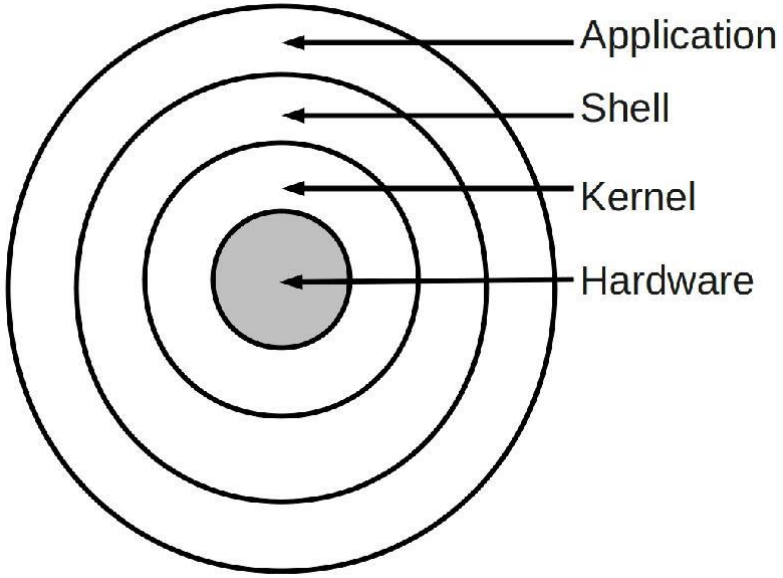
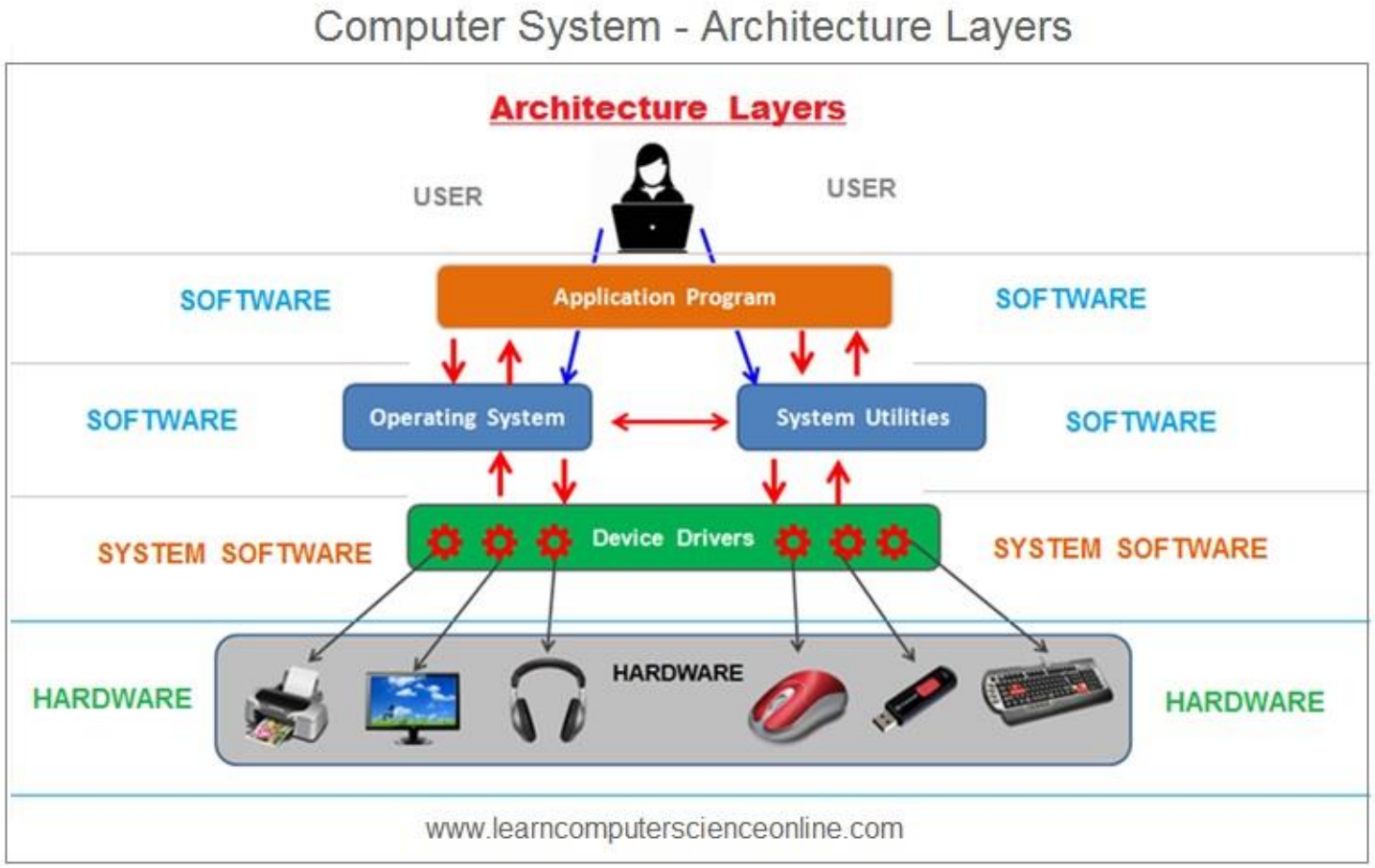
Unit 5

Forensic Analysis

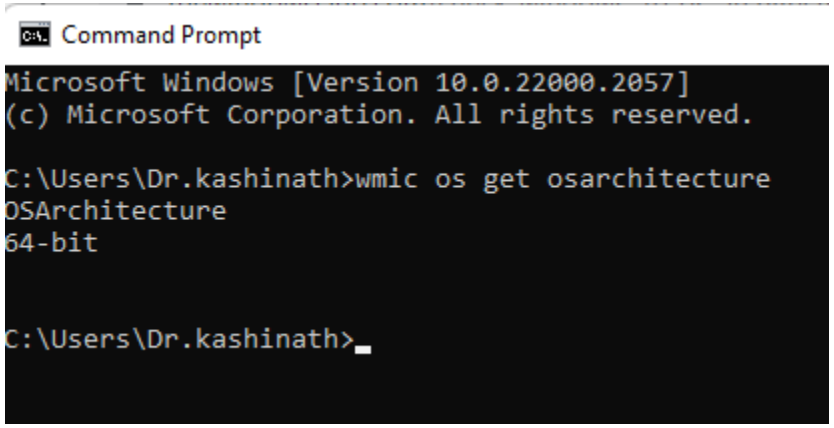
General architecture of Operating system

