Chapter 5
Operating System Investigation

8 hrs

Er. Shiva Ram Dam

Assistant Professor

Gandaki University

Content:

1. **Windows File Systems, Registry Hives and Event Logs**
2. **Linux File System basics**
3. **Android File System basics**
4. **Memory acquisition and analysis in Windows**

5.1 Operating System Investigation

- A computer's Operating System (OS) is the **collection of software that interfaces with computer hardware and controls the functioning** of its pieces, such as the hard disk, processor, memory, and many other components.
- Forensic investigation on an OS can be performed because it is responsible for **file management, memory management, logging, user management, and many other relevant details**.
- The **forensic examiner must understand OSs, file systems,** and numerous tools required to perform a thorough forensic examination of the suspected machine.
- OS investigation, in the context of digital forensics, refers to the process of examining an operating system (OS) to collect, analyze, and interpret evidence related to security incidents, cybercrimes, or system failures.
- It involves analyzing system logs, file systems, registry entries, memory dumps, and other artifacts to uncover malicious activities, unauthorized access, data breaches, or forensic evidence.

5.2 Operating System Forensics

- **Operating System Forensics** is a branch of **digital forensics** that focuses on analyzing and investigating an operating system (OS) to uncover digital evidence.
- The goal is to identify, preserve, and interpret data from an OS that may be used in legal investigations, cybersecurity incidents, or internal audits.

- The **understanding of an OS and its file system is necessary** to recover data for computer investigations.
  - The file system provides an operating system with a roadmap to data on the hard disk.
  - The file system such as FAT, NTFS, EXT, etc. also identifies how hard drive stores data.
  - Data and file recovery techniques for these file systems include data carving, slack space, and data hiding.
  - Another important aspect of OS forensics is memory forensics, which incorporates virtual memory, Windows memory, Linux memory, Mac OS memory, memory extraction, and swap spaces.

Example Case

- Suppose a company suspects an employee of stealing sensitive data.
- An operating system forensic expert may:
  - Examine system logs for file access and USB insertions
  - Analyze deleted files and browsing history
  - Recover data from memory dumps or swap files
  - Provide a timeline of activity that supports the investigation

Why It Is Important?

- Detect **unauthorized access**
- Investigate **malware infections**
- Recover **deleted files**
- Track **user activity**
- Support **legal proceedings**

Key Areas Examined

1. File System Analysis
- Detect deleted, hidden, or altered files
- Analyze file timestamps (creation, modification, access)

2. User Accounts & Logins
- Audit login history, user creation/deletion, privileges

3. Event Logs
- Check for security events, system changes, and errors

4. Processes and Services
- Identify running processes, installed programs, or rogue software

5. System Artifacts
- Windows Registry (in Windows)
- Prefetch files, shortcut files (.lnk)
- Recent documents, clipboard data

6. Network Activity
- Firewall logs, DNS cache, browser history

7. Memory Dump Analysis
- Investigate RAM for active sessions, malware, or password hashes

8. Temporary & Cache Files
- Internet cache, session files, cookies

Common Tools Used

Tool	Purpose
Autopsy/The Sleuth Kit	File recovery, timeline analysis
FTK Imager	Disk imaging and preview
Volatility	Memory analysis
Registry Viewer	Windows Registry forensics
Log2Timeline	Timeline creation from log files
Wireshark	Network packet analysis

Key Aspects of OS Investigation

1. **File System Analysis** – Examining file structures, deleted files, metadata, and timestamps.
2. **Registry and Configuration Analysis** (Windows) – Investigating registry hives for evidence of program execution, USB activity, or user actions.
3. **Log Analysis** – Analyzing system logs, event logs, and audit trails to detect anomalies.
4. **Memory Forensics** – Examining RAM dumps for active processes, malware traces, and encryption keys.
5. **Process and Service Analysis** – Identifying suspicious processes, unauthorized services, or malware persistence mechanisms.
6. **User Activity Analysis** – Tracking user authentication, access logs, and account modifications.
7. **Malware and Rootkit Detection** – Identifying hidden or malicious software.
8. **Network Forensics** – Investigating connections, logs, and traffic patterns to detect attacks or exfiltration.

5.1 Windows File Systems, Registry Hives and Event Logs

File systems

- A **file system** is a method used by the operating system (OS) to **store, organize, retrieve, and manage data** on a storage device like a hard disk, SSD, or USB drive.
- Windows OS mainly supports these file systems:
  - FAT
  - NTFS

5.1.1. Windows File Systems

- A file system stores data on a device so data can be retrieved by the system or a user.
  - File systems are largely independent of an operating system(OS) , and different file systems can be supported on different Oss when necessary drivers are installed.
- Windows operating systems **support several file systems**, each with distinct features and functionalities.
  - The primary file systems include FAT (File Allocation Table), NTFS (New Technology File System), and exFAT (Extended File Allocation Table).

Operating system	Native file systems
Windows 98	FAT16, FAT32
Windows 2000	FAT16, FAT32, NTFS
Windows XP	FAT16, FAT32, NTFS
Windows Vista	FAT16, FAT32, NTFS, exFAT (with SP1 and later)
Windows 7	FAT16, FAT32, NTFS, exFAT
Windows 8	FAT16, FAT32, NTFS, exFAT
Windows 10	FAT16, FAT32, NTFS, exFAT
Linux	EXT2, EXT3, EXT4, XFS
Mac OSX	HPFS, exFAT

Operating Systems and their native file systems.

