





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, Whois, and Sysmon, along with their functionalities and use cases in debugging.
-

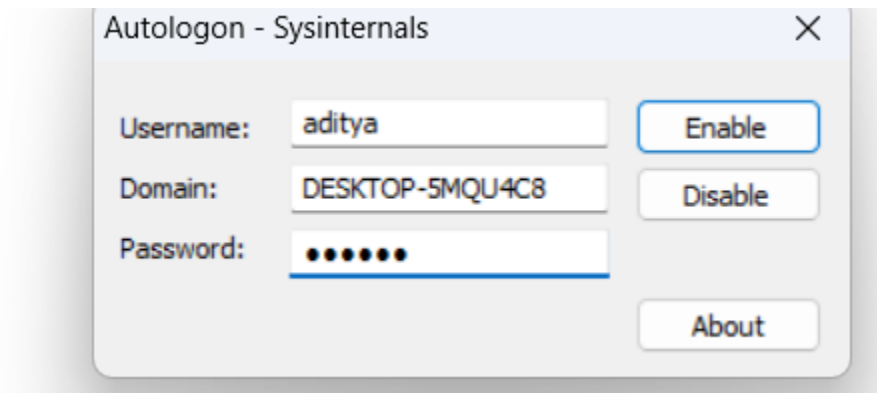
1. LogonSessions

- 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.

 Eula.txt	8/6/2025 4:06 PM	Text Document	8 KB
 logonsessions.exe	8/6/2025 4:06 PM	Application	445 KB
 logonsessions64.exe	8/6/2025 4:06 PM	Application	550 KB
 logonsessions64a.exe	8/6/2025 4:06 PM	Application	633 KB

2. Autologon

- Purpose: Configures Windows to automatically log in with specified credentials.
- Key Details:
 - Automates repeated testing cycles after system reboots in packaging environments.
 - Speeds up virtual machine testing scenarios where manual logon delays progress.
- Use in Debugging:
 - Automates repeated testing cycles after system reboots in packaging environments.
 - Speeds up virtual machine testing scenarios where manual logon delays progress.



