

Batch Information:

- **Batch Start Date:** 2025-08-04
- **Batch Name:** WiproNGA_DWS_B5_25VID2550
- **First Name:** Tirthajit
- **Last Name:** Das
- **User ID:** 34940
- **Batch ID:** B5-25VID2550

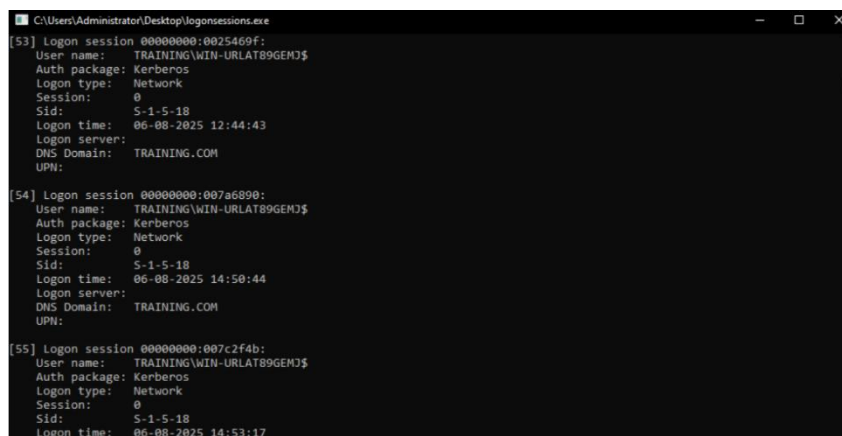
ASSIGNMENTS

- Using Windows Tools for Debugging: LogonSessions, Autologon, Process Explorer, Psexec, PSTools, RegMon, Whois, SysMon.
 - Intune Free trial Subscription - How to enrol.
- Using Windows Tools for Debugging: LogonSessions, Autologon, Process Explorer, Psexec, PSTools, RegMon, Whois, SysMon.

In Windows environments, especially in enterprise IT and system administration tasks like Application Packaging, System Monitoring, and Debugging, Microsoft and Sysinternals provide a set of powerful utilities. These tools help investigate performance issues, identify unauthorized access, understand registry behavior, and automate system tasks.

1. LogonSessions

- **Purpose:** Displays all user logon sessions on the system.
- **Tool:** Part of Sysinternals Suite (command-line tool: LogonSessions.exe)
- **Use Case:**
 - Identifying active user sessions.
 - Detecting suspicious logon activity.



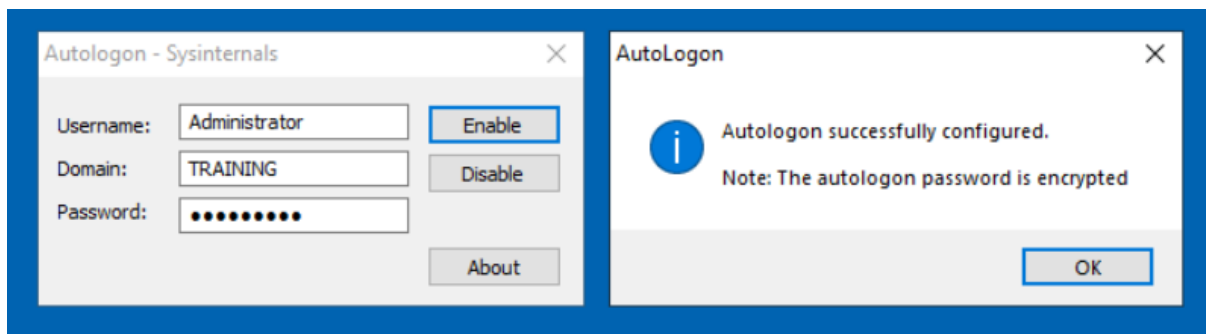
```
C:\Users\Administrator\Desktop\logonsessions.exe
[53] Logon session 00000000:0025469f:
User name: TRAINING\WIN-URLAT89GEMJ$
Auth package: Kerberos
Logon type: Network
Session: 0
Sid: S-1-5-18
Logon time: 06-08-2025 12:44:43
Logon server:
DNS Domain: TRAINING.COM
UPN:

[54] Logon session 00000000:007a6890:
User name: TRAINING\WIN-URLAT89GEMJ$
Auth package: Kerberos
Logon type: Network
Session: 0
Sid: S-1-5-18
Logon time: 06-08-2025 14:50:44
Logon server:
DNS Domain: TRAINING.COM
UPN:

[55] Logon session 00000000:007c2f4b:
User name: TRAINING\WIN-URLAT89GEMJ$
Auth package: Kerberos
Logon type: Network
Session: 0
Sid: S-1-5-18
Logon time: 06-08-2025 14:53:17
```

