

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:

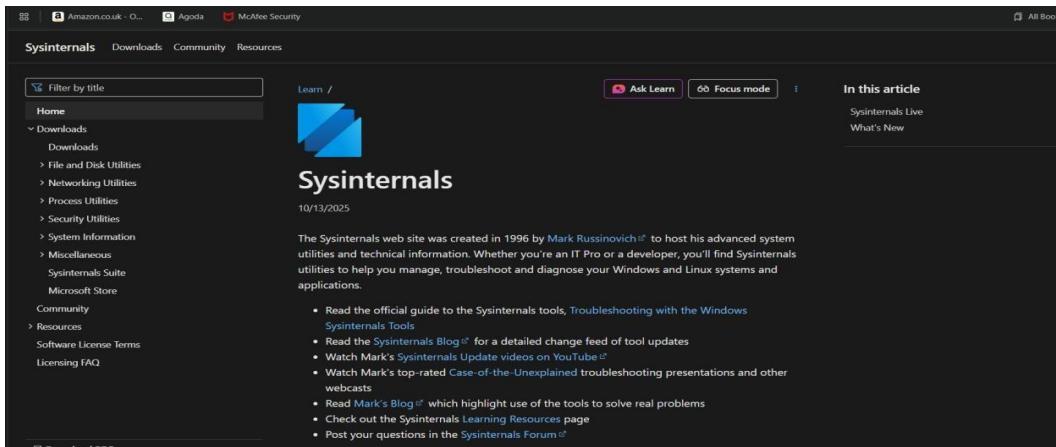
Visit the official Microsoft Sysinternals website and download **Process Explorer**.

2. Extract Files:

Unzip the downloaded file into a specific folder on your system.

3. Run as Administrator:

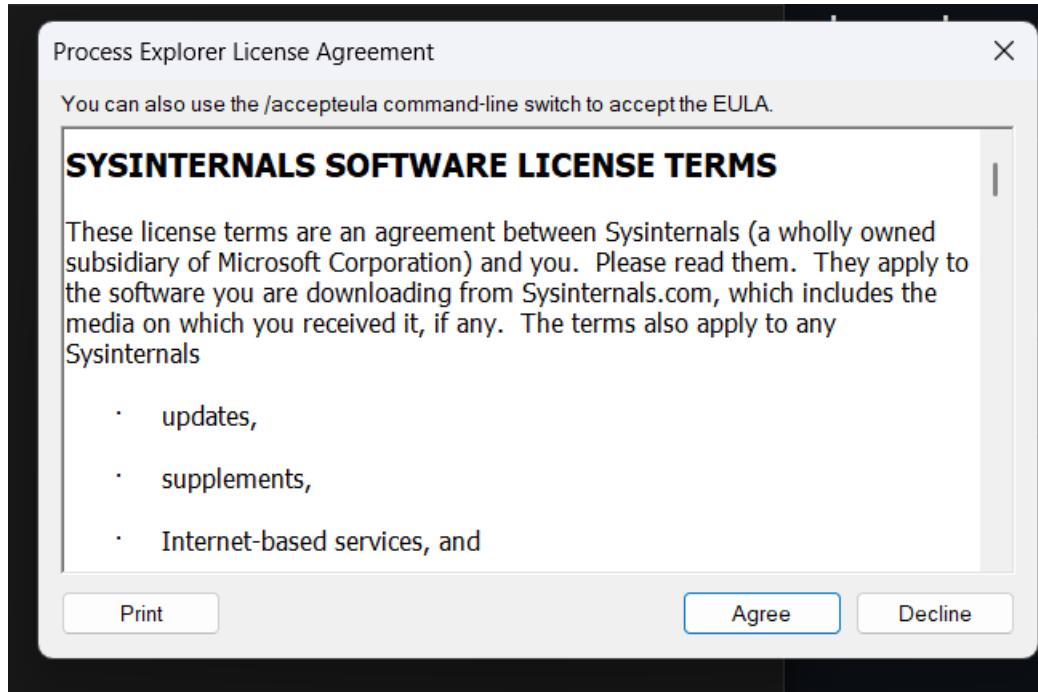
Right-click on procexp64.exe (for 64-bit) or procexp.exe (for 32-bit)
→ **Run as Administrator** to launch the tool.