5.1.1. Windows File Systems

- The **Windows file system** is how Windows organizes and stores files on a computer.
- The key parts of Windows File Systems are:
  1. Drives and Partitions
  2. File System Types
  3. Folders and Files
  4. File Paths
  5. File Attributes and Permissions
  6. Windows Registry and System Files
  7. File Management Tools

Key Parts of the Windows File System:

1. **Drives and Partitions**
   - Windows stores files on **drives** (like C:, D:, or E:).
   - These drives may be **partitions** of a single physical hard drive or separate storage devices.
2. **File System Types**

   Windows mainly uses:

   a) **NTFS (New Technology File System)** – Most modern computers use this; it supports security features, large files, and faster performance.

   b) **FAT32 (File Allocation Table 32)** – An older system; works with USB drives and older Windows versions but has a file size limit of 4GB.

   c) **exFAT (Extended FAT)** – Used for large storage devices like external hard drives and USB drives.
3. **Folders and Files**
   - Files are stored in **folders (directories)**, just like putting papers inside a physical folder.
   - Each file has a **name, size, type**, and other properties.

3. File Paths

- A file path tells the exact location of a file, like an address. Example:

```
C:\Users\John\Documents\report.docx
```

2. File Attributes and Permissions

- Windows allows users to **set permissions** (who can read, write, or delete a file).
- Files can have attributes like **read-only, hidden, or system file** to protect them from accidental changes.

3. Windows Registry and System Files

- Important system settings are stored in the **Windows Registry**.
- Windows has critical **system files** (like .dll and .exe files) that help it function properly.

4. File Management Tools

- Windows provides **File Explorer** for browsing and managing files.
- You can also use the **Command Prompt (cmd)** or **PowerShell** for advanced file operations.

Importance of File Systems in Digital forensics:

- In **digital forensics**, the file system is crucial because it helps investigators **recover, analyze, and trace digital evidence** stored on a computer or storage device.
- Understanding file systems allows forensic experts to uncover hidden or deleted data, track user activity, and analyze file modifications.
- Some of the importance of File Systems in Digital Forensics are:
    1. Data Recovery & Evidence Collection
    2. File Metadata Analysis
    3. Tracking User Activity
    4. Uncovering Hidden & Encrypted Files
    5. Detecting File System Artifacts
    6. Identifying Malicious Activity
    7. Analyzing File System Structures in Different OS

1. Data Recovery & Evidence Collection

- File systems manage how data is stored, deleted, and retrieved.
- Even when files are "deleted," they often remain on the disk until overwritten.
- Forensic tools can **recover deleted files** using file system metadata (like MFT in NTFS).

2. File Metadata Analysis

- File systems store metadata such as: **Timestamps** (created, modified, accessed), **File owner and permissions** (who accessed or modified a file), **File attributes** (hidden, read-only, system files).
- These details help investigators build a **timeline of user activities**.

3. Tracking User Activity

- Many file systems **log file access and modifications**, helping forensics experts track suspicious activity.
- **Windows event logs** and the **NTFS Journal** (USN Journal) record file changes.
- Investigators can **identify unauthorized access** or **file tampering**.

4. Uncovering Hidden & Encrypted Files

- Attackers may hide data using **alternate data streams (ADS) in NTFS**.
- Some file systems allow **encryption** (e.g., BitLocker in NTFS).
- Digital forensics tools can **detect and analyze hidden or encrypted files**.

5. Detecting File System Artifacts

- File systems store **artifacts** that can provide clues in investigations, such as:
  1. **Thumbcache and Prefetch files** (Windows) – show recently accessed files.
  2. **Registry hives** – record user and system activities.
  3. **Recycle Bin records** – show deleted file history.

6. Identifying Malicious Activity

- Malware often **modifies system files** or creates hidden files.
- Investigators can check **file system logs** for unusual changes.
- File hashes can be compared to detect **file tampering**

7. Analyzing File System Structures in Different OS

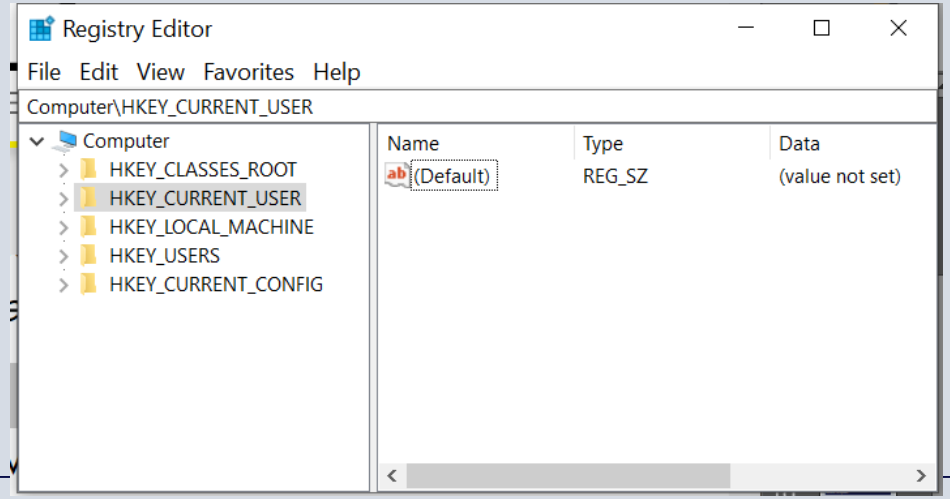
- Different operating systems use different file systems:
  1. **Windows** → NTFS, FAT32, exFAT
  2. **Linux** → Ext4, XFS, Btrfs
  3. **Mac** → APFS, HFS+
- Understanding these file systems helps investigators examine evidence from various devices.