2. Autologon

- **Purpose:** Enables automatic login to Windows without entering a password at startup.
- **Tool Type:** GUI tool from Sysinternals.
- **Use Case:**
 - Useful for kiosks, test environments, or VM automation where secure unattended logon is needed.
- **How it works:**
 - It stores credentials securely in the registry:
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
- **Important:** Autologon encrypts the password and hides it from plain view.



3. Process Explorer

- **Purpose:** Advanced version of Task Manager with detailed insight into system processes.
- **Tool Type:** GUI
- **Use Case:**
 - Analyze running processes.
 - Detect malware or injected DLLs.
 - Check parent-child process trees.
 - Monitor file, registry, and DLL activity per process.

Process Explorer - Sysinternals: www.sysinternals.com [TIRTHAJIT\TIRTHAJIT]

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System		180 K	63,068 K	188		
Registry		14,680 K	56,488 K	232		
System Idle Process	60.30	60 K	8 K	0		
System	1.75	56 K	4,532 K	4		
Interrupts	2.62	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,188 K	1,516 K	828		
Memory Compression	< 0.01	1,900 K	6,55,144 K	3664		
csrss.exe		2,660 K	6,448 K	1120		
wininit.exe		1,592 K	7,808 K	1208		
services.exe	0.12	7,628 K	18,924 K	1356		
svchost.exe		15,072 K	43,944 K	1516	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		3,960 K	13,412 K	7688		
unsecapp.exe		2,256 K	10,436 K	8032		
SearchHost.exe		79,236 K	1,46,876 K	10880		
msedgewebview2...		43,116 K	1,15,540 K	11328	Microsoft Edge Web View2	Microsoft Corporation
msedgewebvie...		2,304 K	11,020 K	12332	Microsoft Edge Web View2	Microsoft Corporation
msedgewebvie...		81,008 K	85,992 K	12972	Microsoft Edge Web View2	Microsoft Corporation
msedgewebvie...		15,676 K	45,084 K	13004	Microsoft Edge Web View2	Microsoft Corporation
msedgewebvie...		9,276 K	22,036 K	13144	Microsoft Edge Web View2	Microsoft Corporation
msedgewebvie...		1,03,228 K	1,50,092 K	12504	Microsoft Edge Web View2	Microsoft Corporation
Start Menu Experience...		82,536 K	1,22,660 K	10868	Windows Start Experience H...	Microsoft Corporation
Widgets.exe		12,796 K	66,636 K	11452		
msedgewebview2...		40,696 K	10,428 K	14068	Microsoft Edge Web View2	Microsoft Corporation
msedgewebvie...		2,280 K	11,220 K	15108	Microsoft Edge Web View2	Microsoft Corporation
msedgewebvie...		1,77,380 K	7,340 K	13596	Microsoft Edge Web View2	Microsoft Corporation
msedgewebvie...		13,792 K	4,756 K	13884	Microsoft Edge Web View2	Microsoft Corporation
msedgewebvie...		10,104 K	100 K	11704	Microsoft Edge Web View2	Microsoft Corporation
msedgewebvie...		1,49,468 K	2,752 K	11796	Microsoft Edge Web View2	Microsoft Corporation
msedgewebvie...		8,392 K	1,772 K	17412	Microsoft Edge Web View2	Microsoft Corporation

CPU Usage: 15.72% Commit Charge: 49.35% Processes: 268 Physical Usage: 63.83%

4. PsExec

- **Purpose:** Execute processes on remote systems.
- **Tool Type:** Command-line tool in **PsTools suite**
- **Use Case:**
 - Remotely launch applications
 - Run command-line tools on other machines without RDP.

