NAME : Talari vyshnavi

USER ID : 34725 – batch5

E-MAIL : [talari.vyshu@gmail.com](mailto:talari.vyshu@gmail.com)

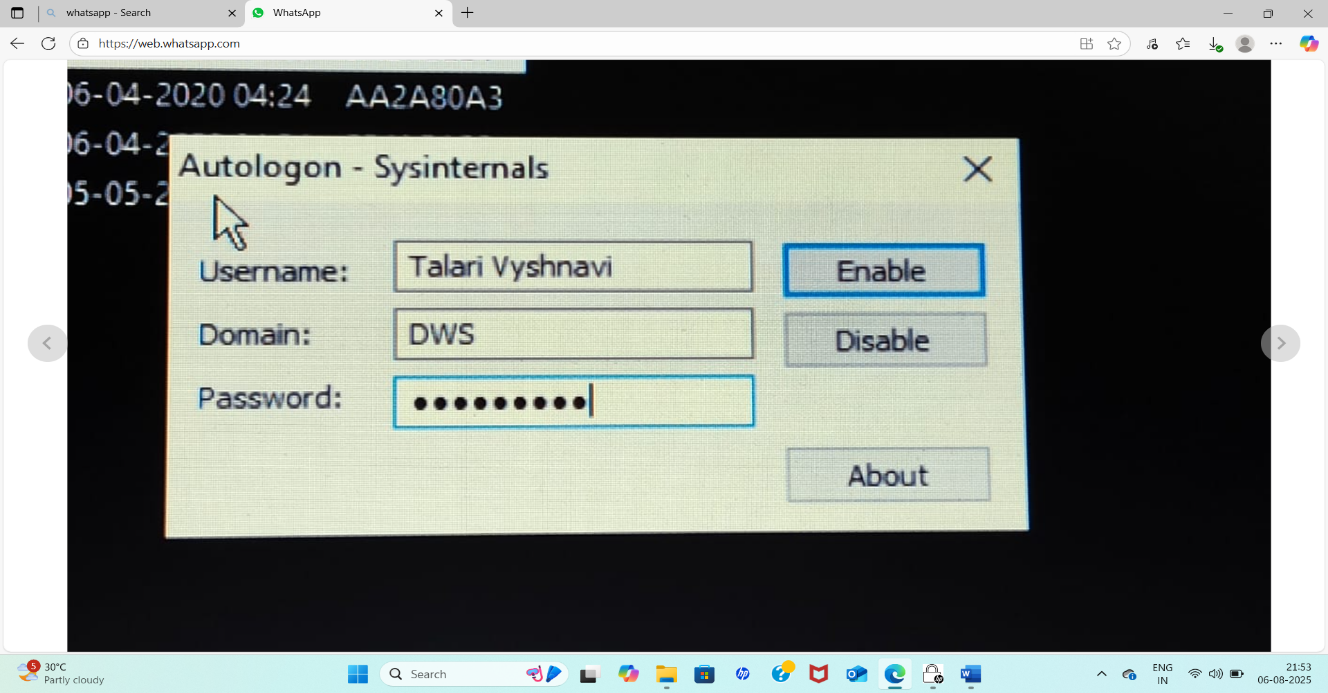
USING WINDOWS TOOLS FOR DEBUGGING :

Antologon , Process tools. Process explorer , whois , process monitor symon

Antologon :-

Autologn is a windows feature that allows a user to automatically log in to the system without typing a username and password each time the computer starts.

Autologon is insecure because the login credentials are stored in the windows Registry . If someone can access to the system ,they could may see or missuse the login info.

