**NAME:** - ANSHUL SAINI  
**MAIL:** - [sainianshul7565@gmail.com](mailto:sainianshul7565@gmail.com)

**User ID**: - 34732

**Date: -** 06/08/2025

**Batch: -** DWS\_B5\_25VID2550

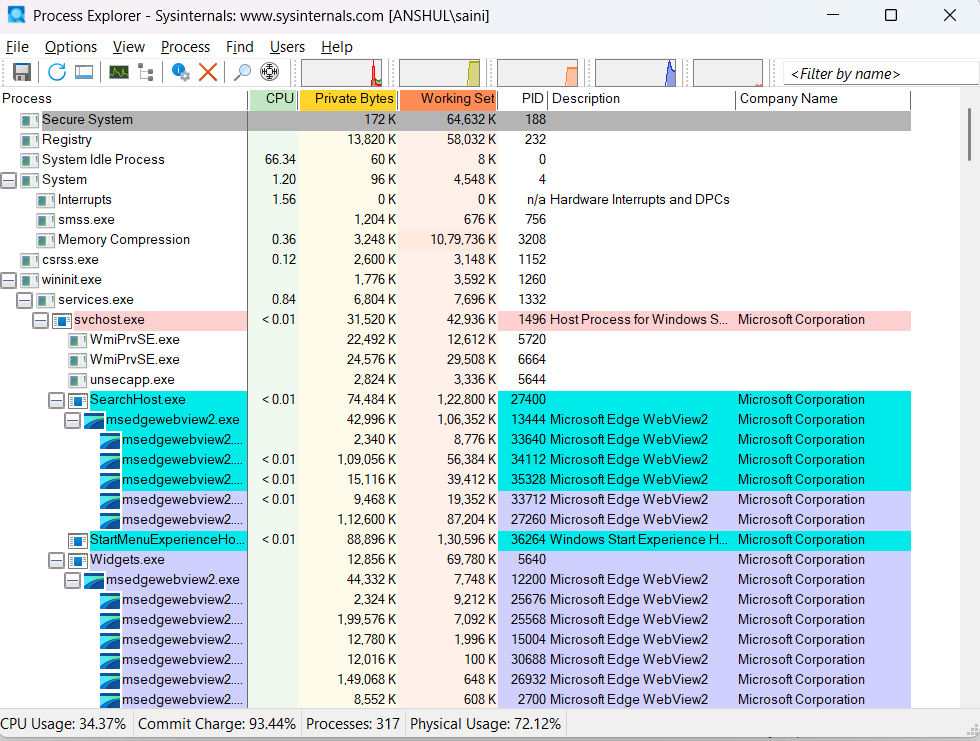
**Topic Assignment: -**

* Using Windows Tools for Debugging: LogonSessions, Autologon, Process Explorer , Psexec, PSTools, RegMon, Whois, SysMon .
* Steps to create for Microsoft Intune
* **Using Windows Tools for Debugging:**

1. **Process Explorer**

Process Explorer is a free Windows task manager and system monitoring tool that details which programs in a user's system have a specific file or directory open.

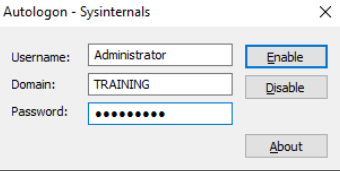
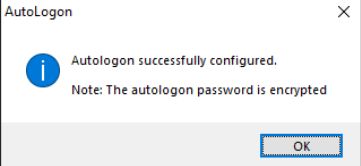
**Practice Activity:** -



1. **Autologon**

By using Autologon feature, other users can start your computer and use the account that you establish to automatically log on.

