

Date: 6/08/25

Name: Mahammad Tanvir Khatri

Email: khatritanveer66@gmail.com

Topic: Sysinternals Tools (Hands-on)

1. Process Explorer

Purpose:

Process Explorer is a system utility from Sysinternals used to view detailed information about running processes, including memory usage, open files, and parent-child relationships between processes.

Activity:

I downloaded Process Explorer, ran the application on my device, and captured the output shown below.

Screenshot:

The screenshot displays the Windows Task Manager application window. The title bar reads "Process Explorer - System Idle...". The menu bar includes File, Options, View, Process, Find, Users, and Help. Below the menu bar is a toolbar with icons for various actions like refresh, stop, and search. A filter bar at the top right shows "<Filter by name>".

Process	CPU	Private Bytes	Working Set	Description	Company Name
Registry		11,640 K	38,876 K	232	
System Idle Process	76.67	60 K	8 K	0	
System	0.62	46 K	164 K	4	
smss.exe	1.00	8 K	0 K	n/a Hardware Interrupts and DPCs	
smss.exe		1,104 K	1,408 K	716	
Memory Compression	<0.01	2,596 K	767,284 K	3128	
csrss.exe	<0.01	2,408 K	6,252 K	992	
csrss.exe		15,512 K	7,268 K	972	
services.exe	0.37	6,324 K	11,016 K	1092	
svchost.exe	<0.01	12,148 K	39,876 K	1332 Host Process for Windows S.	Microsoft Corporation
WmPrvSE.exe	<0.01	17,824 K	30,396 K	5888	
WmPrvSE.exe	<0.01	2,560 K	11,852 K	7008	
WmPrvSE.exe	0.87	39,672 K	54,336 K	7400	
StartMenuExperienceHo...		81,716 K	110,256 K	10256 Windows Start Experience H.	Microsoft Corporation
SearchHost.exe		61,388 K	120,336 K	10300	Microsoft Corporation
microsoftedge.exe		40,720 K	105,632 K	11548 Microsoft Edge WebView2	Microsoft Corporation
microsoftedge.exe		2,296 K	8,862 K	11780 Microsoft Edge WebView2	Microsoft Corporation
microsoftedge.exe		71,712 K	59,512 K	3068 Microsoft Edge WebView2	Microsoft Corporation
microsoftedge.exe		13,172 K	37,572 K	11388 Microsoft Edge WebView2	Microsoft Corporation
microsoftedge.exe		3,564 K	18,844 K	11572 Microsoft Edge WebView2	Microsoft Corporation
microsoftedge.exe		59,744 K	67,812 K	12360 Microsoft Edge WebView2	Microsoft Corporation
Widgets.exe		12,780 K	65,728 K	10460	Microsoft Corporation
microsoftedge.exe		39,520 K	75,616 K	3496 Microsoft Edge WebView2	Microsoft Corporation
microsoftedge.exe		2,300 K	8,944 K	616 Microsoft Edge WebView2	Microsoft Corporation
microsoftedge.exe		110,848 K	6,794 K	14516 Microsoft Edge WebView2	Microsoft Corporation
microsoftedge.exe		12,632 K	1,820 K	14544 Microsoft Edge WebView2	Microsoft Corporation
microsoftedge.exe		10,140 K	100 K	5416 Microsoft Edge WebView2	Microsoft Corporation
microsoftedge.exe		113,048 K	3,472 K	8604 Microsoft Edge WebView2	Microsoft Corporation
microsoftedge.exe		6,388 K	120 K	2372 Microsoft Edge WebView2	Microsoft Corporation
RuntimeBroker.exe		11,728 K	53,672 K	12492 Runtime Broker	Microsoft Corporation
UserOOBEBroker.exe		1,756 K	10,752 K	10552 User OOBEBroker	Microsoft Corporation
RuntimeBroker.exe		5,108 K	35,728 K	10832 Runtime Broker	Microsoft Corporation
WidgetService.exe		5,000 K	26,224 K	10900 WidgetService.exe	Microsoft Corporation
PhoneExperienceHost.e...		88,528 K	163,928 K	10902 Microsoft Phone Link	Microsoft Corporation
TeddingUIHost.exe		52,328 K	81,628 K	15176	Microsoft Corporation
ShellExperienceHost.exe	Susp.	59,448 K	124,524 K	15856 Windows Shell Experience H.	Microsoft Corporation
RuntimeBroker.exe		2,204 K	23,880 K	16090 Runtime Broker	Microsoft Corporation
ApplicationFrameHost.e...		65,148 K	51,524 K	1804 Application Frame Host	Microsoft Corporation
backgroundTaskHost.exe	Susp.	18,164 K	2,340 K	15882 Background Task Host	Microsoft Corporation
WindowsPackageManager...		10,272 K	31,536 K	4624	Microsoft Corporation
RuntimeBroker.exe		3,052 K	21,800 K	1660 Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		14,824 K	53,800 K	18976 Runtime Broker	Microsoft Corporation
AppActions.exe		15,680 K	32,848 K	19108	
SystemSettings.exe		148,016 K	3,388 K	19900 Settings	Microsoft Corporation
WhisperApp.exe	<0.01	27,116 K	29,892 K	18148	
backgroundTaskHost.exe	Susp.	17,512 K	2,168 K	18160 Background Task Host	Microsoft Corporation
RuntimeBroker.exe		3,344 K	26,252 K	21192 Runtime Broker	Microsoft Corporation
backgroundTaskHost.exe	Susp.	4,476 K	25,720 K	2688 Background Task Host	Microsoft Corporation
RuntimeBroker.exe		1,860 K	9,300 K	15544 Runtime Broker	Microsoft Corporation
SmartScreenFilter.exe		5,684 K	29,500 K	15196 Windows Defender SmartScr...	Microsoft Corporation
WUAPHost.exe		5,524 K	8,412 K	1408	
svchost.exe	0.37	10,456 K	19,448 K	1508 Host Process for Windows S.	Microsoft Corporation