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

and analyze 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:

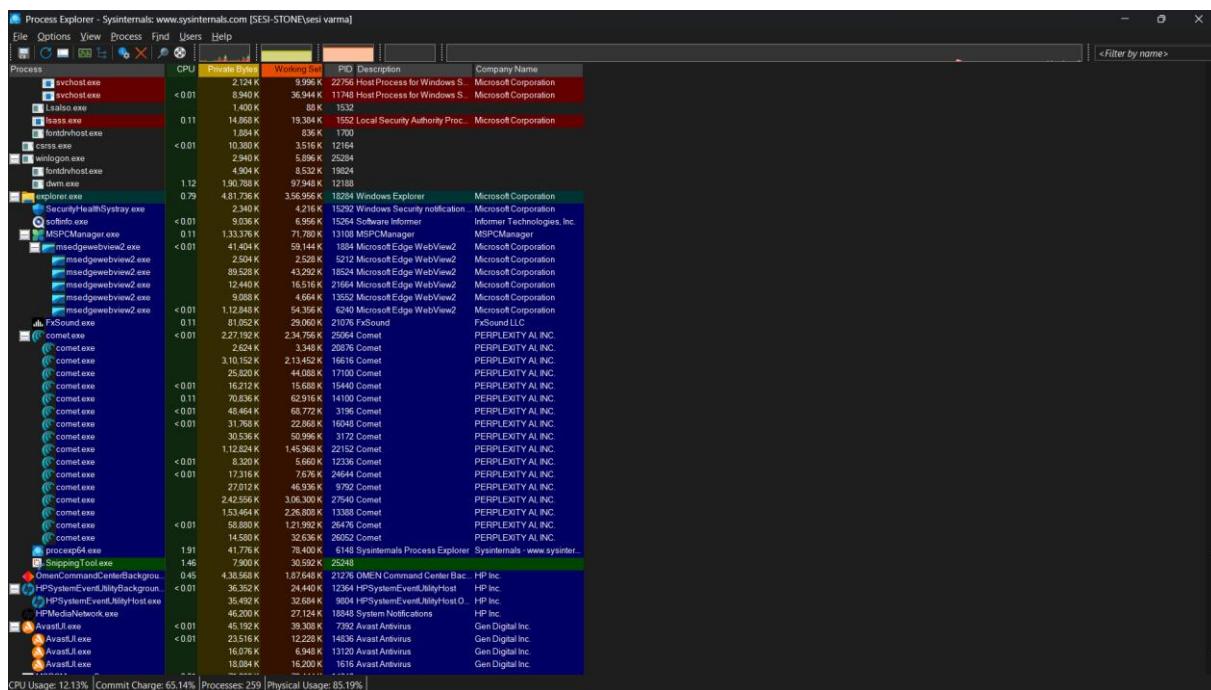