Downloads

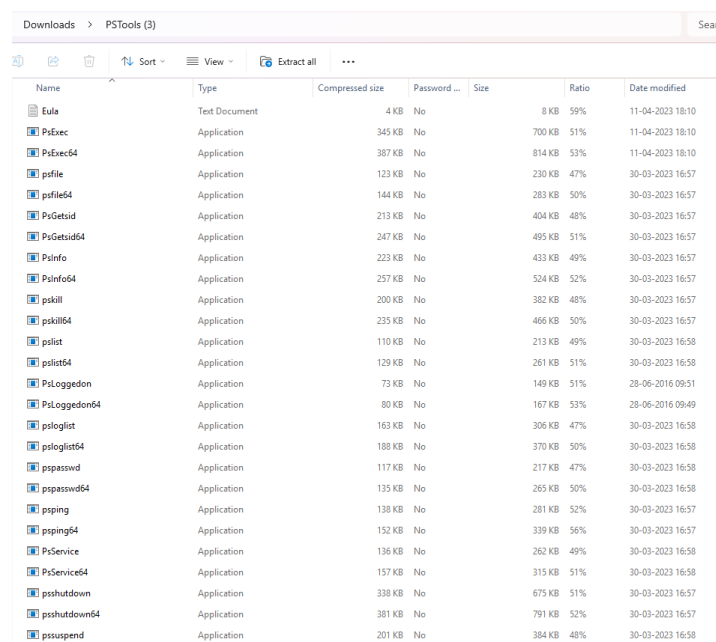
< > This PC > WORK DRIVE (D:) > Downloads

+ New | | | | | Sort | View | ...

Name	Date modified	Type	Size
Eula	06-08-2025 12:48	Text Document	8 KB
PsExec	06-08-2025 12:48	Application	700 KB
PsExec64	06-08-2025 12:48	Application	814 KB
psfile	06-08-2025 12:48	Application	230 KB
psfile64	06-08-2025 12:48	Application	283 KB
PsGetsid	06-08-2025 12:48	Application	404 KB
PsGetsid64	06-08-2025 12:48	Application	495 KB
Psinfo	06-08-2025 12:48	Application	433 KB
Psinfo64	06-08-2025 12:48	Application	524 KB

5. PsTools Suite (Collection)

- A suite of **remote administration tools** for managing local and remote systems.
- Tools include:
 - PsExec – Run remote commands
 - PsList – Show process list
 - PsKill – Kill processes
 - PsLogList – Event log viewer
 - PsShutdown – Remotely shutdown/reboot
 - PsService – Control services
- **Use Case:**
 - Great for scripting administrative tasks across multiple systems.



Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
Eula	Text Document	4 KB	No	8 KB	59%	11-04-2023 18:10
PsExec	Application	345 KB	No	700 KB	51%	11-04-2023 18:10
PsExec64	Application	387 KB	No	814 KB	53%	11-04-2023 18:10
psfile	Application	123 KB	No	230 KB	47%	30-03-2023 16:57
psfile64	Application	144 KB	No	283 KB	50%	30-03-2023 16:57
PsGetsid	Application	213 KB	No	404 KB	48%	30-03-2023 16:57
PsGetsid64	Application	247 KB	No	495 KB	51%	30-03-2023 16:57
PsInfo	Application	223 KB	No	433 KB	49%	30-03-2023 16:57
PsInfo64	Application	257 KB	No	524 KB	52%	30-03-2023 16:57
pskill	Application	200 KB	No	382 KB	48%	30-03-2023 16:57
pskill64	Application	235 KB	No	466 KB	50%	30-03-2023 16:57
pslist	Application	110 KB	No	213 KB	49%	30-03-2023 16:58
pslist64	Application	129 KB	No	261 KB	51%	30-03-2023 16:58
PsLoggedon	Application	73 KB	No	149 KB	51%	28-06-2016 09:51
PsLoggedon64	Application	80 KB	No	167 KB	53%	28-06-2016 09:49
psloglist	Application	163 KB	No	306 KB	47%	30-03-2023 16:58
psloglist64	Application	188 KB	No	370 KB	50%	30-03-2023 16:58
pspasswd	Application	117 KB	No	217 KB	47%	30-03-2023 16:58
pspasswd64	Application	135 KB	No	265 KB	50%	30-03-2023 16:58
psping	Application	138 KB	No	281 KB	52%	30-03-2023 16:57
psping64	Application	152 KB	No	339 KB	56%	30-03-2023 16:57
PsService	Application	136 KB	No	262 KB	49%	30-03-2023 16:58
PsService64	Application	157 KB	No	315 KB	51%	30-03-2023 16:58
psshutdown	Application	338 KB	No	675 KB	51%	30-03-2023 16:57
psshutdown64	Application	381 KB	No	791 KB	52%	30-03-2023 16:57
pssuspend	Application	201 KB	No	384 KB	48%	30-03-2023 16:58

6. RegMon (Note: Replaced by Process Monitor)

- **Purpose:** Real-time monitoring of Registry access.
- **Status:** Now merged into **Process Monitor**.
- **Use Case:**
 - Debug registry reads/writes during software installs.
 - Identify which keys are modified by applications.
- **Example:**

- Monitor what registry keys an installer touches during execution.
- **Replaced by:** Use ProcMon instead, with filters for Operation = RegSetValue, etc.

