Ex.No.9 Use Process Explorer to identify suspicious processes

AIM:

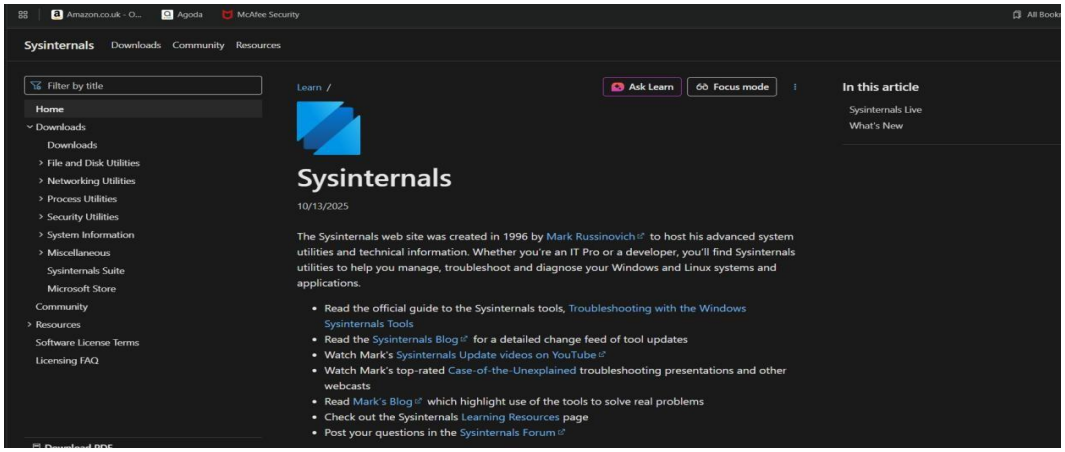
To identify and remove suspicious process from the system using Linux command -line tools.

PROCEDURE:

Process Explorer is a powerful Windows tool that provides detailed information about running processes, allowing users to monitor, troubleshoot, and detect suspicious activities. It can be used to detect potential malware or harmful processes by analyzing various aspects of running applications.

Step 1: Download and Set Up Process Explorer

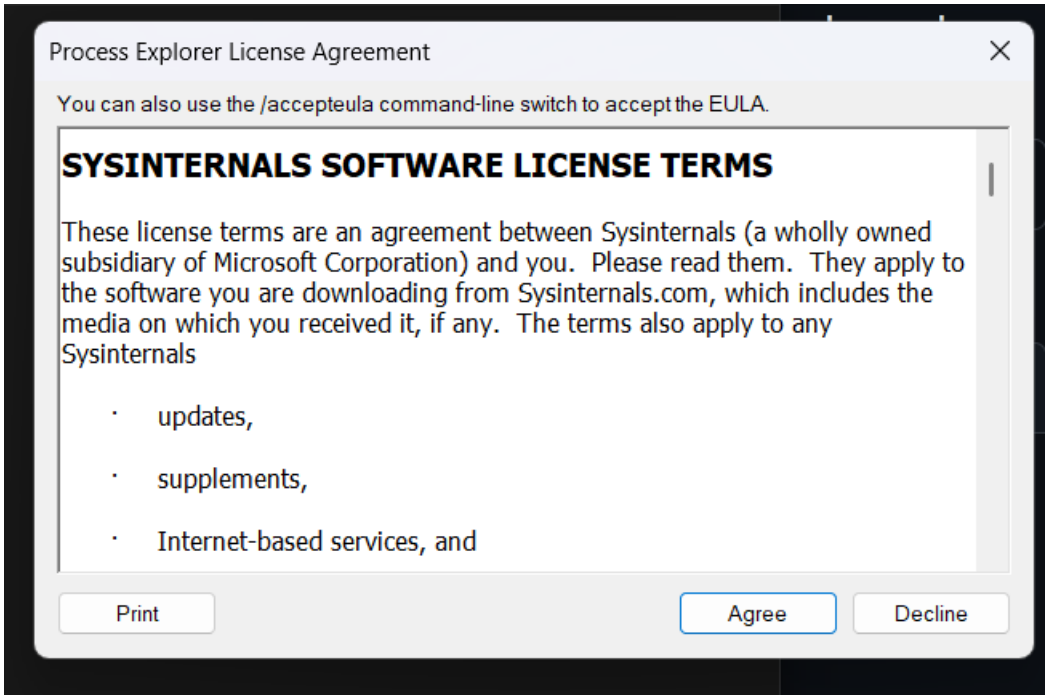
1. **Download Process Explorer:**
   Visit the official Microsoft Sysinternals website and download **Process Explorer**.
2. **Extract Files:**
   Unzip the downloaded file into a specific folder on your system.
3. **Run as Administrator:**
   Right-click on procexp64.exe (for 64-bit) or procexp.exe (for 32-bit) → **Run as Administrator** to launch the tool.