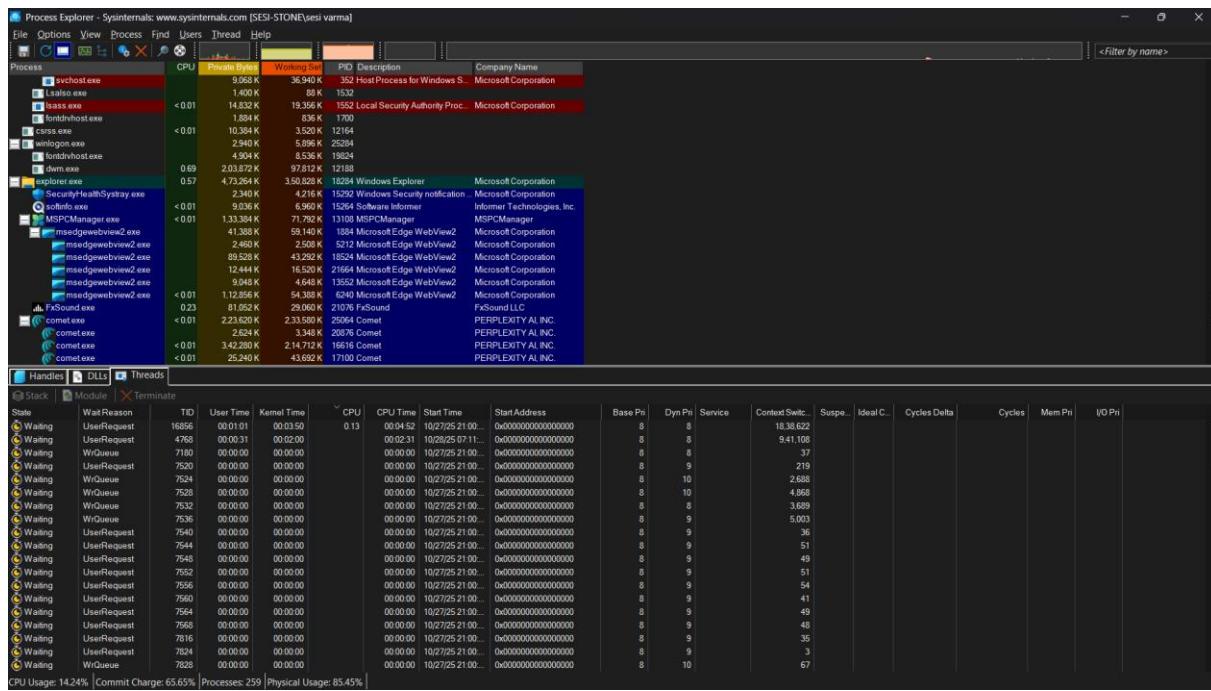
Observe the **CPU**, **Memory**, and **Disk** usage.
High or unusual usage without reason could signal malware.