5.1.2 Windows Registry

- The **Windows Registry** is a **centralized database** in Windows that **stores settings and configurations** for the **operating system, hardware, software, and users**.
  - It acts as a **control center** where Windows and applications save important information.
  - It as a **giant settings file** that Windows constantly reads and updates to ensure the system runs smoothly.
- The Windows Registry is organized in a tree structure, much like the directories and files on your computer.
  - The main parts of the Registry are **Registry Hives.**

Registry Hives

- A **registry hive** **is like a folder** that organizes the various keys and values that make up the Windows Registry.
- To use a more common term, a hive is like a starting folder in the registry.
- They contain registry keys, registry subkeys, and registry values.
- All keys that are considered hives **begin with "HKEY“.**
- Each **hive** is a **major section** of the **Windows Registry**, containing key information for the operating system and users.



- In Windows computers, there is something called the **Windows Registry** — it's like a big database that stores important **settings and configurations** for the system, software, and users.
- A **Registry Hive** is like a **main folder** or **big section** inside the Windows Registry.
- Each hive holds **related information** like:
  - User settings
  - System settings
  - Hardware information
  - Security details
- Registry hives are saved as **files on the disk**, usually in: C:\Windows\System32\config\

Structure of Windows Registry:

The Registry is organized into **five main sections (hives)**:

Hive Name	What it Contains
HKEY_LOCAL_MACHINE (HKLM)	Settings for the whole computer (hardware, software, drivers)
HKEY_CURRENT_USER (HKCU)	Settings for the currently logged-in user
HKEY_CLASSES_ROOT (HKCR)	Information about file types and how programs open them
HKEY_USERS (HKU)	Settings for all user accounts on the system
HKEY_CURRENT_CONFIG (HKCC)	Current hardware configuration info

- Investigators look at these **hive files** to find clues like:
  - When a device was plugged in
  - Which software was used
  - User login history
  - Traces of deleted files

Registry Key Vs Registry hives

- A registry hive is a folder in the Windows Registry, but so is a registry key.
- The only difference between the two is that a **registry hive is the first folder** in the registry, and
  it *contains* registry keys, whereas
- the **registry keys are the folders *inside the hives*** that contain registry values and other registry keys.