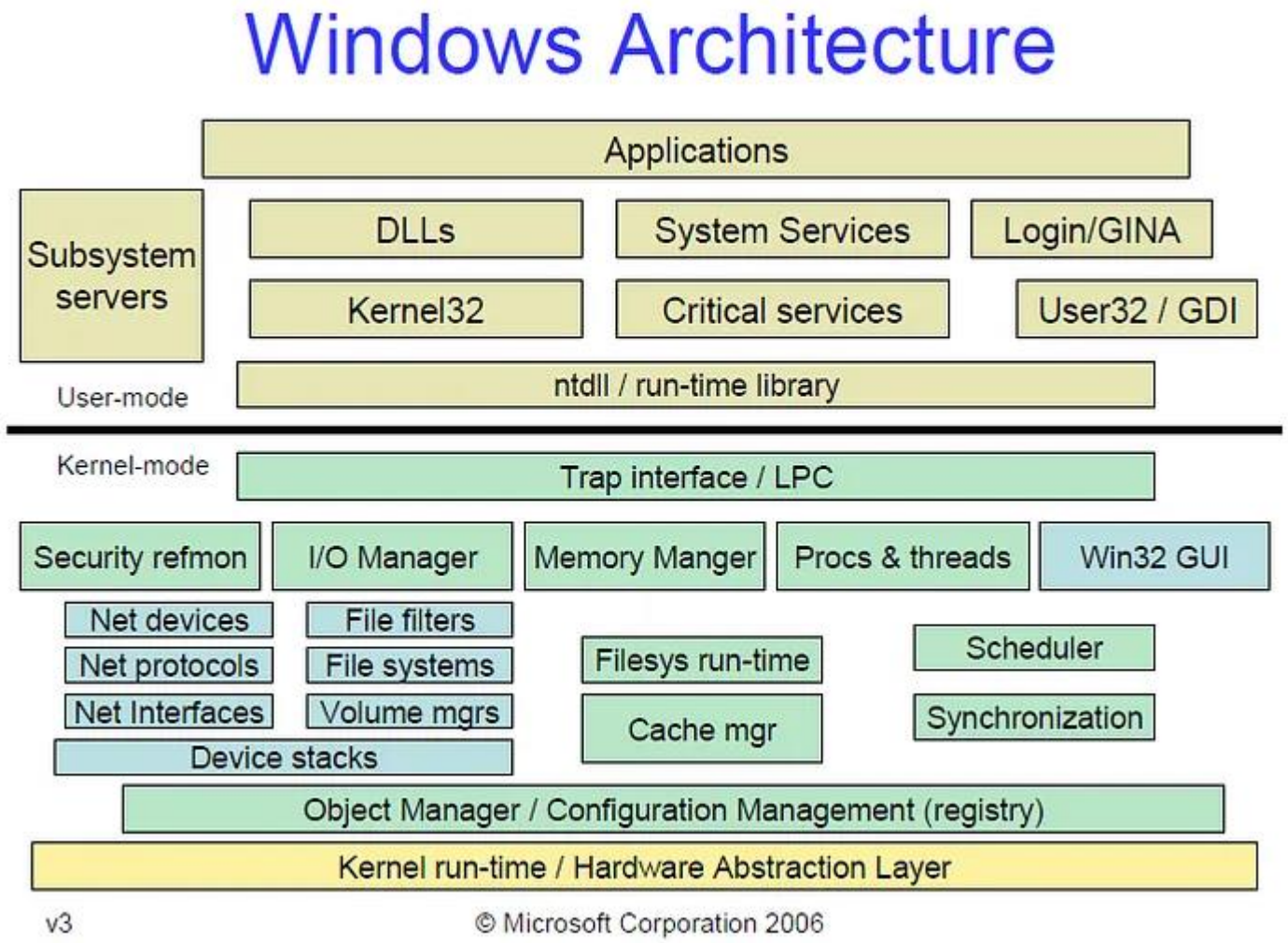




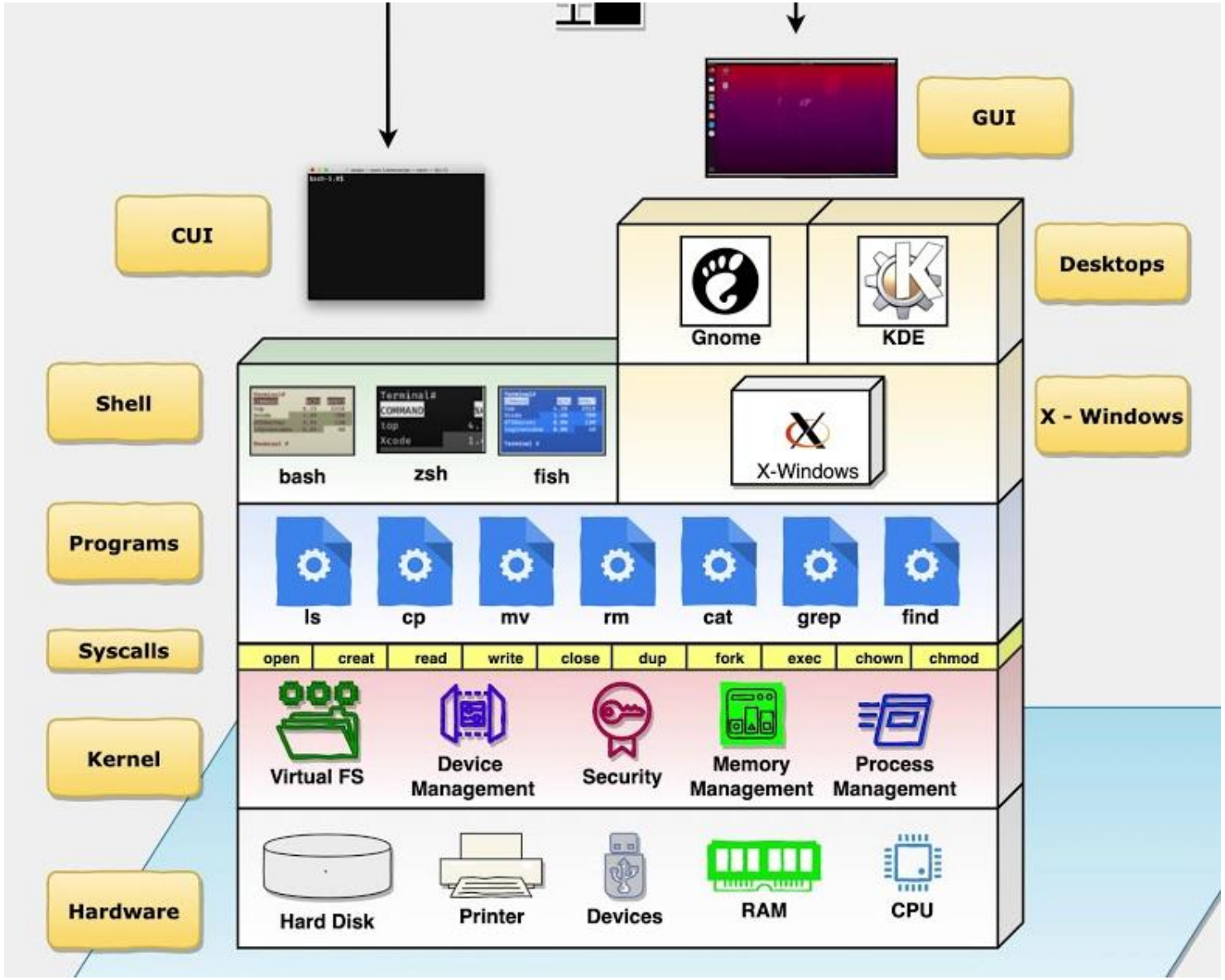
Refer: Experiment -13

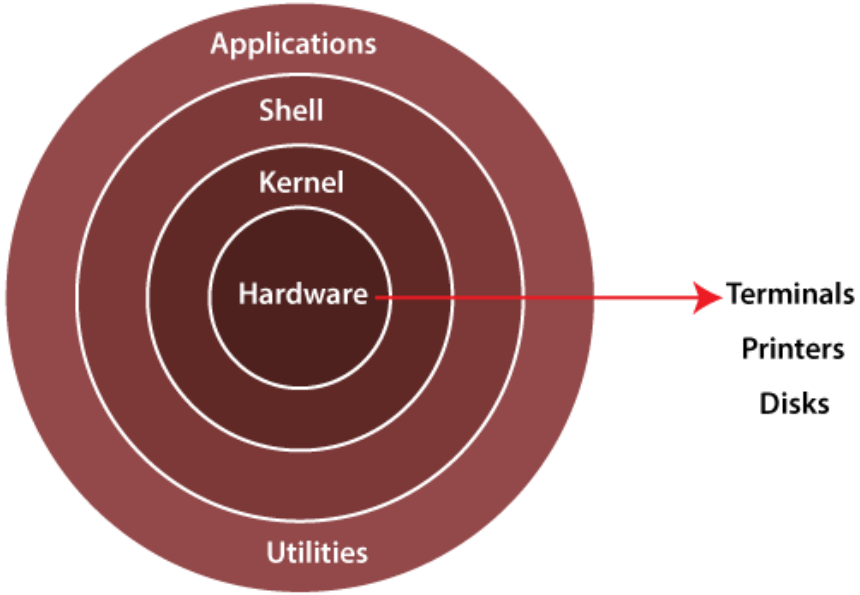
Windows OS Architecture





Linux OS Architecture





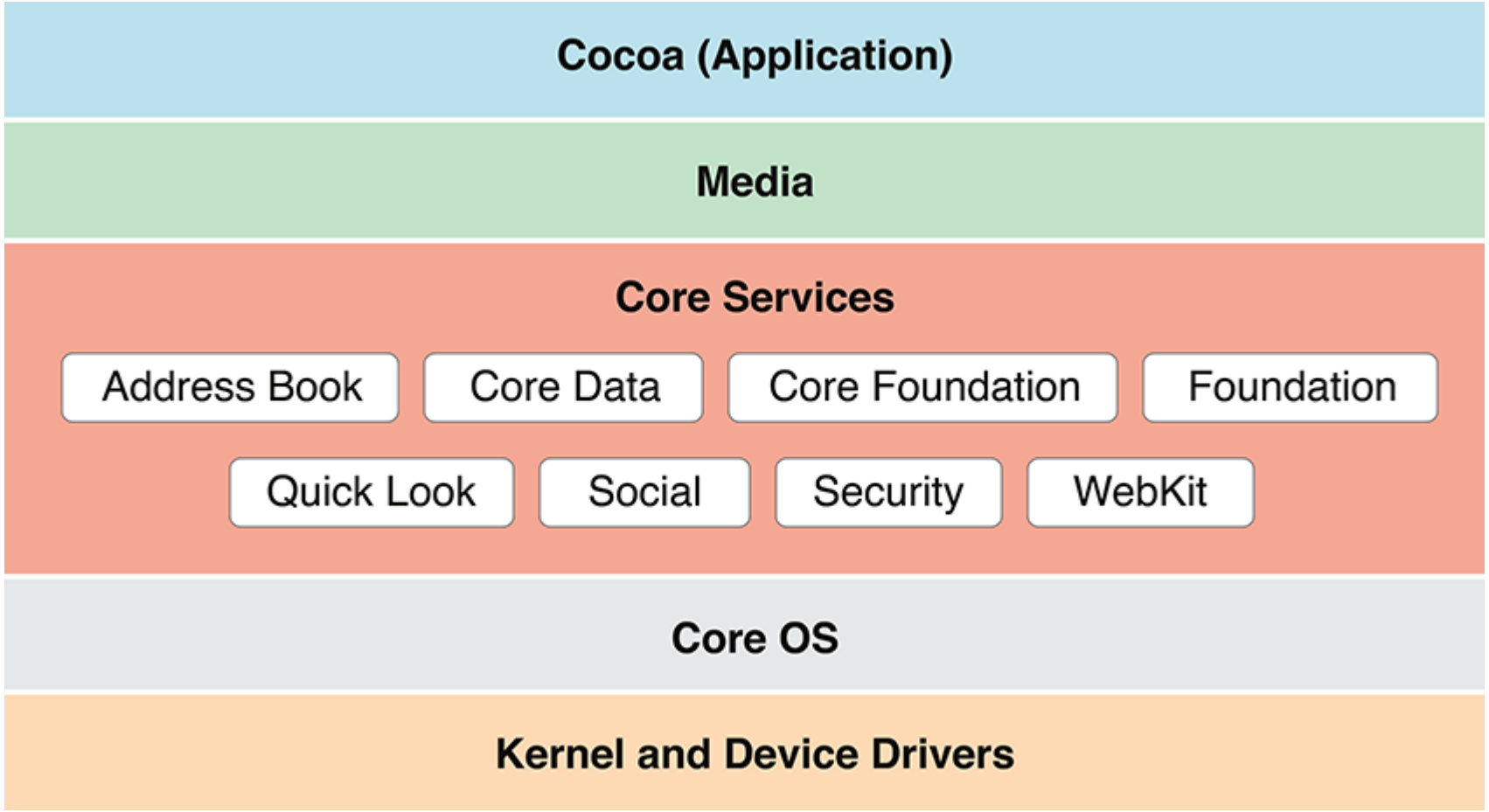
The following is a high-level overview of the main layers of the Linux architecture:

- **Hardware layer:** This is the bottommost layer of the Linux architecture and represents the physical hardware components of the computer, such as the processor, memory, and storage. The hardware layer is responsible for interacting with the various hardware devices and providing access to them for the rest of the operating system.
- **Kernel layer:** The kernel is the core of the operating system and is responsible for managing the resources of the computer, such as the CPU, memory, and I/O devices. It also provides services to the other components of the operating system and acts as the intermediary between the hardware and the software layers.
- **System libraries layer:** This layer consists of a set of libraries that provide functions for the applications to use. These libraries include system calls, which are used to invoke kernel functions, as well as other functions that perform tasks such as file manipulation, networking, and memory management.

- **System utilities layer:** This layer consists of a set of programs that perform various system-level tasks, such as managing processes, controlling user accounts, and configuring system settings. These utilities are usually command-line programs that are invoked by the user or by other programs.
- **Desktop environment layer:** This layer is optional and is not present on all Linux systems. It provides a graphical user interface (GUI) that allows users to interact with the operating system using a mouse and keyboard. The most common desktop environments in Linux are Gnome, KDE, and Xfce.
- **Applications layer:** This is the topmost layer of the Linux architecture and consists of the various applications that run on the operating system. These can be anything from productivity software and games to web browsers and media players.

In summary, the Linux architecture is made up of a number of different layers that work together to provide a stable and flexible operating system. Each layer has a specific purpose and interacts with the other layers to provide the functionality that users expect from an operating system.

