**Name**: Saniya Galib Tamboli

**Email**: [saniyagtamboli2412@gmail.com](mailto:saniyagtamboli2412@gmail.com)

**Batch:** DWS\_B5\_25VID2550

**User Id:** 34749

**Date**: 06/08/2025

ASSIGNMENT

**1.Installation Steps Microsoft Sysinternals:**

1. Go to the official Microsoft Sysinternals website. There is a link to download the Sysinternals Suite in the form of a .zip file.

2. Click on the download option.

3. Go to the Downloads folder and unzip the downloaded file into a folder on your device.

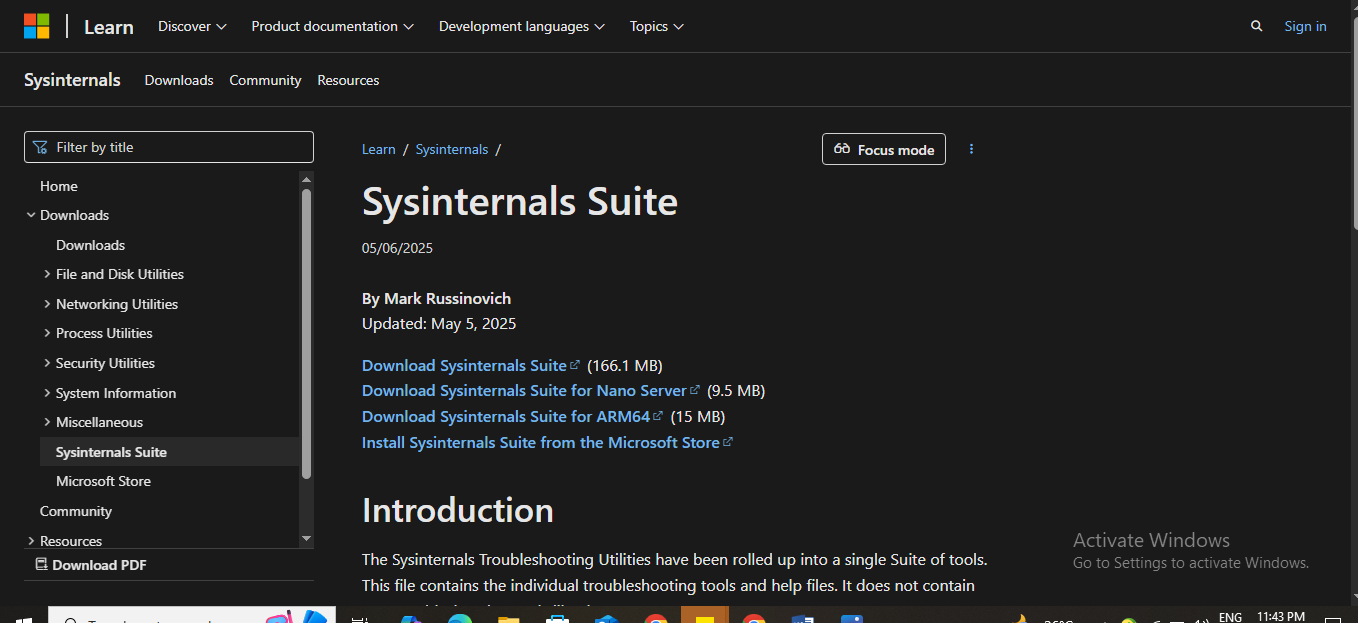


Fig.1. Sysinternals Suite

**2.Steps for Microsoft Intune Setup:**

1. Go to the official website: https://www.microsoft.com/en-in/security/business/microsoft-intune
2. To install Microsoft Intune, start by signing up for a 90-day free trial using your work or school email account.
3. Then, enter your sign-in credentials and complete setting up your account.
4. Install your Microsoft Entra tenant, add devices, install the MDM certificate, and install security, compliance, and app protection policies in the Intune admin center.