Step 2: Understanding the Interface

When launched, Process Explorer shows a **tree view** of running processes. Each process is color-coded based on its type or activity status:These visual indicators make it easier to monitor

andanalyze system behavior in real time.



Step 3: Identifying Suspicious Processes

Follow these steps to investigate any suspicious or unknown processes:

1. **Check Unknown Names:**
   Look for process names you don't recognize. Legitimate processes usually belong to trusted vendors like *Microsoft*, *Intel*, or *Adobe*.

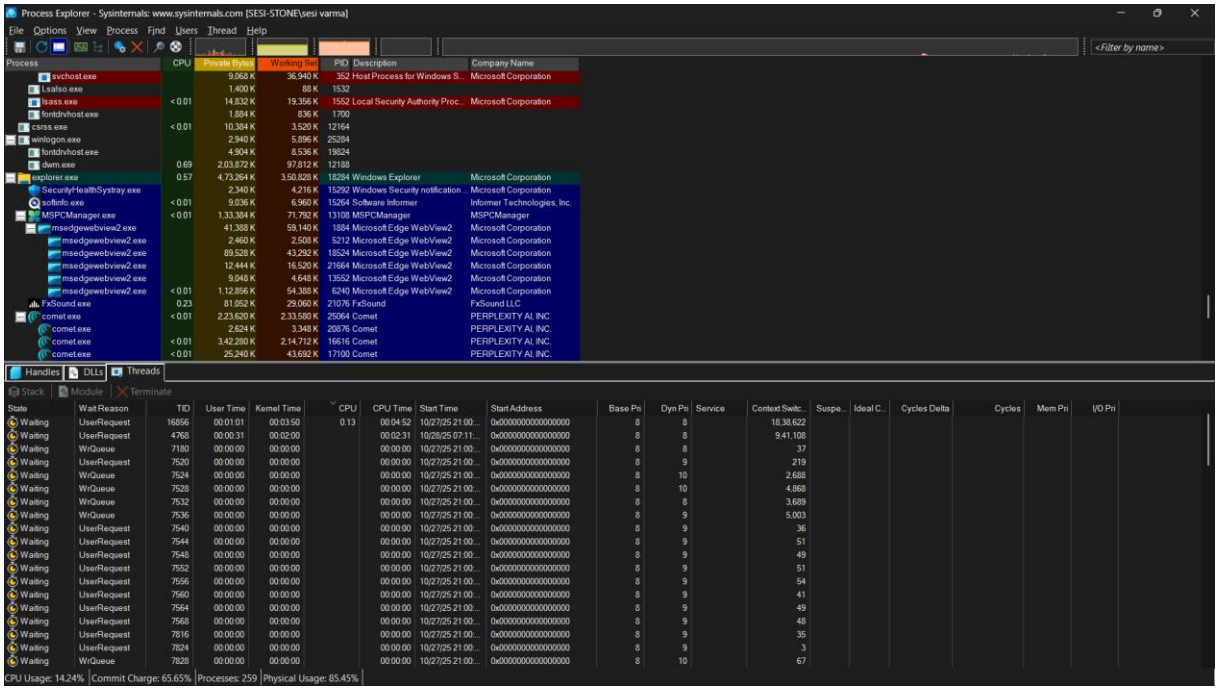
2. **Verify Digital Signature:**
   Right-click the process → **Properties** → **Image tab** → check **Digital Signature**.
   If no signature is found, it could be unsafe.

