**Email:** meghanabadgujar07@gmail.com

**Name:** Meghana Samadhan Badgujar  
**Batch Name:** WiproNGA\_DWS\_B5\_25VID2550

**User ID:** 34737

**Batch ID:** 25VID2550

**Date:** 6th August 2025

**Assignment Topic:**

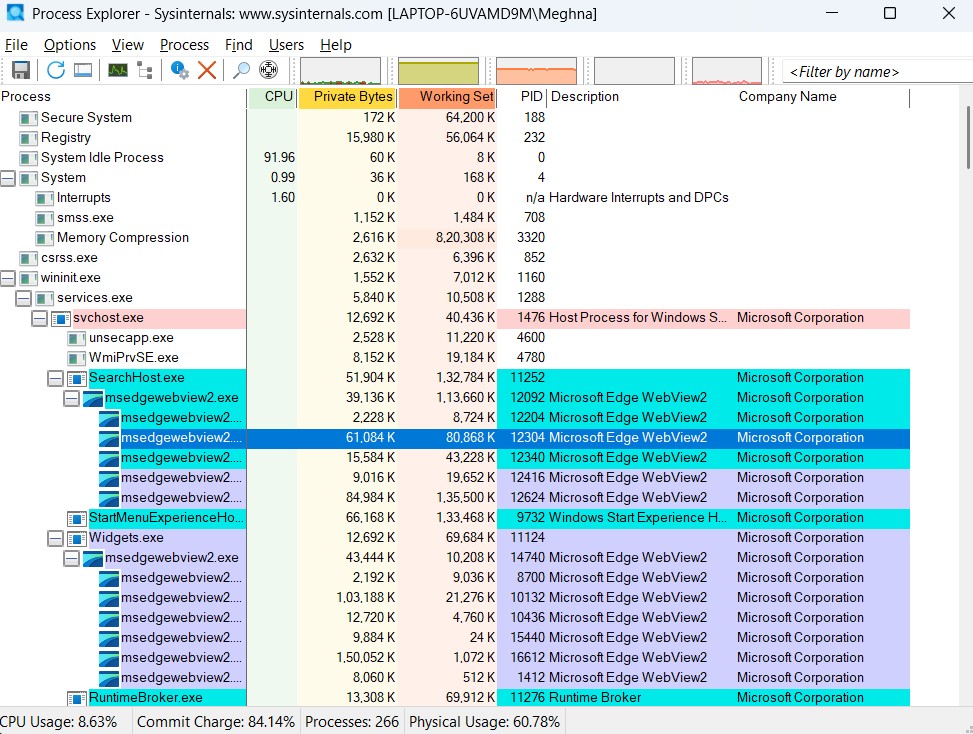
***Mention all windows tools for debugging with screenshots and steps to create for Microsoft intune  portal***

* **Using Windows Tools for Debugging:**

# 1. Process Explorer

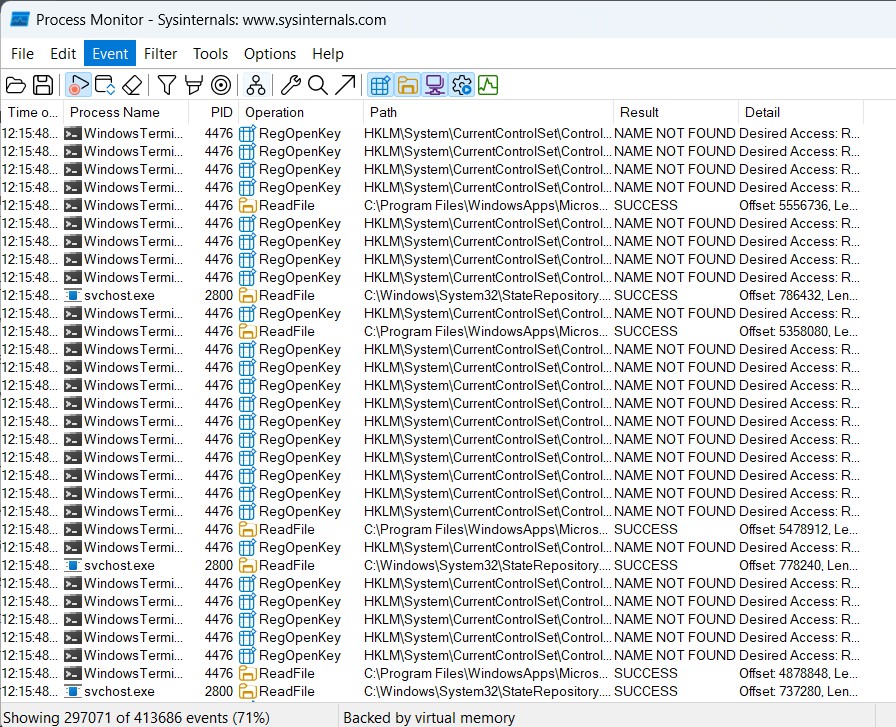
An advanced version of Task Manager that shows detailed information on running processes like memory usage, handles, parent-child relationships, and loaded DLLs.