Macintosh or Mac OS Architecture



macOS Ventura-2023

macOS 14 Sonoma

https://www.apple.com/macos/ventura/

File system analysis

Feature	NTFS	FAT32
Maximum file size	16 TB	4 GB
Maximum volume size	256 TB	2 TB
File compression	Yes	No
File encryption	Yes	No
File permissions	Yes	No
Journaling	Yes	No
Compatibility with other operating systems	Poor [1] [2]	Good [1] [2]

Refer: Experiment -7, 15

Recreating FAT and NTFS partitions

- Press Windows + R button and type Diskpart in the box.
- Type “list disk,” “select disk 1,” “attributes disk clear readonly,” and “clean” to select and clear all data off the disk.
- Then type format fs=**fat**32 to complete the process.
- Alternatively, you can use EaseUS Partition Master to create a FAT32 partition in Windows 10. Here are the steps:
- Launch EaseUS Partition Master and shrink any partition to find unallocated space.
- Right-click on unallocated space and select Create.
- Choose the FAT32 File Format, set Partition Size, and click OK to finish the process.

- Download **NTFS** recovery software AOMEI Partition Assistant and run it.
- Click Recover on the top pane, and then select Partition Recovery from the menu.
- Select the disk containing deleted NTFS partition and click Next.
- Select Fast Search. This is the recommended choice. It takes less time.
- Select the deleted partition to recover and click Proceed.1
- Alternatively, you can try using TestDisk which is excellent at rebuilding NTFS partitions. It’s available on the Knoppix Linux distribution, so you can boot using the Knoppix Live CD and recover from there.

Refer: Experiment-2

Analyzing Unallocated Partitions

Refer : Experiment -9,11

Analyzing unallocated partitions can be done by using the Disk Management tool in Windows. Here are the steps:

- Press Windows key + X and select Disk Management.
- Right-click on the unallocated partition and select New Simple Volume.
- Follow the wizard to create a new partition.
- If you want to recover an unallocated partition, you can use the DiskPart command-line tool. Here are the steps:
- Search for “CMD” in the start bar and right-click to “Run as Administrator”.
- After entering “diskpart”, type the following commands in sequence:
  - list volume and press Enter.
  - select volume X (where X is the number of the unallocated partition) and press Enter.
  - extend filesystem and press Enter.
- After saving and exiting, check whether the unallocated partition is recovered.