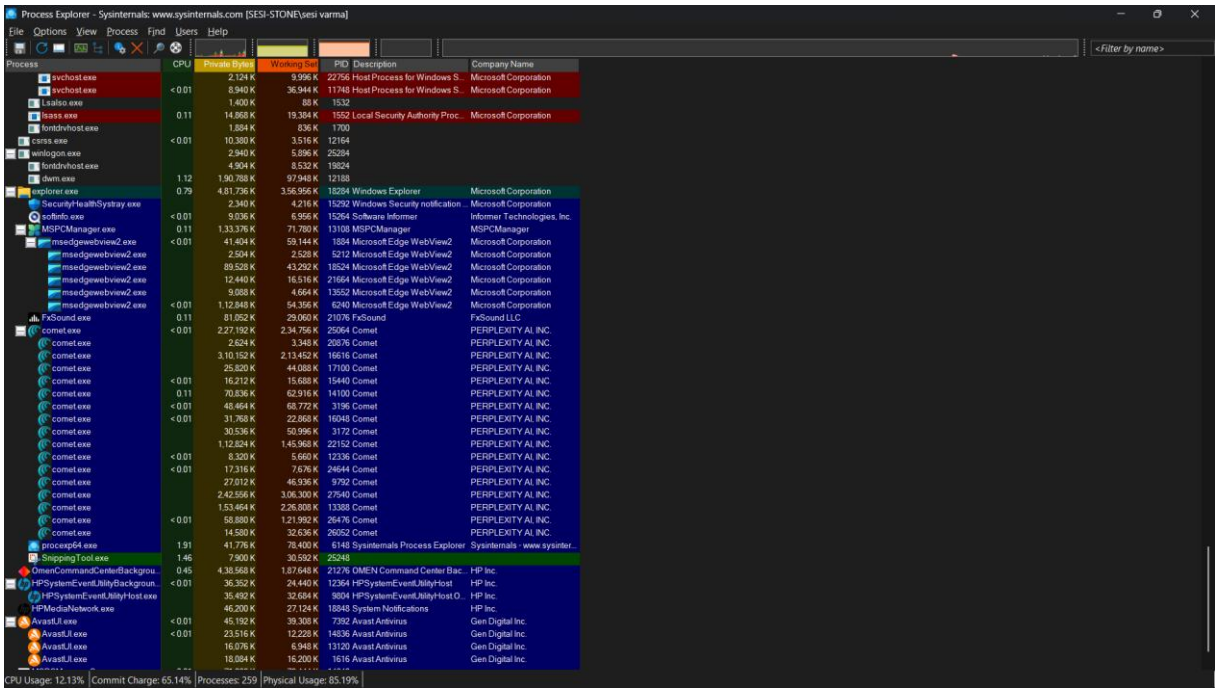
3. **Inspect File Location:**
   Check the **Path** field. Genuine Windows processes usually reside in:
   C:\Windows\System32\
   Files located in Temp or User folders may be malicious.

4. **Monitor Resource Usage:**
   Observe the **CPU**, **Memory**, and **Disk** usage.
   High or unusual usage without reason could signal malware.

5. **Check Description and Company Info:**
   Missing or strange details under the **Description** or **Company Name** column can indicate a fake or harmful process.

6. **View Network Activity:**
   Right-click → **Properties** → **TCP/IP tab** to check for unexpected internet connections.