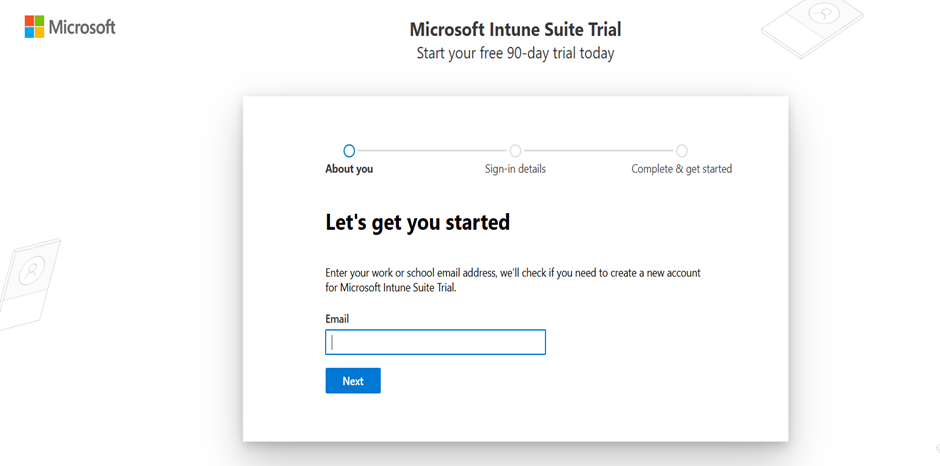


Fig.2.1. Microsoft Intune Suite

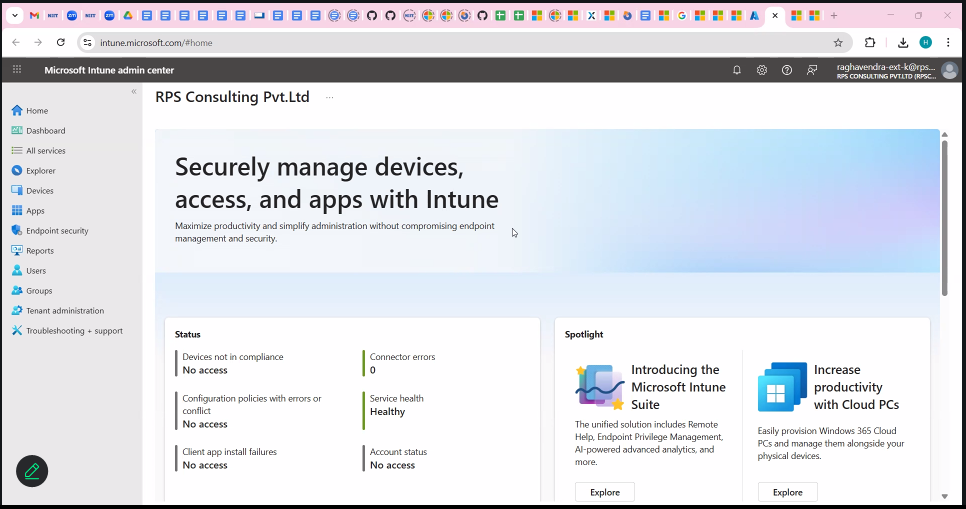


Fig.2.2. Microsoft Intune

**3. SysInternals Tools for Debugging:**

Sysinternals tools used for security and troubleshooting on Windows. Autologon logs you in, Process Explorer provides process information in detail and PsExec provides command execution on remote systems. PSTools handles logon sessions, RegMon monitors registry use and Sysmon allows system monitoring. Whois is not a Sysinternals tool but it is useful for network information.

1. Autologon Logs:

It logs in to a Windows machine automatically. It is a GUI application that sets up the Windows registry to log on automatically with credentials given by the user. It is suitable for headless environments or automation testing. With the Autologon function, however, someone else might be capable of booting up your system and logging in under your account automatically.

