**WIPRO ASSIGNMENT – 2**

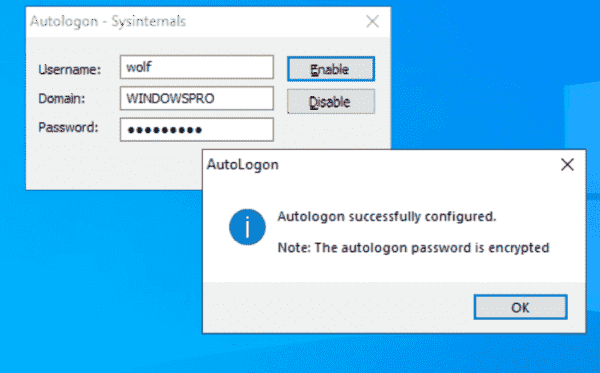
* **Submitted By:** Anuj Bose
* **User ID:** 34757
* **Batch Name:** WiproNGA\_DWS\_B5\_25VID2550
* **Date:** 6th August, 2025
* **Email ID:** anujbose01012004@gmail.com

**Windows Tools For Debugging**

These tools are also known as **Sysinternals Tools**. These Sysinternals tools are essential for Windows troubleshooting and security. Key tools include: **Autologon** for automated logins, **Process Explorer** for detailed process information, **PsExec** for remote command execution, **PSTools** for logon session management, **RegMon** for registry monitoring, **Sysmon** for system-level tracking, and **Whois** for network information.