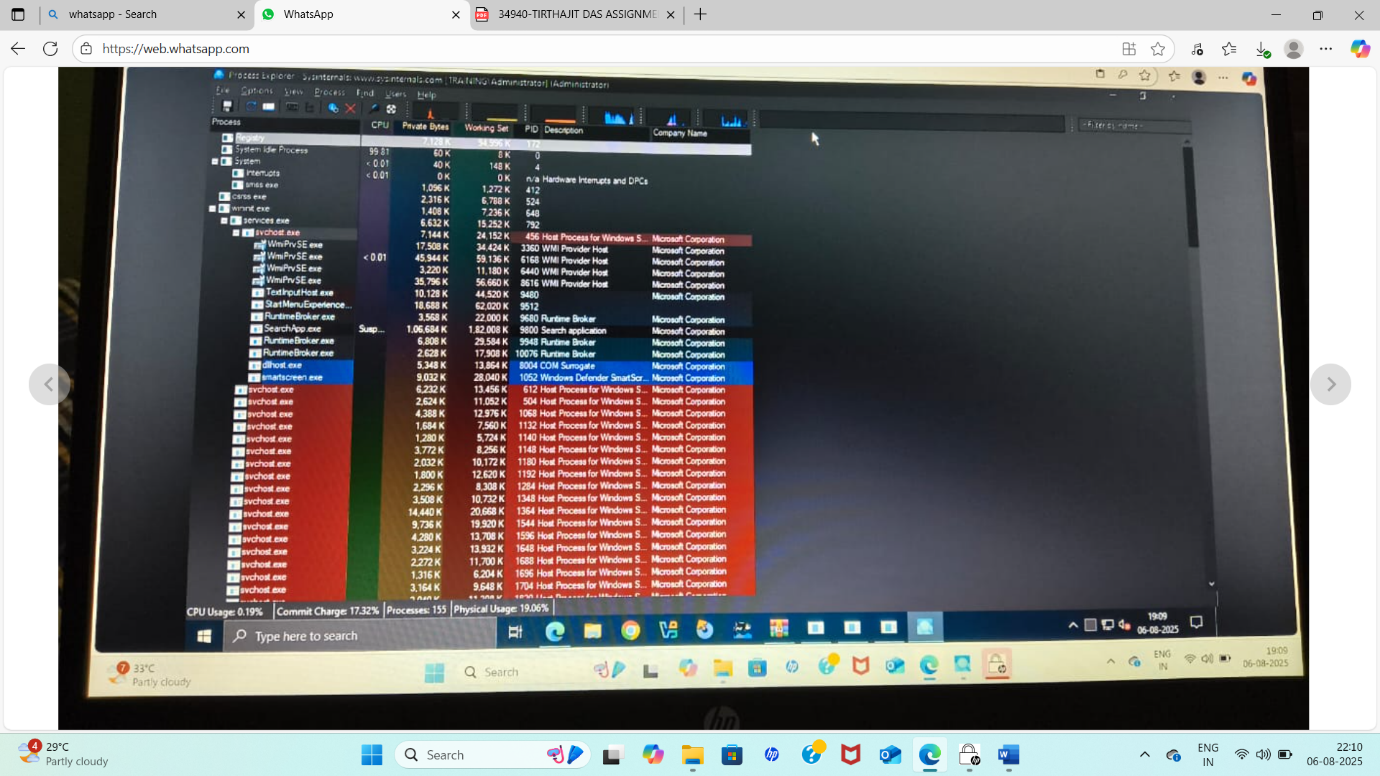


Process Tools :-

A process tool is a software or method used to help and plan , manage ,control , and improves technical processes.



. Process Explorer :-



• Purpose: Advanced version of Task Manager with detailed insight into system processes.

• Tool Type: GUI

• Use Case: o Analyze running processes. o Detect malware or injected DLLs. o Check parent-child process trees. o Monitor file, registry, and DLL activity per process.

RegMon (Note: Replaced by Process Monitor)

• Purpose: Real-time monitoring of Registry access.

• Status: Now merged into Process Monitor.