At the bottom, system statistics are displayed:

- CPU Usage: 23.46% | Commit Charge: 51.91%
- Processes: 245 | Physical Usage: 60.67%

2. Process Monitor

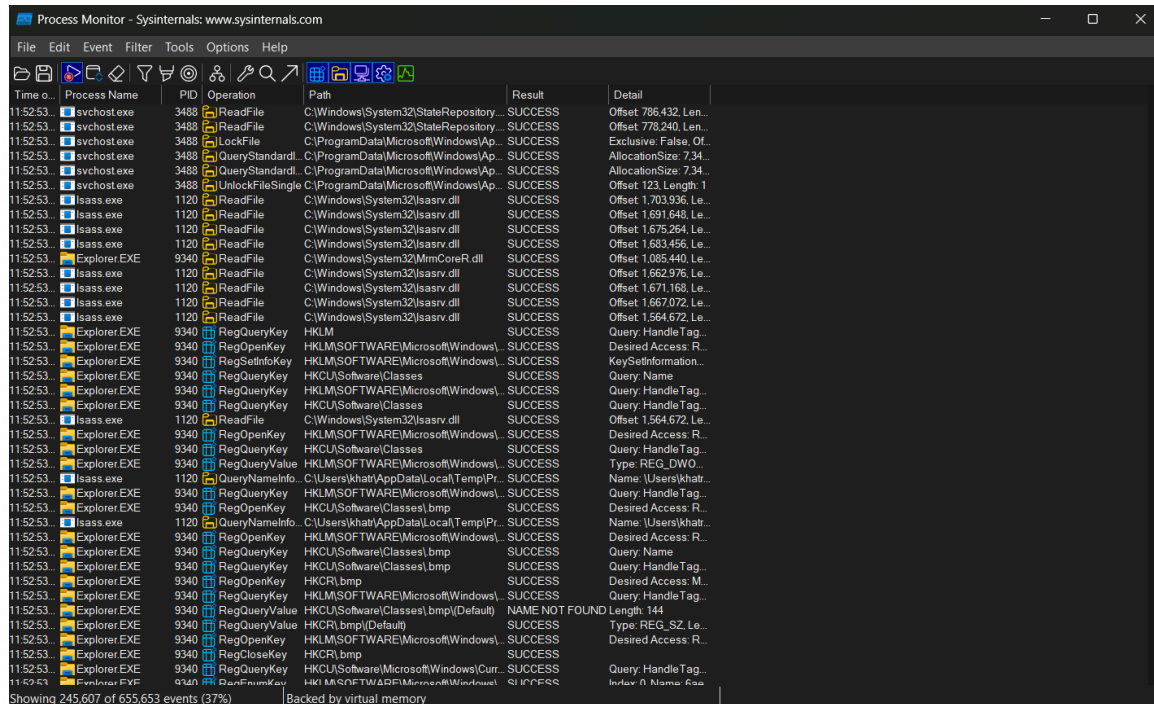
Purpose:

Process Monitor is a real-time monitoring tool from Sysinternals that captures file system, registry, and process/thread activity.

Activity:

I downloaded Process Monitor, launched it on my device, and captured the live activity as shown below.

Screenshot:



The screenshot displays the Process Monitor application window with a menu bar (File, Edit, Event, Filter, Tools, Options, Help) and a toolbar. The main window is divided into two panes. The left pane shows a list of events with columns for Time of Day, Process Name, PID, Operation, Path, Result, and Detail. The right pane shows a detailed view of the selected event. The events list shows various file system operations (ReadFile, LockFile, QueryStandardQuery, UnlockFileSingle) and registry operations (RegOpenKey, RegSetInfoKey, RegQueryValue, RegOpenKey, RegCloseKey) performed by processes like svchost.exe, lsass.exe, Explorer.EXE, and smss.exe. The status bar at the bottom indicates 'Showing 245,607 of 655,653 events (37%)' and 'Backed by virtual memory'.

Time of Day	Process Name	PID	Operation	Path	Result	Detail
11:52:53	svchost.exe	3488	ReadFile	C:\Windows\System32\StateRepository	SUCCESS	Offset 786,432, Len...
11:52:53	svchost.exe	3488	ReadFile	C:\Windows\System32\StateRepository	SUCCESS	Offset 778,240, Len...
11:52:53	svchost.exe	3488	LockFile	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Exclusive False, Of...
11:52:53	svchost.exe	3488	QueryStandardQuery	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	AllocationSize: 734...
11:52:53	svchost.exe	3488	QueryStandardQuery	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	AllocationSize: 734...
11:52:53	svchost.exe	3488	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Offset 123, Length: 1...
11:52:53	lsass.exe	1120	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1,703,936, Le...
11:52:53	lsass.exe	1120	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1,691,648, Le...
11:52:53	lsass.exe	1120	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1,675,264, Le...
11:52:53	lsass.exe	1120	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1,683,456, Le...
11:52:53	Explorer.EXE	9340	ReadFile	C:\Windows\System32\WmmCoreR.dll	SUCCESS	Offset 1,085,440, Le...
11:52:53	lsass.exe	1120	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1,662,976, Le...
11:52:53	lsass.exe	1120	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1,671,168, Le...
11:52:53	lsass.exe	1120	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1,667,072, Le...
