**ASSIGNMENT**

Name: Rahul kumar

Batch Start Date: 2025-08-04

Batch Name: WiproNGA\_DWS\_B5\_25VID2550

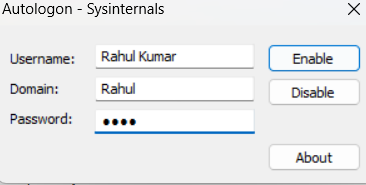
User ID: 34722

* Sysinternals

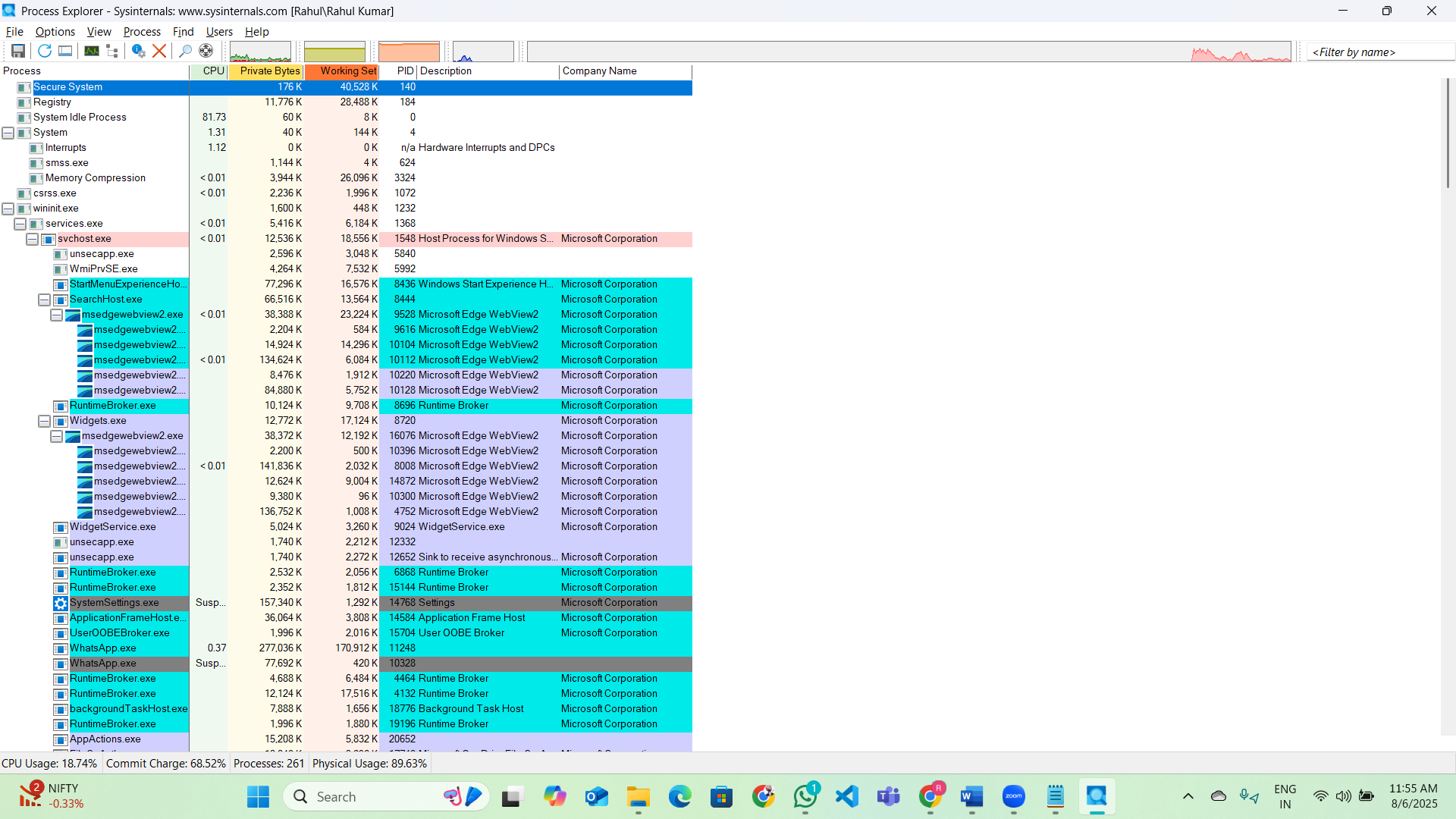
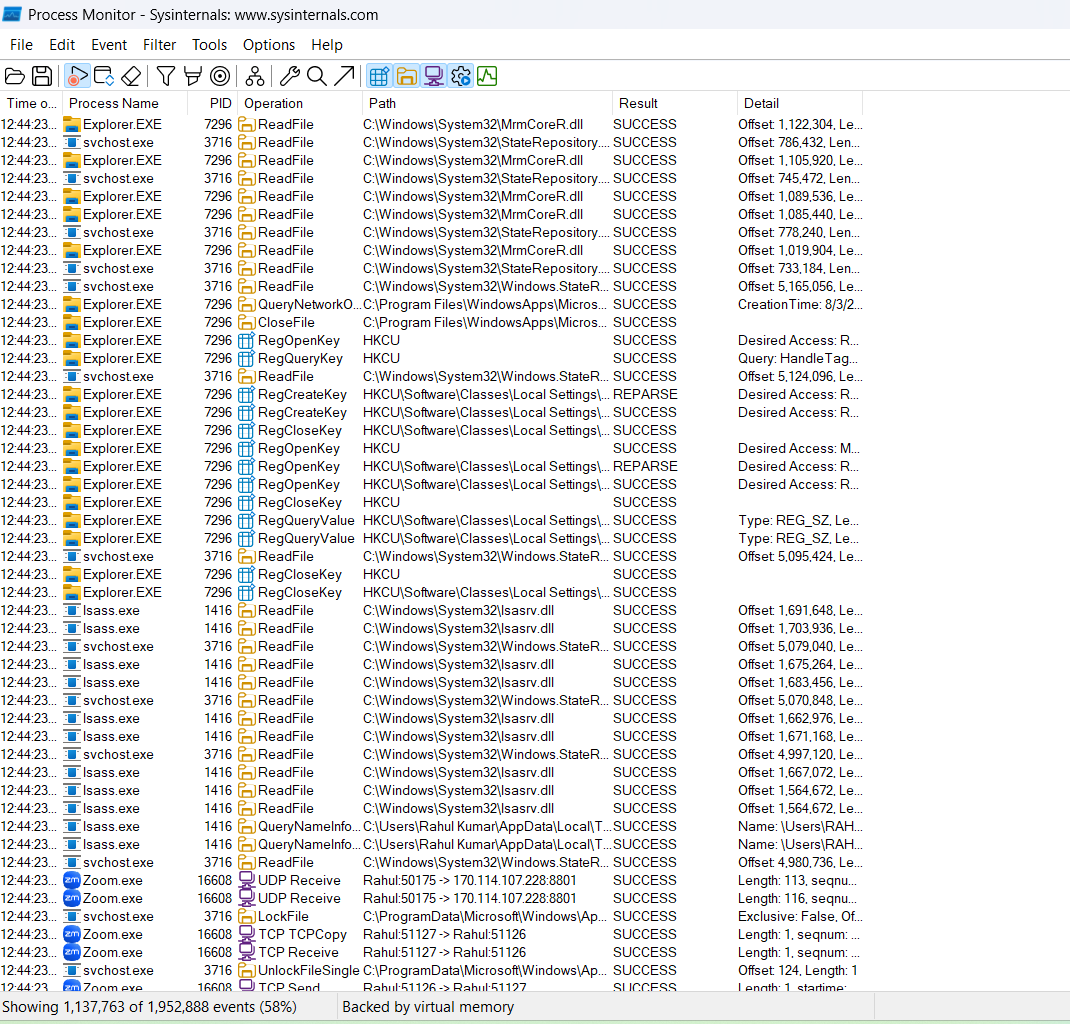
These Sysinternals tools are valuable for troubleshooting and security analysis on Windows systems. Autologon automates user logins, while Process Explorer provides detailed process information. PsExec enables remote execution of commands and programs. PSTools helps manage logon sessions, and RegMon monitors registry activity. Sysmon provides system-level monitoring, and Whois (though not explicitly part of Sysinternals) is useful for network information.

