Batch Information:

- **Batch Start Date: 2025-08-04**
- **Batch Name: WiproNGA_DWS_B5_25VID2550**
- **First Name: Kamran**
- **Last Name: Akmal**
- **User ID: 34958**
- **Batch ID: 25VID2557**

Assignments

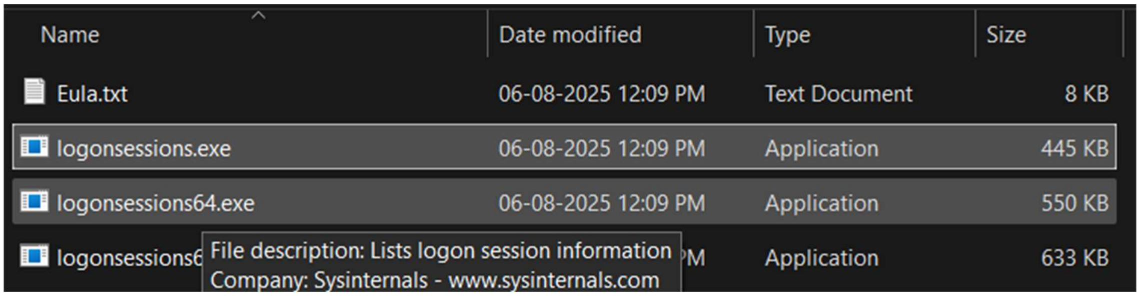
Topics-Using Windows Tools for Debugging: LogonSessions, Autologon, Process Explorer, Psexec, PSTools, RegMon, Whois, SysMon

Introduction

In Windows environments, troubleshooting application issues, installations, and security events often requires specialized utilities. The Sysinternals suite and other Windows tools provide deep insights into processes, registry activity, network connections, and system behavior. This assignment explains key tools including LogonSessions, Autologon, Process Explorer, PsExec, PsTools, RegMon, Wh**ois, and Sysmon, along with their functionalities and use cases in debugging.**

1. LogonSessions

- **Purpose:** Displays information about all active logon sessions on a computer.
- **Key Details:**
  - Shows logon session IDs, usernames, logon type (interactive, service, remote), and authentication method.
  - Useful for auditing current and past user sessions.
- **Use in Debugging:**
  - Detects orphaned sessions that might lock resources.
  - Helps trace suspicious logins during incident response.

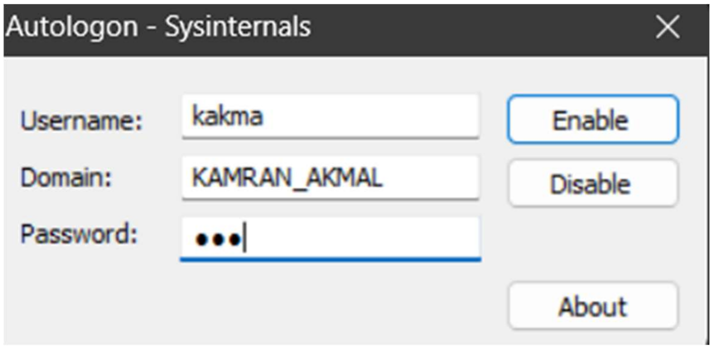


Name	Date modified	Type	Size
Eula.txt	06-08-2025 12:09 PM	Text Document	8 KB
logonsessions.exe	06-08-2025 12:09 PM	Application	445 KB
logonsessions64.exe	06-08-2025 12:09 PM	Application	550 KB
logonsessions6	PM	Application	633 KB

File description: Lists logon session information
Company: Sysinternals - www.sysinternals.com

2. Autologon

- **Purpose**: Configures Windows to automatically log in with specified credentials.
- **Key Details:**
  - Credentials are encrypted in the registry and used during system startup.
  - Removes the need for manual user input at every reboot.
- **Use in Debugging:**
  - Automates repeated testing cycles after system reboots in packaging environments.
  - Speeds up virtual machine testing scenarios where manual logon delays progress.