Understanding Windows Registry

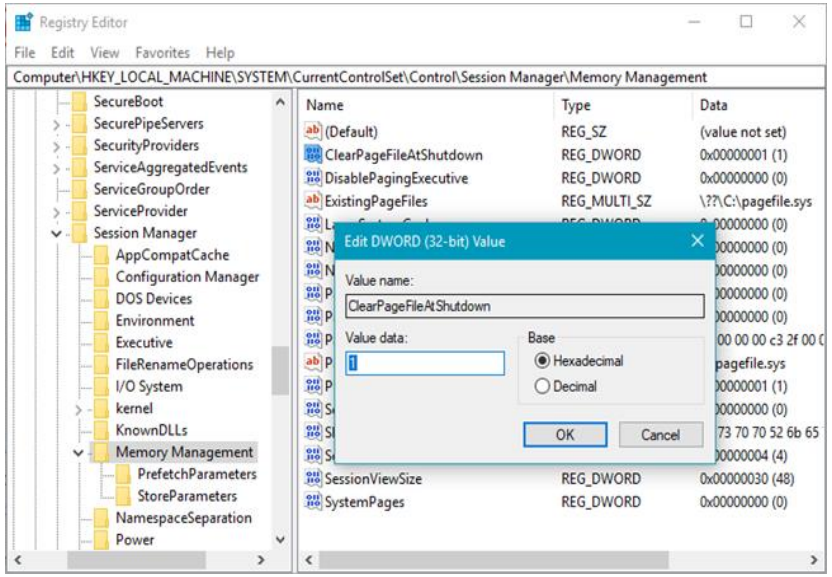
- The Windows Registry is a hierarchical database that **stores low-level settings** for the **Microsoft Windows** operating system and **for applications** that opt to use the registry.
- It contains information, settings, options, and other values for programs and hardware installed on all versions of Microsoft Windows operating systems.
- You can **open the Registry Editor** in Windows 10 by typing "**regedit**" in the search box on the taskbar and selecting the top result for Registry Editor (Desktop app) or by pressing and holding or right-clicking the Start button, then selecting Run. Enter "regedit" in the Open: box and select OK

Refer: Experiment-2

Registry Analysis: Understanding Windows Registry

Analyzing the Windows Registry can be done by using the Registry Editor tool in Windows. Here are the steps:

- Press Windows key + R and type “regedit” in the Run dialog box.
- Navigate to the registry key you want to analyze.
- Right-click on the key and select Export.
- Save the exported file to your preferred location.
- Open the exported file with a text editor or a registry analysis tool.



There are many registry analysis tools available online that can help you analyze the Windows Registry. Some of them are free, while others are paid. Here are some popular ones:

- RegScanner
- RegShot
- RegFromApp
- Process Monitor

What are important artefacts related to user activities?

In the context of user activities, artifacts are the digital footprints that users leave behind while interacting with a system. These artifacts can be used to reconstruct user activities and provide insights into user behavior.

Some examples of important artifacts related to user activities are:

- Log files
- Browser history
- Cache files
- Cookies
- Registry keys

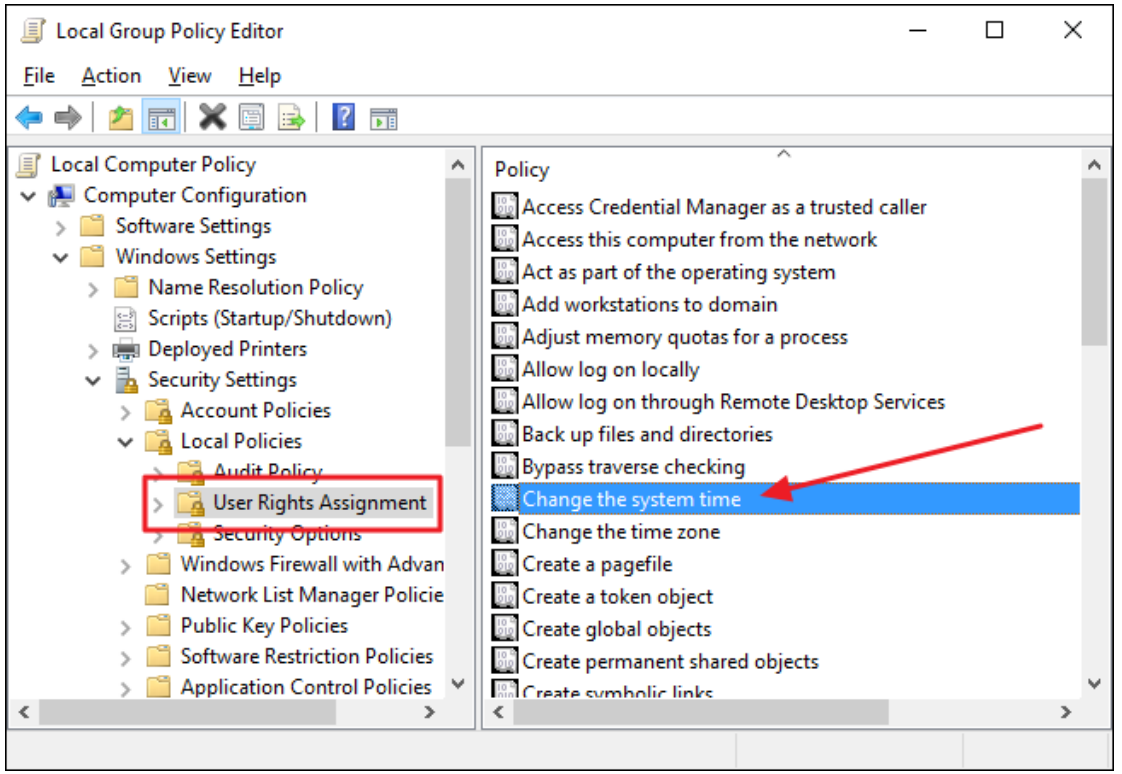
Refer: Experiment -9,10

Analyzing these artifacts can help you understand how users interact with your system and identify areas for improvement

User/Application Configurations and Preferences

- User/Application configurations and preferences are settings that users can customize to suit their needs and preferences. These settings can include things like font size, colour scheme, language preference, and more.

- Application configurations and preferences are usually stored in configuration files or in the Windows Registry.