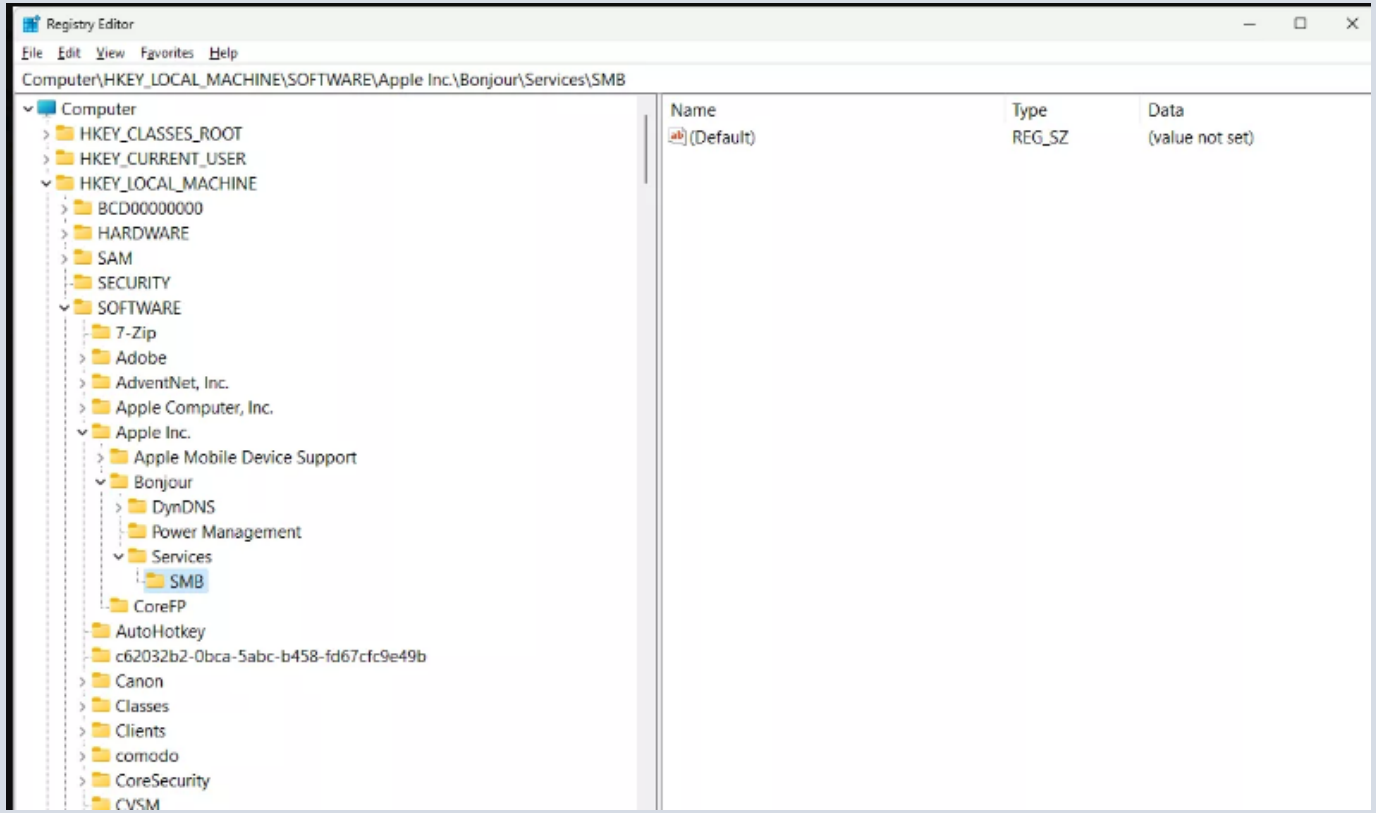


Image courtesy:
https://www.lifewire.com/what-is-a-registry-hive-2625986

Roles of Registry Hives and Registry Keys in Digital Forensic:

- Registry hives are essential for gathering comprehensive information about the state and history of a system, making them a critical component in digital forensics investigations.
- In OS forensics, registry hives are valuable for:
  1. **User Activity Tracking:**
     - Identifying recent user activities, such as accessed files and executed programs.
  2. **System Configuration History:**
     - Understanding system configurations and changes over time.
  3. **Installed Software:**
     - Determining installed applications and their usage patterns.
  4. **Hardware Information:**
     - Investigating connected hardware devices and drivers.
  5. **Network Information:**
     - Details about network settings and recent connections.

Important information provided by Registry hives:

1. **System Configuration and Settings:**
   - Contains information about hardware and software configurations, system settings, and user preferences.
2. **User Profiles:**
   - Stores data related to user profiles, including user-specific settings and preferences.
3. **Installed Software:**
   - Information about installed applications and their configurations.
4. **Hardware Information:**
   - Details about the hardware components and their drivers.
5. **System Boot and Startup:**
   - Configuration settings required for system boot and startup processes.

What does the windows Registry store?

1. **System Settings** – Boot configurations, installed drivers, network settings.
2. **User Preferences** – Desktop background, screen resolution, keyboard/mouse settings.
3. **Software Information** – Installed applications, licensing details, file associations.
4. **Hardware Configurations** – Connected devices like printers, USB drives, graphics cards.
5. **Security & Permissions** – User accounts, login credentials, access controls.

Registry Viewer Tools:

1. **RegRipper:**
   - A powerful open-source tool for extracting and analyzing registry data.
2. **Registry Explorer:**
   - Provides a GUI for browsing offline registry hives.
3. **FTK Imager:**
   - Can be used to mount and view registry files.

- These tools will generate a text file with the extracted registry data, which you can then review.

5.1.3. Event Logs

- **Event Logs** are **records of system, security, and application activities** in Windows.
- The operating system logs these events in a database called the **Windows Event Log**, which helps track user actions, system errors, and security incidents.
- Think of it as a **black box recorder** for Windows—it keeps track of everything happening on the system!
- Windows stores event logs in **.evtx** files at: **C:\Windows\System32\winevt\Logs**
- You can view event logs using the **Event Viewer** (eventvwr.msc), a built-in Windows tool.

