**Name : Jyoti Sahebrao Jagtap**

**Email : [jyotishinge60@gmail.com](mailto:jyotishinge60@gmail.com)**

**INSTALLATION STEPS (Downloading the sysinternals suite package):**

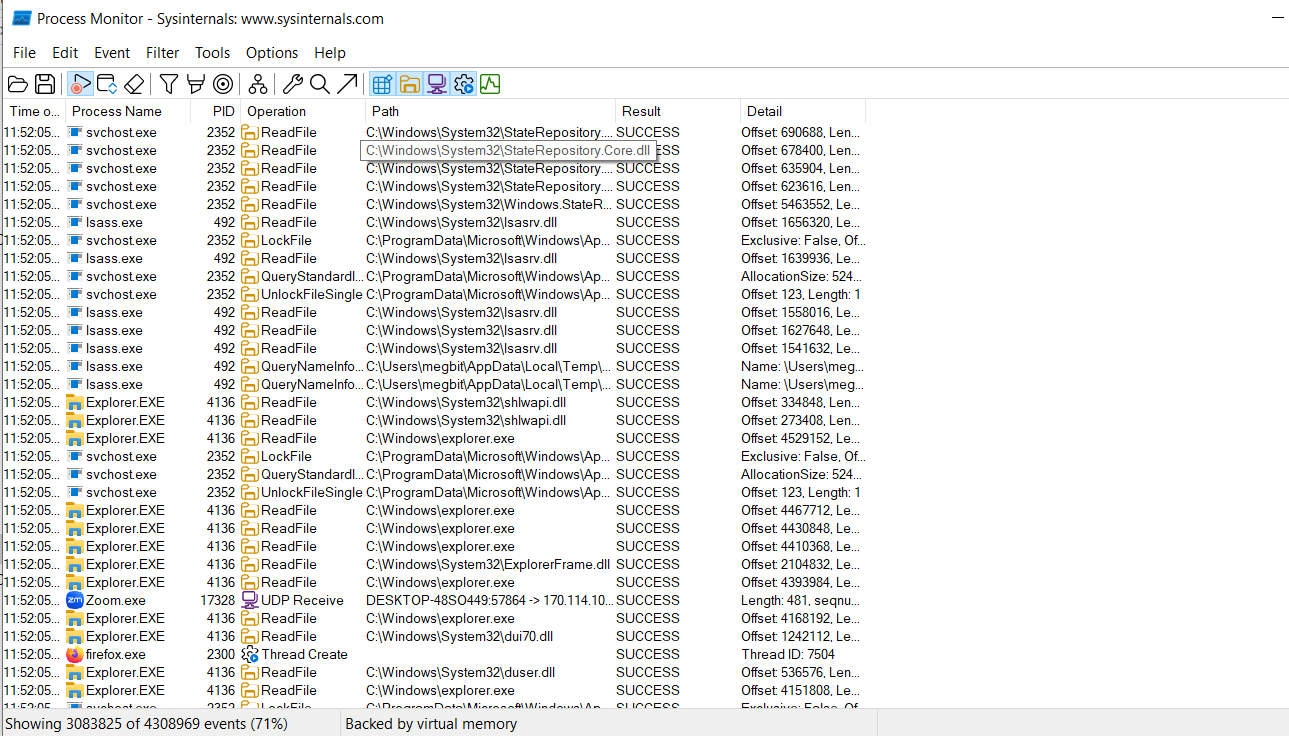
1. **Download:** Go to the official [Microsoft Sysinternals](https://learn.microsoft.com/en-us/sysinternals/downloads/) page. You'll find a link to download the Sysinternals Suite as a .zip file.
2. **Extract:** Unzip the downloaded file to a folder on your computer, for example, C:\Sysinternals.
3. **Use:** You can run the tools directly from this folder.
4. **Process Monitor:**

Introduction**:** This is an advanced monitoring tool from the Sysinternals Suite that combines the functionality of the older FileMon and RegMon utilities.

Use**:** It provides a comprehensive, real-time view of file system, registry, and process/thread activity.

It's a key tool for **troubleshooting difficult application problems**, especially those related to file or registry access permissions, DLL loading issues, and application crashes.

It can also be used for **malware analysis** to see what files and registry keys a malicious program is accessing.