Use case: Detecting malware, investigating resource-hogging apps.



# 2. Process Monitor (Real-Time System Monitoring Tool)

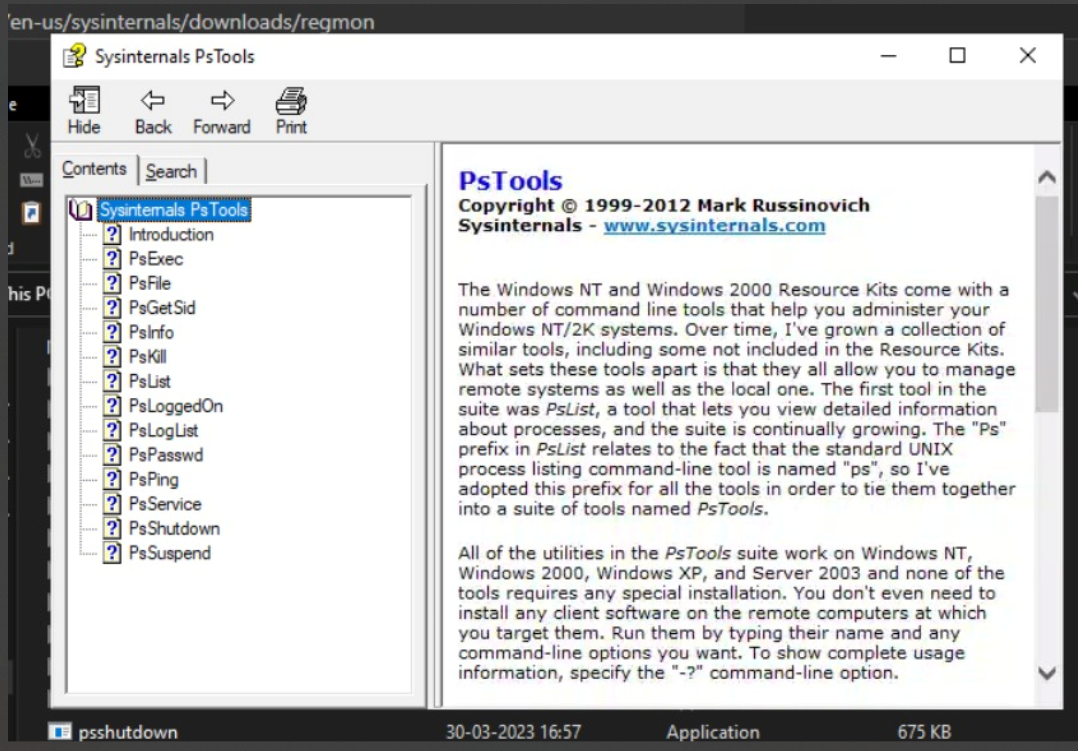
Combines the features of RegMon and FileMon to monitor real-time file system, registry, and process/thread activity on a Windows system. Use case: Troubleshooting application errors, identifying permission issues, tracking what an app is doing behind the scenes.