Types of Event Logs

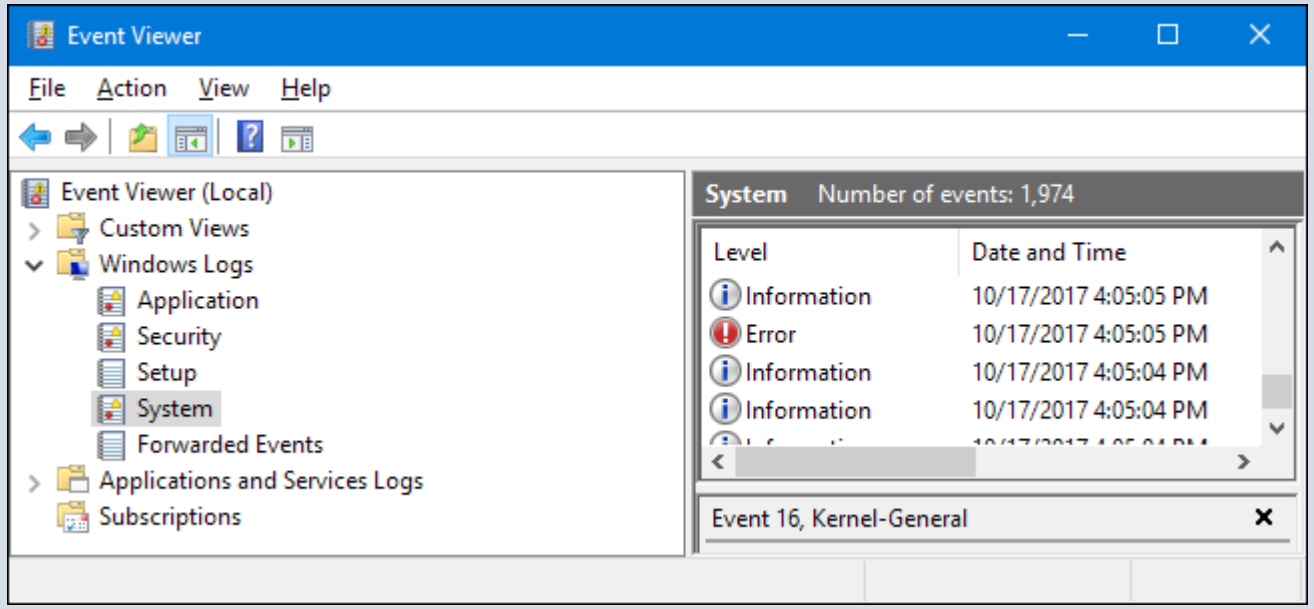
1. **Application Logs**
   - Records events related to **installed programs** (e.g., crashes, updates).
   - Example: "Microsoft Word encountered an unexpected error."
2. **Security Logs** 🔒
   - Tracks **login attempts, failed logins, account lockouts**, and security-related events.
   - Useful for detecting **unauthorized access** or **malware activity**.
   - Example: "User Admin failed to log in 3 times."
3. **System Logs**
   - Logs **hardware and system events** like driver failures, OS updates, and startup issues.
   - Example: "Hard drive error detected."
4. **Setup Logs**
   - Records **installation events**, such as Windows updates and system setups.
   - Example: "Windows update successfully installed."
5. **Forwarded Events**
   - Collects logs from **other computers** on the network for centralized monitoring.
   - Example: Useful in enterprise environments for **network security monitoring**.

Roles of Event logs for Forensics:

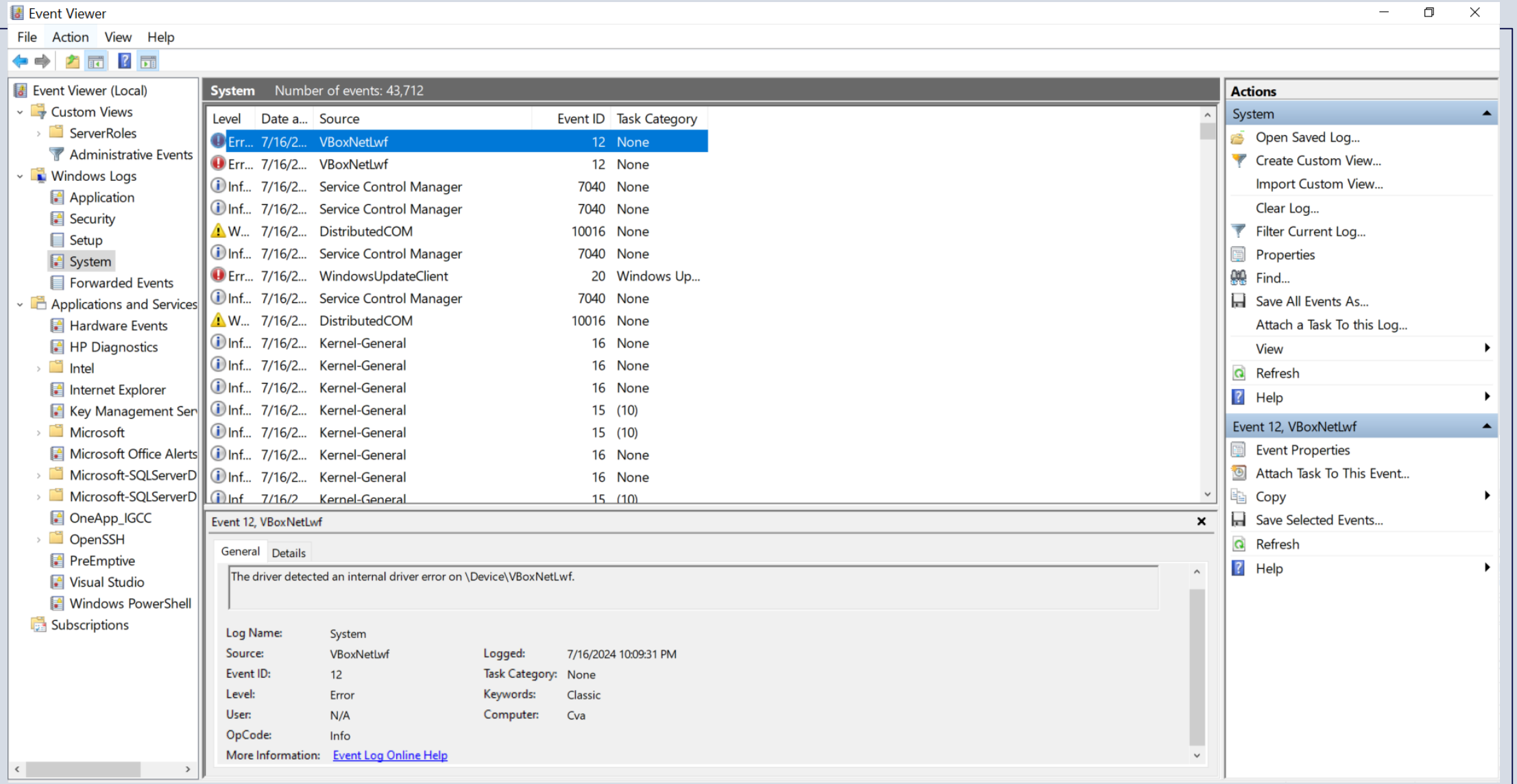
- In OS forensics, event logs provide a wealth of information for reconstructing user activities, system changes, and potential security incidents.
- Forensic analysts use event logs to:
  a) **Identify Unauthorized Access**: Track login attempts, account lockouts, and privilege escalations.
  b) **Monitor System Changes**: Identify software installations, updates, and system modifications.
  c) **Detect Malicious Activity**: Look for signs of malware, such as unusual process activity, network connections, and system errors..
  d) **Audit User Actions**: Examine file access, program executions, and other user activities.