Refer: Experiment -12,13

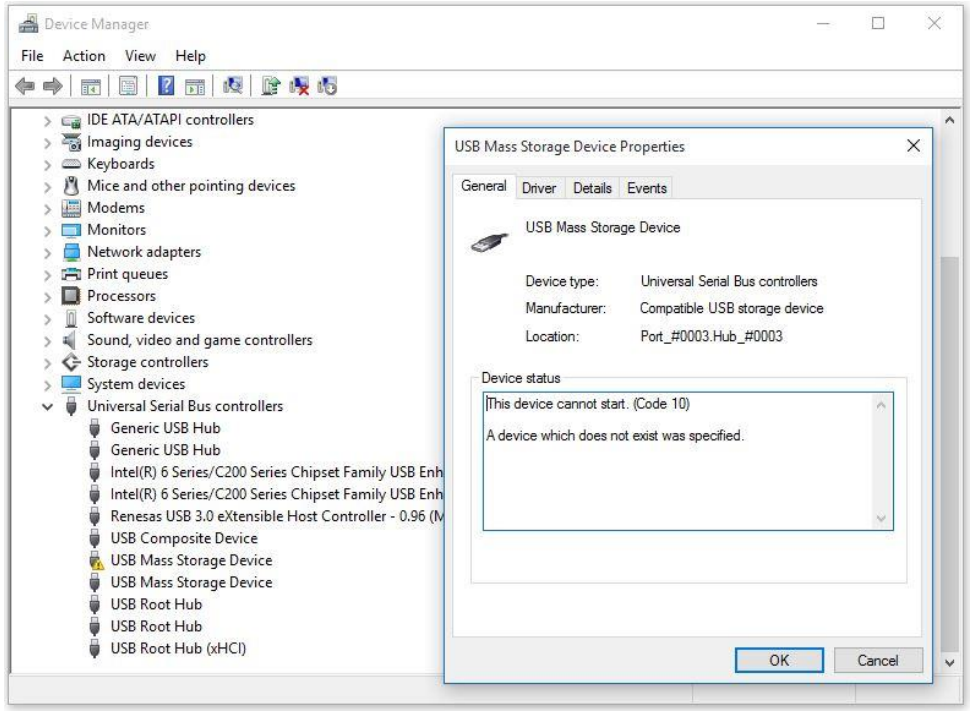
Attached Devices

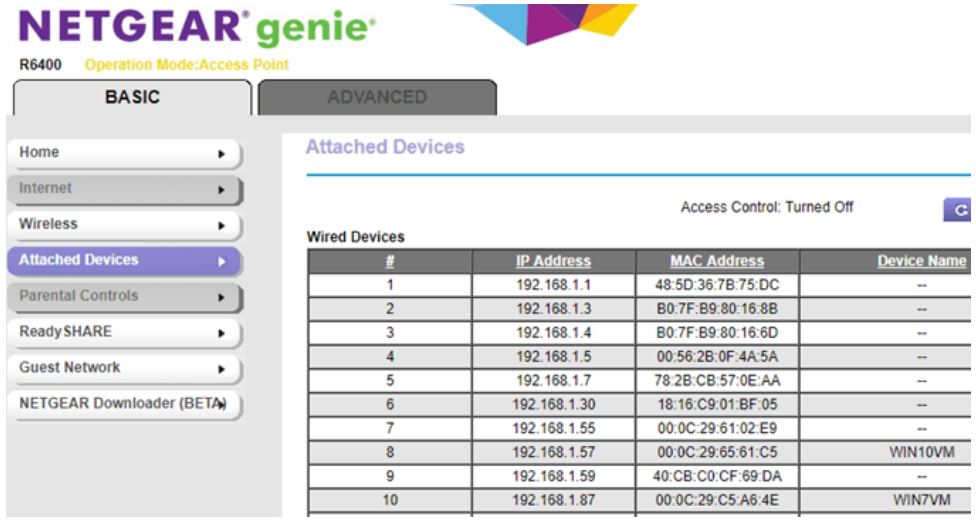
Attached devices refer to any hardware devices that are connected to your computer or mobile device. Some examples of attached devices include:

- USB drives
- External hard drives
- Printers
- Scanners
- Cameras

You can view a list of attached devices by opening the Device Manager in Windows. Here are the steps:

- Press Windows key + X and select Device Manager.
- Expand the category for the type of device you want to view.
- The list of attached devices will be displayed.





Refer: Experiment -14,15

Shared Locations

Shared locations refer to any **folders or drives** that are shared on a network. When a folder or drive is shared, other users on the network can access the contents of that folder or drive.

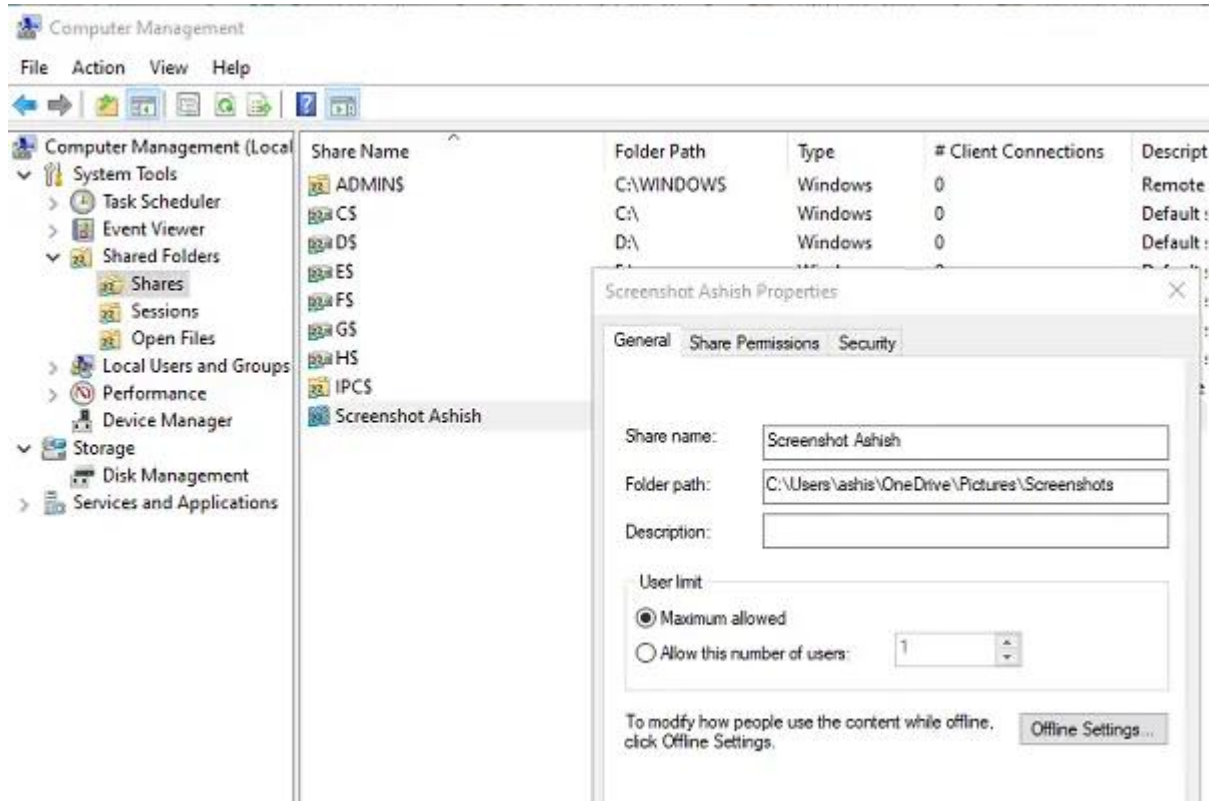
You can view a list of shared locations by opening File Explorer and selecting Network. Here are the steps:

- Open File Explorer.
- Select Network from the left-hand menu.
- A list of shared locations will be displayed.

Refer: Experiment-11

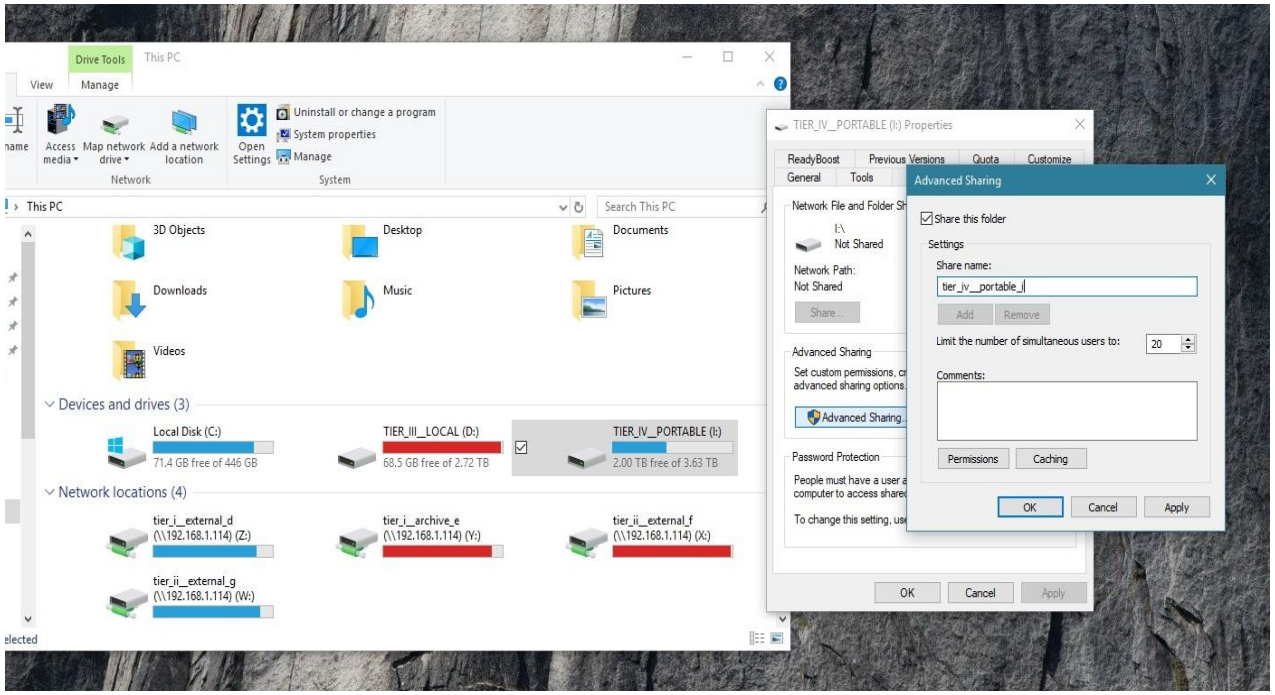
Here are the steps to share a folder on a Windows computer:

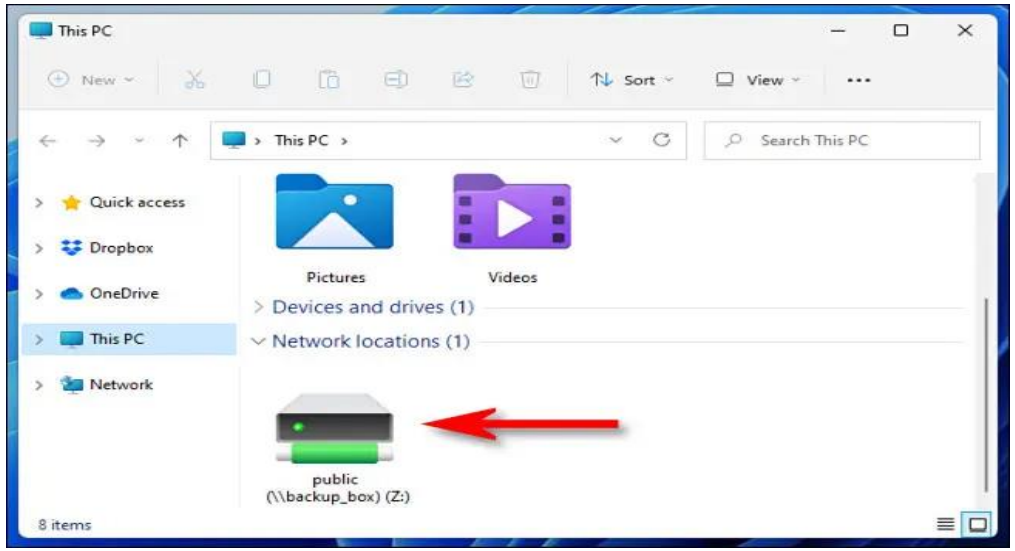
1. Right-click on the folder you want to share and select Properties.
2. Click on the Sharing tab.
3. Click the Share button.
4. Select the users or groups you want to share the folder with.
5. Click the Add button.
6. Set the permission level for each user or group.
7. Click the Share button.
8. That’s it! The folder should now be shared with the selected users or groups.



Here are the steps to share a drive on a Windows computer:

1. Open File Explorer.
2. Right-click on the drive you want to share and select Properties.
3. Click on the Sharing tab.
4. Click the Advanced Sharing button.
5. Check the box next to “Share this folder”.
6. Enter a share name for the drive.
7. Click the Permissions button.
8. Select the users or groups you want to share the drive with.
9. Set the permission level for each user or group.
10. Click OK.





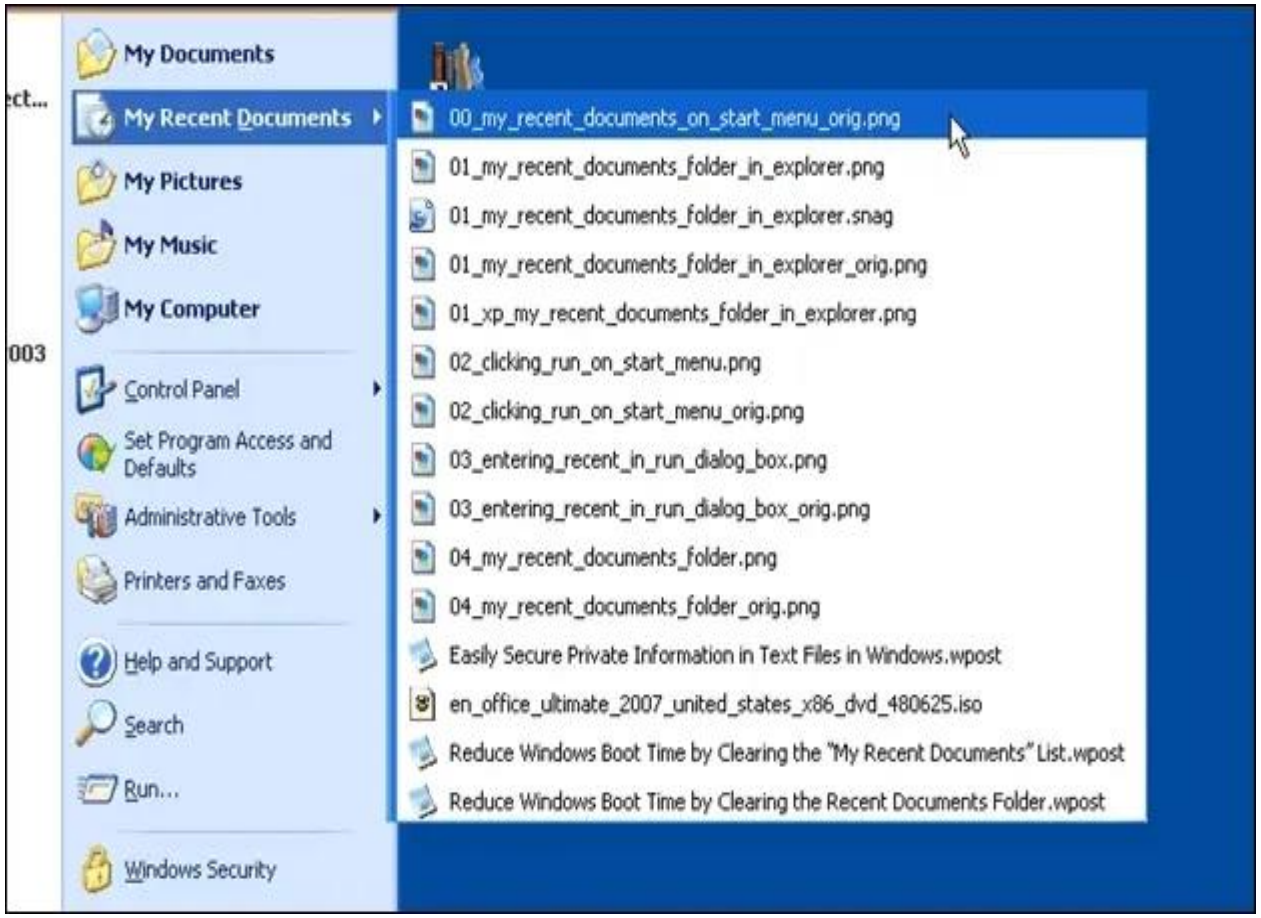
Recently Accessed Documents, Programs and Locations

Recently accessed documents, programs, and locations refer to files, applications, and folders that you have recently opened or accessed on your computer.

You can view a list of recently accessed documents and programs by opening the Start menu and selecting Recent Items. Here are the steps:

Click the Start button.
Select Recent Items.
You can view a list of recently accessed locations by opening File Explorer and selecting Quick Access. Here are the steps:

Open File Explorer.
Select Quick Access from the left-hand menu.



