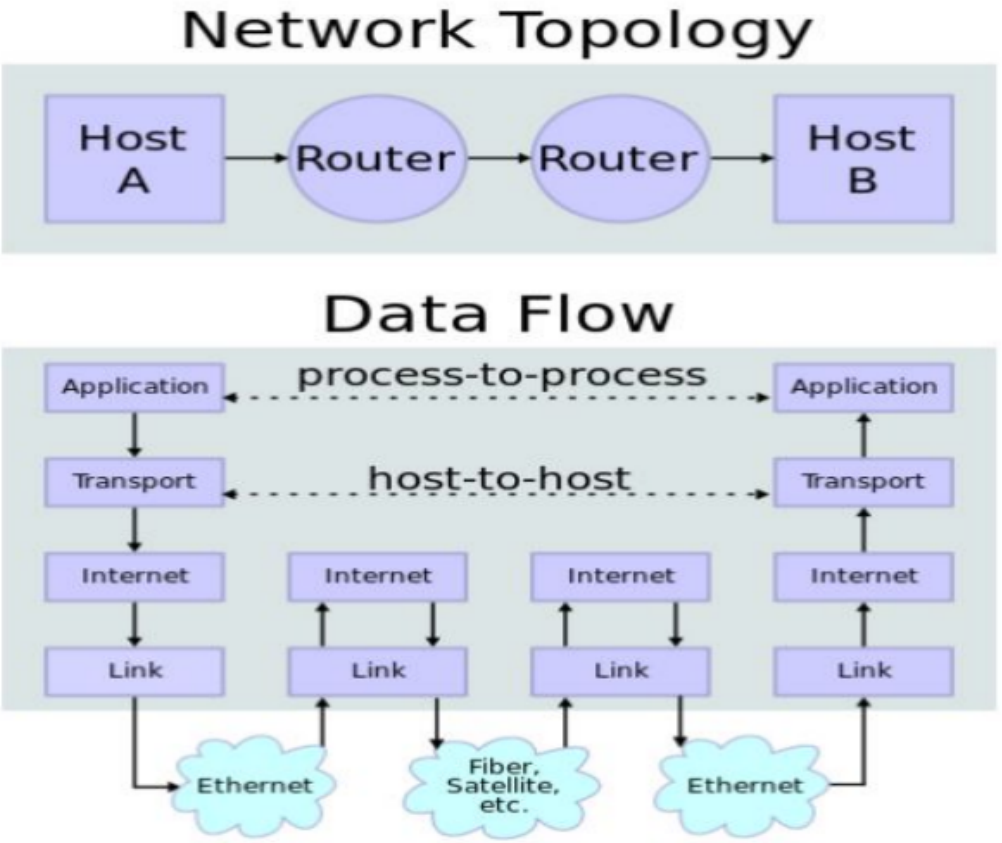
5. Hub

- Definition: Device for connecting multiple Ethernet devices and making them act as a single network segment.
- Characteristics:
  - Works at the physical layer (layer 1) of the OSI model.
  - Participates in collision detection.
- Importance:
  - Largely obsolete, replaced by network switches.
  - Some still used in old installations or specialized applications.

6. Network Interface Card (NIC)

- Definition: Hardware component connecting a computer to a computer network.
- Characteristics:
  - Holds the MAC address of the computer.
  - Physical bridge between the network and the host.
- Importance:
  - Essential for connecting the host to the network.
  - Key component for network communication.


APPLICATION LAYER
7
Human-computer interaction layer, where applications can access the network services
PRESENTATION LAYER
6
Ensures that data is in a usable format and is where data encryption occurs
SESSION LAYER
5
Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER
4
Transmits data using transmission protocols including TCP and UDP
NETWORK LAYER
3
Decides which physical path the data will take
DATA LINK LAYER
2
Defines the format of data on the network
PHYSICAL LAYER
1
Transmits raw bit stream over the physical medium



Log Analysis

- **Data Collection in IDPS:**
  - Large amounts of data gathered during Intrusion Detection and Prevention Systems (IDPS) are typically analyzed by a dedicated team using a different database system.
  - Live systems are usually not equipped to perform in-depth individual analyses without causing disruptions to normal users.
  - Methodologically, it is better to analyze copies of the data on separate systems to maintain the integrity of the original data.