* Here's a more detailed look at each tool:

**🔹 1. Autologon**

* **What it does:** Automatically logs in a user to without typing a password.
* **Why use it:** Great for systems with no monitor (headless) or for testing setups.
* **How it works:** Saves login details in the registry to skip the login screen. 

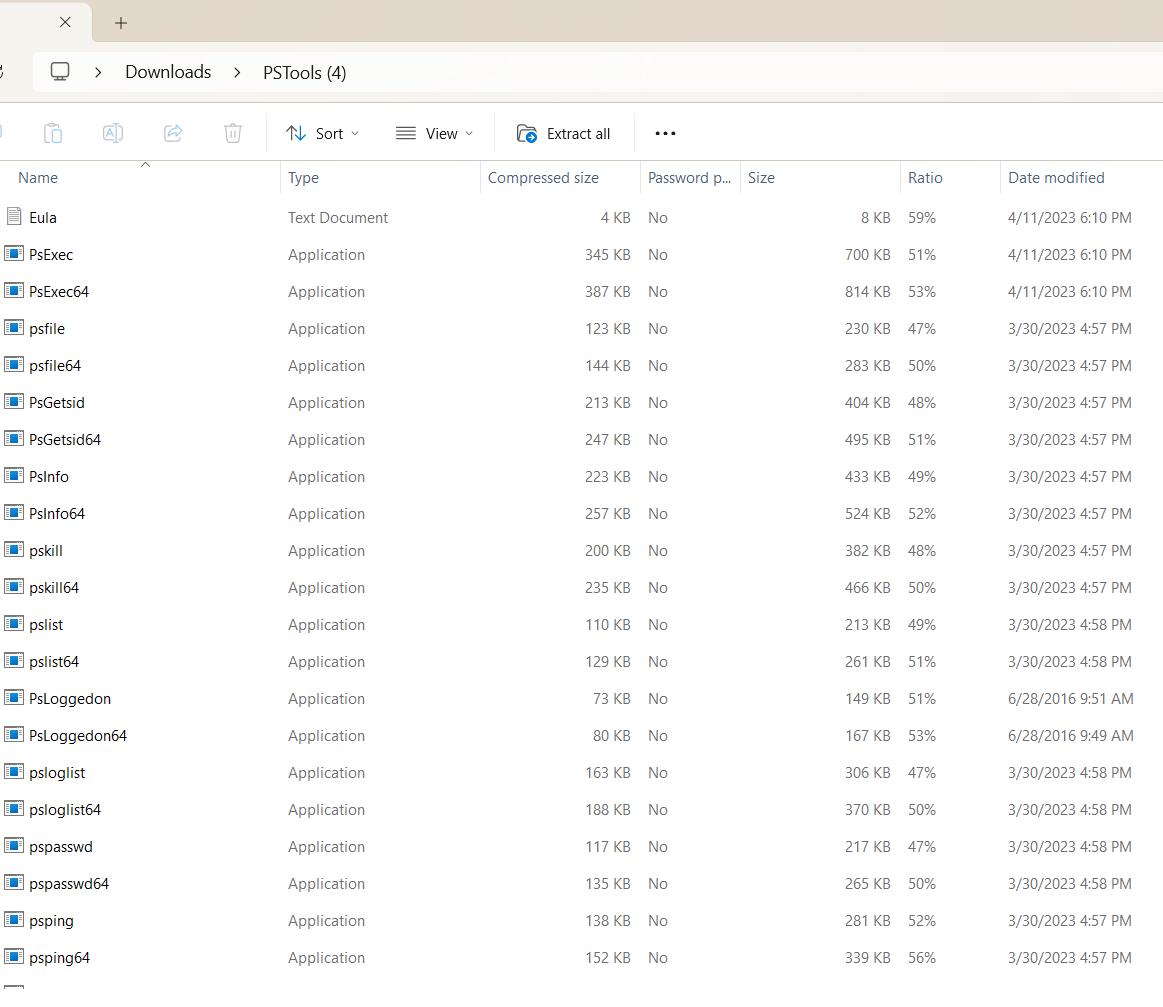
**🔹 2. Process Explorer**

* **What it does:** Shows detailed info about running processes (like Task Manager, but better).
* **Why use it:** Helps find which apps use the most memory, or check for malware.
* 
* **How it works:** Shows memory usage, open files, handles, etc.
* 