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 [DESKTOP-5MQU4C8\Abhimanyu]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		9,840 K	55,816 K	176		
System Idle Process	65.03	60 K	8 K	0		
System	1.12	40 K	160 K	4		
Interrupts	1.68	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,136 K	412 K	520		
Memory Compression	< 0.01	2,896 K	10,11,556 K	2944		
csrss.exe	< 0.01	2,268 K	3,212 K	836		
wininit.exe		1,512 K	1,976 K	944		
services.exe	0.75	5,480 K	7,024 K	1016		
svchost.exe	< 0.01	13,844 K	25,968 K	1060	Host Process for Windows S...	Microsoft Corporation
dllhost.exe		7,524 K	13,044 K	8768	COM Surrogate	Microsoft Corporation
dllhost.exe		6,764 K	15,144 K	9208	COM Surrogate	Microsoft Corporation
SearchHost.exe	Susp...	1,99,468 K	1,16,144 K	3920		Microsoft Corporation
StartMenuExperienceHo...		71,564 K	1,33,228 K	5780	Windows Start Experience H...	Microsoft Corporation
RuntimeBroker.exe		14,732 K	47,600 K	984	Runtime Broker	Microsoft Corporation
TextInputHost.exe		78,364 K	56,860 K	9800		Microsoft Corporation
backgroundTaskHost.exe	Susp...	2,656 K	628 K	9072	Background Task Host	Microsoft Corporation
UserOOBEBroker.exe		1,924 K	5,192 K	7572	User OOBEBroker	Microsoft Corporation
WmiPrivSE.exe	3.18	21,320 K	28,136 K	10528		
unsecapp.exe		1,616 K	2,116 K	6772	Sink to receive asynchronou...	Microsoft Corporation
RuntimeBroker.exe		2,596 K	3,640 K	9312	Runtime Broker	Microsoft Corporation
Widgets.exe		13,432 K	46,956 K	9644		Microsoft Corporation
msedgewebview2.exe		39,384 K	20,280 K	10588	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2...		2,180 K	2,864 K	3364	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2...		13,120 K	8,848 K	3720	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2...		67,172 K	6,212 K	7340	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2...		8,596 K	2,952 K	6380	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2...		1,01,352 K	7,096 K	11380	Microsoft Edge WebView2	Microsoft Corporation
WidgetService.exe		5,548 K	8,568 K	7568	WidgetService.exe	Microsoft Corporation
RuntimeBroker.exe		2,188 K	2,876 K	4308	Runtime Broker	Microsoft Corporation
dllhost.exe		1,516 K	4,576 K	3708	COM Surrogate	Microsoft Corporation
RtkUWP.exe	Susp...	9,308 K	42,932 K	14152		
ApplicationFrameHoste...		13,524 K	40,828 K	13072	Application Frame Host	Microsoft Corporation
RuntimeBroker.exe		1,980 K	8,180 K	6708	Runtime Broker	Microsoft Corporation
dllhost.exe		1,540 K	10,908 K	15640	COM Surrogate	Microsoft Corporation
FileCoAuth.exe		11,524 K	26,540 K	10456	Microsoft OneDriveFile Co-A...	Microsoft Corporation
dllhost.exe		3,028 K	24,000 K	14280	COM Surrogate	Microsoft Corporation
WindowsPackageMana...		7,960 K	31,584 K	8704		
dllhost.exe		2,852 K	22,664 K	16268	COM Surrogate	Microsoft Corporation
smartscreen.exe		5,660 K	29,136 K	8900	Windows Defender SmartScr...	Microsoft Corporation
dllhost.exe		5,076 K	30,660 K	10276	COM Surrogate	Microsoft Corporation
svchost.exe	< 0.01	10,096 K	17,664 K	1152	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,952 K	4,752 K	1200	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,048 K	1,656 K	1380	Host Process for Windows S...	Microsoft Corporation

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.

Name	Date modified	Type	Size
▼ Today			
Eula	06-08-2025 12:18	Text Document	8 KB
PsExec	06-08-2025 12:18	Application	700 KB
PsExec64	06-08-2025 12:18	Application	814 KB
psfile	06-08-2025 12:18	Application	230 KB
psfile64	06-08-2025 12:18	Application	283 KB
PsGetsid	06-08-2025 12:18	Application	404 KB
PsGetsid64	06-08-2025 12:18	Application	495 KB
PsInfo	06-08-2025 12:18	Application	433 KB
PsInfo64	06-08-2025 12:18	Application	524 KB
pskill	06-08-2025 12:18	Application	382 KB
pskill64	06-08-2025 12:18	Application	466 KB
pslist	06-08-2025 12:18	Application	213 KB
pslist64	06-08-2025 12:18	Application	261 KB
psloglist	06-08-2025 12:18	Application	306 KB
psloglist64	06-08-2025 12:18	Application	370 KB
pspasswd	06-08-2025 12:18	Application	217 KB
pspasswd64	06-08-2025 12:18	Application	265 KB
PsService	06-08-2025 12:18	Application	262 KB
PsService64	06-08-2025 12:18	Application	315 KB
pssuspend	06-08-2025 12:18	Application	384 KB





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.

 Eula	06-08-2025 14:29	Text Document	8 KB
 whois	06-08-2025 14:29	Application	390 KB
 whois64	06-08-2025 14:29	Application	512 KB
 whois64a	06-08-2025 14:29	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.

 Eula	06-08-2025 17:47	Text Document	8 KB
 Sysmon	06-08-2025 17:47	Application	8,282 KB
 Sysmon64	06-08-2025 17:47	Application	4,457 KB
 Sysmon64a	06-08-2025 17:47	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.