- **Database Forensics:**
  - Used when the database itself is of interest.

    - Focuses on the content of the data rather than the database it is stored in.
    - Helps prevent claims of altering the original data during analysis.

- **Log Analysis Tasks:**
    - **Time Stamp Analysis:**
        - Examination of time stamps to establish the chronological sequence of events.
    - **Data Analysis:**
        - In-depth analysis of the content of the data obtained from logs.
    - **Other Analysis Techniques:**
        - Various techniques employed to recreate criminal incidents.

Importance of Log Analysis

1. **Investigation Reconstruction:**
    - Detailed record of events in system/network.
    - Aids forensic investigators in reconstructing sequences.
    - Provides insights into incident scope, impact, and timeline.
2. **Evidence Collection:**
    - Contains crucial evidence: timestamps, IP addresses, user activities.
    - Log analysis identifies and collects evidence for investigations.
    - Supports legal proceedings, source identification, and actions determination.
3. **Detection of Suspicious Activities:**
    - Reveals patterns of suspicious/malicious activities.
    - Real-time/retrospective log analysis identifies indicators of compromise.
    - Enables proactive threat detection and response.
4. **Malware Analysis:**
    - Provides info on malware behavior and impact.
    - Identifies entry points, propagation methods, and activities.

- Crucial for understanding compromise extent and countermeasure development.

5. **Incident Response:**
   - Detailed account of events aids incident response.
   - Identifies root causes, understands attacker techniques.
   - Assists in containing incidents, mitigating risks, and preventing future occurrences.
6. **Auditing and Compliance:**
   - Essential for regulatory compliance and internal auditing.
   - Verifies adherence to security policies and tracks user activities.
   - Ensures compliance with industry standards and legal requirements.

Network-Based Evidences

- **Ethernet:**
  - IP address, MAC address, ARP (Address Resolution Protocol).
- **TCP/IP:**
  - Includes analysis of packets data and GPRS data.
- **Internet:**
  - Covers web browsing, email, newsgroup, synchronous chat, and peer-to-peer traffic.
- **Wireless:**
  - Involves analysis of voice communication, location information, data communication, etc.

Types of Analysis Done by Network Forensic Tools

1. **Network Traffic Capturing and Analysis:**
   - Capturing and analyzing data packets flowing through a network.
2. **Evaluation of Network Performance:**

- Assessing the overall performance and efficiency of the network.

3. **Detection of Anomalies and Misuse of Resources:**
   - Identifying unusual patterns or unauthorized use of network resources.
4. **Determination of Network Protocols in Use:**
   - Analyzing and identifying the network protocols being utilized.
5. **Aggregating Data from Multiple Sources:**
   - Consolidating data from various sources for comprehensive analysis.
6. **Security Investigations and Incident Response:**
   - Investigating security incidents and responding to security breaches.
7. **Protection of Intellectual Property:**
   - Safeguarding against theft or misuse of intellectual property through network analysis.

Windows Log Analysis

- **Primary Source of Evidence:**
  - Windows Event Logs log every system activity.
  - Crucial for forensic investigations.
- **Timeline Construction:**
  - Windows Event Log analysis aids in creating a timeline.
  - Depends on audit features; logs can be turned off with administrative privileges.
- **Forensic Significance:**
  - Captures significant data for forensic analysis.
- **Event Log Components:**
  - **Application Log**
  - **System Log**
  - **Security Log**
- **Log Storage Location:**

    - Windows logs are saved in `%System32%\\winevt\\Logs` in binary format.
- **Offline Log File Size:**
    - User can set the offline event log file size.
- **Log Maintenance:**
    - When the maximum log size is reached:
        - Oldest events are overwritten.
        - Logs can be archived when full.
        - Manual clearing of logs prevents event overwriting.

Main Event Logs

1. **System Log:**
    - Records events by OS segments.
    - Contains data on hardware changes, device drivers, system changes, and related activities.
2. **Security Log:**
    - Records Logon/Logoff and security-related activities.
    - Specified by system's audit policy.
    - Crucial for detecting and investigating unauthorized activities.
3. **Application Log:**
    - Records application-related events.
    - Captures errors, informational events, and warnings.
    - Troubleshoots software problems.