**🔹 3. PsExec**

* **What it does:** Lets you run commands or apps on other computers remotely.
* **Why use it:** Useful for admins managing multiple PCs without going to each one.
* **How it works:** Runs apps on remote machines as if they were local.

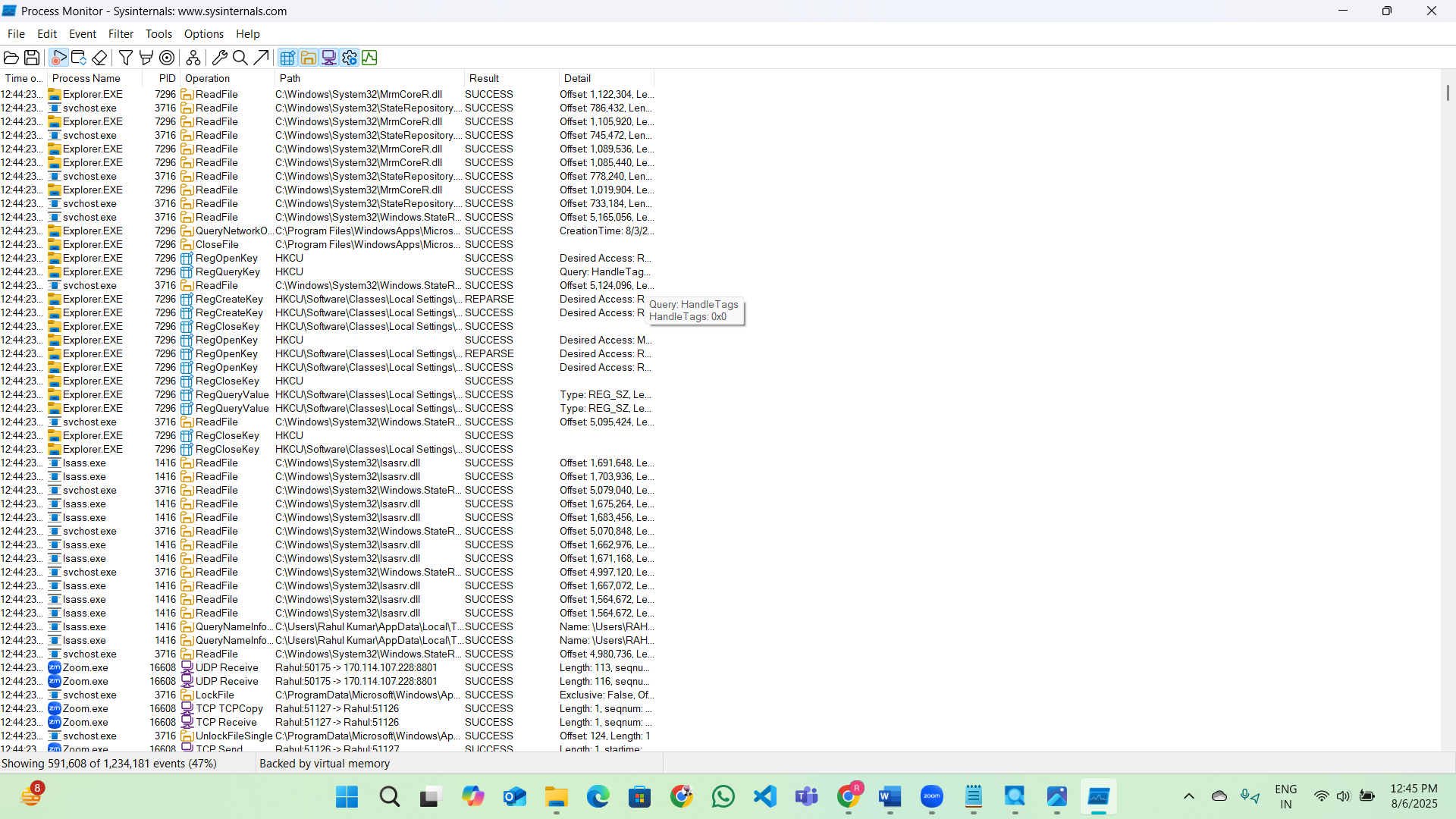
**🔹 4. PSTools**

* **What it does:** A set of command-line tools for managing and checking Windows systems.
* **Why use it:** Lets you check who’s logged on, see processes, open files, etc.
* **How it works:** Includes tools like PsLoggedOn, PsList, PsFile, etc.
* 

**🔹 5. RegMon**

* **What it does:** Watches what’s happening in the Windows registry in real-time.
* **Why use it:** Useful to catch programs that are making unwanted changes.
* **How it works:** Shows read/write/delete actions in the registry.

**NOTE-** RegMon and FileMon are no longer available for download. They have been replaced by [Process Monitor](https://learn.microsoft.com/en-us/sysinternals/downloads/procmon) on versions of Windows starting with Windows 2000 SP4, Windows XP SP2, Windows Server 2003 SP1, and Windows Vista.

* 

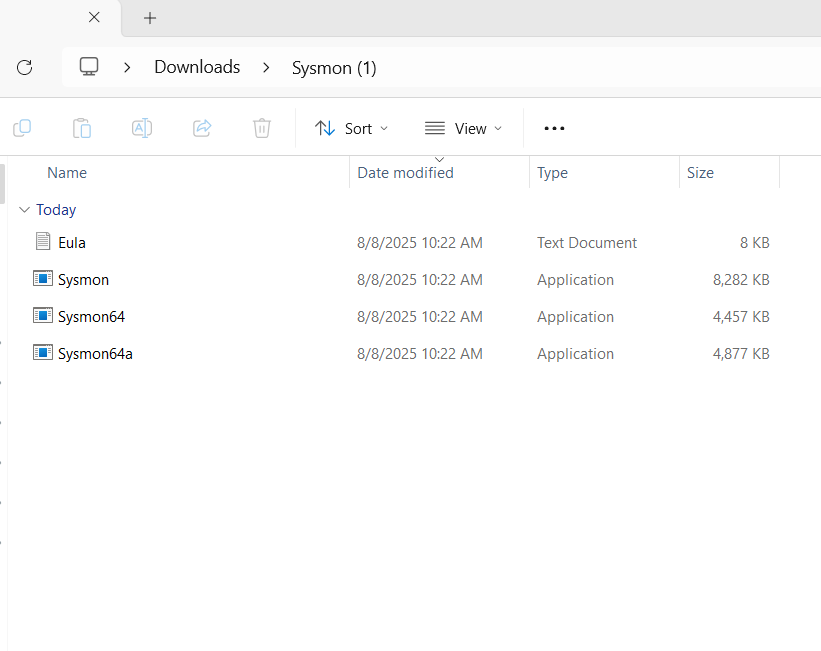
**🔹 6. Sysmon**

Introduction

*System Monitor* (*Sysmon*) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using [Windows Event Collection](https://msdn.microsoft.com/library/windows/desktop/bb427443(v=vs.85).aspx) or [SIEM](https://en.wikipedia.org/wiki/security_information_and_event_management) agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network. The service runs as a [protected process](https://learn.microsoft.com/en-us/windows/win32/services/protecting-anti-malware-services-#system-protected-process), thus disallowing a wide range of user mode interactions.

Note that *Sysmon* does not provide analysis of the events it generates, nor does it attempt to hide itself from attackers.

* **What it does:** Tracks system activities like process starts, file changes, and network access.
* **Why use it:** Good for security checks, detecting threats, and digital forensics.
* **How it works:** Runs as a system service and logs useful system events.



**🔹 7. Whois**

* **What it does:** Finds details about domain names and IP addresses.
* **Why use it:** Helps identify who owns a website or domain.
* **How it works:** Pulls info from Whois database (not part of Sysinternals, but still useful).