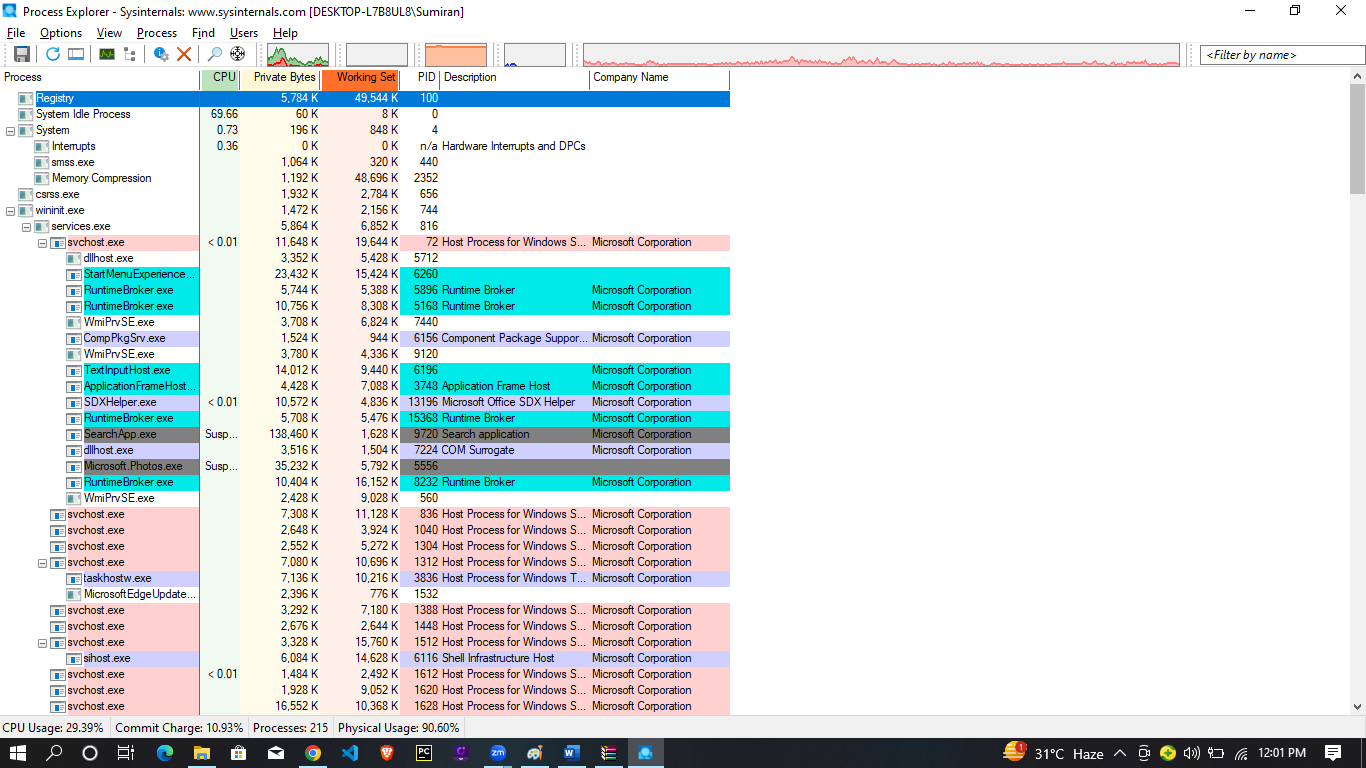
1. **Autologon**

* **Purpose:** Automates user login on Windows systems.
* **How it works:** Uses a GUI to set registry entries for auto-login with saved credentials.
* **Usage:** Ideal for headless setups or automated testing environments.