Other Important Event Logs

- **Directory Service Events:**
    - Domain controllers record Active Directory changes.
- **File Replication Service Events:**
    - Records File Replication service events, especially `Sysvol` changes.
- **DNS Events:**

- DNS servers record DNS-specific events.

Windows Event Log Vulnerabilities

1. Disabling Event Log Service:

- Possible to disable the event log service in Windows.

2. Modification of Important Data:

- Critical data such as Date and Time, Computer Name, and Usernames can be altered.

3. Transplanting Event Logs:

- Event logs from one machine can be transplanted into another, leading to potential misinterpretation.

4. Timestamp Inaccuracy:

- Logs use the internal host clock for timestamps, impacting accuracy if the clock is inaccurate.

Tools for Parsing Event Logs

1. **LogParser**
2. **Event Log Explorer**
3. **ManageEngine Event Log Analyzer**
4. **LOGAlyze**
5. **SolarWinds Event & Log Manager**
6. **NetVizura EventLog Analyzer**
7. **GrayLog**
8. **LogCheck**

Forensic Procedures for Acquiring Windows Event Logs

1. Storage Format:

- Windows Event Logs stored in Binary XML format.

2. Readability:

- Readable format provided by built-in Windows feature for troubleshooting.

3. Non-Volatile Storage:

- Logs stored in the Hard Drive, accessible even when the machine is powered off.

4. Default Storage Location (Windows 10):

- `%Windows%System32/Winevt/Logs`

5. Customization (Windows 10):

- Registry Location:
  `HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\EventLog`

6. Storage Location (Windows XP):

- `%Windows%System32/config/*.evt`

Log Analysis Using Splunk

- **Overview:**
  - Splunk Inc. provides software for searching, monitoring, and analyzing machine-generated data.
- **Functionality:**
  - Captures, indexes, and correlates real-time data.
  - Generates graphs, reports, alerts, dashboards, and visualizations.
- **Use Cases:**
  - Application management, security, compliance, business analytics, and web analytics.
- **Key Features:**
  - Identifying data patterns, providing metrics, diagnosing problems, and offering business intelligence.

Removing LM Hash

- Most versions of Windows allow configuring the disabling of the creation and storage of valid LM hashes when users change their passwords.
- Default setting in Windows Vista, but disabled by default in previous versions.
- **Note:** Enabling this setting doesn't immediately clear LM hash values from SAM. It activates an additional check during password change operations, storing a "dummy" value in the SAM database where the LM hash is stored. This dummy value is the same for all user accounts and is unrelated to the user's password.

Active Directory (AD)

Overview:

- Directory service developed by Microsoft for Windows domain networks.
- Included in most Windows Server operating systems as processes and services.

AD Domain Controller:

- Authenticates and authorizes all users and computers in a Windows domain network.
- Assigns and enforces security policies for all computers.
- Installs or updates software.

User Authentication:

- When a user logs into a computer in a Windows domain, Active Directory checks the submitted password.
- Determines the user's role as a system administrator or a normal user.

Components:

- **Database:** Stores objects and corresponding executable code.
- **Directory System Agent:** Executable part, consisting of Windows services and processes running on Windows 2000 and later.

Accessing Objects:

- Objects in Active Directory databases can be accessed via LDAP, ADSI (a component object model interface), messaging API, and Security Accounts Manager services.

Password Cracking

- **Definition:**
  - Process using an application to identify unknown or forgotten passwords.
  - Can lead to unauthorized access and various criminal activities.
- **Methods:**
  1. **Brute Force:**
     - Iterates through character combinations until finding the correct password.
  2. **Dictionary Searches:**
     - Searches each word in a dictionary for the correct password.
  3. **Syllable Attack:**
     - Combines dictionary words' syllables in various ways for brute force searches.
  4. **Rule-Based Attack:**
     - Uses preoccupied information to form rules, narrowing down searches.
  5. **Hybrid Attack and Password Guessing:**
     - Concatenates known passwords with symbols or guesses common passwords.
  6. **Rainbow Attack:**
     - Generates possible passwords using different words from the original password.