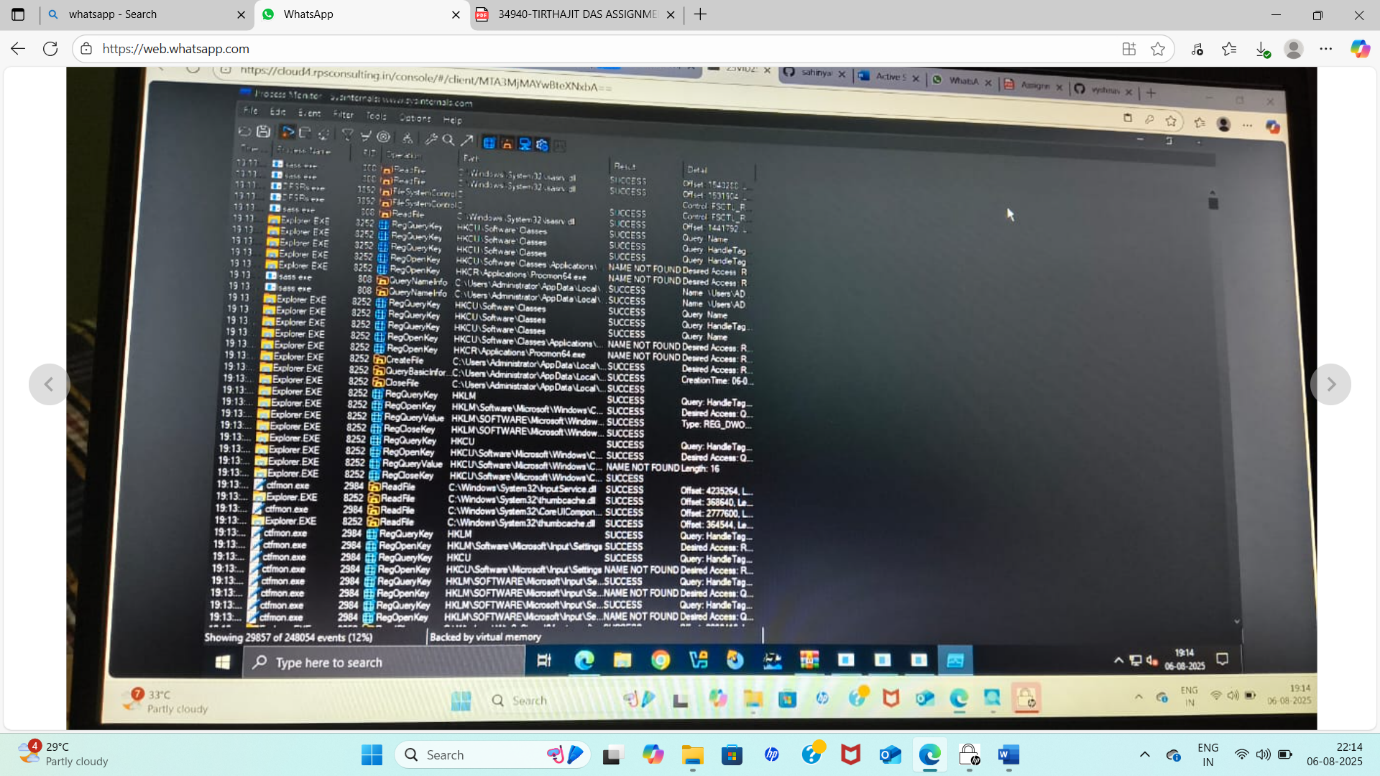
• Use Case: o Debug registry reads/writes during software installs. o Identify which keys are modified by applications.

• Example: o Monitor what registry keys an installer touches during execution.

• Replaced by: Use ProcMon instead, with filters for Operation = RegSetValue, etc. 7. Whois

• Purpose: Query domain registration details.

• Tool Type: Command-line tool.



• Use Case: o Troubleshooting suspicious network connections or domains.

Sysmon (System Monitor)

• Purpose: Logs detailed system activity to the Windows Event Log.

