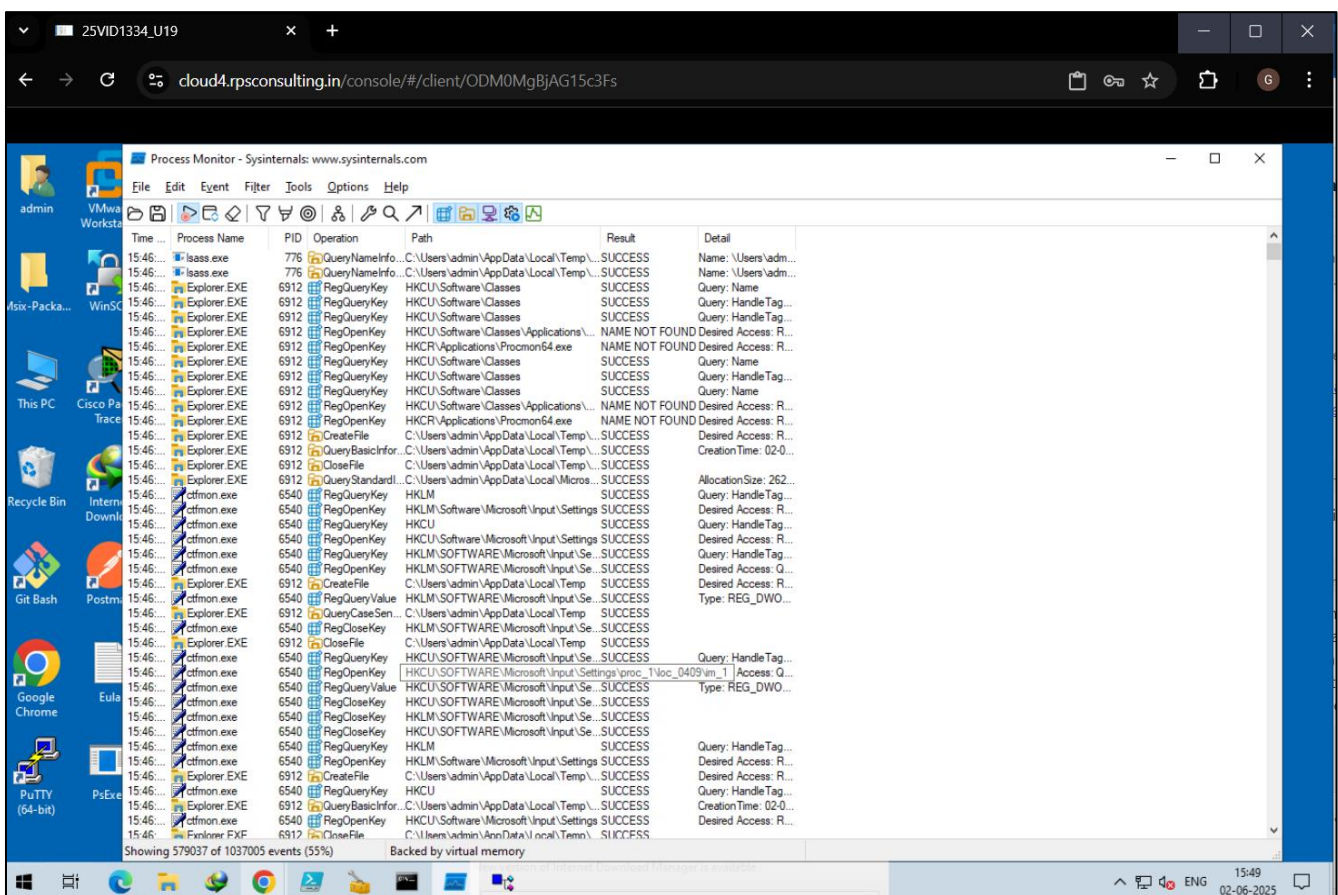


Process Monitor

- **Process Monitor** is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity.
- It combines the features of two legacy Sysinternals utilities, **Filemon** and **Regmon**.
- Its **functions** are Captures file system, registry, and process activity in real-time.
- Use filters to narrow down the captured events to specific processes or operations.
- It monitors file access, registry keys and process behaviour to pinpoint issues.
- The **benefits** include offering a detailed view of system interactions, helping to diagnose application startup issues, file access problems and more.