Password Cracking Tools:

1. **Cain and Abel:**
   - *Functionality:* Recovers passwords for Microsoft Windows user accounts and Microsoft Access passwords.
   - *Features:* Utilizes a graphical user interface, making it user-friendly. Employs dictionary lists and brute-force attack methods.
2. **Ophcrack:**

- *Functionality:* Uses rainbow tables and brute-force attacks for password cracking.
- *Compatibility:* Runs on Windows, macOS, and Linux.

3. **John the Ripper:**
    - *Approach:* Utilizes a dictionary list approach.
    - *Compatibility:* Primarily designed for macOS and Linux systems.
    - *Interface:* Command-line prompt for password cracking.

Wireless Network Vulnerabilities:

Wireless communications provide convenience but introduce security challenges, making networks susceptible to various attacks.

1. Wi-Fi Attacks:

- *Advantages:* Enhances device mobility but exposes networks to attacks.
- *Comparison:* Wired networks require physical access; wireless networks can be targeted remotely.
- *Primary Use:* Connects endpoints (e.g., computers, tablets) to routers via wireless access points.

2. Evil Twin Attacks:

- *Description:* Malicious creation of a Wi-Fi network mimicking a legitimate one.
- *Example:* Attacker sets up an access point with a similar name to a public Wi-Fi network.
- *Risk:* Unencrypted traffic can be intercepted, enabling Man-in-the-Middle attacks.

3. Rogue Access Points:

- *Definition:* Unauthorized device connected to a network.
- *Examples:* Personal devices or malicious backdoors.
- *Risk:* Potential security breaches; not approved by the network administrator.

4. Wi-Fi DOS Attacks:

- *Description:* Disassociation attack breaks the connection between victim and access point.
- *Attack Type:* Denial of Service (DOS).
- *Method:* Attacker poses as the victim, instructs access point to disassociate from the victim device.

5. Jamming Attacks:

- *Method:* Purposeful use of electromagnetic interference.
- *Risk:* Interferes with victims' connections, potentially blocking communication.
- *Legality:* Spectacularly illegal; likely to incur regulatory penalties from entities like the FCC.

Short-Range Communication Attacks: Bluesnarfing and Bluejacking

1. Bluesnarfing:

- *Bluetooth Technology:* Standard protocol for connecting various devices.
- *Devices:* Computers, laptops, smartphones, I/O devices.
- *Communication:* Uses radio transmissions with a frequency range similar to Wi-Fi.
- *Pairing:* Devices pair for data transfer, depending on security settings.
- *Attack Technique:* Bluesnarfing retrieves data from a victim's device.
- *Condition:* Occurs when Bluetooth is discoverable to others.
- *Exploitation:* Uses Object Exchange Protocol (OBEX) to exchange information.
- *OBEX Protocol:* Vendor-independent protocol implemented on various operating systems.
- *Attack Process:*
    1. Attacker exploits OBEX Protocol vulnerabilities.

2. Bluesnarfing attack initiated when Bluetooth is discoverable.
3. Attacker pairs with victim's device.
4. Data retrieval occurs if the victim's firmware protection is weak.

- *Bluesnarfing Software:* Examples include Bluediving, BlueBug, BlueSnarf, BlueSnarf++, BlueSmack.
- *Usage:* Penetration testing of Bluetooth devices, available on the dark web.

2. Bluejacking:

- *Description:* Unsolicited sending of messages to Bluetooth-enabled devices.
- *Objective:* Typically harmless, aims to send a message or contact without user consent.
- *Process:*
  1. Attacker identifies nearby Bluetooth-enabled devices.
  2. Sends messages or contacts without pairing.
- *Intent:* Often for pranks, harmless communication, or to gain attention.
- *Prevention:* Set Bluetooth device to non-discoverable mode.

	WiFi 4	**WiFi 5**	**WiFi 6**
Release time	2009	2014	2019
Frequency bands	2.4 GHz and 5 GHz	5 GHz	2.4 GHz and 5 GHz
Channel width	20 Mhz, optional 40 Mhz	20 Mhz, 40 Mhz, 80 Mhz, optional 160 Mhz	20 Mhz, 40 Mhz, 80 Mhz, 160 Mhz
Maximum data rate	150 Mbps	3.5 Gbps*	9.6 Gbps*
Highest modulation	64-QAM	256-QAM	1024-QAM
Advanced antenna technology	MIMO	UL MU-MIMO	UL & DL MU-MIMO
Underlying technology	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11ax

WiFi (Wireless LAN Standard):

- *Definition:* Wireless LAN standard, part of IEEE 802.11, enabling communication among different devices.
- *Transmission Medium:* Radio waves, similar to Bluetooth and cellular networks.
- *Scale of Use:* Small-scale communication for houses, malls, public areas.
- *Applications:* Web browsing, online gaming, video streaming, VOIP calling.
- *Statistics (2019):* Over 310 million WiFi devices shipped.