Refer: Experiment-9

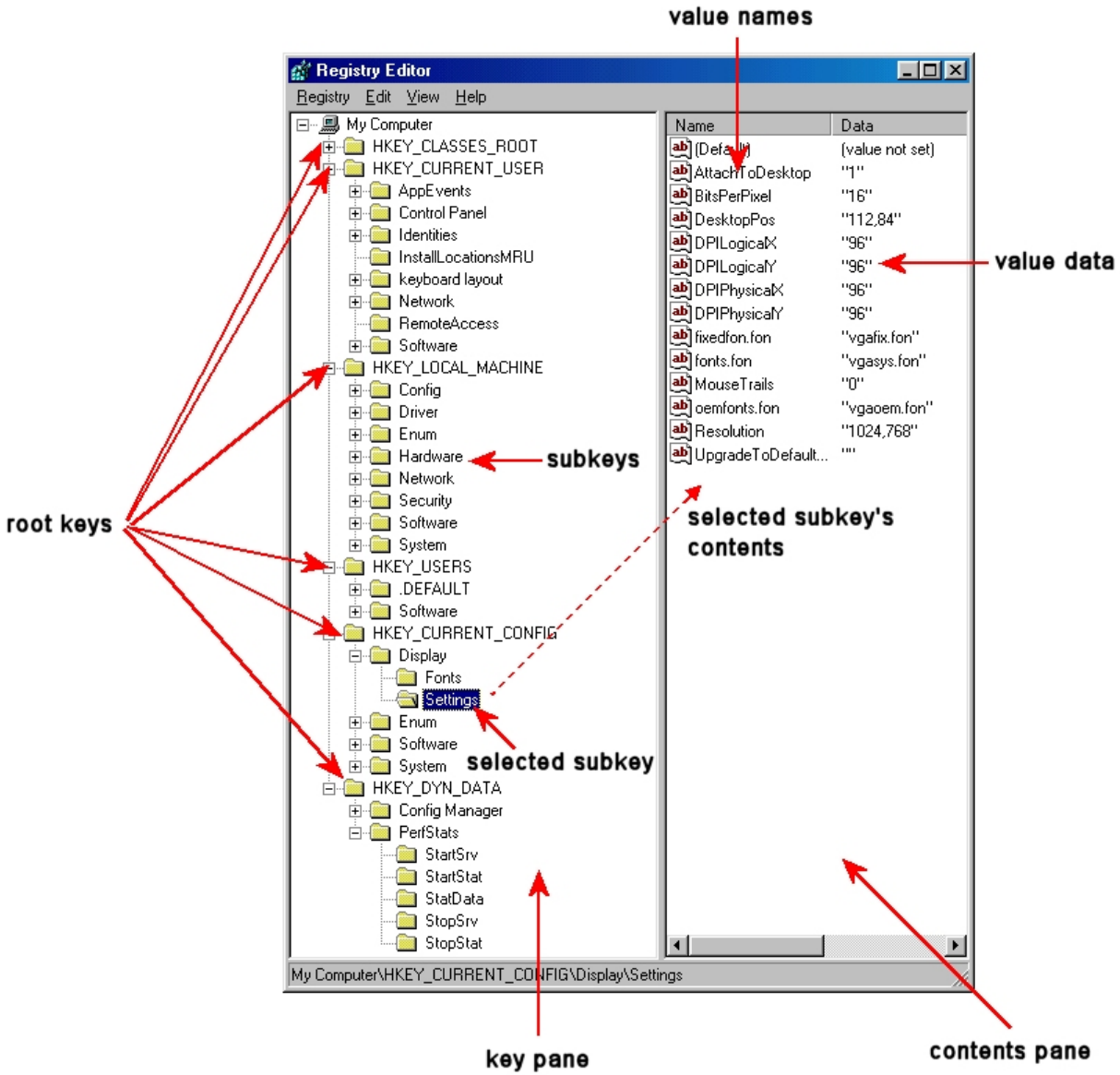
Installed Applications and Others from Windows Registry

Installed applications and other information can be found in the Windows Registry. The Windows Registry is a database that stores configuration settings and options for Windows and many applications.

Here are the steps to view installed applications in the Windows Registry:

- Press Windows key + R to open the Run dialog box.
- Type “regedit” (without quotes) and press Enter.
- Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall.
- A list of installed applications will be displayed.

Refer: Experiment-2,3

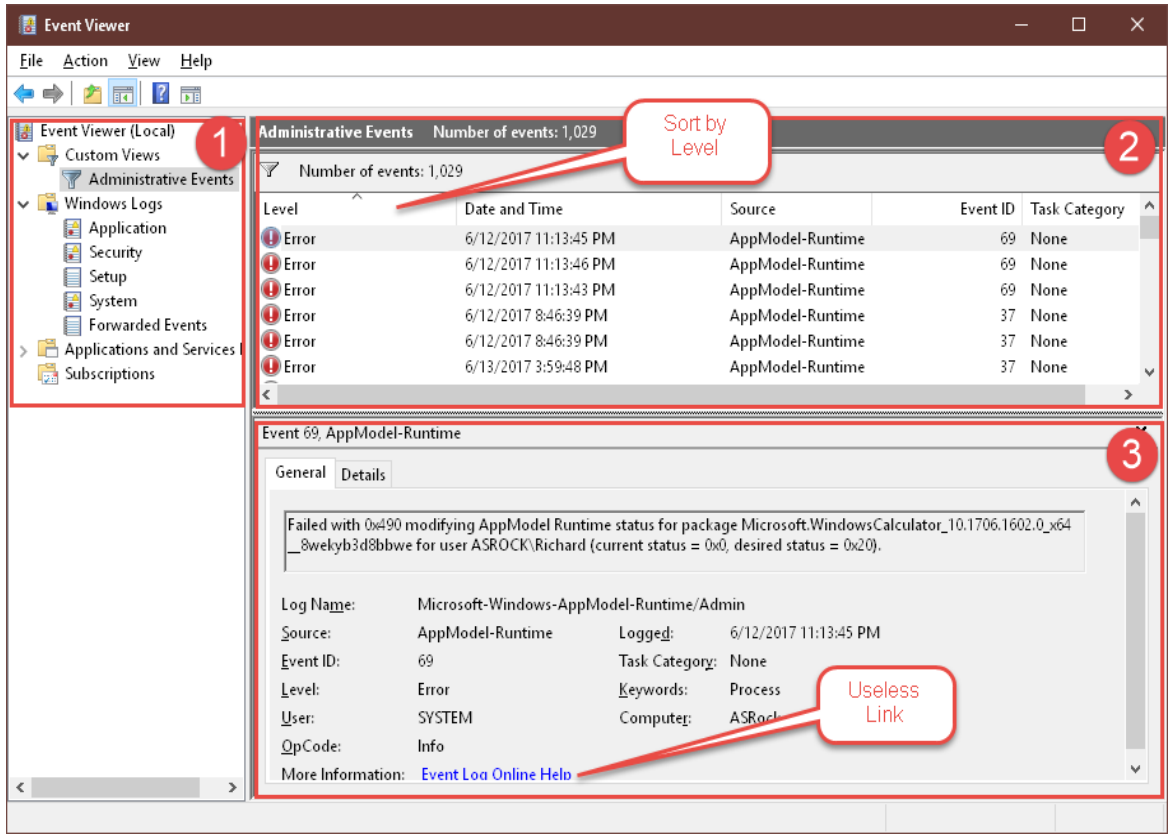


Event and Log Analysis: Introduction to Windows Events

Windows events are records of system activity that are stored in the Windows Event Log. The Event Log is a database that contains information about hardware and software events that occur on your computer.

Here are the steps to view Windows events:

- Press Windows key + X and select Event Viewer.
- Expand the category for the type of event you want to view.
- The list of events will be displayed.