# 3. PSTools Suite (Remote Management Toolset)

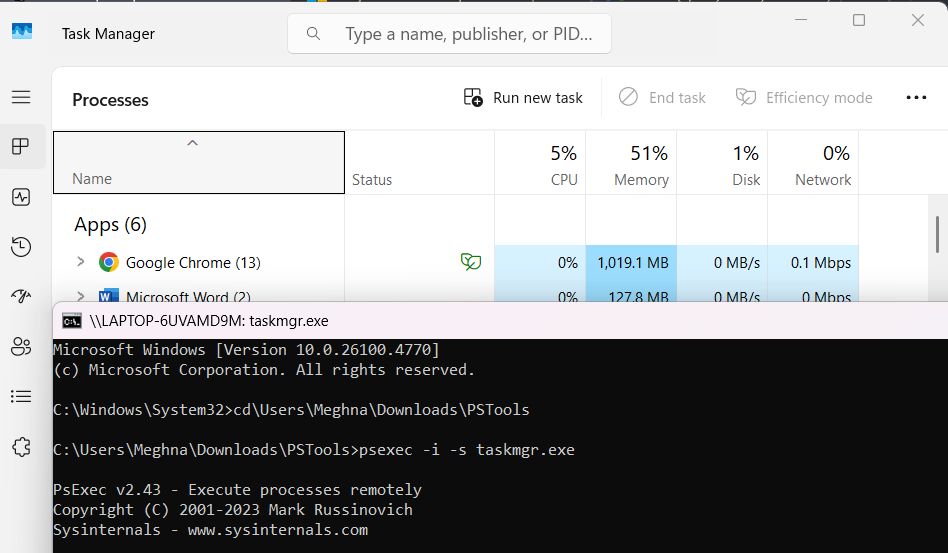
A collection of lightweight command-line tools like PsKill, PsList, PsShutdown, etc., to manage local and remote systems.

Use case: Process control, system shutdowns, system info retrieval.



# 4. PsExec (Remote Execution Tool)

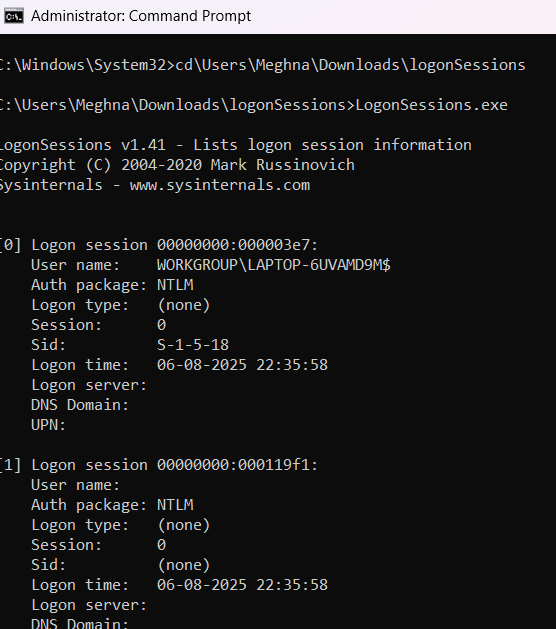
Allows execution of programs or commands on remote machines. Use case: Remote troubleshooting, software deployment, or command execution without logging in physically.



# 4. LogonSessions (Logon Access Tool)

Displays all currently active logon sessions on a system. Shows details like logon ID, user name, session type, and logon time.

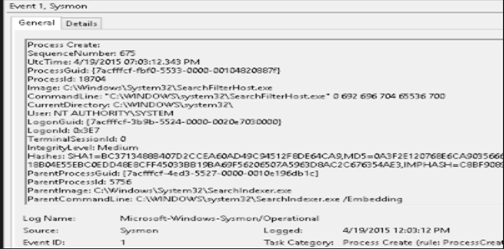
Use case: Identifying unauthorized or suspicious login activity.



# 5. SysMon (Advanced System Monitoring Tool)

Logs detailed event data such as process creation, network connections, and file changes to the Windows Event Log.