11:52:53	lsass.exe	1120	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1,564,072, Le...
11:52:53	Explorer.EXE	9340	RegOpenKey	HKLM	SUCCESS	Query Handle Tag...
11:52:53	Explorer.EXE	9340	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Desired Access: R...
11:52:53	Explorer.EXE	9340	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	KeySetInformation...
11:52:53	Explorer.EXE	9340	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query Name
11:52:53	Explorer.EXE	9340	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Query Handle Tag...
11:52:53	Explorer.EXE	9340	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query Handle Tag...
11:52:53	lsass.exe	1120	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1,564,672, Le...
11:52:53	Explorer.EXE	9340	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Desired Access: R...
11:52:53	Explorer.EXE	9340	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query Handle Tag...
11:52:53	Explorer.EXE	9340	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Type: REG_DWORD...
11:52:53	lsass.exe	1120	QueryNameInfo	C:\Users\khat\AppData\Local\Temp\Pr...	SUCCESS	Name: \Users\khat...
11:52:53	Explorer.EXE	9340	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Query Handle Tag...
11:52:53	Explorer.EXE	9340	RegOpenKey	HKCU\Software\Classes\bmp	SUCCESS	Desired Access: R...
11:52:53	lsass.exe	1120	QueryNameInfo	C:\Users\khat\AppData\Local\Temp\Pr...	SUCCESS	Name: \Users\khat...
11:52:53	Explorer.EXE	9340	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Desired Access: R...
11:52:53	Explorer.EXE	9340	RegQueryValue	HKCU\Software\Classes\bmp	SUCCESS	Query Name
11:52:53	Explorer.EXE	9340	RegQueryValue	HKCU\Software\Classes\bmp	SUCCESS	Query Handle Tag...
11:52:53	Explorer.EXE	9340	RegOpenKey	HKCR\bmp	SUCCESS	Desired Access: M...
11:52:53	Explorer.EXE	9340	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Query Handle Tag...
11:52:53	Explorer.EXE	9340	RegQueryValue	HKCU\Software\Classes\bmp(Default)	NAME NOT FOUND	Length 144
11:52:53	Explorer.EXE	9340	RegQueryValue	HKCR\bmp(Default)	SUCCESS	Type: REG_SZ, Le...
11:52:53	Explorer.EXE	9340	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Desired Access: R...
11:52:53	Explorer.EXE	9340	RegCloseKey	HKCR\bmp	SUCCESS	
11:52:53	Explorer.EXE	9340	RegQueryValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Query Handle Tag...
11:52:53	Explorer.EXE	9340	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	Index 0 Name: Ess...

3. Whois

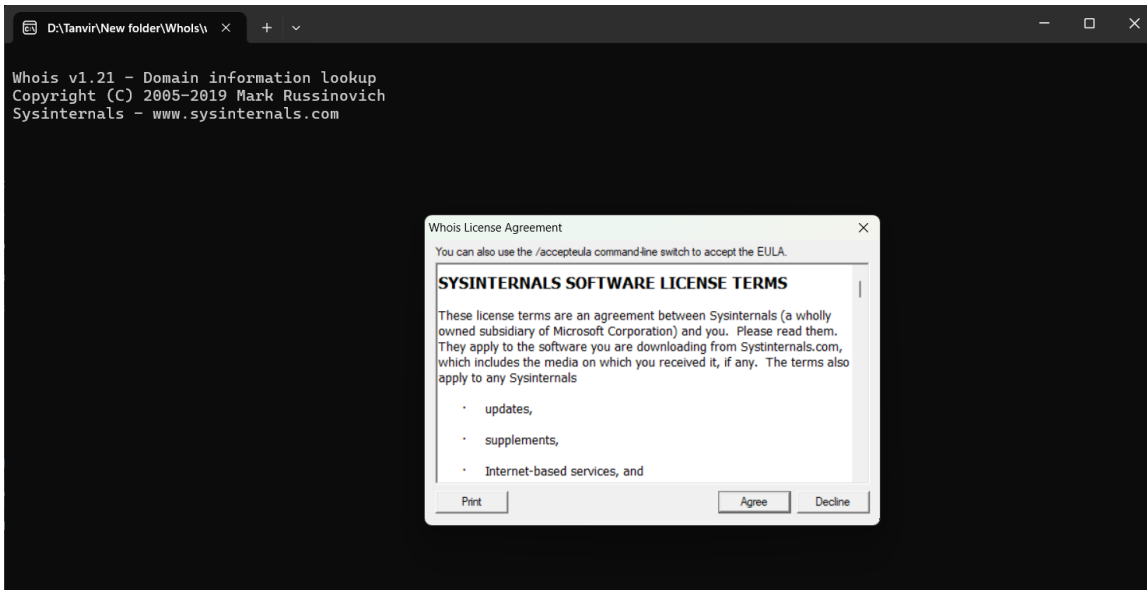
Purpose:

Whois is a command-line utility that retrieves registration information of domain names or IP addresses.

Activity:

I downloaded Whois from Sysinternals and ran the application on my device. The license agreement appeared as expected. Since no domain was provided, the tool exited after accepting the license.

Screenshot:



4.PSTools

Purpose:

PSTools is a collection of command-line utilities from Sysinternals used for remote system management and local administrative tasks. It includes tools like PsExec, PsKill, PsList, PsLoggedOn, and others.

Activity:

I downloaded PsTools from the official Microsoft Sysinternals website, extracted the ZIP file on my device, and viewed the list of tools included in the package.

Screenshot:

Name	Date modified	Type	Size
Eula.txt	4/11/2023 6:10 PM	Text Document	8 KB
PsExec.exe	4/11/2023 6:10 PM	Application	700 KB
PsExec64.exe	4/11/2023 6:10 PM	Application	814 KB
psfile.exe	3/30/2023 4:57 PM	Application	230 KB
psfile64.exe	3/30/2023 4:57 PM	Application	283 KB
PsGetsid.exe	3/30/2023 4:57 PM	Application	404 KB
PsGetsid64.exe	3/30/2023 4:57 PM	Application	495 KB
PsInfo.exe	3/30/2023 4:57 PM	Application	433 KB
PsInfo64.exe	3/30/2023 4:57 PM	Application	524 KB
pskill.exe	3/30/2023 4:57 PM	Application	382 KB
pskill64.exe	3/30/2023 4:57 PM	Application	466 KB
pslist.exe	3/30/2023 4:58 PM	Application	213 KB
pslist64.exe	3/30/2023 4:58 PM	Application	261 KB
PsLoggedon.exe	6/28/2016 9:51 AM	Application	149 KB
PsLoggedon64.exe	6/28/2016 9:49 AM	Application	167 KB
psloglist.exe	3/30/2023 4:58 PM	Application	306 KB
psloglist64.exe	3/30/2023 4:58 PM	Application	370 KB
pspasswd.exe	3/30/2023 4:58 PM	Application	217 KB
pspasswd64.exe	3/30/2023 4:58 PM	Application	265 KB
psping.exe	3/30/2023 4:57 PM	Application	281 KB
psping64.exe	3/30/2023 4:57 PM	Application	339 KB
PsService.exe	3/30/2023 4:58 PM	Application	262 KB
PsService64.exe	3/30/2023 4:58 PM	Application	315 KB
pssshutdown.exe	3/30/2023 4:57 PM	Application	675 KB
pssshutdown64.exe	3/30/2023 4:57 PM	Application	791 KB
pssuspend.exe	3/30/2023 4:58 PM	Application	384 KB