**Practice Activity:** -



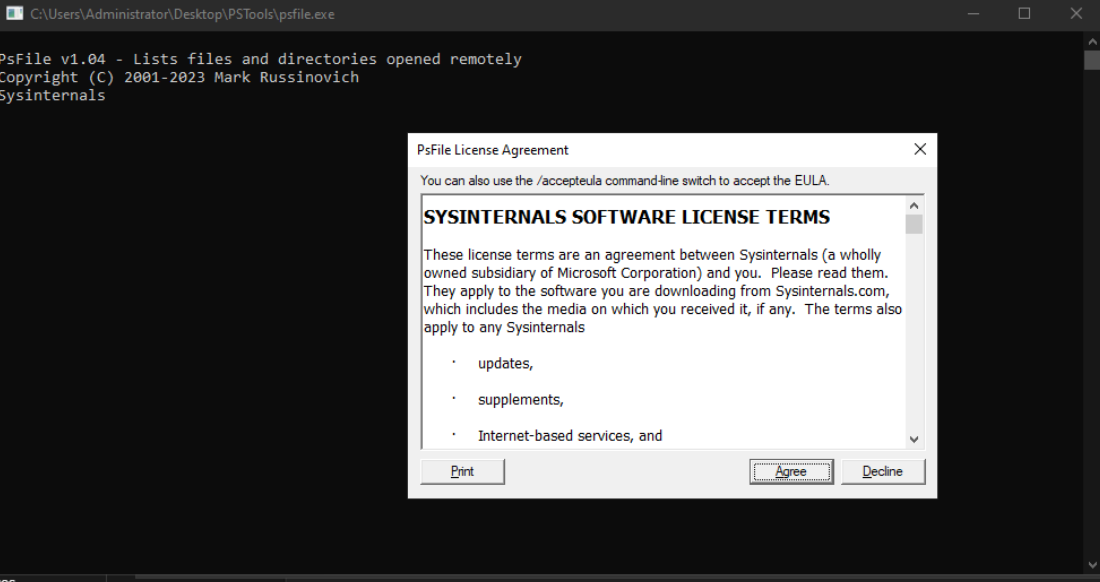
1. **PsExec**

PsExec is a powerful remote administration tool that enables execution of commands and applications on remote Windows systems. It allows administrators to perform tasks on other computers as if locally present. Commonly used for troubleshooting, system maintenance, and automating administrative tasks without needing physical access to the target machine.

1. **PSTools**

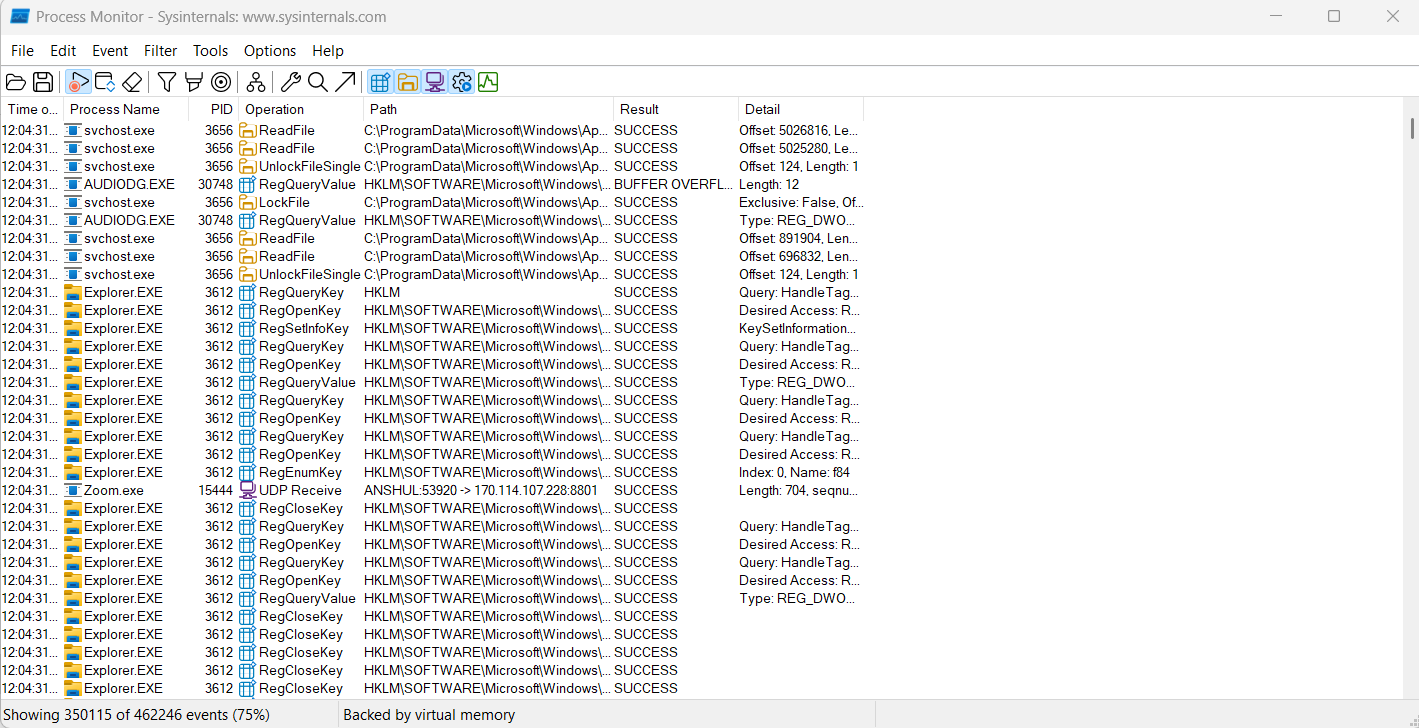
PSTools is a suite of command-line utilities designed for system management. It includes tools like PsLoggedOn, PsList, and PsKill to manage processes, sessions, and system information remotely. Administrators rely on PSTools for efficient system control, user monitoring, and troubleshooting across networks without requiring remote desktop connections.