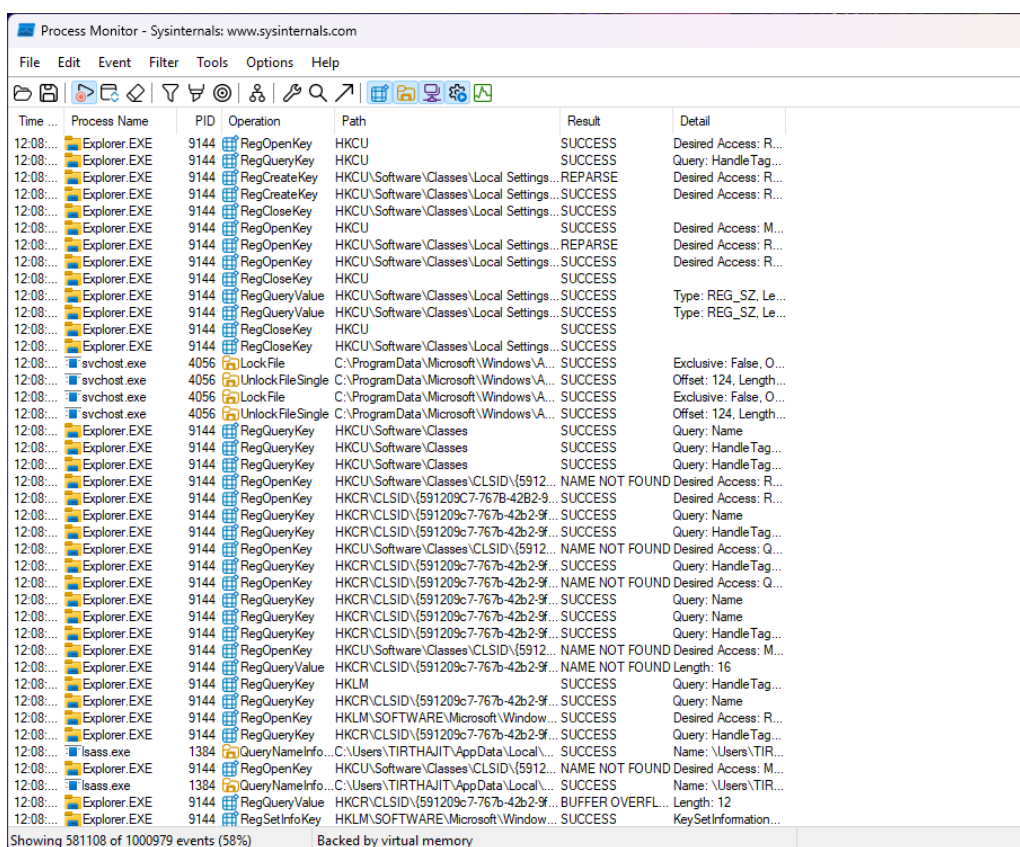
RegMon v7.04

03/24/2021

By Mark Russinovich

Published: November 1, 2006

RegMon and FileMon are no longer available for download. They have been replaced by [Process Monitor](#) on versions of Windows starting with Windows 2000 SP4, Windows XP SP2, Windows Server 2003 SP1, and Windows Vista.