5. Logon Sessions:

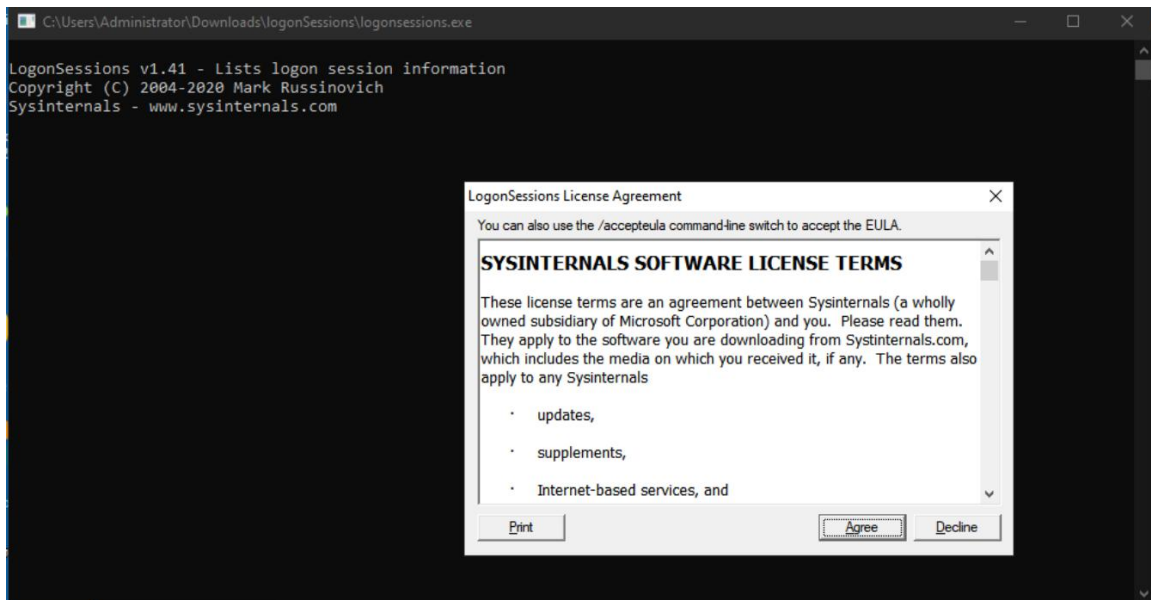
Purpose:

LogonSessions.exe is a Sysinternals command-line tool that displays details about all active user logon sessions on the system. It shows session IDs, logon times, usernames, domains, and authentication methods. It's commonly used for security monitoring and session tracking.

Activity:

I downloaded LogonSessions.exe from the official Sysinternals website and ran it on my device. The license agreement (EULA) prompt appeared. After accepting it, the window closed immediately as the tool was not executed from the command line.

Screenshot:



6. sysmon

Purpose:

Sysmon (System Monitor) is a powerful Windows system service and driver from Sysinternals that logs detailed system activity to the Windows Event Log. It captures events like process creation, network connections, file changes, and more, making it a valuable tool for security monitoring and incident response.

Screenshot:

Name	Date modified	Type	Size
Eula	23-07-2024 14:08	Text Document	8 KB
Sysmon	23-07-2024 14:08	Application	8,282 KB
Sysmon64	23-07-2024 14:08	Application	4,457 KB
Sysmon64a	23-07-2024 14:08	Application	4,877 KB

7.PSExec

Purpose:

PSEXEC is a Sysinternals command-line utility that allows administrators to run processes and commands on remote systems as if they were running locally. It's widely used for remote software installations, patch deployment, and system administration without needing remote desktop access.

Screenshot:

Name	Date modified	Type	Size
Eula	11-04-2023 18:10	Text Document	8 KB
PSEXEC	11-04-2023 18:10	Application	700 KB
PSEXEC64	11-04-2023 18:10	Application	814 KB

8. steps to create for Microsoft intune portal

Here are the basic steps to create and configure in Microsoft Intune portal:

1. **Sign in** to Microsoft Intune Admin Center
2. Go to **Devices** > Choose platform (e.g., Windows)
3. Click on **Configuration profiles**
4. Click **+ Create profile**
5. Choose platform (e.g., Windows 10 and later) and profile type
6. Configure the **profile settings** (like policies, restrictions, etc.)
7. Click **Next**, assign to user or device groups
8. Review and click **Create**

Screenshot:

