**Batch Name:** WiproNGA\_DWS\_B5\_25VID2550

**First Name:** MahammadTanvir

**Last Name:** Khatri

**User ID:** 34936

**Batch ID:** B5-25VID2550

**Assignment – 06/08/2025**

## 1. Process Explorer

**Purpose:**  
Process Explorer is a system utility from Sysinternals used to view detailed information about running processes, including memory usage, open files, and parent-child relationships between processes.

**Activity:**  
I downloaded Process Explorer, ran the application on my device, and captured the output shown below.

**Screenshot:**  
*A screenshot of a computer program

AI-generated content may be incorrect.*

**2. Process Monitor**

## Purpose: Process Monitor is a real-time monitoring tool from Sysinternals that captures file system, registry, and process/thread activity.

## Activity: I downloaded Process Monitor, launched it on my device, and captured the live activity as shown below.

## Screenshot:

A screenshot of a computer program

AI-generated content may be incorrect.

## 3. Whois

Purpose:  
Whois is a command-line utility that retrieves registration information of domain names or IP addresses.

Activity:  
I downloaded Whois from Sysinternals and ran the application on my device. The license agreement appeared as expected. Since no domain was provided, the tool exited after accepting the license.

A screenshot of a computer

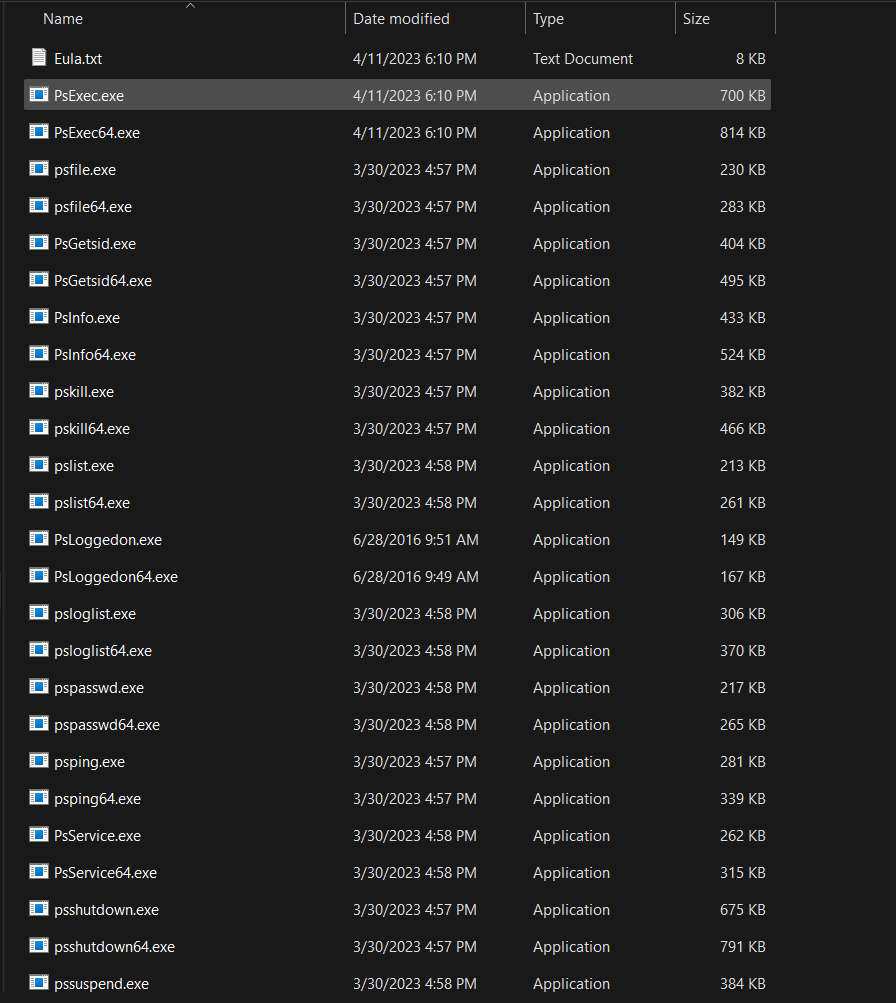
AI-generated content may be incorrect.Screenshot:

**4.PSTools**

**Purpose:**  
PsTools is a collection of command-line utilities from Sysinternals used for remote system management and local administrative tasks. It includes tools like PsExec, PsKill, PsList, PsLoggedOn, and others.

**Activity:**  
I downloaded PsTools from the official Microsoft Sysinternals website, extracted the ZIP file on my device, and viewed the list of tools included in the package.

**Screenshot:**

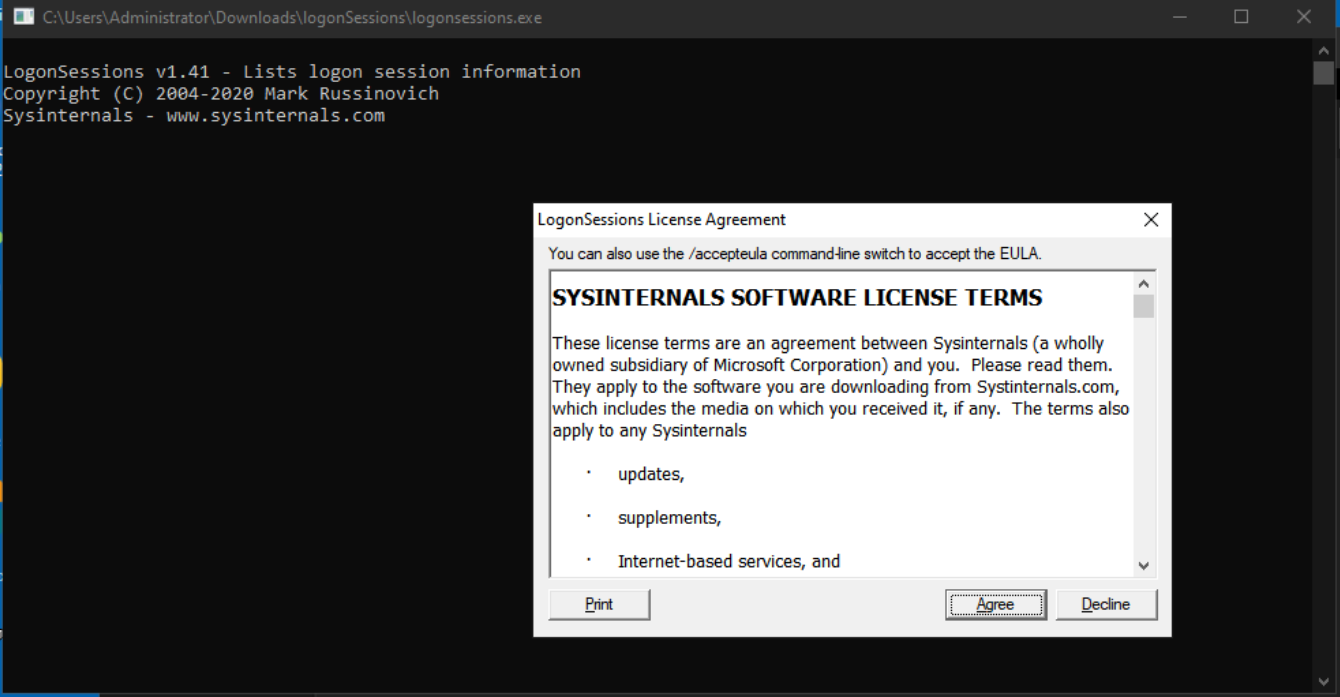


**5. Logon Sessions:**

Purpose:  
LogonSessions.exe is a Sysinternals command-line tool that displays details about all active user logon sessions on the system. It shows session IDs, logon times, usernames, domains, and authentication methods. It's commonly used for security monitoring and session tracking.

Activity:  
I downloaded LogonSessions.exe from the official Sysinternals website and ran it on my device. The license agreement (EULA) prompt appeared. After accepting it, the window closed immediately as the tool was not executed from the command line.

**Screenshot:**

****

**6. sysmon**

Purpose:  
Sysmon (System Monitor) is a powerful Windows system service and driver from Sysinternals that logs detailed system activity to the Windows Event Log. It captures events like process creation, network connections, file changes, and more, making it a valuable tool for security monitoring and incident response.

Screenshot:

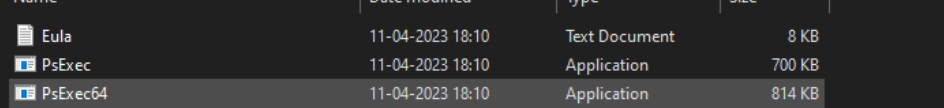
A screenshot of a computer

AI-generated content may be incorrect.

**7.PSExce**

Purpose:  
PsExec is a Sysinternals command-line utility that allows administrators to run processes and commands on remote systems as if they were running locally. It's widely used for remote software installations, patch deployment, and system administration without needing remote desktop access.

**Screenshot:**

****

**8. steps to create for Microsoft intune portal**

Here are the basic steps to create and configure in Microsoft Intune portal:

1. **Sign in** to Microsoft Intune Admin Center
2. Go to **Devices** > Choose platform (e.g., Windows)
3. Click on **Configuration profiles**
4. Click **+ Create profile**
5. Choose platform (e.g., Windows 10 and later) and profile type
6. Configure the **profile settings** (like policies, restrictions, etc.)
7. Click **Next**, assign to user or device groups
8. Review and click **Create**

**Screenshot:**

**A screenshot of a computer

AI-generated content may be incorrect.**