**Practice Activity:** -



1. **RegMon**

RegMon have been replaced by Process Monitor . RegMon, or Process Monitor, is a diagnostic tool that captures and displays real-time registry activity. It shows which applications access, modify, or delete registry keys and values. This visibility helps in debugging software behavior, detecting unwanted changes, and investigatingregistry-based malware or configuration issues on Windows systems.

**Practice Activity:** -

1. **Sysmon**

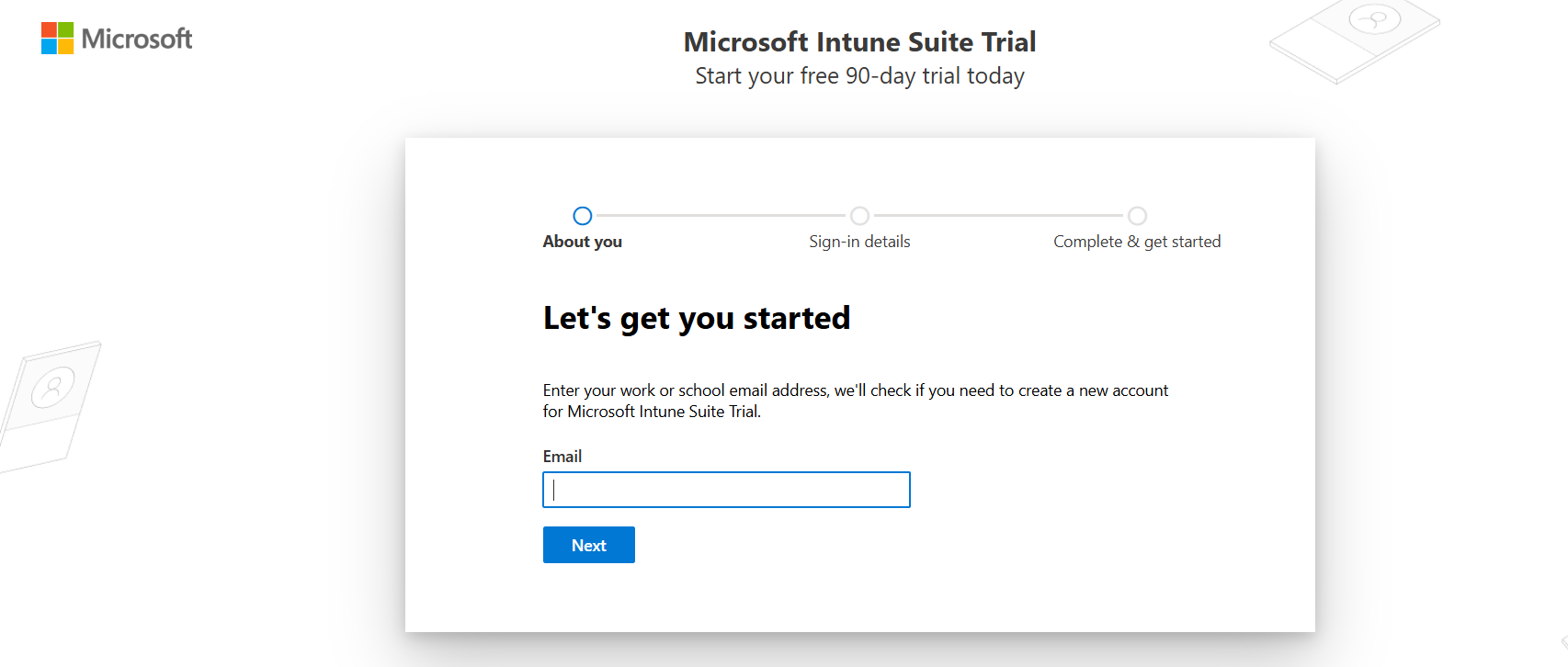
System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time.

