**Batch information:**

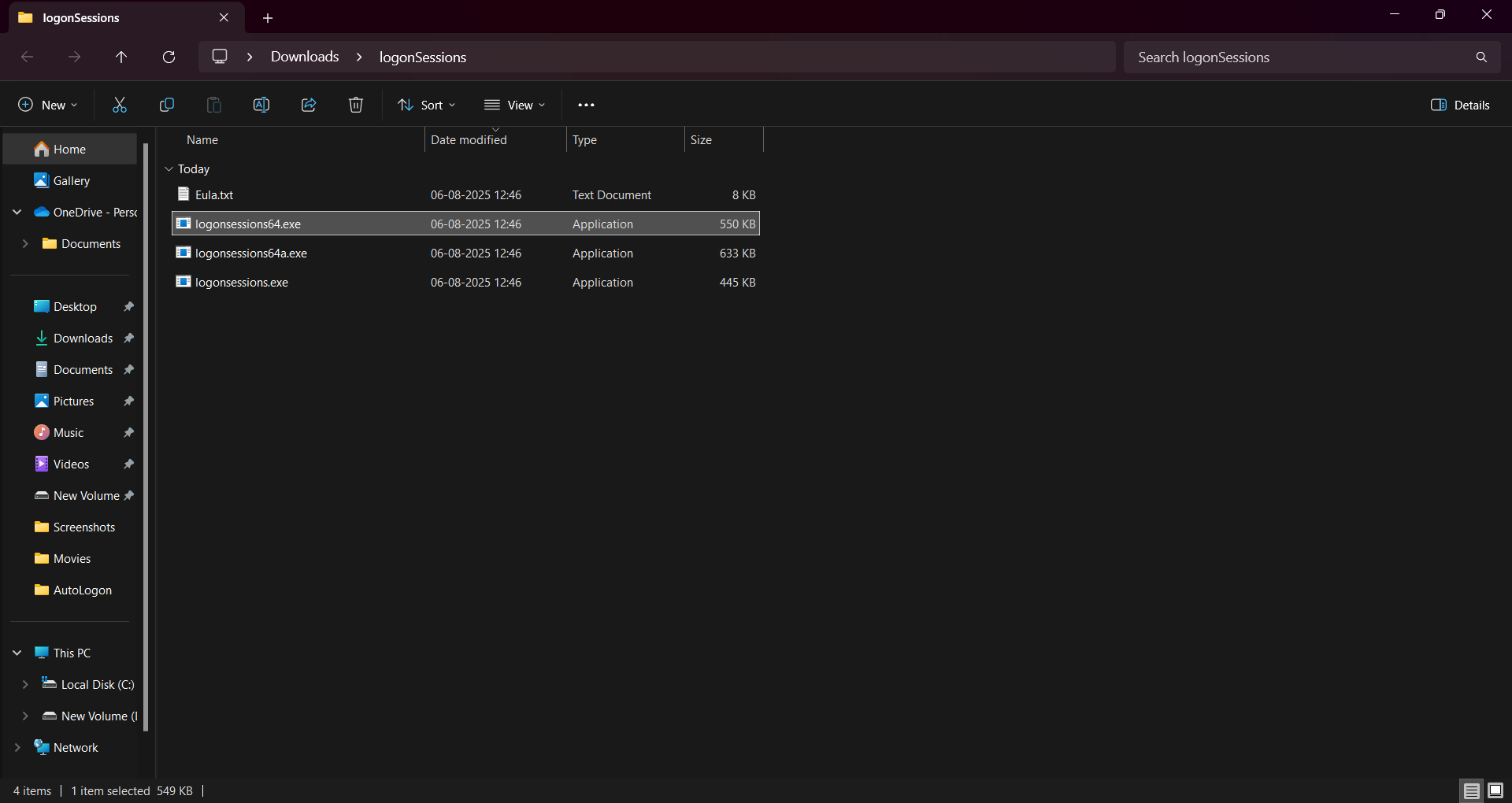
* **Batch Start Date: 2025-08-04**
* **Batch Name: WiproNGA\_DWS\_B7\_25VID2550**
* **First Name: Seetal**
* **Last Name: Biswal**
* **User Id: 34933**
* **Batch ID: 25VID2550**
* **Assignment Name-Using Windows Tools for Debugging\_ LogonSessions, Autologon, Process Explorer ,Psexec, PSTools, RegMon, Whois, SysMon and steps to create for Microsoft Intune portal**

1. **Logon Session:-** A logon session refers to the period of time a user is actively logged in to a computer, network, or application. During this session:

1. User authentication: The user provides credentials (e.g., username, password) to access the system.

2. Session establishment: The system verifies the credentials and grants access.

3. Session activities: The user performs actions, such as accessing files, running applications, or modifying settings.



1. **Autologon:-** AutoLogon is a Windows feature that allows a user to automatically log into their account when the computer starts up, without manually entering a username and password.

**How it works:** When enabled, the username, domain, and password are securely stored in the Windows registry. During boot, Windows uses this info to log in the user automatically.

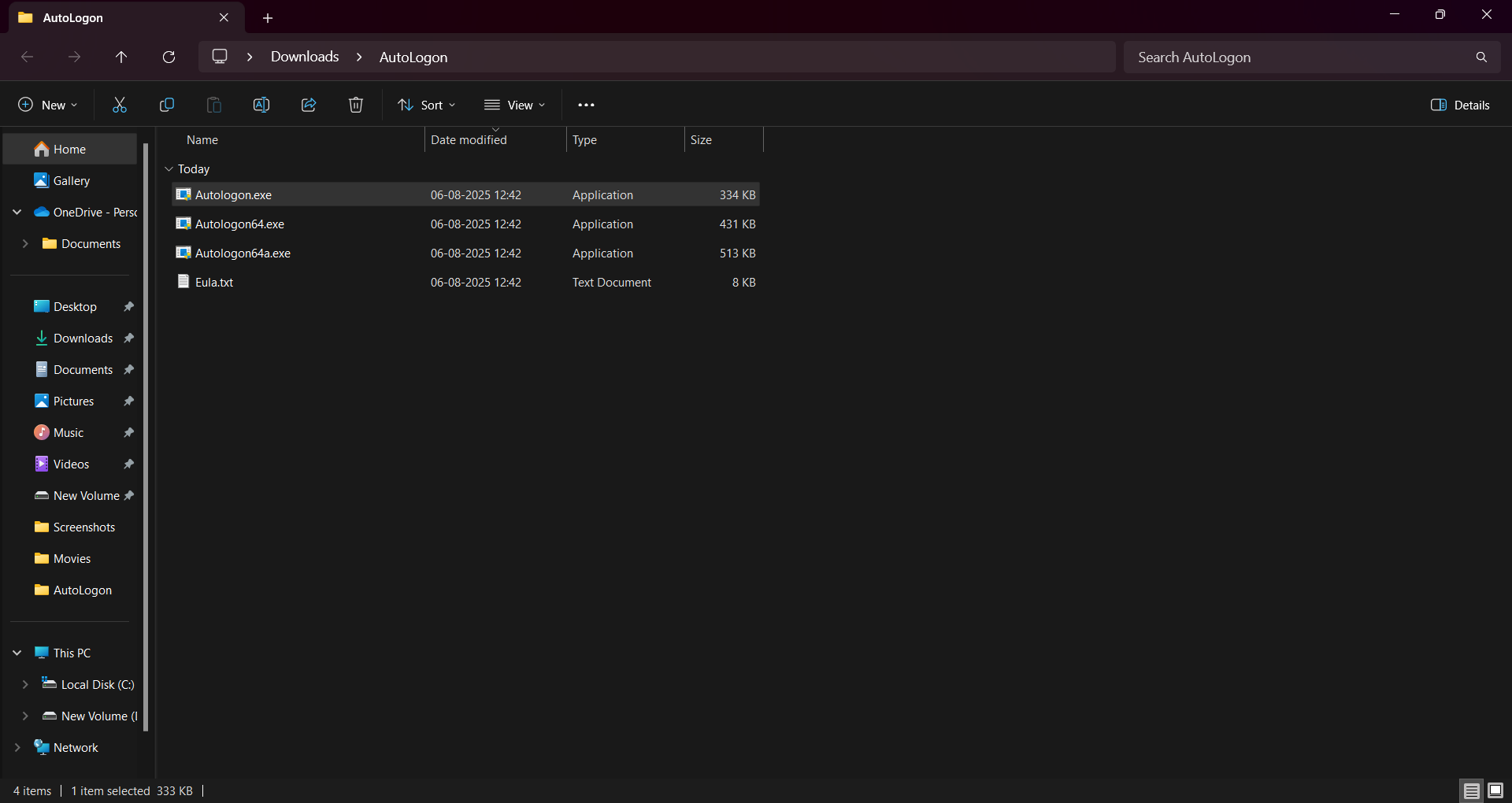
**Use Cases:**

Kiosks or Digital Signage systems

Lab or classroom computers

Testing environments

Corporate devices with single-user setups



1. **Process Explorer:-**

Process Explorer is an advanced system monitoring and troubleshooting tool from Microsoft Sysinternals that shows detailed information about all the processes running on your Windows computer.

**Use Cases:**

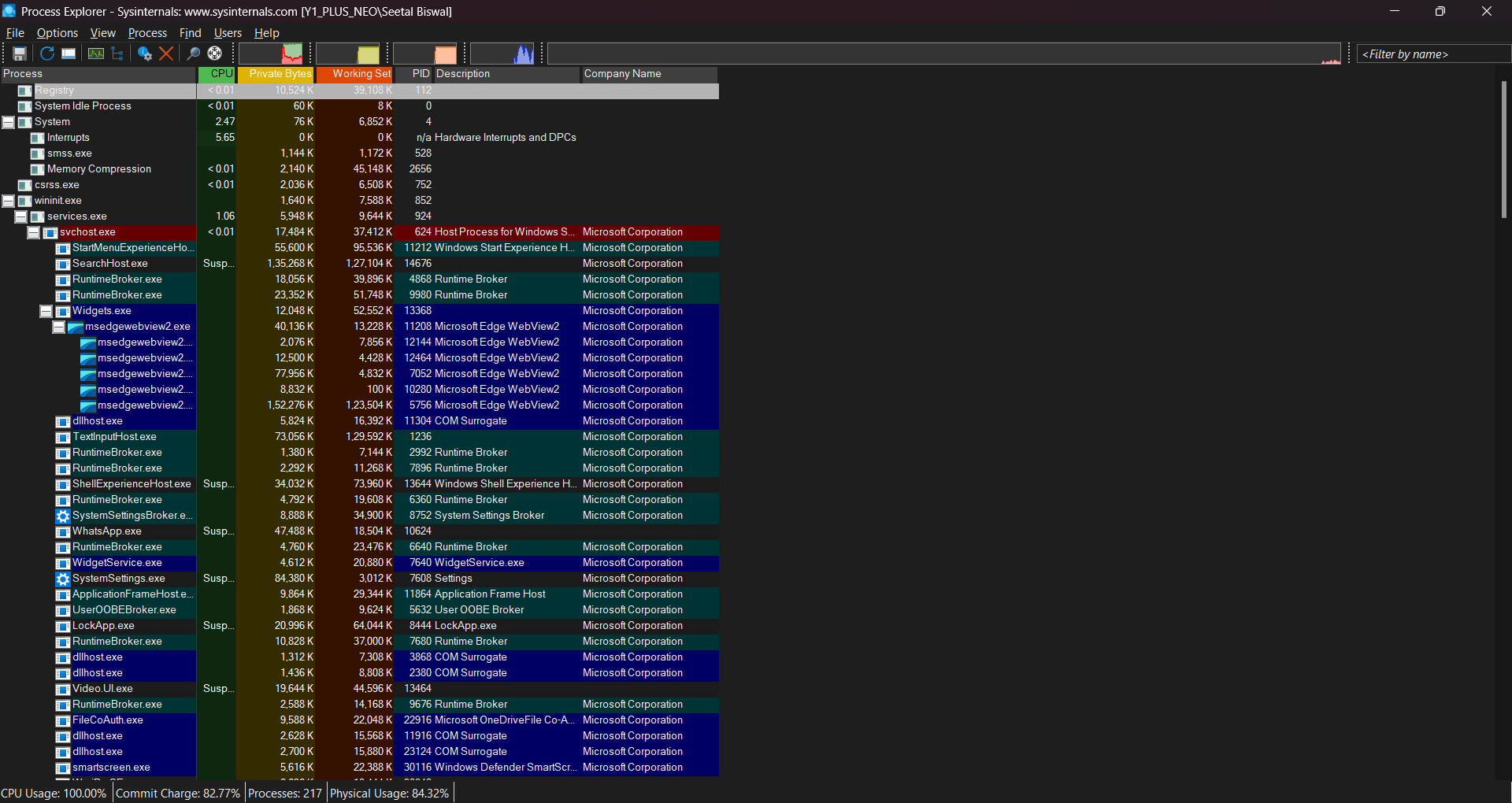
Debugging application behaviour

Finding malware or suspicious processes

Identifying which process is hogging CPU or RAM.

Unlocking files that can’t be deleted

Exploring what a process is doing behind the scenes.



1. **PSexec:-** PsExec is a powerful command-line tool from Microsoft Sysinternals that lets you run processes on remote systems — as if you were sitting at that computer.

**Common Use Cases:**

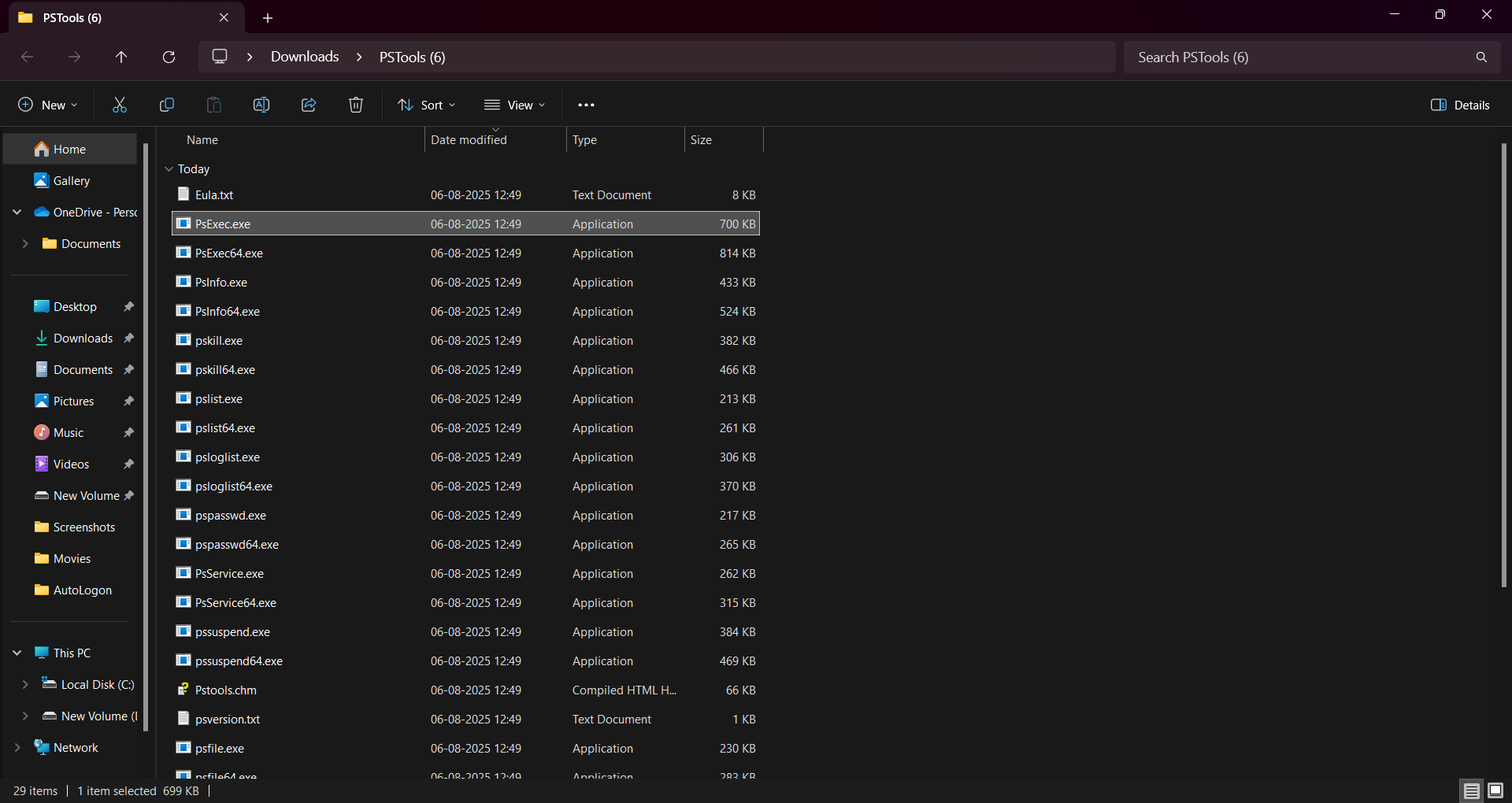
Remote software deployment

Admin tasks (without logging in)

Troubleshooting remote systems

Running processes as SYSTEM (for deep testing)

1. **PsTools:-** PsTools is a suite of powerful command-line utilities from Microsoft Sysinternals that let you manage local and remote Windows systems — without needing a GUI or RDP.

****

**RegMon:-** Registry Monitor is a tool that tracks and monitors changes made to the Windows Registry. It's useful for troubleshooting, detecting malware, or understanding how applications interact with the registry.

Some popular registry monitoring tools include:

1. Process Monitor: A powerful tool from Sysinternals that monitors registry, file, and process activity.

2. Registry Monitor (Regmon): A legacy tool from Sysinternals that specifically monitored registry activity.

1. **Sysmon:-** Registry Monitor is a tool that tracks and monitors changes made to the Windows Registry. It's useful for troubleshooting, detecting malware, or understanding how applications interact with the registry.

Some popular registry monitoring tools include:

1. Process Monitor: A powerful tool from Sysinternals that monitors registry, file, and process activity.

2. Registry Monitor (Regmon): A legacy tool from Sysinternals that specifically monitored registry activity.

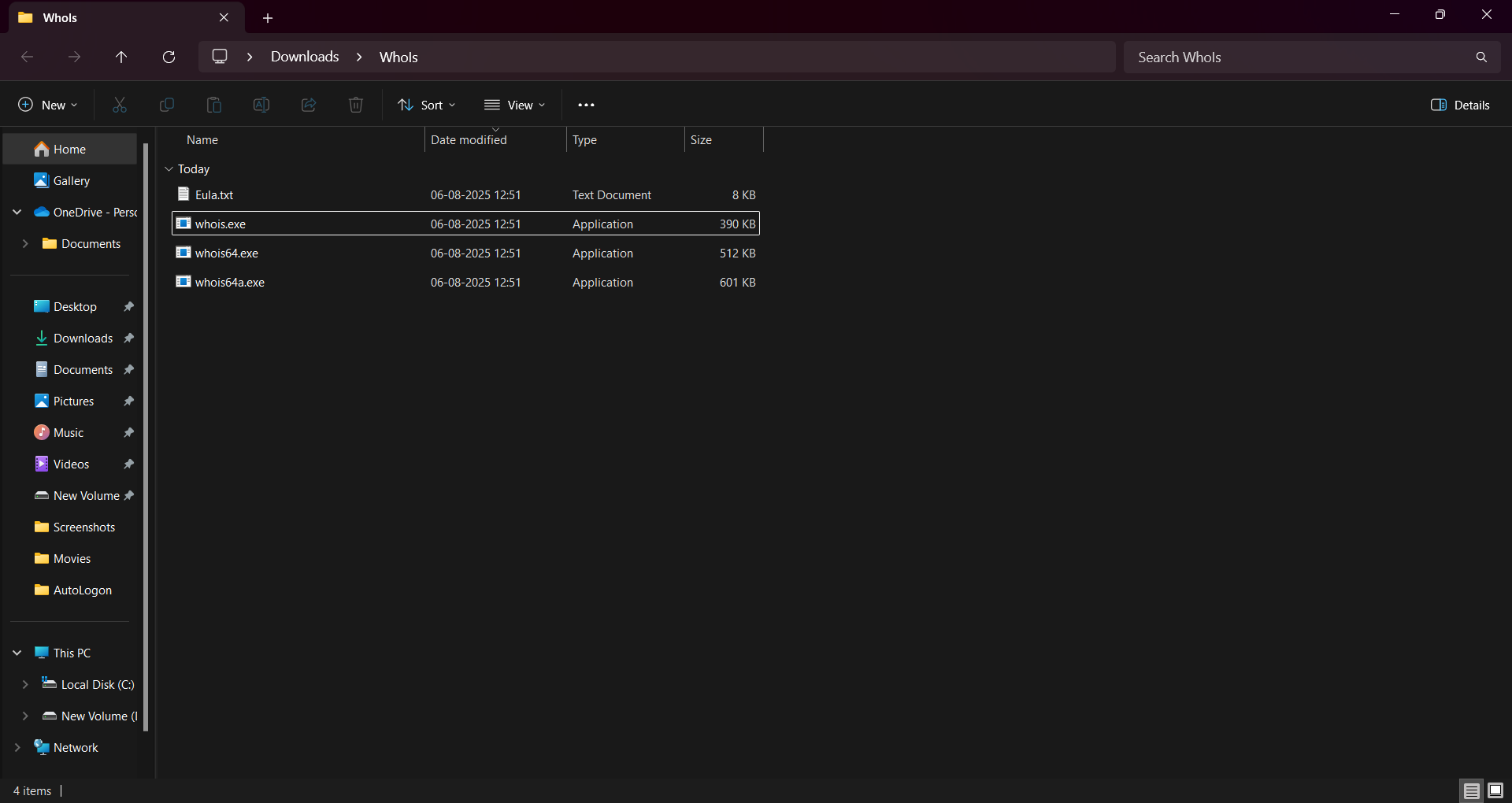
1. **Whois:-** WHOIS is a protocol used to query databases that store information about domain name registrations, IP addresses, and other internet resources.

It helps you find details about:

1. Domain ownership: Who owns a domain name?

2. Contact information: How to reach the domain owner or registrar?

3. Registration details: When was the domain registered, and when does it expire?



**To create a Microsoft Intune portal, follow these steps:**

**Prerequisites:**

1. Azure AD Premium subscription: Ensure you have an Azure Active Directory (Azure AD) Premium subscription.

2. Intune licenses: Assign Intune licenses to users or groups.

**Step-by-Step Guide:**

1. Sign in to Microsoft Endpoint Manager admin center: Go to [(link unavailable)]((link unavailable)) and sign in with your Azure AD credentials.

2. Create an Intune tenant: If you haven't already, create an Intune tenant by following the on-screen instructions.

3. Configure Intune settings: Set up Intune settings, such as:

- Device settings: Configure device restrictions, enrollment, and compliance policies.

- User settings: Set up user policies, such as conditional access and app protection.

4. Enroll devices: Enroll devices into Intune, either:

- Automatically: Through Azure AD join or hybrid Azure AD join.

- Manually: Using the Intune Company Portal app or other enrollment methods.

5. Deploy apps: Deploy apps to users or devices using Intune.

6. Monitor and manage: Monitor device and user activity, and manage Intune settings as needed.

**Additional Resources:**

1. Microsoft Intune documentation: Visit the official Microsoft Intune documentation for detailed guides and tutorials.

2. Intune tutorials: Explore Microsoft's Intune tutorials and training resources.