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.

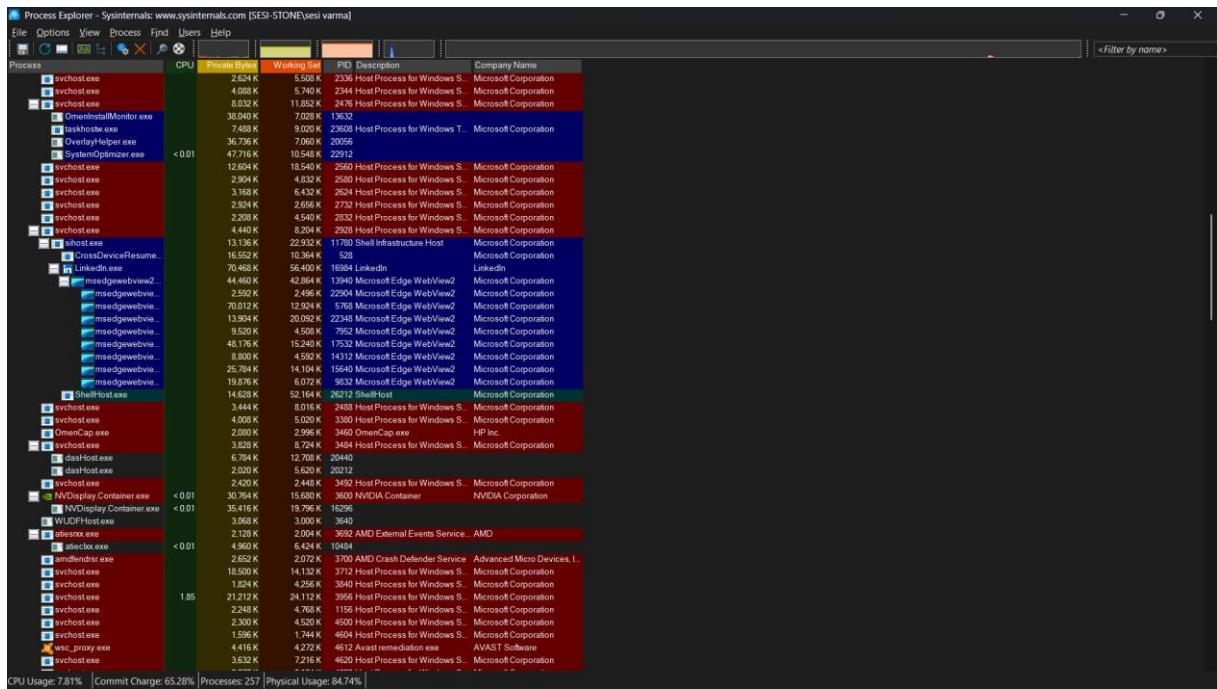
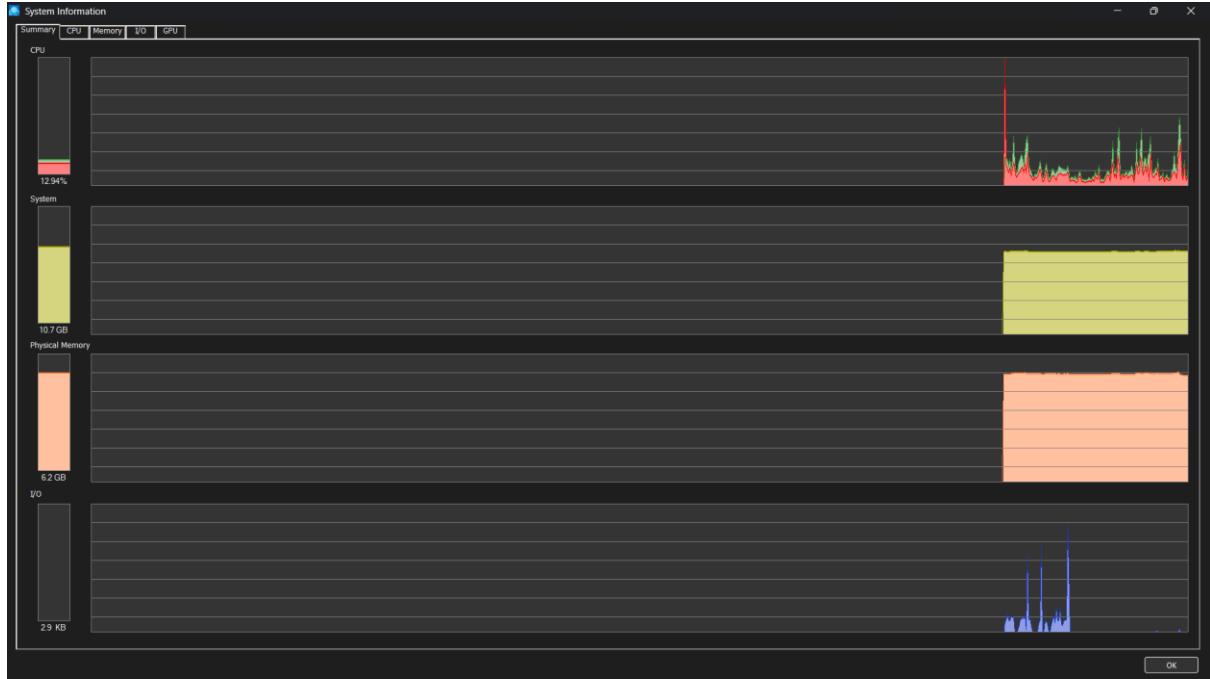