Event viewer:

- The Windows Event Viewer is a built-in tool that shows a log of application and system messages, including errors, information messages, and warnings.
- It's a useful tool for troubleshooting all kinds of different Windows problems.



More Understanding: https://www.youtube.com/watch?v=tuL8wzftbkk



More Understanding: https://www.youtube.com/watch?v=tuL8wzftbkk

Example: Checking Login Activity in Event Viewer

- Open **Event Viewer** (eventvwr.msc).
- Navigate to **Windows Logs → Security**
- Look for **Event ID 4624 (Successful Login)** or **Event ID 4625 (Failed Login Attempt)**.

5.2 Linux File System

5.2 Linux File System basics

- The **Linux File System** is the way Linux organizes and manages data on a storage device (like a hard drive or SSD).
- It controls **how files are stored, accessed, and managed** on the system.
- The Linux file system is organized in a hierarchical structure starting from the root directory '/'
- **Understanding the Linux file system is crucial** for forensic investigations as it helps in recovering deleted files, analyzing metadata, and understanding file storage and thus for forensic analysis.

Key Features of the Linux File System

- **Everything is a File** – In Linux, everything (including text files, images, hardware devices, and even processes) is treated as a file.
- **Hierarchical Structure** – Linux uses a **tree-like structure**, starting from a single root directory (/).
- **Permissions & Ownership** – Every file has an **owner**, a **group**, and specific **read, write, and execute permissions** for security.
- **Multiple File Systems** – Linux supports various file systems like **ext4, XFS, Btrfs, and FAT32**.

Main Directories in Linux:

Directory	Description	Forensic Relevance
/	Root directory (top-level)	Starting point for investigation
/bin	Essential binary executables	May contain system utilities
/sbin	System administration binaries	Stores commands used by root
/etc	Configuration files	Stores system and application settings
/home	User home directories	Contains user data and personal files
/root	Root user's home directory	Stores superuser files
/var	Variable files (logs, cache, etc.)	Important for log analysis
/tmp	Temporary files	May store forensic artifacts
/mnt & /media	Mounted file systems (external drives, USBs)	Can be used for external storage
/proc	Virtual directory for process info	Useful for live forensics
/dev	Device files (disks, partitions, USBs)	Provides access to hardware
/boot	Bootloader and kernel files	Crucial for OS forensic analysis
/usr	User applications and utilities	Stores non-essential software

Forensic Value of the Linux File System:

1. **Log files:**
   - Located in **'/var/log', log files provides a history of system application, and security events**.
   - Important log files include ' syslog', 'auth.log' 'dmesg' and application–specific logs.
2. **Configuration Files:**
   - Founded in **'/etc'.** These files **offer insights into system settings and installed software**.
3. **User Activity:**
   - User-specific data in **'/home'** directories, including **documents and browser history** .
4. **Device Information:**
   - Files in ***'/dev'* provide details about connected hardware**, while */proc* and */sys* contain runtime system information.
5. **System Metadata:**
   - nodes store metadata about files, such as **permissions, ownership, and timestamps**, which are crucial for forensic analysis
6. **Deleted Files:**
   - Even when files are deleted, **remnants might remain in unallocated space**, allowing for potential recovery.