****

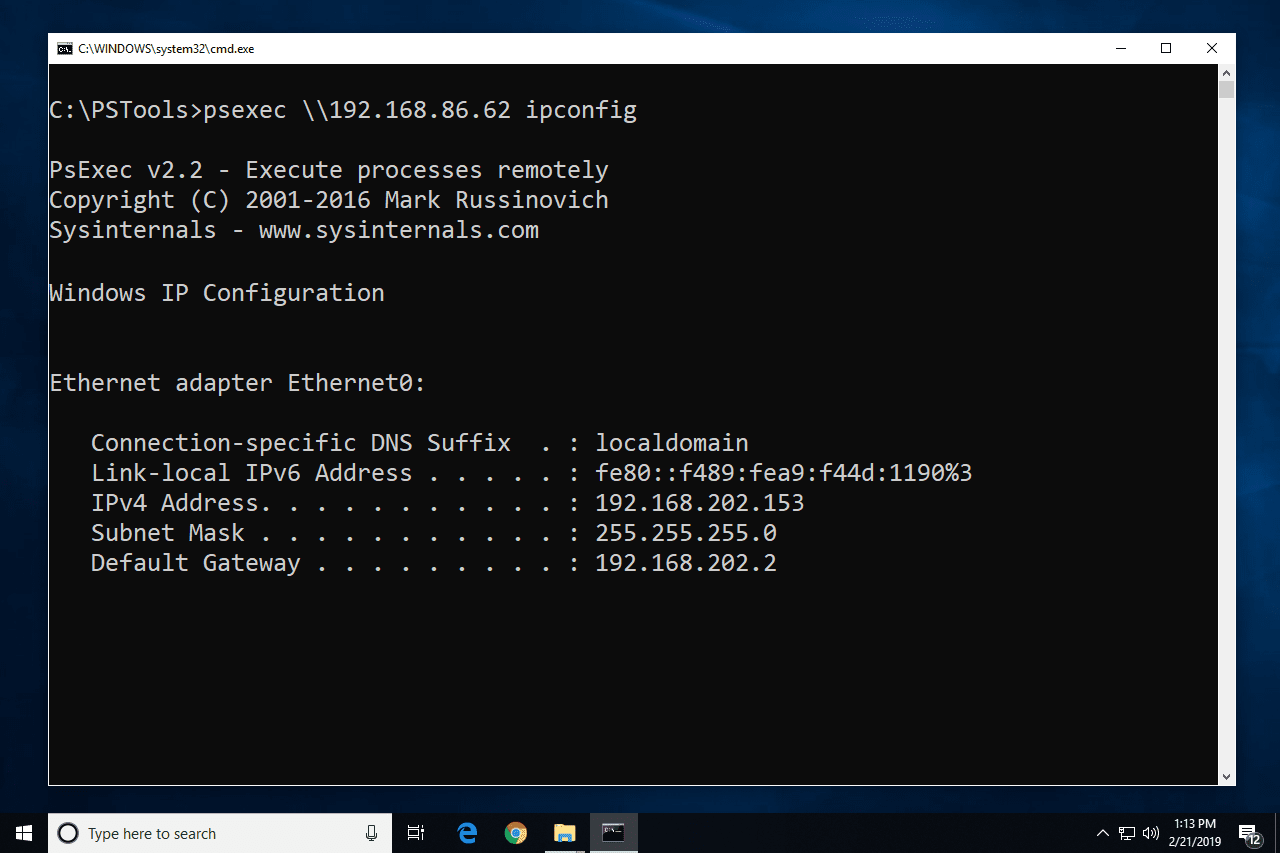
1. **Process Explorer**

* **Purpose:** Monitors and manages active processes on a system.
* **How it works:** Displays detailed data like memory usage, open files, and system handles for each process.
* **Usage:** Useful for diagnosing process issues, finding performance bottlenecks, and detecting malware.



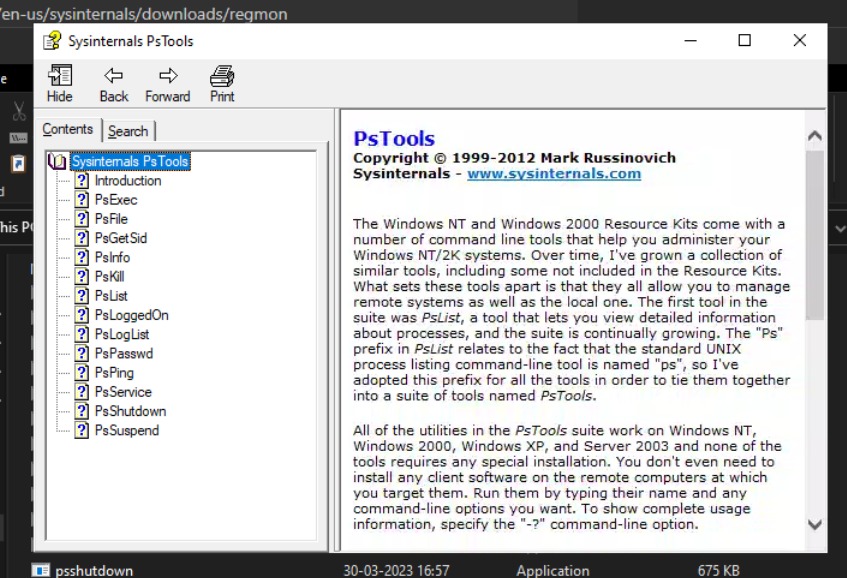
1. **PsExec**

* **Purpose:** Enables remote execution of commands and programs.
* **How it works:** Runs applications on remote systems as if executed locally.
* **Usage:** Ideal for remote management, software patching, and system troubleshooting.

****

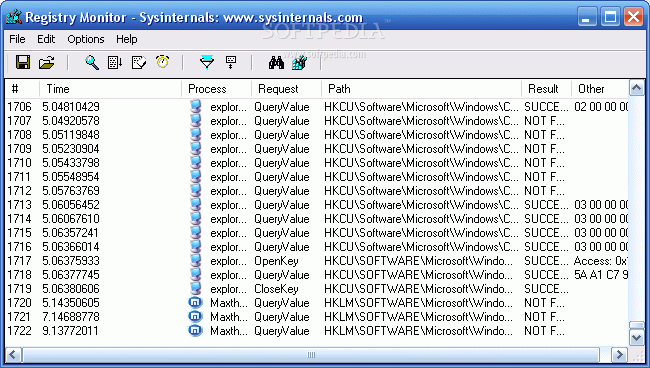
1. **PSTools**

* **Purpose:** Offers a set of command-line tools for system administration and troubleshooting.
* **How it works:** Includes utilities like PsLoggedOn, PsFile, and PsList to perform various tasks.
* **Usage:** Enables powerful admin functions on both local and remote machines.



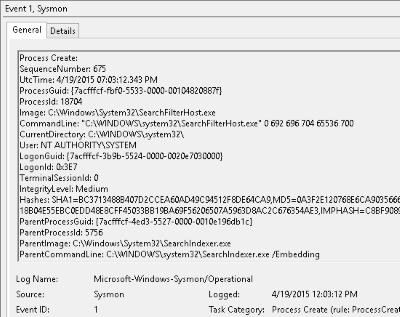
1. **RegMon**

* **Purpose:** Monitors registry access and changes in real-time.
* **How it works:** Tracks all registry activity, including reads, writes, and deletes.
* **Usage:** Useful for diagnosing registry issues, detecting suspicious apps, and investigating security problems.



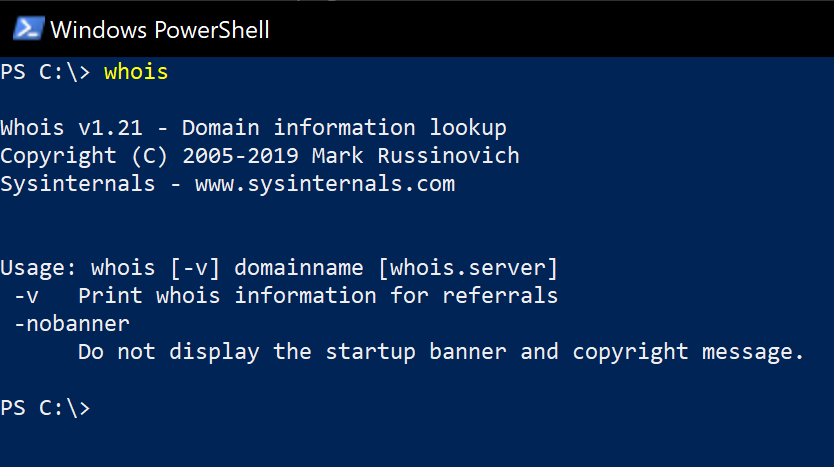
1. **Sysmon**

* **Purpose:** Monitors and logs detailed system activity as a Windows service and driver.
* **How it works:** Provides detailed information about process creations, network connections, and file access changes.
* **Usage:** Essential for security monitoring, intrusion detection, and forensic analysis.

****

1. **Whois**

* **Purpose:** A command-line tool (though not directly from Sysinternals) used to retrieve information about domain names and IP addresses.
* **How it works:** Queries a Whois database to retrieve registration details.
* **Usage:** Useful for network troubleshooting, identifying domain owners, and checking domain availability.

****

**How To Set Up Microsoft Intunes**

**1. Plan and Prepare**

* Use the Intune Planning Guide to define your goals and deployment phases.
* Understand supported platforms, browsers, and network requirements.

**2. Set Up Your Tenant**

* Sign in or create a Microsoft 365 tenant.
* Configure a custom domain (optional but recommended).

**3. Add and Organize Users**

* Add users manually or sync them via Microsoft Entra Connect.
* Use groups to assign policies and apps based on roles or departments.

**4. Assign Licenses**

* Assign Intune licenses to users; a free trial is available for up to 25 users.

**5. Configure Roles and Permissions**

* Use Role-Based Access Control (RBAC) to manage who can do what.
* Use scope tags to control access visibility for different admins.

**6. Set MDM Authority**

* Confirm that Microsoft Intune is selected as your Mobile Device Management (MDM) authority — a required step to start managing devices.