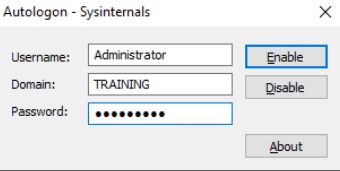


Fig.3.1.1. Autologon – Sysinternals

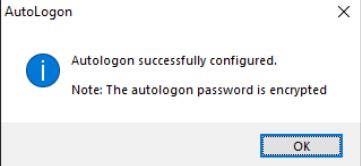


Fig.3.1.2. Autologon Successful

ii) Process Monitor:

This is a very strong Sysinternals utility that merged the older tools RegMon and FileMon. It quickly captures what is happening in the process, registry and file system.

It assists in repairing difficult application issues, particularly registry or file permissions, DLL loading and crashes.

You can use it to scan for malicious software and see what files and registry keys an offending program is reading.

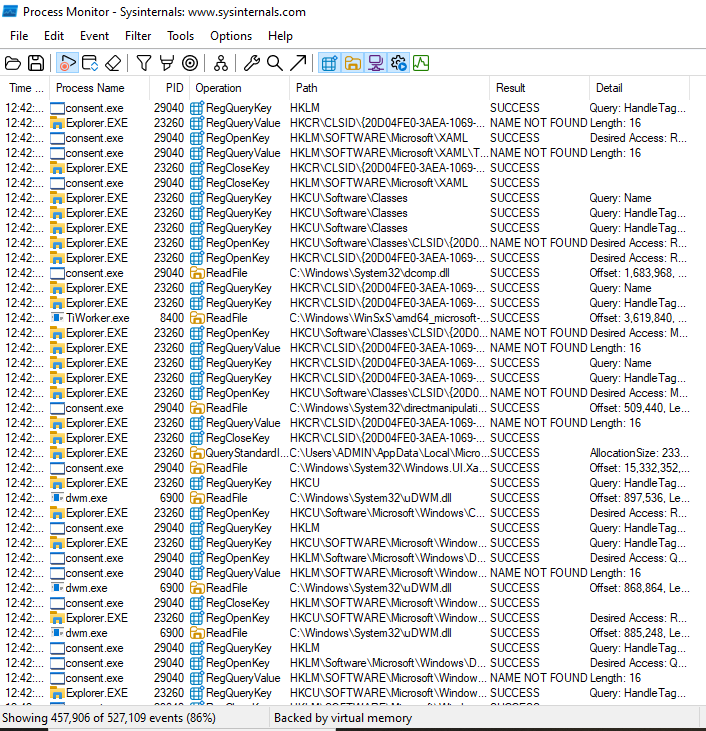


Fig.3.2. Process Monitor

iii) Process Explorer:

It is an effective utility for displaying and controlling running processes. It provides precise information on processes such as memory usage, handles and open files.

It is extremely critical in process problem-solving, resource constraint identification and malware analysis.

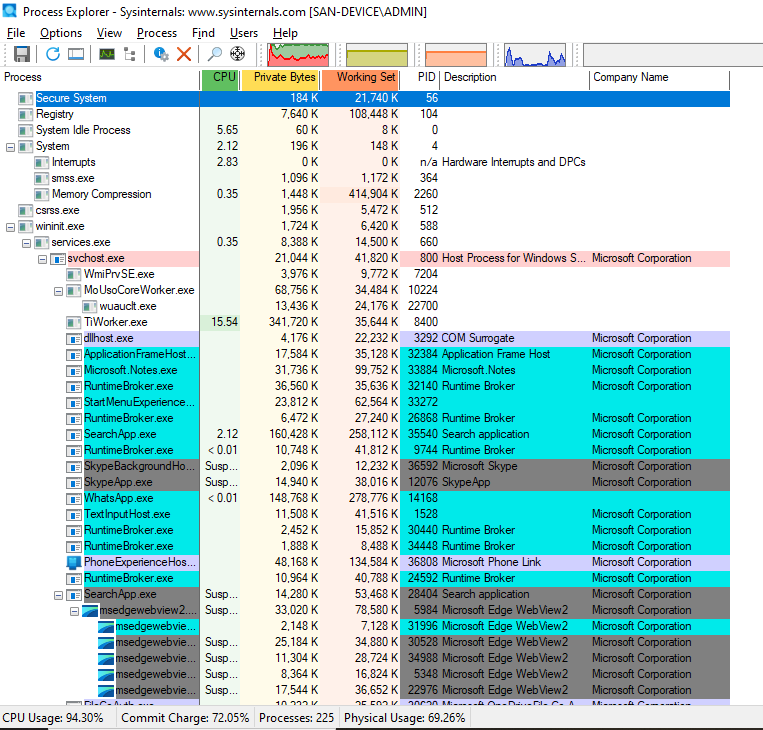


Fig.3.3. Process Explorer

iv)PsExec:

It is a powerful means of executing commands and programs remotely. It let administrators access applications on a remote computer as if they are using them on their own computer. It is employed for remote system management, patching and debugging.

PsExec is a highly valuable remote computer management tool. It allows system administrators to execute commands and applications on remote Windows computers as if they were physically sitting in front of them. It is commonly used to troubleshoot problems, maintain systems and automate operations without physically sitting in front of the computer.

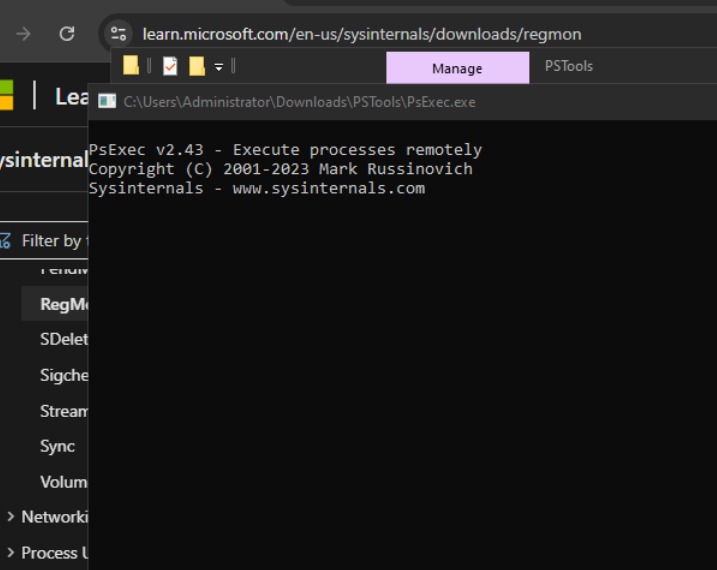


Fig.3.4. PsExec

v) PSTools:

It is a collection of system administration and debugging command-line utilities. It has tools like PsLoggedOn, PsFile and PsList and many more. It offers various administrative features for local and remote systems.

System administrators utilize PSTools for efficient system management, monitoring and troubleshooting over networks without remote desktop sessions.

A collection of command-line utilities that includes PsExec and other tools for the management and repair of local and remote Windows computers.

The suite has various features like viewing process data, managing services and retrieving system data.

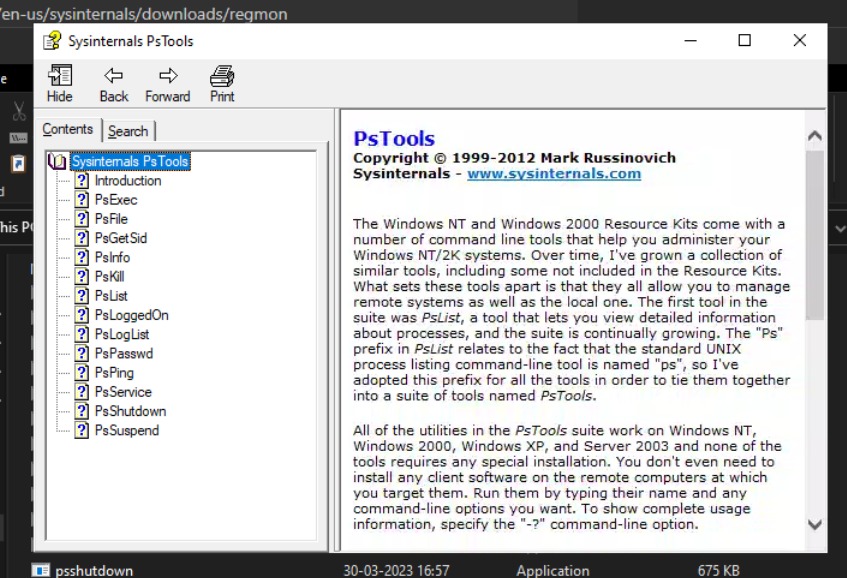


Fig.3.5. Sysinternals PsTools

The PsTools set of tools can be downloaded as a package. They include:

• PsExec - run processes remotely

• PsFile - shows files opened remotely

• PsGetSid - displays the SID of a user or computer.