Reference:

https://www.youtube.com/watch?v=HbgzrKJvDRw

5.3 Android File System

5.3 Android File System basics

- The Android file system **is a structured way to store and manage data on devices running the Android operating system**.
- It organizes data in a hierarchical directory structure, similar to other Unix-like operating systems, and includes various partitions and directories that serve different purposes.
- Android devices are divided into several partitions, each serving a specific purpose:
  - /Boot
  - /system
  - /data
  - /cache
  - /sdcard

Major Partitions in Android

Partition	Mount Point	Description	Forensic Relevance
Boot	/boot	Contains kernel and RAM disk	Cannot be modified after booting
System	/system	Stores Android OS files (APKs, frameworks)	Critical for forensic analysis
Data	/data	Stores user data, apps, databases	Most valuable for forensic evidence
Cache	/cache	Stores temporary app data	May hold residual artifacts
Recovery	/recovery	Contains recovery tools	Useful in root analysis
SD Card	/sdcard or /storage/emulated/0	User-accessible storage	Stores images, videos, documents
Vendor	/vendor	Vendor-specific device drivers	Stores proprietary hardware files

Significance in Digital Forensics

- Understanding the Android file system is crucial for digital forensics as it helps investigators locate and analyze data stored on Android devices.
- Key forensic artifacts include:
  - **App Data**: Databases, shared preferences, and files stored by applications.
  - **System Logs**: Logs of system events and errors.
  - **Call Logs and SMS**: Communication records typically stored in databases within the ***/data/data/com.android.providers.telephony/*** directory.
  - **Browser History and Cookies**: Found in the app-specific directories of browsers like Chrome (*/data/data/com.android.chrome/*)

Android Storage Types

Android provides different types of storage to separate system files, app data, and user data.

1. **Internal Storage (/data)**
   - Stores installed **apps, databases, and user data**.
   - Requires **root privileges** to access.
   - Location of sensitive data such as:
     - **App databases** (/data/data/com.appname/databases/)
     - **Shared preferences** (/data/data/com.appname/shared_prefs/)
     - **Cached data** (/data/data/com.appname/cache/)

2. External Storage (/sdcard or /storage/emulated/0)

- Stores user files such as **photos, videos, documents**.
- Shared among apps with permissions.
- Can be analyzed using **forensic tools** like ADB or Autopsy
- .

3. SD Card (/mnt/sdcard)

- Physically removable storage.
- Can be formatted with **FAT32, exFAT, NTFS, EXT4**.
- May contain **deleted files** that can be recovered.

4. Cloud Storage

- Data may be synced to **Google Drive, OneDrive, Dropbox**.
- Requires cloud forensic techniques to extract data.

Important Android File Locations for Forensics

File Type	Location	Forensic Importance
User Contacts	/data/data/com.android.providers.contacts/databases/contacts.db	Stores call logs, contacts
SMS/MMS	/data/data/com.android.providers.telephony/databases/mmssms.db	Contains text messages
Call Logs	/data/data/com.android.providers.contacts/databases/calllog.db	Stores call history
WhatsApp Chats	/data/data/com.whatsapp/databases/msgstore.db.crypt12	Stores encrypted messages
Browser History	/data/data/com.android.chrome/app_chrome/Default/History	Stores browsing history
Wi-Fi Connections	/data/misc/wifi/wpa_supplicant.conf	Stores saved Wi-Fi credentials
Photos & Videos	/sdcard/DCIM/	Stores multimedia files
Application Data	/data/data/com.appname/	Stores app-specific files

Important Android Logs

Log File	Location	Purpose
System Logs	/var/log/syslog	Records general system events
Kernel Logs	/proc/kmsg	Logs kernel messages
Boot Logs	/proc/last_kmsg	Stores last boot sequence
Event Logs	/data/system/events.log	Tracks system events
App Logs	/data/data/com.appname/logs/	Contains app-specific logs