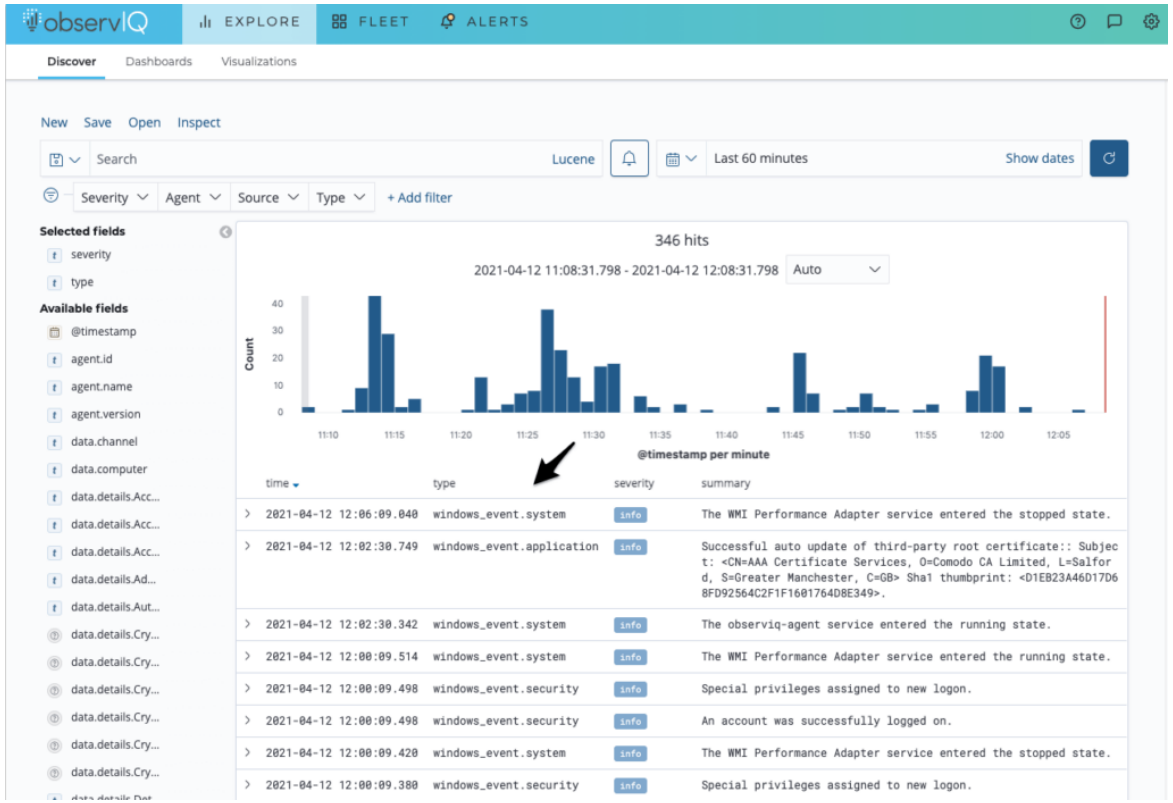


Refer: Experiment-2

Understanding Windows Events (Evt and Evtx Files)

- Windows events are stored in files with the extension “.evt” or “.evtx”. These files can be viewed using the Event Viewer.
- The “.evt” file format is used in older versions of Windows, while the “.evtx” file format is used in newer versions of Windows.

Refer: experiment -4

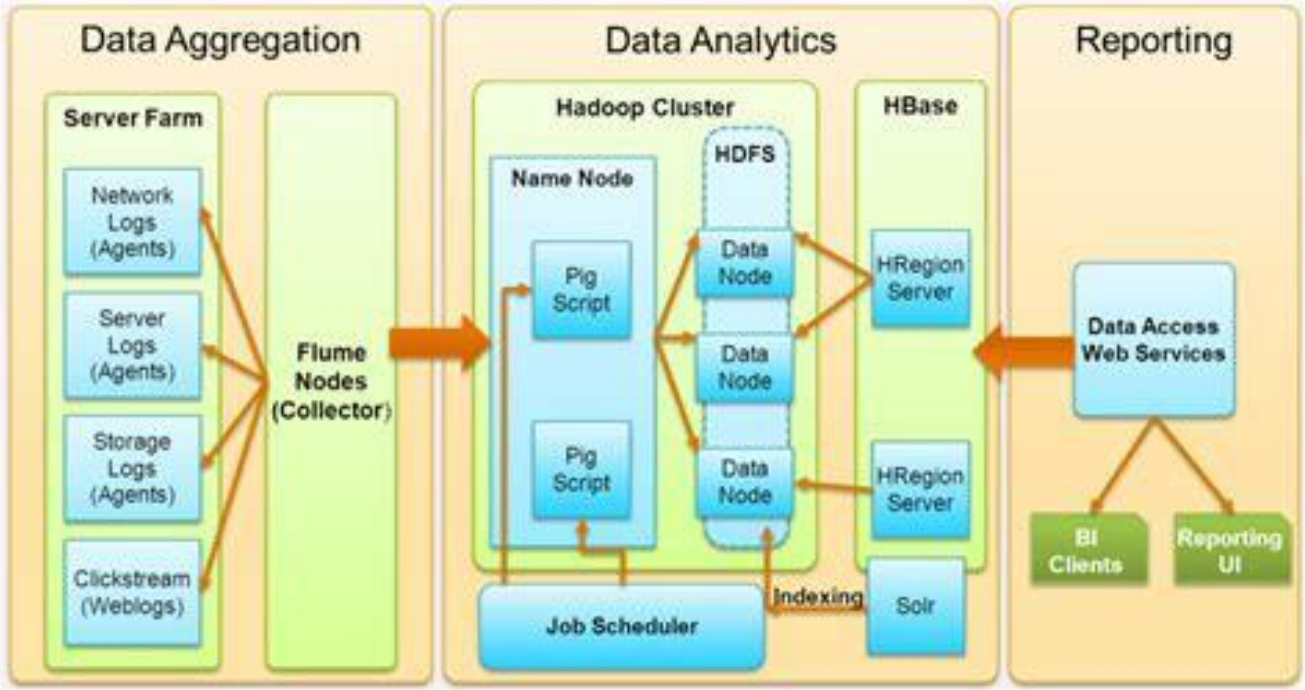


Ref -https://observiq.com/

Analyzing Logs of Third-Party Applications

Analyzing logs of third-party applications can be a complex process that varies depending on the application. However, here are some general steps you can follow:

- Locate the log files for the application. These files are usually stored in a specific folder or directory.
- Open the log files using a text editor or log viewer.
- Look for error messages or other information that may indicate a problem with the application.
- Use the information in the log files to troubleshoot issues with the application.



Ref: Experiment -1,6

What is Log Analytics?

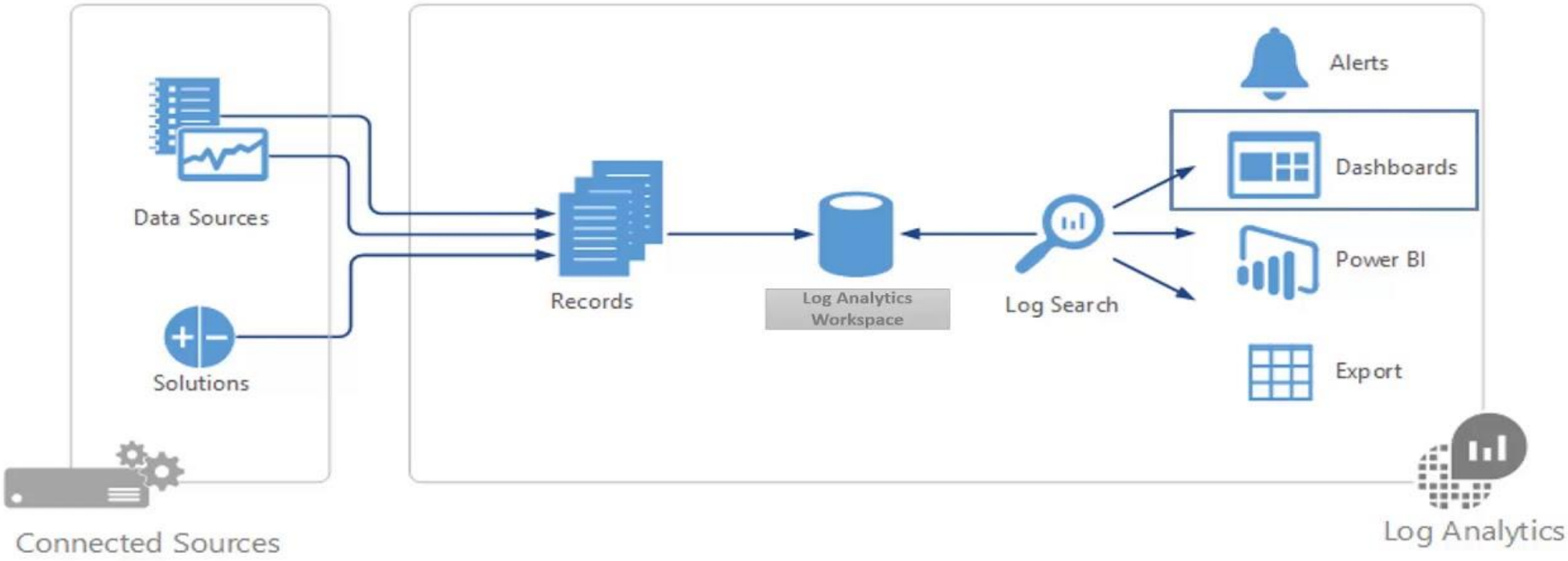


Image credit: Microsoft

Log analysis at Microsoft Azure