• Tool Type: Service + Driver

• Use Case: o Monitor:

▪ Process

▪ Network connections

▪ File creation time changes

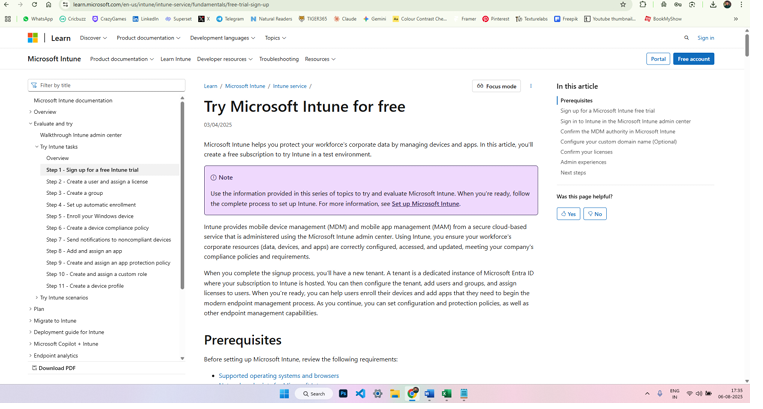
**.Whois:**

* **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. [37, 37, 38, 39, 40, 41, 42, 43]

➢ Intune Free trial Subscription - How to enrol

1. Access the Intune Setup Account Page:

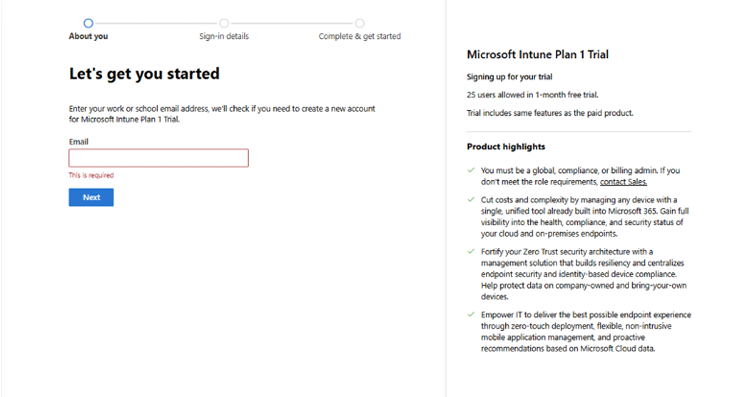
• Open a web browser and go to the Intune setup account page.



1. Sign Up or Sign In:

• For new users: Enter your email address and click "Next." Follow the prompts to create a new account and provide the necessary information.

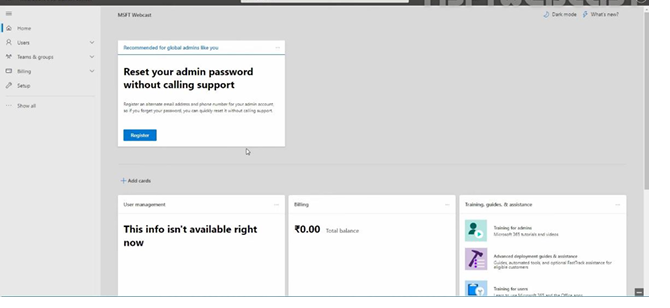
• For existing users: Sign in with your existing work or school account.



1. Complete the Sign-Up Process:

• If creating a new account, you'll be asked to verify your email address and potentially provide additional information like your name, company details, and region.

• After signing up or signing in, you'll be directed to the Microsoft 365 Admin Center.



1. Considerations for Existing Work or School Accounts:

• If you're using an existing work or school account, you might need to add Intune to your existing subscription.

• If you plan to use your organization's custom domain name or synchronize with on premises Active Directory, you might need to close the browser window after the initial setup and configure these aspects separately

5. Accessing Intune After Enrollment:

• Once the free trial is set up, you can access the Microsoft Intune Admin Center to manage the service.

• You can use any device with a supported browser to sign in.

A screenshot of a computer

AI-generated content may be incorrect.