1. **Process Explorer**

**Introduction:** A much more advanced and powerful tool from the Sysinternals Suite.

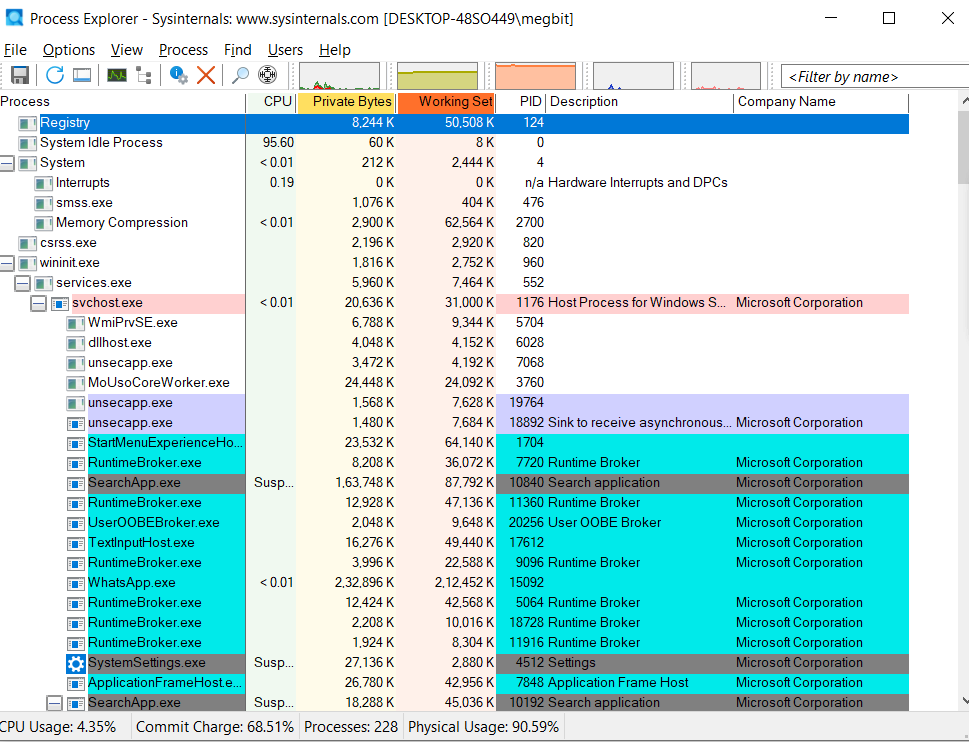
**Use:**

It goes far beyond the basic capabilities of Task Manager.

Process Explorer is a debugging and troubleshooting tool for power users and administrators.

It provides a detailed, hierarchical view of processes and their threads, DLLs, and handles. Key uses include:

* Identifying which process is locking a file.
* Viewing the full command line and parent/child relationships of processes.
* Analyzing a process's security properties.
* Detecting malware by checking for unsigned processes or unusual process behavior.

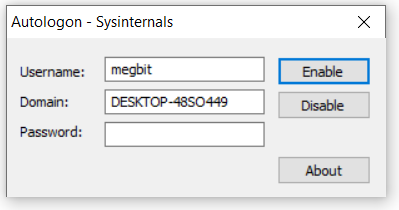


1. **AutoLogon:**

Autologon enables you to easily configure Windows’ built-in autologon mechanism.

Instead of waiting for a user to enter their name and password, Windows uses the credentials you enter with Autologon, which are encrypted in the Registry, to log on the specified user automatically.

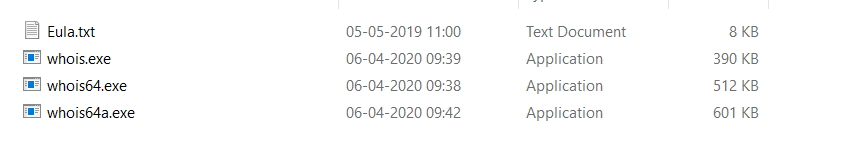
**Useful for automated systems or test environments** where user interaction isn't required after a reboot.



1. **WhoIs**:

**Use:** A command-line utility for **querying public "whois" directory information** about a domain name or IP address.

It's used for network troubleshooting and security investigations to identify the owner and contact details of a website or IP address.