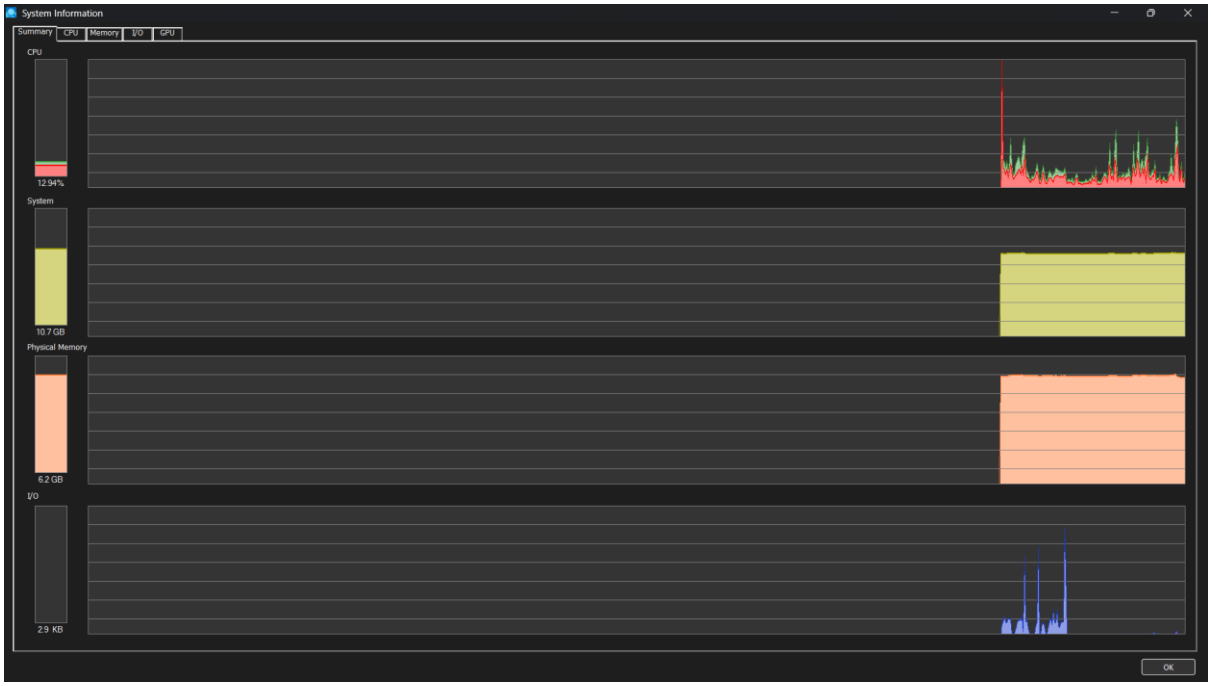


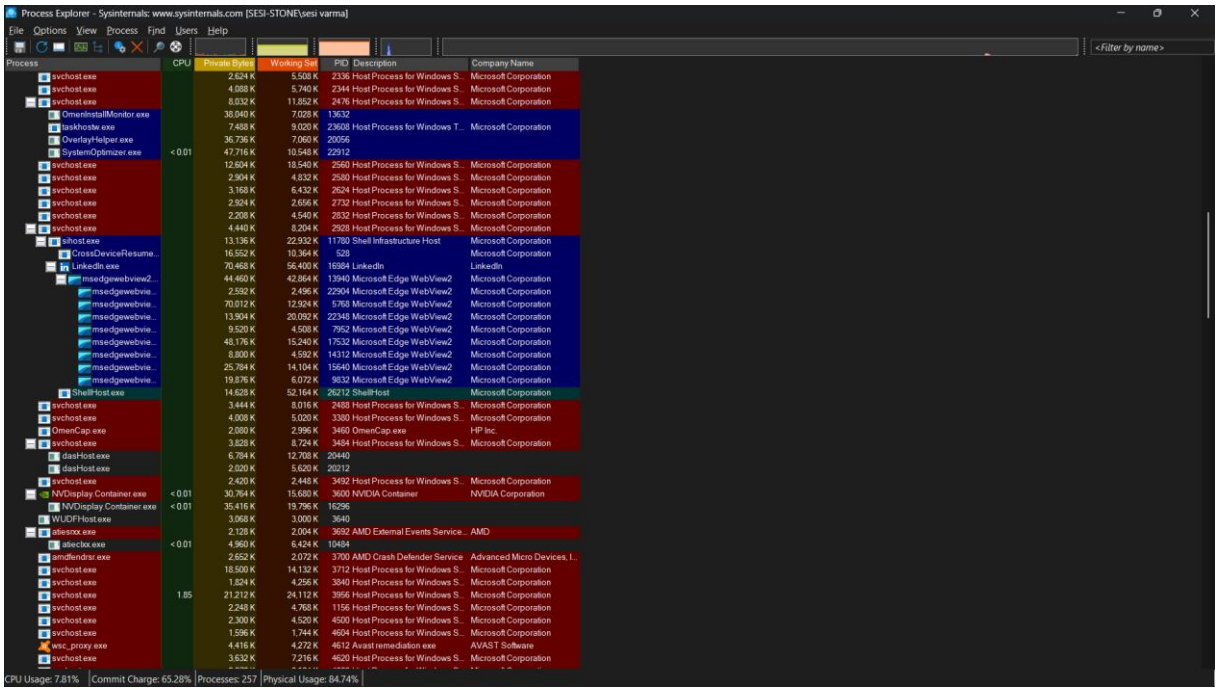
Step 4: Research Suspicious Processes

If a process looks strange:

- Search its name online (e.g., cmd.exe, svchost.exe).
- Check with trusted sources like **VirusTotal**, **ProcessLibrary**, or **Windows Defender Security Intelligence**.

This helps confirm whether the process is safe, a system file, or malware.

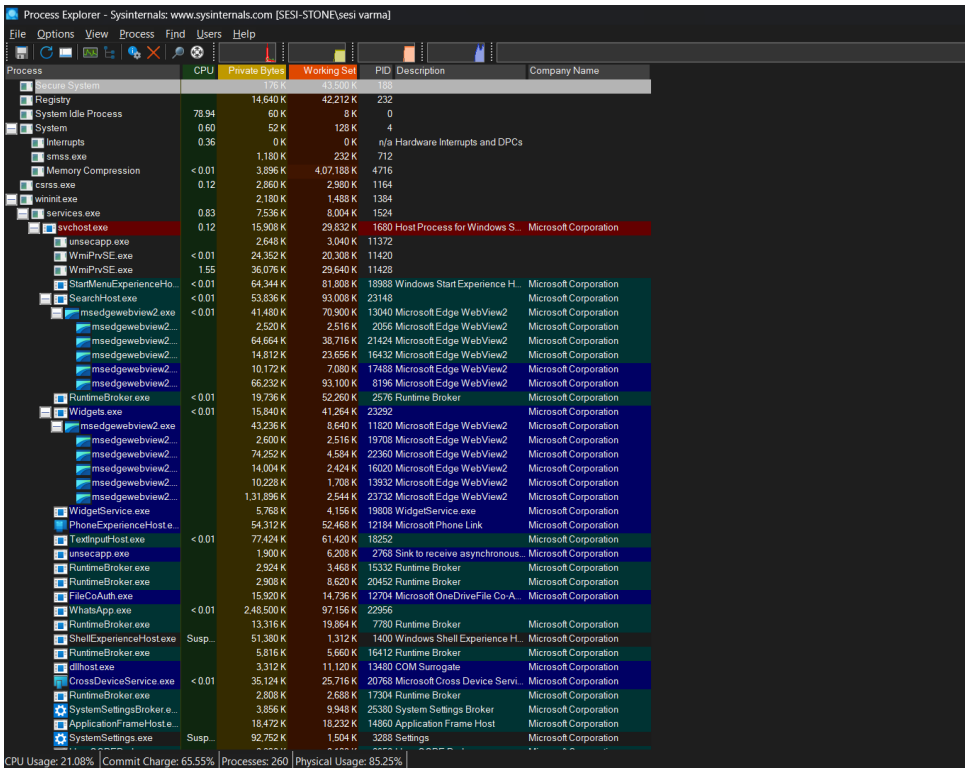




Step 5: Handling Malicious or Unwanted Processes

Once you identify a harmful process, take action:

- **Terminate:**
  Right-click → **Kill Process** to stop it immediately.
- **Suspend:**
  Right-click → **Suspend** to temporarily freeze it.
- **Locate and Delete Source File:**
  Right-click → **Properties** → check the **Path**, navigate to the location, and delete the executable if confirmed malicious



Step 6: Perform a System-Wide Cleanup

- Run a **full antivirus scan** using Windows Defender or any trusted antivirus software.
- Use dedicated **malware removal tools** like *Malwarebytes* or *AdwCleaner* for deeper cleanup.
- Restart your computer and verify that the suspicious process no longer appears.

Final Output

Action	Result
Identified suspicious process	Process Explorer showed unknown process consuming high CPU
Verified digital signature	Process found unsigned and located in Temp directory
Killed and deleted process	Process terminated and file removed
Ran antivirus scan	No further threats detected
System status	Clean and stable