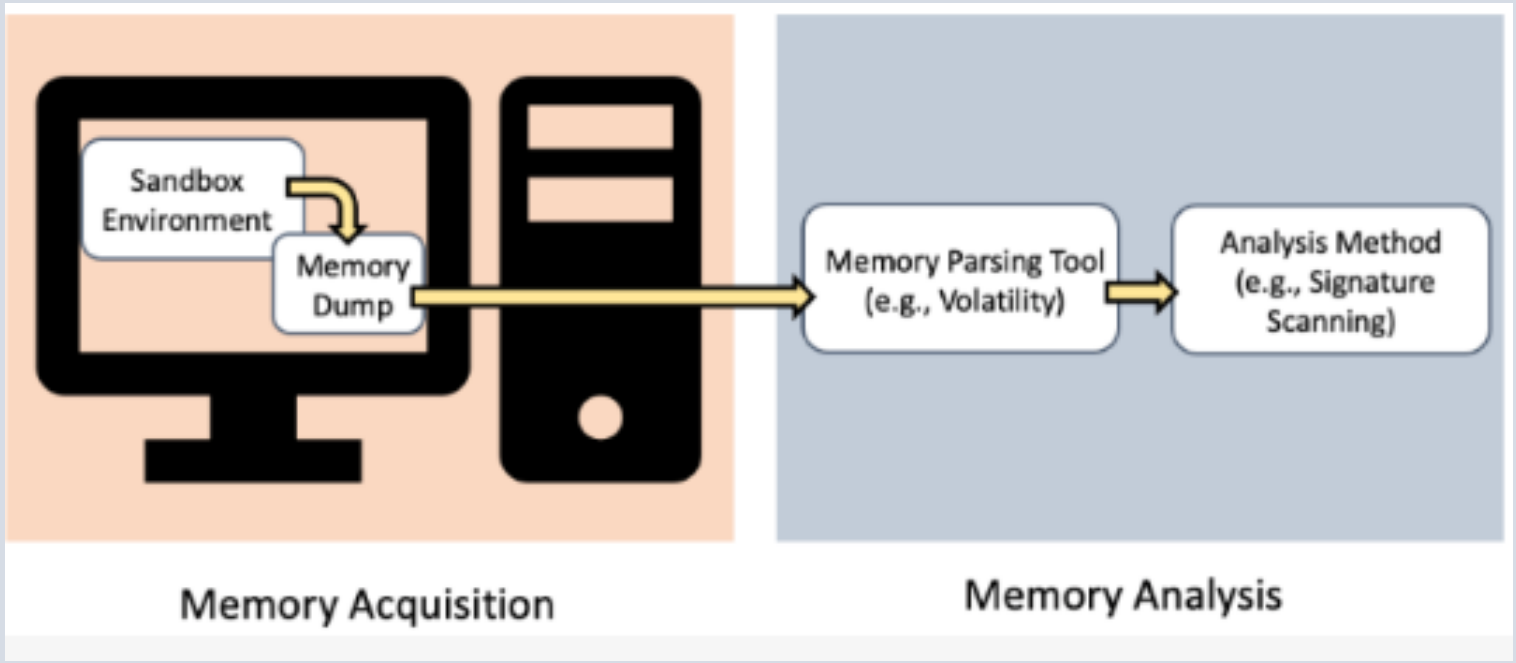
Forensic Tools for Android Analysis

Tool	Purpose
ADB (Android Debug Bridge)	Access file system and logs
Autopsy	Extract and analyze deleted files
Oxygen Forensic Suite	Extract SMS, contacts, call logs
UFED Cellebrite	Full mobile forensic extraction
Magnet AXIOM	Extract cloud data from Google account
Mobisleuth	Android malware analysis

5.4 Memory acquisition and analysis in Windows

4. Memory acquisition and analysis in Windows

- **Memory Acquisition** refers to the process of capturing the contents of a computer's volatile memory (RAM) at a given point in time.
- **Memory Analysis** involves the examination and interpretation of the data extracted during memory acquisition.



a) Memory Acquisition

- is the **process of capturing the contents of a computer's volatile memory (RAM) for analysis.**
- It is a critical process in digital forensics for capturing the volatile data stored in a computer's RAM.
- RAM contains crucial information such as running processes, network connections, open files, encryption keys, and potentially malicious code.
- Since RAM is **volatile** (data disappears when the system is turned off), investigators must collect it while the system is still running.
- Memory acquistion is typically done during digital forensics investigations to gather evidence related to the state of the system, such as running processes, open files, network connections, and other system activities that are stored in memory.
- Memory acquisition is crucial because it allows investigators to recover data that might not be present on the disk, such as unsaved documents, encryption keys, or other live system artifacts.
- Common Tools for Memory Acquisition:
    a) FTK Imager
    b) Belkasoft RAM Capturer
    c) Dumplt
    d) WinPmem

Memory acquisition (RAM capture) process

1. **Choose a Tool**: Select a memory acquisition tool like **FTK Imager**, **DumpIt**, or **Belkasoft RAM Capture**.
2. **Prepare the System**: Ensure the system remains powered on and connect an **external storage device** (e.g., USB drive) to store the memory dump.
3. **Run the Tool**: Execute the memory acquisition tool (e.g., **DumpIt** or **FTK Imager**) to capture the entire RAM. The tool will generate a memory dump file (usually .raw or .dmp).
4. **Verify Integrity**: After capturing, use a **hashing tool** (e.g., MD5, SHA256) to verify that the memory dump has not been altered.
5. **Analyze the Dump**: Use memory analysis tools like **Volatility** or **Rekall** to extract valuable information, such as running processes, network connections, and malware artifacts.

Memory dump

- A **memory dump** is a snapshot of a computer's RAM (Random Access Memory) at a specific moment in time.
- It captures the entire contents of memory, including running programs, system processes, open files, and data structures.

- **Types of Memory Dumps**
  1. **Full Memory Dump** – Captures the entire RAM content.
  2. **Kernel Memory Dump** – Captures only the kernel-mode memory.
  3. **Small Memory Dump (Minidump)** – Captures minimal crash-related information (useful for debugging).
  4. **Automatic Memory Dump** – Similar to kernel memory dump but optimized by the system.
  5. **Live Memory Dump** – Taken while the system is running, used in forensics and debugging.

- **Uses of Memory Dumps**
  1. **Debugging and Crash Analysis** – Helps developers analyze system crashes (BSOD in Windows).
  2. **Digital Forensics** – Used in cybersecurity to analyze malware, passwords, or unauthorized activities.
  3. **Reverse Engineering** – Extracts information from running applications.

b) Memory analysis

- Memory analysis involves **parsing and examining the contents** of a memory dump to uncover forensic artifacts and evidence.
- Provides insights into the system's state at the time of acquisition, which can include evidence of malware, user activity, and system configuration.
- Common tools for Memory analysis are:
  a) Volatility Framework
  b) Rekall
  c) Redline
  d) Memdump

End of Chapter