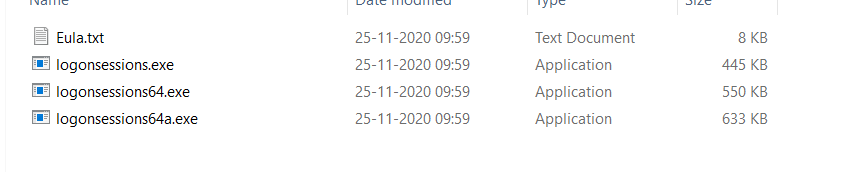
1. **LogonSessions:**

It lists the currently active logon sessions and, if you specify the -p option, the processes running in each session.

This is a debugger extension for Windows debuggers like WinDbg.

It helps in analyzing user logon sessions by providing a unique LogonId, which can be used to trace all processes and activities tied to a specific user's login.

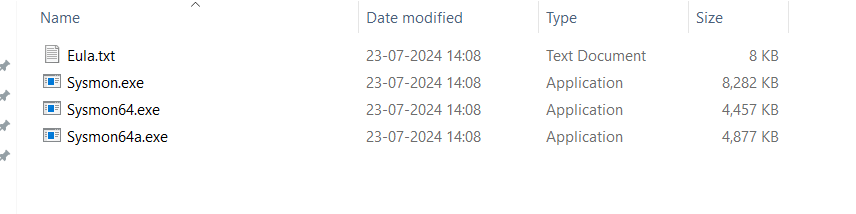
This is crucial for **investigating security incidents and understanding the scope of a breach.**



1. **Sysmon***:*

**Use:** A powerful system service and device driver that **continuously monitors and logs system activity to the Windows event log**.

It provides detailed logs for process creation, network connections, and file modifications, making it a critical tool for security monitoring and threat detection.