Wireless Connection Basics:

- *Communication:* Two-way communication between a router and a client device.
- *Equipment:* Both equipped with radio transmitters and receivers.
- *Frequency:* Signals transmitted over radio frequencies (2.4 GHz or 5 GHz).
- *Router Connection:* Physically connected to the internet via an Ethernet outlet or modem.
- *SSID Broadcast:* Router broadcasts its WiFi name (SSID) to nearby devices.
- *Connection Establishment:* Device signals router, connection established upon router acceptance.

IEEE 802.11 Standard:

- *Definition:* Globally-used specification for wireless LAN networking by IEEE.
- *Improvement Focus:* Enhance wireless network performance.
- *Evolution:* Updated versions (802.11n, 802.11ac, 802.11ax) with backward compatibility.
- *Compatibility:* All WLAN devices should meet the same 802.11 specification.

QAM (Quadrature Amplitude Modulation):

- *Definition:* Modulation technique combining phase and amplitude modulation.

- *Effective Bandwidth:* Doubles effective bandwidth by changing both amplitude and phase of a carrier wave.
- *Other Names:* Quadrature carrier multiplexing.
- *Characteristics:* Phase difference between carriers is 90 degrees with the same frequency.

Wireless Security:

- *Complexity:* Wireless networks offer convenience but are complex.
- *Concerns:* Data packets travel wirelessly, potentially accessible to eavesdroppers.
- *Security Areas:*
  - *Authentication:* Identifying endpoints and end-users.
  - *Privacy:* Protecting wireless data packets from interception.
  - *Integrity:* Ensuring the integrity of wireless data packets.

Rogue Devices:

- *Association:* Wireless clients form associations with Access Points (AP).
- *Coexistence:* All devices coexist when following 802.11 standards.
- *Threats:* Rogue devices may pose a threat to wireless security.
- *Potential Risks:* Data theft, network unavailability.

Wireless Security Methods

1. **Authentication:**
   - *Objective:* Verify the identity of wireless clients.
   - *Methods:*
     1. **Wired Equivalent Privacy (WEP):**
        - Encryption: Uses RC4 cipher algorithm for frame encryption.
        - WEP Key: Key for authentication and encryption.

- Association: Client associates with AP only with the correct WEP key.
- Challenge-Response: AP challenges client with a phrase, and access is granted if encrypted responses match.

2. **Extensible Authentication Protocol (802.1x/EAP):**
    - Centralized Authentication: Involves a dedicated authentication server.
    - Participants: Supplicant (device requesting access), Authenticator (provides access, usually WLAN controller), Authentication Server (grants/denies access).

    - EAP Types:
        - LEAP (Lightweight Extensible Authentication Protocol): Introduced by Cisco Systems, aims to counter vulnerabilities.
        - EAP-FAST (Flexible Authentication via Secure Tunneling): Addresses earlier vulnerabilities in CHAP and PAP.
        - PEAP (Protected Extensible Authentication Protocol): Developed to safeguard EAP conversations.
        - EAP-TLS (Transport Layer Security): Relies on digital certificates for secure key exchange and authentication.
        - EAP-TTLS (Tunneled Transport Layer Security): Similar to EAP-TLS but eliminates the need for digital certificates on the client's end.

Notes:

- *Authentication Types:* WEP (RC4 Cipher) and Extensible Authentication Protocol (802.1x/EAP).
- *WEP Encryption:* Uses RC4 cipher; access granted based on correct WEP key.
- *802.1x/EAP:* Centralized authentication involving supplicant, authenticator, and authentication server.

- *EAP Types:* LEAP, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS.
- *EAP-TLS:* Relies on digital certificates for secure key exchange and authentication.
- *EAP-TTLS:* Similar to EAP-TLS but doesn't require digital certificates on the client's end.