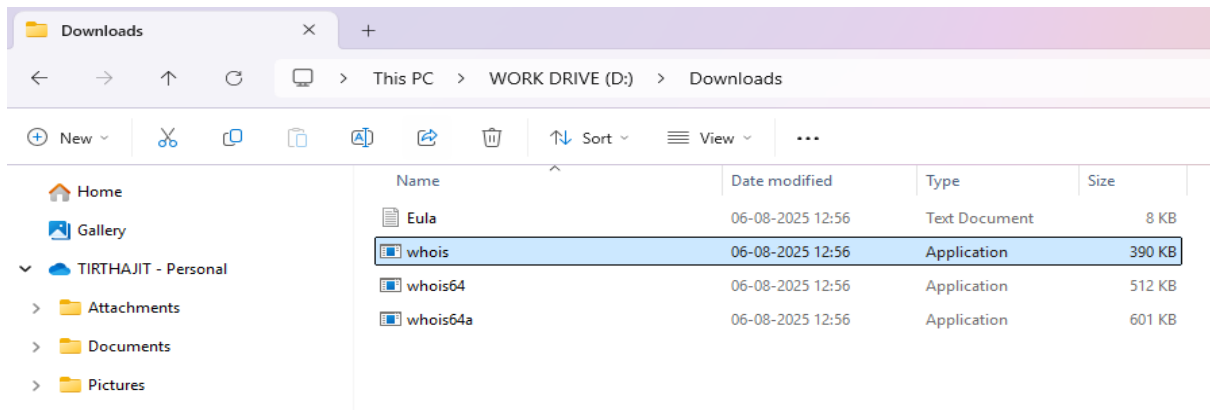


Time ...	Process Name	PID	Operation	Path	Result	Detail
12:08...	Explorer.EXE	9144	RegOpenKey	HKCU	SUCCESS	Desired Access: R...
12:08...	Explorer.EXE	9144	RegQueryValue	HKCU	SUCCESS	Query: HandleTag...
12:08...	Explorer.EXE	9144	RegCreateKey	HKCU\Software\Classes\Local Settings...	REPARSE	Desired Access: R...
12:08...	Explorer.EXE	9144	RegCreateKey	HKCU\Software\Classes\Local Settings...	SUCCESS	Desired Access: R...
12:08...	Explorer.EXE	9144	RegCloseKey	HKCU\Software\Classes\Local Settings...	SUCCESS	
12:08...	Explorer.EXE	9144	RegOpenKey	HKCU	SUCCESS	Desired Access: M...
12:08...	Explorer.EXE	9144	RegOpenKey	HKCU\Software\Classes\Local Settings...	REPARSE	Desired Access: R...
12:08...	Explorer.EXE	9144	RegOpenKey	HKCU\Software\Classes\Local Settings...	SUCCESS	Desired Access: R...
12:08...	Explorer.EXE	9144	RegCloseKey	HKCU	SUCCESS	
12:08...	Explorer.EXE	9144	RegQueryValue	HKCU\Software\Classes\Local Settings...	SUCCESS	Type: REG_SZ, Le...
12:08...	Explorer.EXE	9144	RegQueryValue	HKCU\Software\Classes\Local Settings...	SUCCESS	Type: REG_SZ, Le...
12:08...	Explorer.EXE	9144	RegCloseKey	HKCU	SUCCESS	
12:08...	Explorer.EXE	9144	RegCloseKey	HKCU\Software\Classes\Local Settings...	SUCCESS	
12:08...	svchost.exe	4056	LockFile	C:\ProgramData\Microsoft\Windows\VA...	SUCCESS	Exclusive: False, O...
12:08...	svchost.exe	4056	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\VA...	SUCCESS	Offset: 124, Length...
12:08...	svchost.exe	4056	LockFile	C:\ProgramData\Microsoft\Windows\VA...	SUCCESS	Exclusive: False, O...
12:08...	svchost.exe	4056	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\VA...	SUCCESS	Offset: 124, Length...
12:08...	Explorer.EXE	9144	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:08...	Explorer.EXE	9144	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:08...	Explorer.EXE	9144	RegOpenKey	HKCU\Software\Classes\CLSID\{5912...	NAME NOT FOUND	Desired Access: R...
12:08...	Explorer.EXE	9144	RegOpenKey	HKCR\CLSID\{591209C7-767B-42B2-9...	SUCCESS	Desired Access: R...
12:08...	Explorer.EXE	9144	RegQueryKey	HKCR\CLSID\{591209C7-767B-42B2-9...	SUCCESS	Query: Name
12:08...	Explorer.EXE	9144	RegQueryKey	HKCR\CLSID\{591209C7-767B-42B2-9...	SUCCESS	Query: HandleTag...
12:08...	Explorer.EXE	9144	RegOpenKey	HKCU\Software\Classes\CLSID\{5912...	NAME NOT FOUND	Desired Access: Q...
12:08...	Explorer.EXE	9144	RegQueryKey	HKCR\CLSID\{591209C7-767B-42B2-9...	SUCCESS	Query: HandleTag...
12:08...	Explorer.EXE	9144	RegOpenKey	HKCR\CLSID\{591209C7-767B-42B2-9...	NAME NOT FOUND	Desired Access: Q...
12:08...	Explorer.EXE	9144	RegQueryKey	HKCR\CLSID\{591209C7-767B-42B2-9...	SUCCESS	Query: Name
12:08...	Explorer.EXE	9144	RegQueryKey	HKCR\CLSID\{591209C7-767B-42B2-9...	SUCCESS	Query: Name
12:08...	Explorer.EXE	9144	RegOpenKey	HKCU\Software\Classes\CLSID\{5912...	NAME NOT FOUND	Desired Access: M...
12:08...	Explorer.EXE	9144	RegQueryValue	HKCR\CLSID\{591209C7-767B-42B2-9...	NAME NOT FOUND	Length: 16
12:08...	Explorer.EXE	9144	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
12:08...	Explorer.EXE	9144	RegQueryKey	HKCR\CLSID\{591209C7-767B-42B2-9...	SUCCESS	Query: Name
12:08...	Explorer.EXE	9144	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...
12:08...	Explorer.EXE	9144	RegQueryKey	HKCR\CLSID\{591209C7-767B-42B2-9...	SUCCESS	Query: HandleTag...
12:08...	Isass.exe	1384	QueryNameInfo...	C:\Users\TIRTHAJIT\AppData\Local\...	SUCCESS	Name: \Users\TIR...
12:08...	Isass.exe	1384	RegOpenKey	HKCU\Software\Classes\CLSID\{5912...	NAME NOT FOUND	Desired Access: M...
12:08...	Isass.exe	1384	QueryNameInfo...	C:\Users\TIRTHAJIT\AppData\Local\...	SUCCESS	Name: \Users\TIR...
12:08...	Explorer.EXE	9144	RegQueryValue	HKCR\CLSID\{591209C7-767B-42B2-9...	BUFFER OVERFL...	Length: 12
12:08...	Explorer.EXE	9144	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	KeySetInformation...