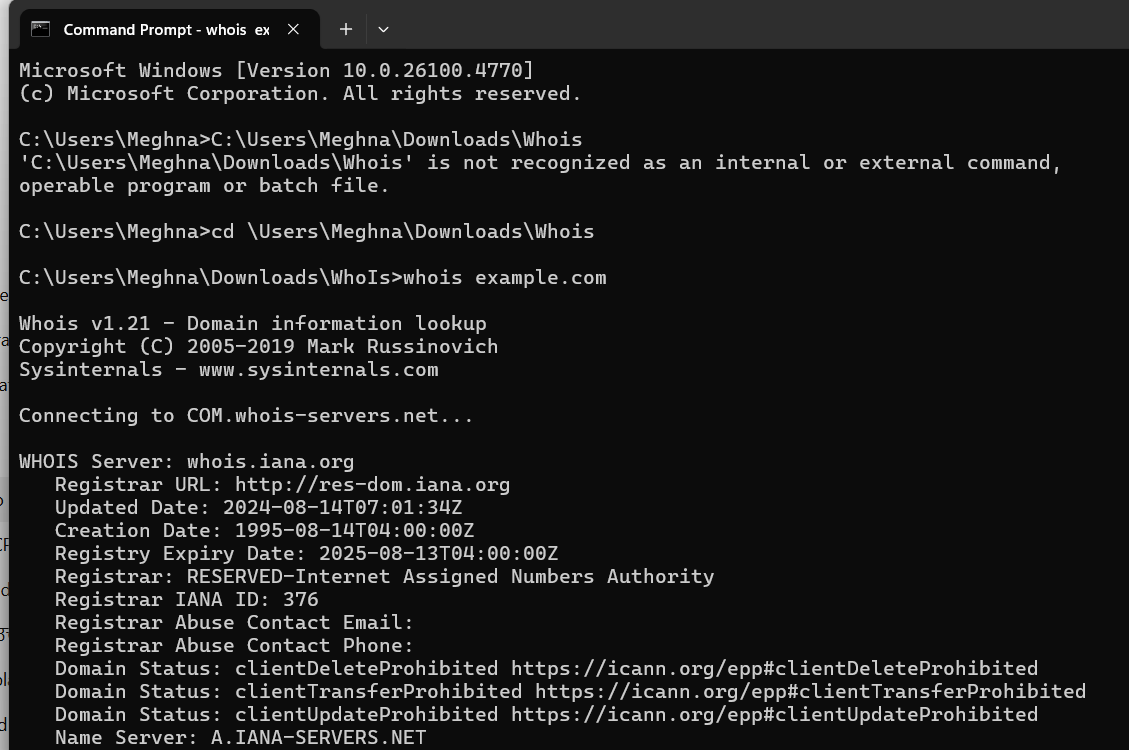
Use case: Security monitoring, digital forensics, and malware tracking.



# 6. Whois (Network Investigation Tool)

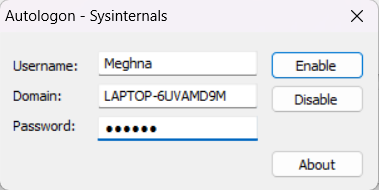
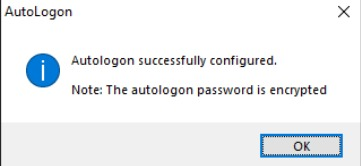
Fetches domain registration info.

Use case: Identifying suspicious websites or checking domain owners in security investigations.



# 7. Autologon (Login Configuration Tool)

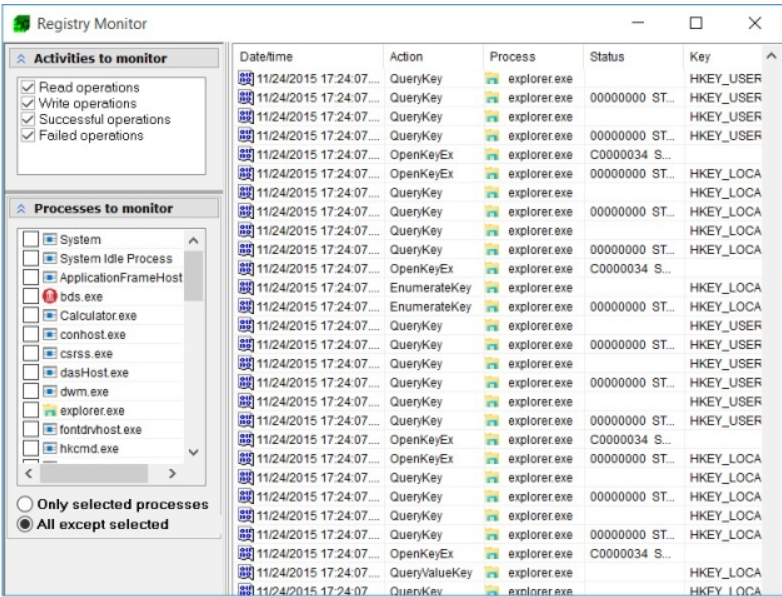
Configures automatic login using stored credentials. Useful for testing environments, kiosks, and labs where manual login is not necessary. Credentials are stored securely in the registry.

# 8. RegMon (Registry Monitoring Tool)

Monitors real-time access to Windows Registry. Shows which apps are reading, writing, or deleting registry keys.

Use case: Diagnosing app behavior or registry-related errors.



* **Microsoft Intune Portal**
* **Setting Up Microsoft Intune Portal**

1. Log in to Microsoft Intune Admin Center
2. Navigate to **Devices > Configuration profiles**
3. Click **+ Create profile**
4. Platform: Windows 10 and later  
   Profile Type: Settings catalog
5. Enter profile name and description
6. Click **Next**, add configuration settings
7. Assign it to users or groups
8. Review + Create