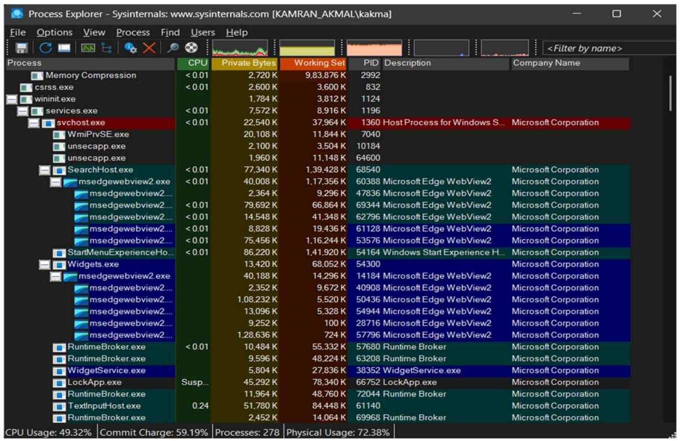
Username: kakma

Domain: KAMRAN_AKMAL

Password: •••

3. Process Explorer

- **Purpose:** Advanced process management tool, often referred to as "Task Manager on steroids."
- **Key Details:**
  - Displays process hierarchy, open handles, loaded DLLs, CPU/memory usage, and verified signatures.
  - Highlights recently launched or suspicious processes in real time.
- **Use in Debugging:**
  - Identifies which process is locking a file or preventing an installer from running.
  - Checks for unsigned binaries or malicious software.


Process Explorer - Sysinternals: www.sysinternals.com [KAMRAN_AKMAL\kakma]
File
Options
View
Process
Find
Users
Help
<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Memory Compression	< 0.01	2,720 K	9,83,876 K	2992		
csrss.exe	< 0.01	2,600 K	3,600 K	832		
wininit.exe		1,784 K	3,812 K	1124		
services.exe	< 0.01	7,572 K	8,916 K	1196		
svchost.exe	< 0.01	22,540 K	37,964 K	1360	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		20,108 K	11,844 K	7040		
unsecapp.exe		2,100 K	3,504 K	10184		
unsecapp.exe		1,960 K	11,148 K	64600		
SearchHost.exe	< 0.01	77,340 K	1,39,428 K	68540		Microsoft Corporation
msedgewebview2.exe	< 0.01	40,008 K	1,17,356 K	60388	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		2,364 K	9,296 K	47836	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....	< 0.01	79,692 K	66,864 K	69344	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....	< 0.01	14,548 K	41,348 K	62796	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....	< 0.01	8,828 K	19,436 K	61128	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....	< 0.01	75,456 K	1,16,244 K	53576	Microsoft Edge WebView2	Microsoft Corporation
StartMenuExperienceHo...	< 0.01	86,220 K	1,41,920 K	54164	Windows Start Experience H...	Microsoft Corporation
Widgets.exe		13,420 K	68,052 K	54300		Microsoft Corporation
msedgewebview2.exe		40,188 K	14,296 K	14184	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		2,352 K	9,672 K	40908	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		1,08,232 K	5,520 K	50436	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		13,096 K	5,328 K	54944	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		9,252 K	100 K	28716	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		1,28,636 K	724 K	57796	Microsoft Edge WebView2	Microsoft Corporation
RuntimeBroker.exe	< 0.01	10,484 K	55,332 K	57680	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		9,596 K	48,224 K	63208	Runtime Broker	Microsoft Corporation
WidgetService.exe		5,804 K	27,836 K	38352	WidgetService.exe	Microsoft Corporation
LockApp.exe	Susp...	45,292 K	78,340 K	66752	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		11,964 K	48,760 K	72044	Runtime Broker	Microsoft Corporation
TextInputHost.exe	0.24	51,780 K	84,448 K	61140		Microsoft Corporation
RuntimeBroker.exe		2,452 K	14,064 K	69968	Runtime Broker	Microsoft Corporation