Showing 581108 of 1000979 events (58%) Backed by virtual memory

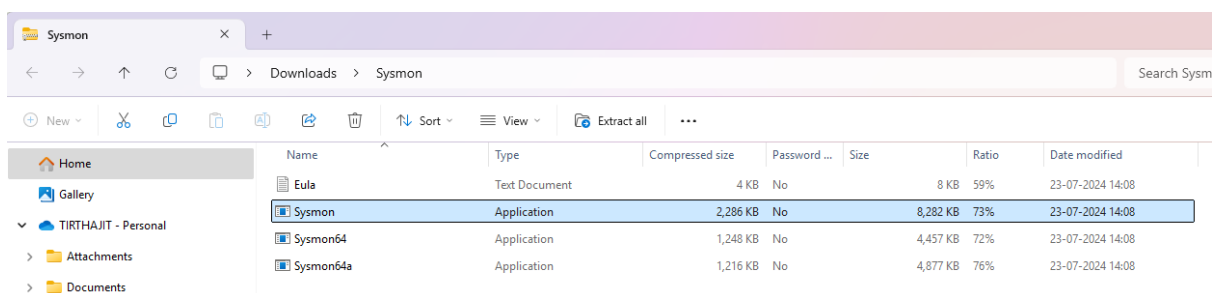
7. Whois

- **Purpose:** Query domain registration details.
- **Tool Type:** Command-line tool.
- **Use Case:**
 - Troubleshooting suspicious network connections or domains,
 - Identifying the owner of a domain or IP.



8. Sysmon (System Monitor)

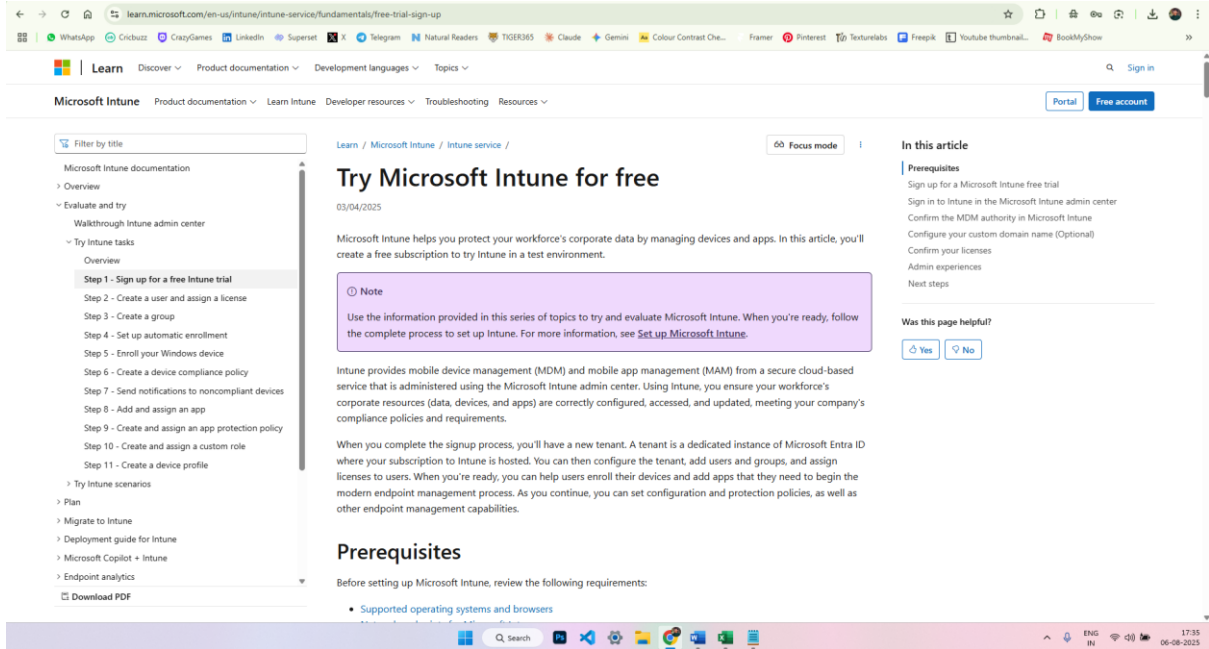
- **Purpose:** Logs detailed system activity to the Windows Event Log.
- **Tool Type:** Service + Driver
- **Use Case:**
 - Monitor:
 - Process creation
 - Network connections
 - File creation time changes
 - Registry modifications
 - Used in security analytics and threat detection.