• PsInfo - displays information about a system

• PsPing - measure network performance

• PsKill - terminate processes by name or ID

• PsList - provides thorough details on processes

• PsLoggedOn - see who is logged on directly and via shared resources

• PsLogList - display event log entries

• PsPasswd - alters account passwords

• PsService - view and control services

• PsShutdown - shuts down and potentially reboots a computer.

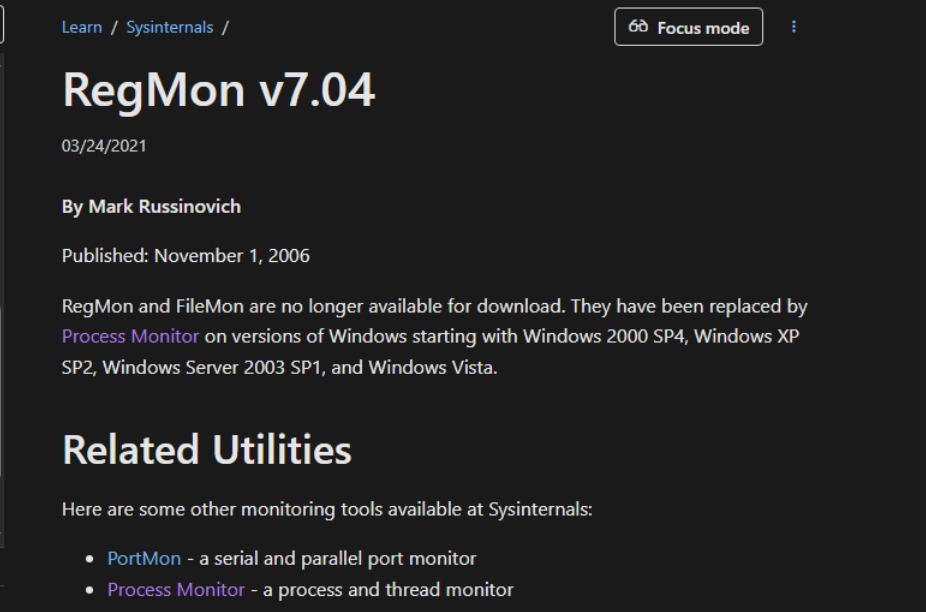
•PsSuspend - pauses processes

• PsUptime - specifies how long a system has been running since it was last rebooted.

vi) RegMon:

It tracks and logs any registry usage and any alterations to it, all in real-time.

This tool closely tracks and maintains a highly precise account of each and every action that takes place within the registry, including a wide range of different activities including reading, writing and deleting entries. It helps to diagnose registry-related issues, identify malicious programs and scan for security threats.

Fig.3.6. About - RegMon

vii) Sysmon (System Monitor):

The general purpose of this tool is to act as a Windows system service and driver that monitors and carefully logs different activities taking place within the system environment. It supplies detailed information regarding process creations, network connections and file access changes. It is absolutely required for security monitoring, for intrusion detection and forensic analysis.