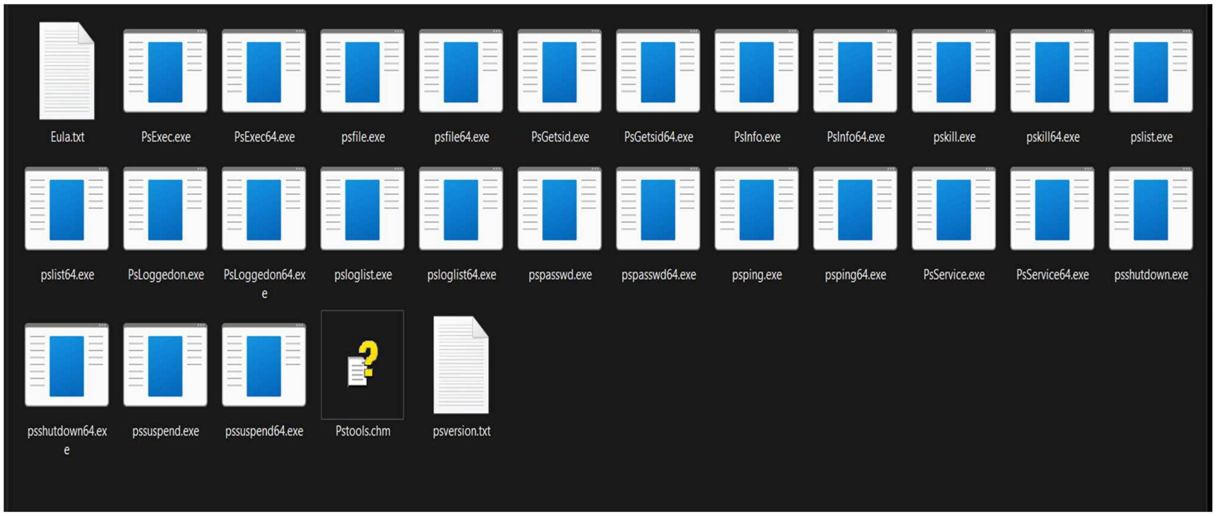
CPU Usage: 49.32% | Commit Charge: 59.19% | Processes: 278 | Physical Usage: 72.38%

4. PsExec

- **Purpose:** Executes processes on remote systems or under different user contexts.
- **Key Details:**
  - Allows launching commands as SYSTEM, administrator, or another user.
  - Does not require manual login to the remote machine.
- **Use in Debugging:**
  - Testing MSI packages under SYSTEM context (similar to SCCM deployment).
  - Troubleshooting permission-related installation failures.

5. PsTools

- **Purpose:** A collection of command-line tools for remote administration.
- **Key Utilities in the Suite:**
  - **PsList:** View processes on remote systems.
  - **PsKill**: Terminate processes remotely.
  - **PsLoggedOn:** View logged-on users.
  - **PsShutdown:** Reboot or shut down systems remotely.
- **Use in Debugging:**
  - Manage processes and sessions across multiple machines in a testing lab.
  - Quickly restart services or kill problematic processes blocking an installation.