1. **Whois**

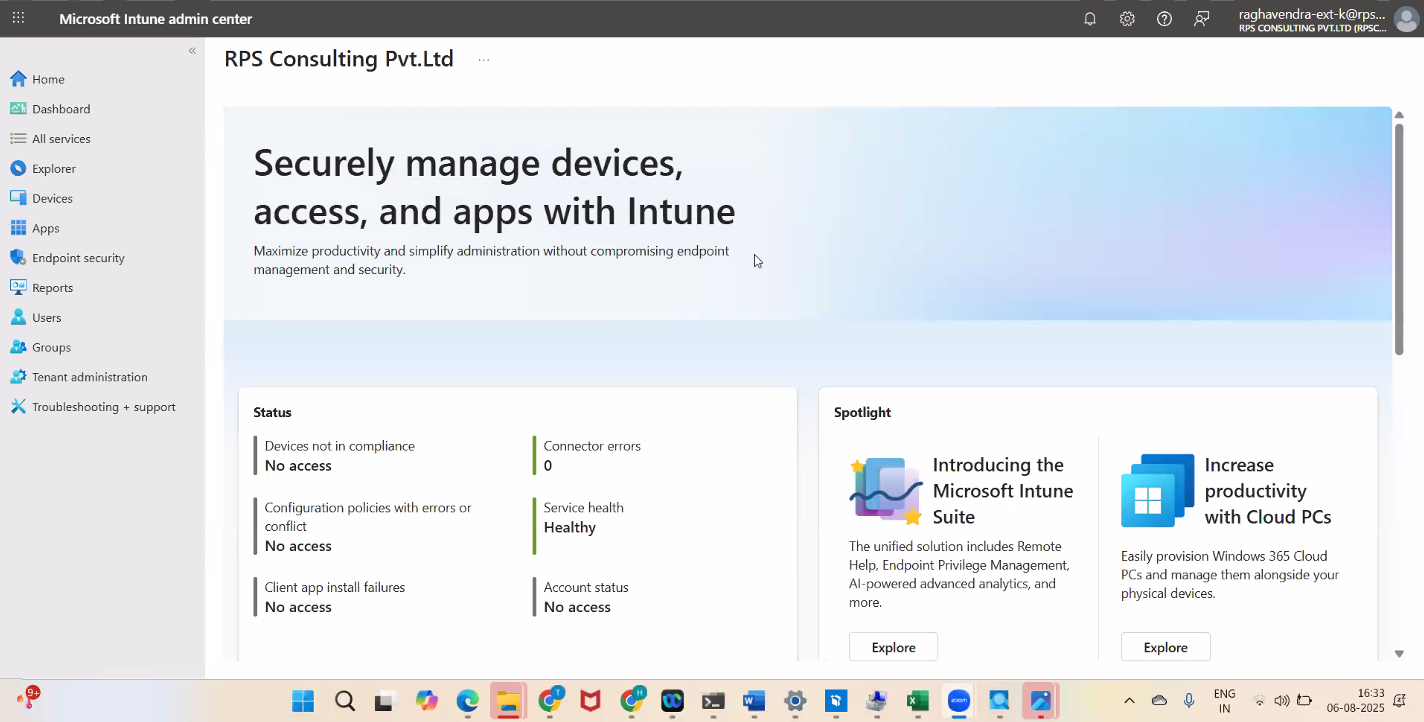
Whois is a command-line tool used to gather ownership and registration details of domain names and IP addresses. It queries online databases to return information like domain registrant, contact, and expiration data. Useful for network diagnostics, it helps verify domain legitimacy and investigate suspicious online activity or cyber threats.

* **Steps to create for Microsoft Intune:**

To create Microsoft Intune setup, start by signing up for a free 90-day trial with a work or school email. Then fill sign-in details and Complete account creation and sign-in steps. Set up your Microsoft Entra tenant, enroll devices, assign the MDM certificate, and configure policies for security, compliance, and app protection using the Intune admin center.



**Practice Activity:** -

****