WADS/WIDS (Wireless Attack Detection System)

Overview:

- **Function:** Analyze network traffic, detect anomalies, and identify suspicious behavior in wireless networks.
- **Purpose:** Detect security breaches, unauthorized access attempts, and rogue access points compromising network security.

Capabilities:

1. **Alert Generation:**
    - *Action:* Generates alerts or notifications upon detecting potential security threats.
    - *Benefit:* Enables prompt investigation and response by network administrators or security personnel.
2. **Automated Response:**
    - *Advanced Feature:* Some solutions have automated response capabilities.
    - *Actions:* May include blocking or quarantining devices exhibiting suspicious behavior.

Detection Mechanisms:

- **Known Attack Signatures:**
    - *Identification:* Detection based on known attack signatures.
- **Device Signatures:**
    - *Comparison:* Compares device signatures to an approved device database.

- **Traffic Anomalies:**
  - *Identification:* Detects anomalies differing from normal network behavior patterns.

Example:

- **Rogue Access Point Detection:**
  - *Method:* MAC address verification against an approved database.
  - *Anomaly Detection:* Drastic increase in network traffic as an indication of an encryption key cracking attempt.

Wireless Attack Detection Systems:

1. **Snort-Wireless:**
   - *Type:* Open-source Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).
   - *Features:* Real-time network traffic analysis and packet logging.
   - *Rule-Based Language:* Combines anomaly, protocol, and signature inspection methods.
   - *Detection Abilities:* Identifies DoS and DDoS attacks, CGI attacks, buffer overflows, and stealth port scans.
   - *Deployment:* Free-to-use, open-source software deployable by individuals and organizations.
   - *Rule Language Use:* Determines collected network traffic and defines actions upon detecting malicious packets.

Introduction to Web Applications:

Definition:

- **Web Applications:** Programs on a central server enabling users to submit and retrieve data via the Internet.

Workflow:

1. User visits a website.

2. Client makes a request to a web server through a web application.
3. Web application generates response documents (e.g., HTML, XML) for better client service.
4. Web documents are in standard formats supported by all browsers.

Web Application Forensics:

Significance:

- Crucial in the aftermath of attacks on web applications.

Focus Areas:

- Forensic examination of web applications, logs, www directory, and config files.
- Tracing and identifying attack origin, propagation, devices used, and individuals involved.
- Examining logs, configuration files of server, network, and host machine.

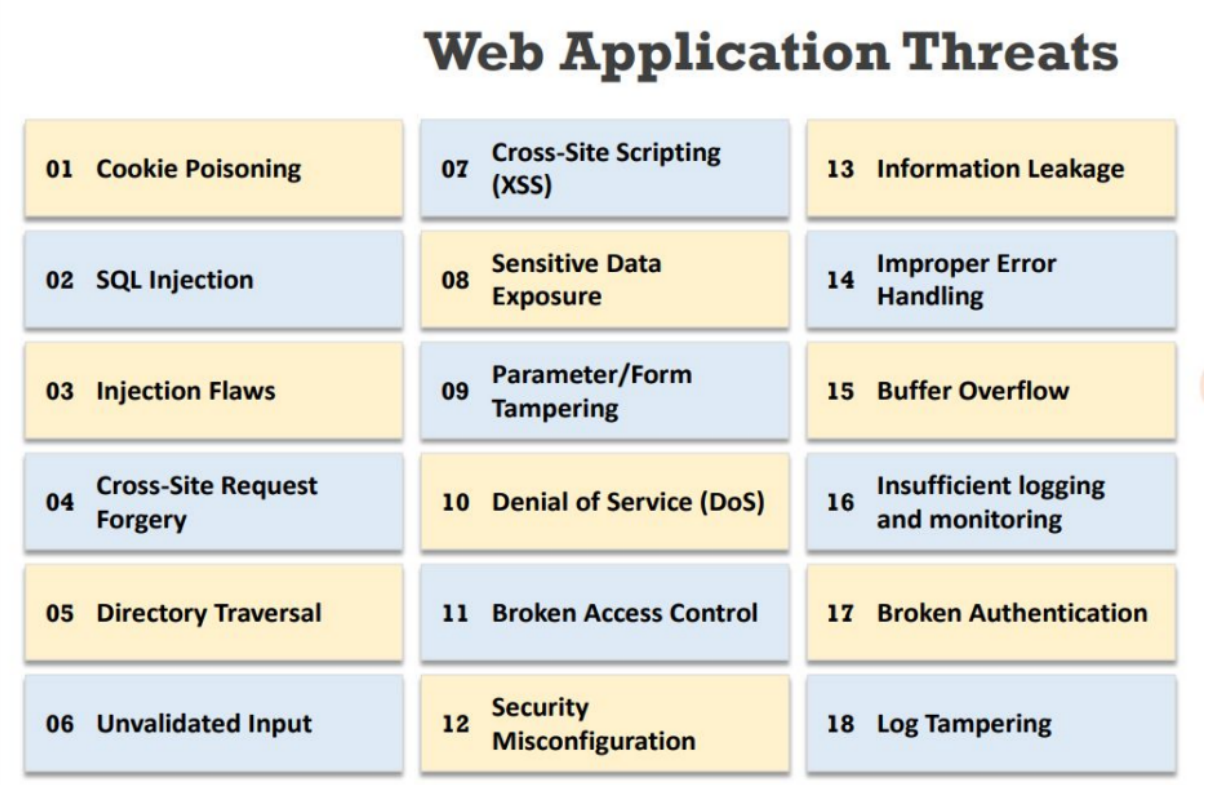
Investigator's Tasks:

- Understand various web and application servers.
- Analyze and correlate logs from different sources.
- Gather digital fingerprints left by attackers.
- Collect data fields associated with each HTTP request:
  - Date and time
  - IP address
  - HTTP method (GET/POST)
  - Uniform Resource Identifier (URI)
  - Query sent via HTTP
  - HTTP headers
  - HTTP request body

Challenges:

- Attackers use reverse proxies and anonymizers.

- Limited access to HTTP information may make it challenging to differentiate valid and malicious requests.



Indicators of Web Attack:

Components Indicating Web Attacks:

1. **Denial of Service (DoS):**
   - Users denied access to target web server's information or services.
2. **Redirection to Unknown Website:**
   - User redirected to a malicious site upon entering the website's URL.
3. **Network Performance Issues:**
   - Unusually slow performance and frequent server reboots.
4. **Anomalies in Log Files:**
   - Unusual activities recorded in log files.
5. **Password Changes and New User Accounts:**

- Indicative of attack attempts.

6. **Leakage of Sensitive Data and Defacement:**
    - Indications of web attacks.
7. **Error Messages:**
    - HTTP 500, "internal server error," and other error messages indicate potential attacks.

WEB ATTACK FORENSICS:

Objective:

- Trace the attacker and gather evidence for legal proceedings.

Areas of Investigation:

a) **Web Application Forensics:**

- Focus on evidence collection and protection, particularly logs.
- Utilize robust forensic tools for preliminary analysis.
- Standard methodologies ensure admissibility in court.

b) **Web Services Forensics:**

- Investigate beyond web applications to encompass web services.

Major Investigator Tasks in Web Application Forensics:

a) **Preliminary Analysis:**

- Focus on evidence collection, especially logs.
- Utilize robust forensic tools for confidence-building.

b) **Standard Methodology:**

- Protect web application during forensic examination to prevent modification.

- Extract evidence files: web and application server logs, scripts, configuration files, third-party software logs, OS logs.

c) **Analysis:**

- Divide log files by user sessions for clarity.
- Explore fingerprints of web application security attacks:
  - Unusual entries in logs.
  - Script abuse.
  - Excessive attempts from the same IP.
  - Unusually long processing times.
  - Files created or modified around the time of the suspected attack.

d) **Report Preparation:**

- Compile a report based on data extracted from web application logs.

Website Traffic Analysis:

Terms in Website Traffic Analysis:

- **URL:** Uniform Resource Locator.
- **Hit:** Each HTTP request submitted by the browser.
- **Page:** Successful HTTP request for primary website content.
- **File:** Each successful HTTP request.
- **Visitor:** Actual person browsing the website.
- **Visit:** Series of HTTP requests by a visitor within a set time.

Indicators of Web Attacks:

- Denial of Service (DoS).
- Redirection to unknown websites.
- Network performance issues.
- Anomalies in log files.

- Password changes and new user accounts.
- Leakage of sensitive data and defacement.
- Error messages (e.g., HTTP 500).