Step 4: Research Suspicious Processes

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

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System	176 K	43,500 K	188			
Registry	14,640 K	42,212 K	232			
System Idle Process	78.94	60 K	8 K	0		
System	0.60	52 K	128 K	4	n/a Hardware Interrupts and DPCs	
Interrupts	0.36	0 K	0 K			
smss.exe	1.180 K	232 K	712			
Memory Compression	< 0.01	3,896 K	4,071,88 K	4716		
crss.exe	0.12	2,860 K	2,980 K	1164		
wininit.exe		2,180 K	1,488 K	1384		
services.exe	0.83	7,536 K	8,004 K	1524		
svchost.exe	18	15,908 K	29,832 K	1680	Host Process for Windows S...	Microsoft Corporation
unscapp.exe	2,648 K	3,040 K	11372			
WmiPrvSE.exe	< 0.01	24,352 K	20,308 K	11420		
WmiPrvSE.exe	1.55	36,076 K	29,640 K	11428		
StartMenuExperienceHo...	< 0.01	64,344 K	81,808 K	18988	Windows Start Experience H...	Microsoft Corporation
SearchHost.exe	< 0.01	53,836 K	93,008 K	23148		
msedgewebview2.exe	< 0.01	41,480 K	70,900 K	13040	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2...		2,520 K	2,516 K	2056	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2...		64,664 K	38,716 K	21242	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2...		14,812 K	23,656 K	16432	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2...		10,172 K	7,080 K	17488	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2...		66,232 K	93,100 K	8196	Microsoft Edge WebView2	Microsoft Corporation
RuntimeBroker.exe	< 0.01	19,736 K	52,260 K	2576	Runtime Broker	Microsoft Corporation
Widgets.exe	< 0.01	15,840 K	41,264 K	2392		
msedgewebview2.exe		43,236 K	8,640 K	11820	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2...		2,600 K	2,516 K	19708	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2...		74,1252 K	4,584 K	22360	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2...		14,004 K	2,424 K	16020	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2...		10,228 K	1,708 K	13932	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2...		131,896 K	2,544 K	23732	Microsoft Edge WebView2	Microsoft Corporation
WidgetService.exe		5,768 K	4,156 K	19808	WidgetService.exe	Microsoft Corporation
PhoneExperienceHost.e...		56,312 K	52,468 K	12184	Microsoft Phone Link	Microsoft Corporation
TextInputHost.exe	< 0.01	77,424 K	61,420 K	1825		
unscapp.exe		1,900 K	6,208 K	2768	Sink to receive asynchronous...	Microsoft Corporation
RuntimeBroker.exe		2,924 K	3,468 K	15332	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2,908 K	8,620 K	20452	Runtime Broker	Microsoft Corporation
FileCoAuth.exe		15,920 K	14,736 K	12704	Microsoft OneDriveFile Co-A...	Microsoft Corporation
WhatsApp.exe	< 0.01	24,6500 K	97,156 K	22956		
RuntimeBroker.exe		13,316 K	19,864 K	7780	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	Susp...	51,1380 K	1,312 K	1400	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		5,816 K	5,660 K	16412	Runtime Broker	Microsoft Corporation
dlhost.exe		3,312 K	11,120 K	13480	COM Surrogate	Microsoft Corporation
CrossDeviceService.exe	< 0.01	36,124 K	25,716 K	20768	Microsoft Cross Device Servi...	Microsoft Corporation
RuntimeBroker.exe		2,808 K	2,688 K	17304	Runtime Broker	Microsoft Corporation
SystemSettingsBroker.e...		3,856 K	9,948 K	25390	System Settings Broker	Microsoft Corporation
ApplicationFrameHost.e...		18,847 K	18,232 K	14960	Application Frame Host	Microsoft Corporation
SystemSettings.exe	Susp...	92,752 K	1,504 K	3288	Settings	Microsoft Corporation

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