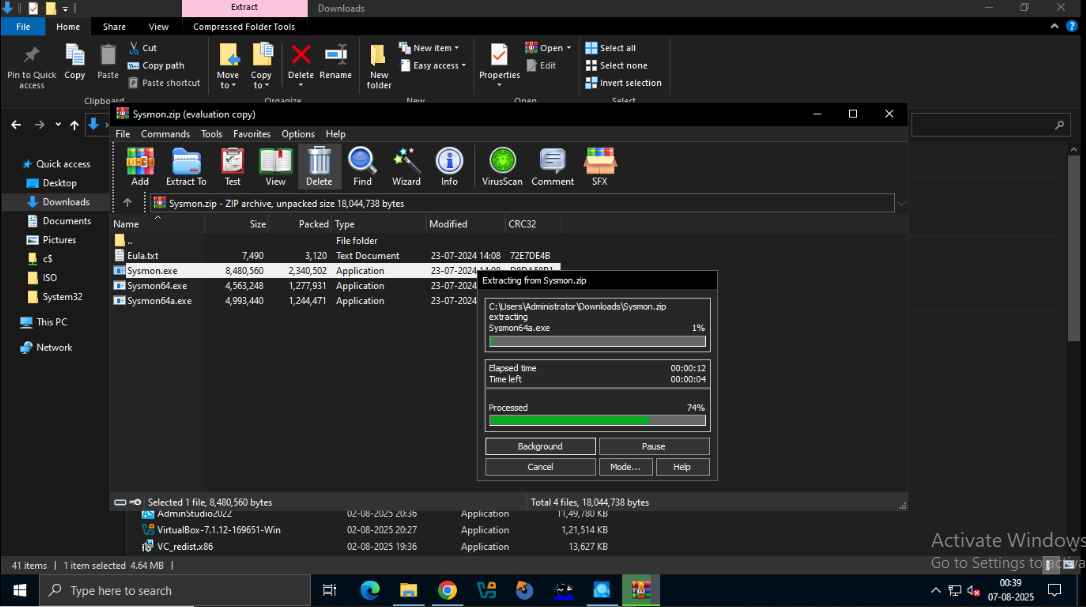


Fig.3.7. Sysmon

viii) Whois:

It is a command-line tool (not actually from Sysinternals) to extract details about domain names and IP addresses. It checks a Whois database to get registration information. It is helpful for fixing network problems, finding domain owners and seeing if a domain is available.

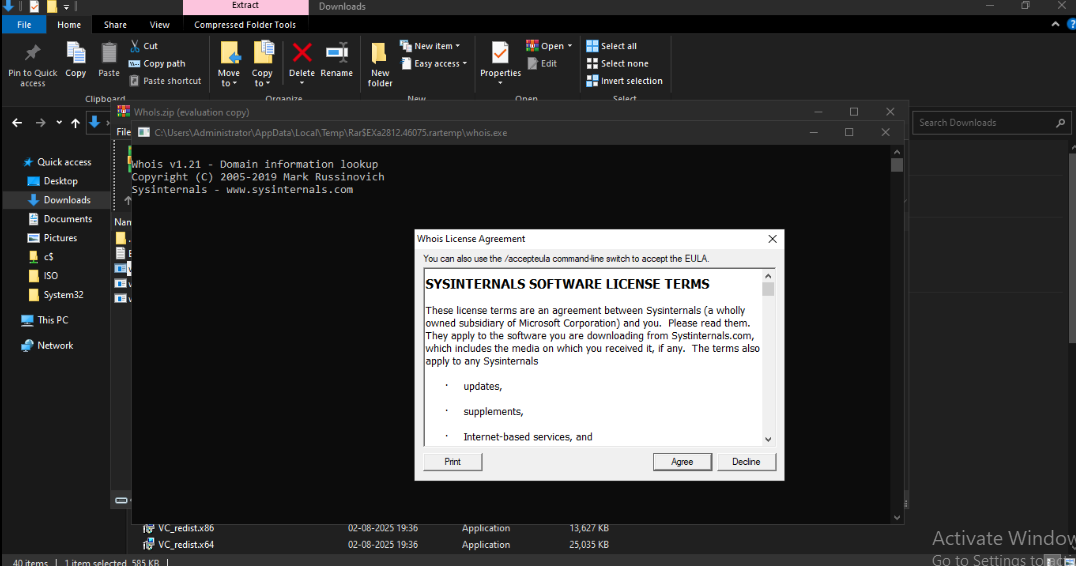


Fig.3.8. Whois