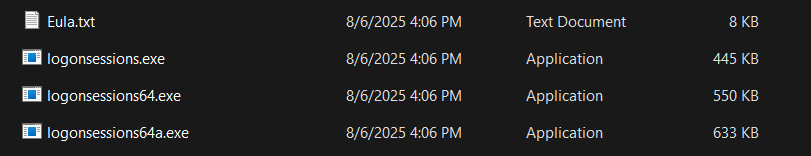
# **Topics-Using Windows Tools for Debugging: LogonSessions, Autologon, Process Explorer, Psexec, PSTools, RegMon, Whois, SysMon**

## 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.

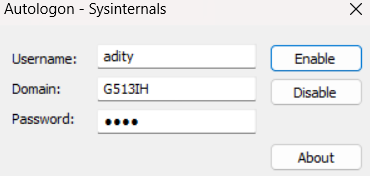
### **1. LogonSessions**

* 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.



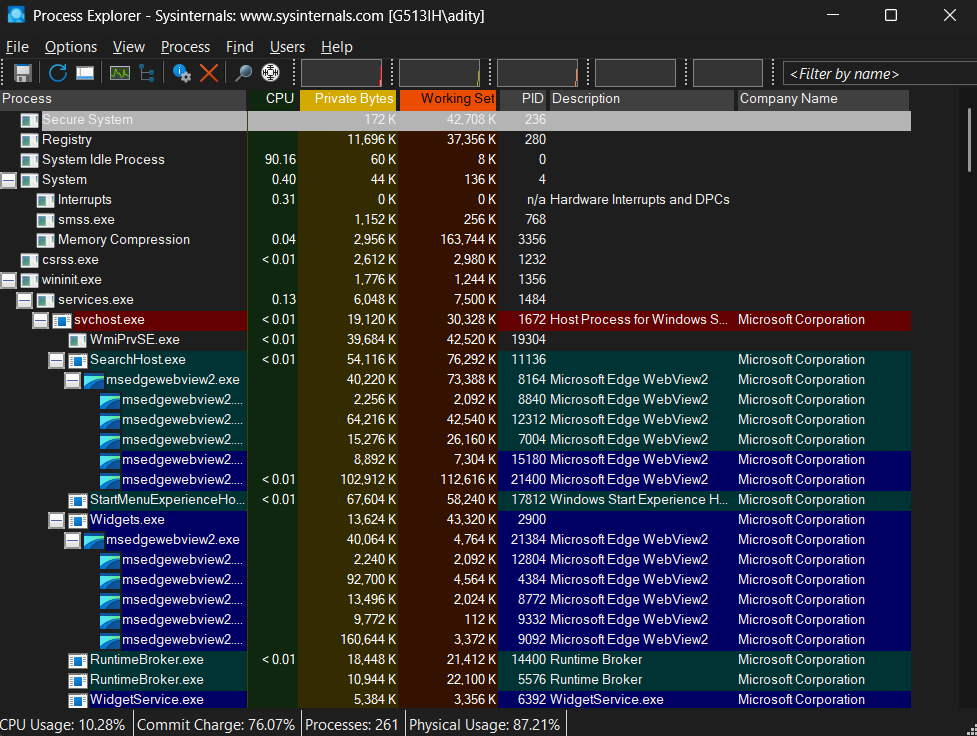
### **2. Autologon**

* 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.

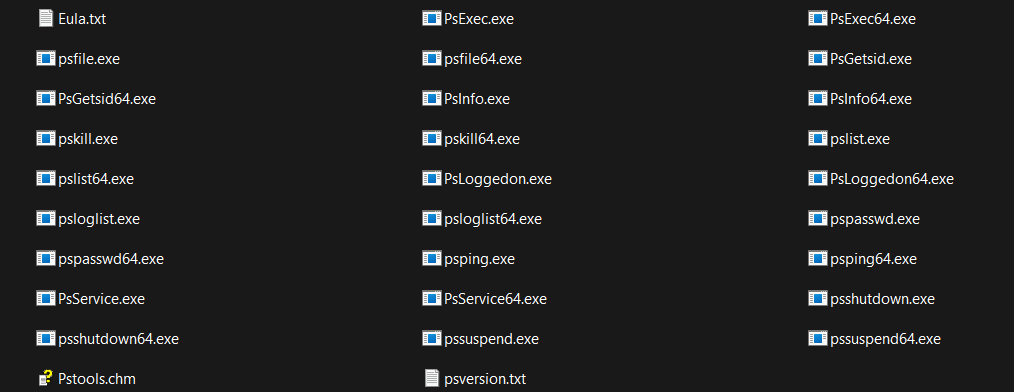


### **4. PsExec**

* Purpose: Executes processes on remote systems or under diAerent 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.

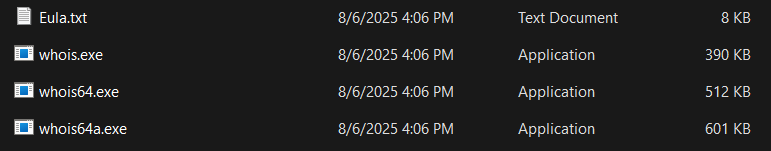


### **6. RegMon (Registry Monitor)**

* 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.

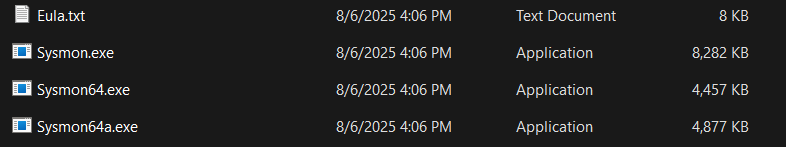
### **7. Whois**

* 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.



### **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.



### 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 eAiciency.