➤ Intune Free trial Subscription - How to enrol

1. Access the Intune Setup Account Page:

- Open a web browser and go to the Intune setup account page.



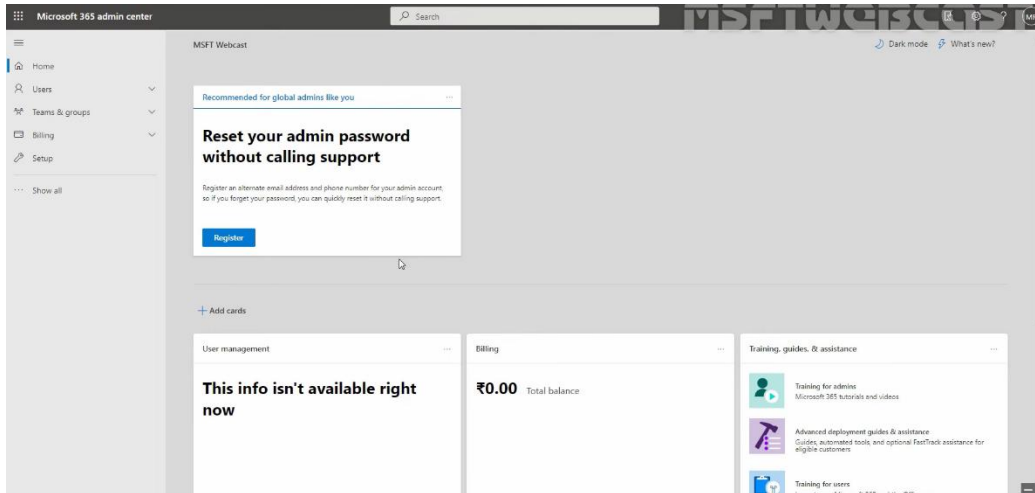
2. Sign Up or Sign In:

- **For new users:** Enter your email address and click "Next." Follow the prompts to create a new account and provide the necessary information.
- **For existing users:** Sign in with your existing work or school account.

A screenshot of the Microsoft Intune Plan 1 Trial sign-up page. The page has a progress bar at the top with three steps: "About you", "Sign-in details", and "Complete & get started". The "About you" step is currently active. The main heading is "Let's get you started". Below this, there is a text prompt: "Enter your work or school email address, we'll check if you need to create a new account for Microsoft Intune Plan 1 Trial." A text input field for "Email" is shown with a red border and a red error message "This is required" below it. A blue "Next" button is positioned below the input field. On the right side of the page, there is a section titled "Microsoft Intune Plan 1 Trial" which includes the text "Signing up for your trial", "25 users allowed in 1-month free trial.", and "Trial includes same features as the paid product." Below this is a "Product highlights" section with a list of four bullet points, each preceded by a green checkmark, describing the benefits of the trial.

3. Complete the Sign-Up Process:

- If creating a new account, you'll be asked to verify your email address and potentially provide additional information like your name, company details, and region.
- After signing up or signing in, you'll be directed to the Microsoft 365 Admin Center.



4. Considerations for Existing Work or School Accounts:

- If you're using an existing work or school account, you might need to add Intune to your existing subscription.
- If you plan to use your organization's custom domain name or synchronize with on-premises Active Directory, you might need to close the browser window after the initial setup and configure these aspects separately.

5. Accessing Intune After Enrollment:

- Once the free trial is set up, you can access the Microsoft Intune Admin Center to manage the service.
- You can use any device with a supported browser to sign in.