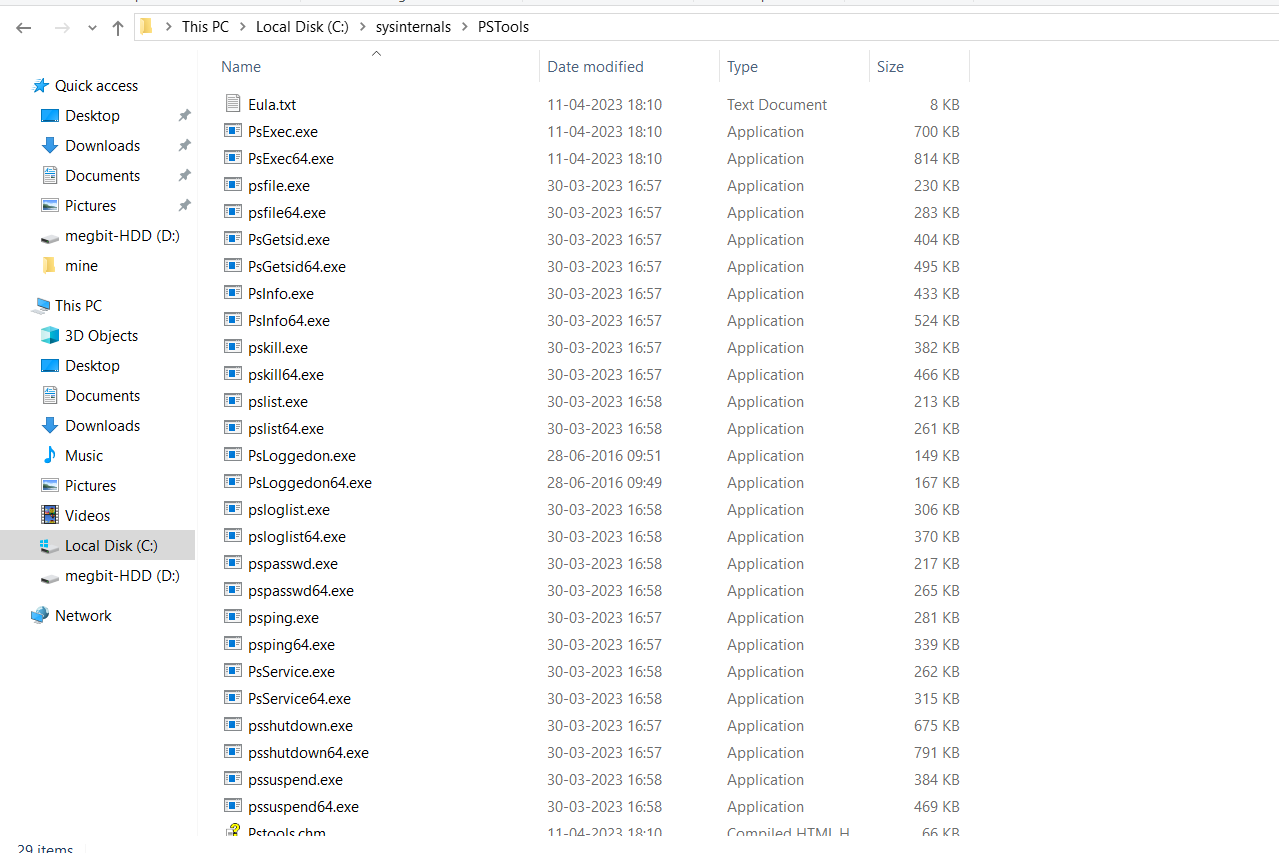
1. **psTools:**

**Use:** A suite of command-line tools that includes PsExec and others for **managing and troubleshooting both local and remote Windows systems**.

The suite offers various functionalities like viewing process information, managing services, and gathering system data.

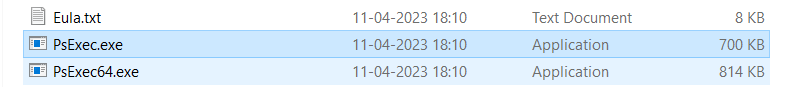
*The tools included in the PsTools suite, which are downloadable as a package, are:*

* *[PsExec](https://learn.microsoft.com/en-us/sysinternals/downloads/psexec) - execute processes remotely*
* *[PsFile](https://learn.microsoft.com/en-us/sysinternals/downloads/psfile) - shows files opened remotely*
* *[PsGetSid](https://learn.microsoft.com/en-us/sysinternals/downloads/psgetsid) - display the SID of a computer or a user*
* *[PsInfo](https://learn.microsoft.com/en-us/sysinternals/downloads/psinfo) - list information about a system*
* *[PsPing](https://learn.microsoft.com/en-us/sysinternals/downloads/psping) - measure network performance*
* *[PsKill](https://learn.microsoft.com/en-us/sysinternals/downloads/pskill) - kill processes by name or process ID*
* *[PsList](https://learn.microsoft.com/en-us/sysinternals/downloads/pslist) - list detailed information about processes*
* *[PsLoggedOn](https://learn.microsoft.com/en-us/sysinternals/downloads/psloggedon) - see who's logged on locally and via resource sharing (full source is included)*
* *[PsLogList](https://learn.microsoft.com/en-us/sysinternals/downloads/psloglist) - dump event log records*
* *[PsPasswd](https://learn.microsoft.com/en-us/sysinternals/downloads/pspasswd) - changes account passwords*
* *[PsService](https://learn.microsoft.com/en-us/sysinternals/downloads/psservice) - view and control services*
* *[PsShutdown](https://learn.microsoft.com/en-us/sysinternals/downloads/psshutdown) - shuts down and optionally reboots a computer*
* *[PsSuspend](https://learn.microsoft.com/en-us/sysinternals/downloads/pssuspend) - suspends processes*
* *[PsUptime](https://learn.microsoft.com/en-us/sysinternals/downloads/pssuptime) - shows you how long a system has been running since its last reboot (PsUptime's functionality has been incorporated into [PsInfo](https://learn.microsoft.com/en-us/sysinternals/downloads/psinfo)*

**

1. ***PsExec-***

* **Use:** A command-line tool for **executing processes on remote systems.**
* It allows administrators to run commands or scripts on other computers without needing to install any client software on them, making it an invaluable tool for remote administration and debugging.

******

1. ***RegMon –***

* **Use:** A now-discontinued Sysinternals tool for **monitoring real-time registry access**.
* Its functionality has been integrated into **Process Monitor.**
* It was used to debug registry-related problems by tracking which applications were interacting with the registry.

**Step for create microsoft intune portal -**

* Create a Microsoft 365 or Azure subscription.
* Sign in it.
* Assign Intune license to users via Microsoft 365 Admin Center.
* Set Microsoft Intune as the MDM authority.
* Configure compliance and app protection policies.
* Set up device enrollment for each platform.
* Add and assign apps to users or devices.
* Monitor devices and users through reports and dashboards.
* (Optional) Set up Conditional Access in Azure AD.
* (Optional) Deploy the Company Portal app to user devices.