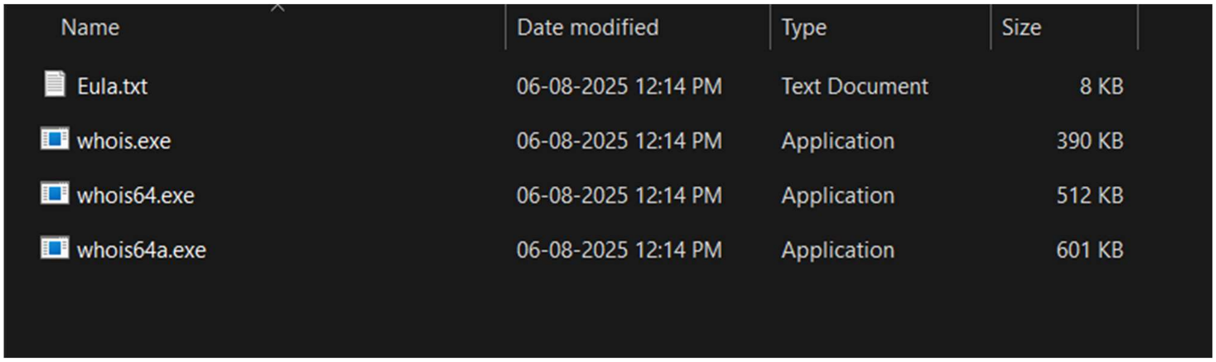


6. RegMon (Registry Monitor)

- **Purpose:** Monitors and logs real-time registry activity by applications and processes.
- **Key Details:**
    - Displays registry keys accessed, modified, or created by each process.
    - Supports filters for processes and paths to narrow down data.
- **Use in Debugging:**
    - Tracks registry changes during installation to understand application dependencies.
    - Identifies access denied errors causing setup failures.
- **Note:** RegMon is now merged into Process Monitor (ProcMon), which combines registry and file monitoring.

7. Whois

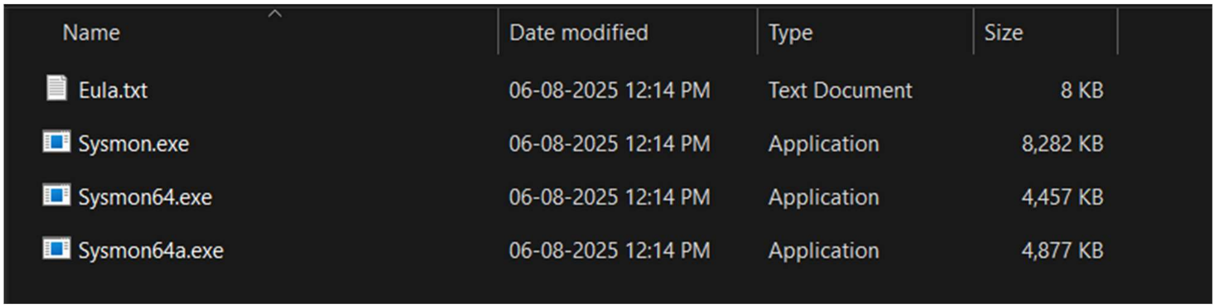
- **Purpose:** Looks up registration details of a domain.
- **Key Details:**
    - Provides information on domain ownership, registrar, and contact details.
    - Helps verify if a domain is legitimate.
- **Use in Debugging:**
    - Useful in security analysis when applications connect to suspicious external servers.
    - Validates network endpoints used by software.



Name	Date modified	Type	Size
Eula.txt	06-08-2025 12:14 PM	Text Document	8 KB
whois.exe	06-08-2025 12:14 PM	Application	390 KB
whois64.exe	06-08-2025 12:14 PM	Application	512 KB
whois64a.exe	06-08-2025 12:14 PM	Application	601 KB

8. Sysmon (System Monitor)

- **Purpose**: A Windows service and driver for logging detailed system activity into Event Viewer.
- **Key Details:**
  - Records process creation (with hashes, command line), network connections, and file creation events.
  - Supports custom configuration for filtering events of interest.
- **Use in Debugging:**
  - Tracks which processes and files are created by an installer or application.
  - Detects unexpected or malicious activity that standard event logs miss.



Name	Date modified	Type	Size
Eula.txt	06-08-2025 12:14 PM	Text Document	8 KB
Sysmon.exe	06-08-2025 12:14 PM	Application	8,282 KB
Sysmon64.exe	06-08-2025 12:14 PM	Application	4,457 KB
Sysmon64a.exe	06-08-2025 12:14 PM	Application	4,877 KB

Conclusion

Each of these tools plays a vital role in application packaging, deployment, and security analysis. From monitoring process and registry activity (Process Explorer, RegMon, Sysmon) to managing remote executions (PsExec, PsTools) and session tracking (LogonSessions), they provide comprehensive visibility into Windows systems. Mastering these utilities helps in resolving installation issues, diagnosing application failures, and improving overall troubleshooting efficiency.