WEB APPLICATION FORENSICS TOOLS:

Useful Tools:

1. **Microsoft LogParser.**
2. **EventLogAnalyzer.**
3. **Http-analyze.**
4. **Pyflag.**
5. **Analog.**
6. **Open Web Analytics (OWA).**
7. **Mywebalizer.**
8. **CORE Wisdom.**
9. **Logjam.**
10. **Sawmill.**
11. **Lire.**

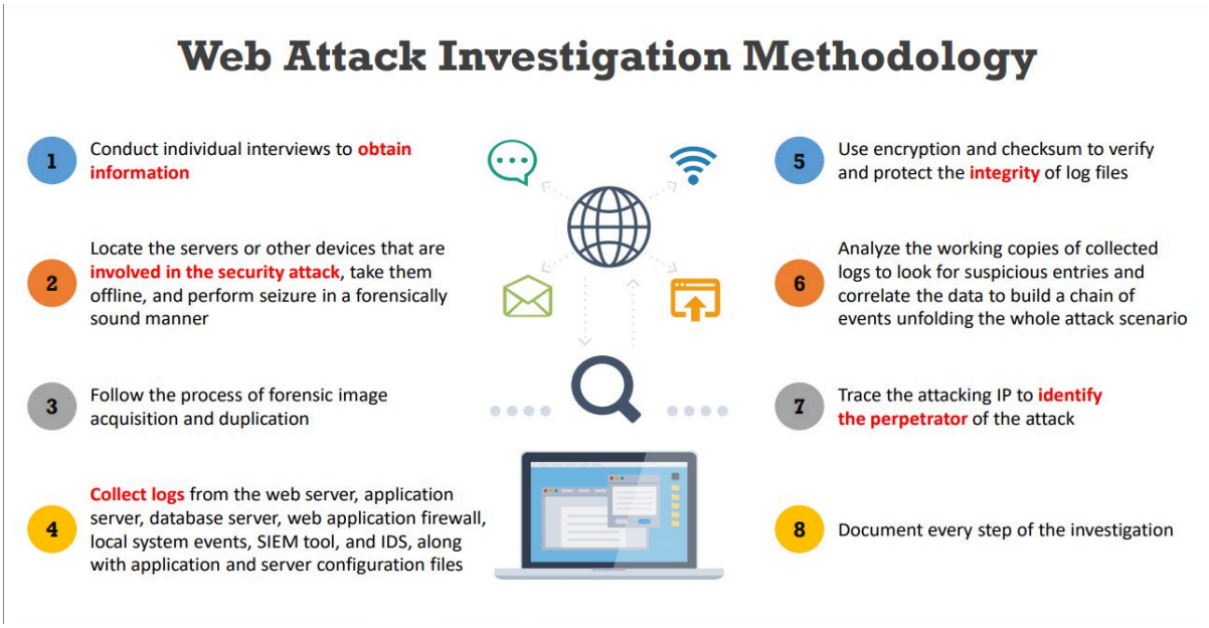
Logparser:

- A flexible command-line utility for analyzing log files.
- Originally designed for IIS logging on Windows.
- Supports querying text-based data and various data sources.
- Provides output customization options.
- Part of the IIS 6.0 Resource Kit Tools.

Open Web Analytics (OWA):

- Open-source web analytics software in PHP with a MySQL database.
- Comparable to Google Analytics but installable and run on user's host.

- Supports tracking with WordPress and MediaWiki.
- Enables tracking of website views and competitor analysis.



Thanks for reading my notes! I hope it was helpful in your learning curve. For more such content follow me on my GitHub and Twitter :)

GitHub:

cyph3rryx - Overview

21 y/o 😁 • Cybersecurity Student💫 • CTF & Bug Bounty 👾• Security Researcher 🪲 • Screenwriter 😉• Nerd 😎 • Top 3% on TryHackMe (New Ranking System) 😌 - cyph3rryx

https://github.com/cyph3rryx

Twitter:

Ryx (@PadhiyarRushi) / X

21 y/o • Cybersecurity Student • CTF & Bug Bounty • Security Researcher • Screenwriter • Graphic Designer • In Top 3% @RealTryHackMe

https://twitter.com/PadhiyarRushi