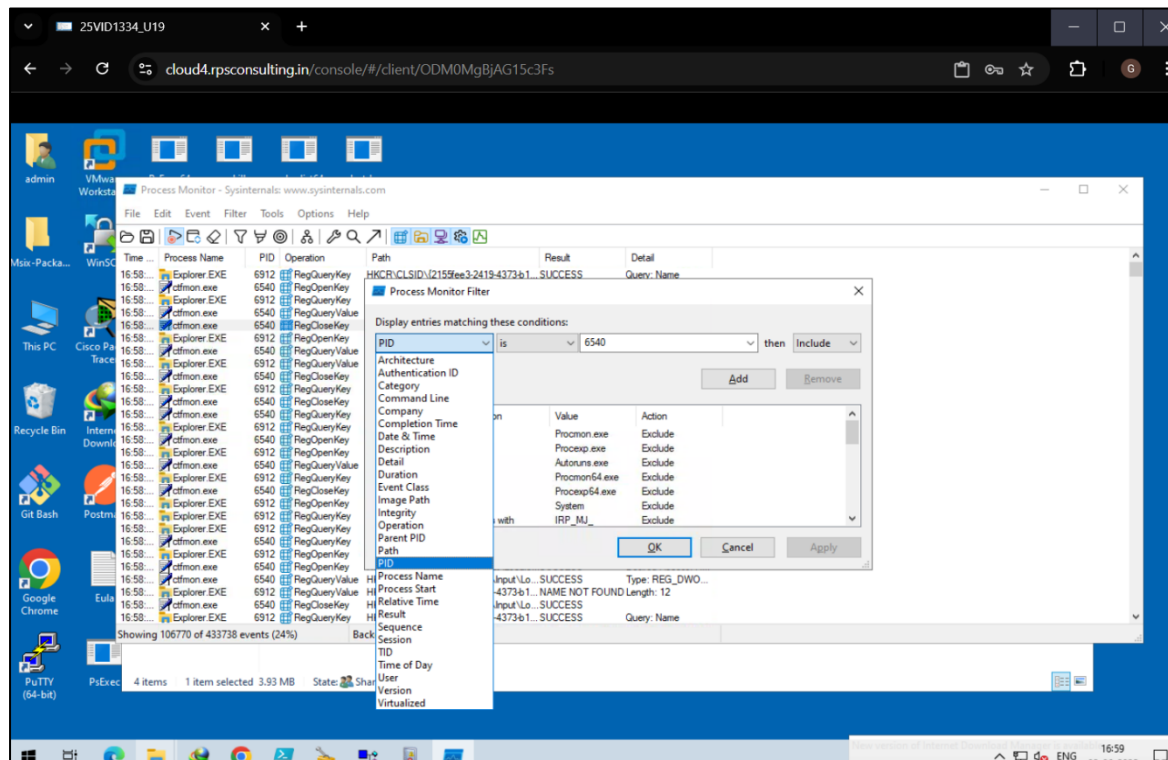


STEPS OF PROCESS MONITOR

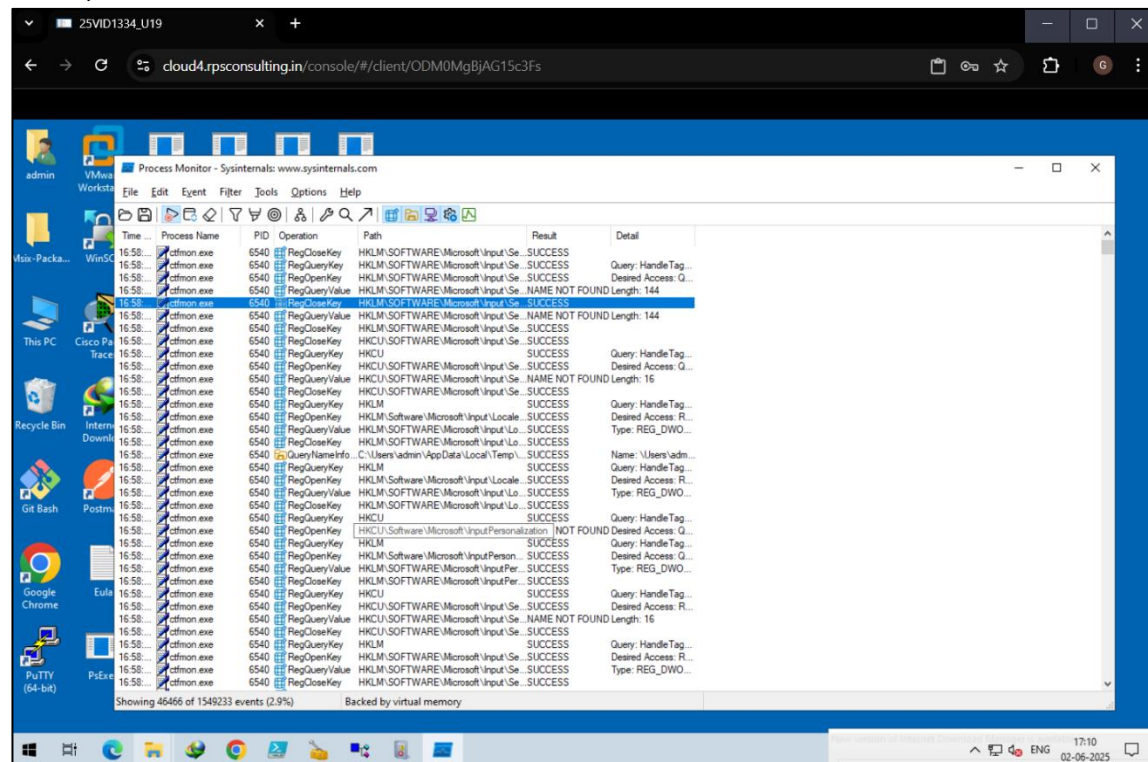
Step 1: Download the process monitor from the link (<https://learn.microsoft.com/en-us/sysinternals/downloads/procmon>)

Step 2: Extract the zip files and run the **Procmon.exe**

Step 3: To filter the Process Use the **Filter** (or use Ctrl+L) and then a window will appear in that select the **Process Name (Ex:- PID)** first dropdown then in the text field specify the value (Ex:- 6540 this is the PID) then press **OK**



Step 4: All the processes which are filtered will be shown (Here, for example the PID with 6540 are shown)



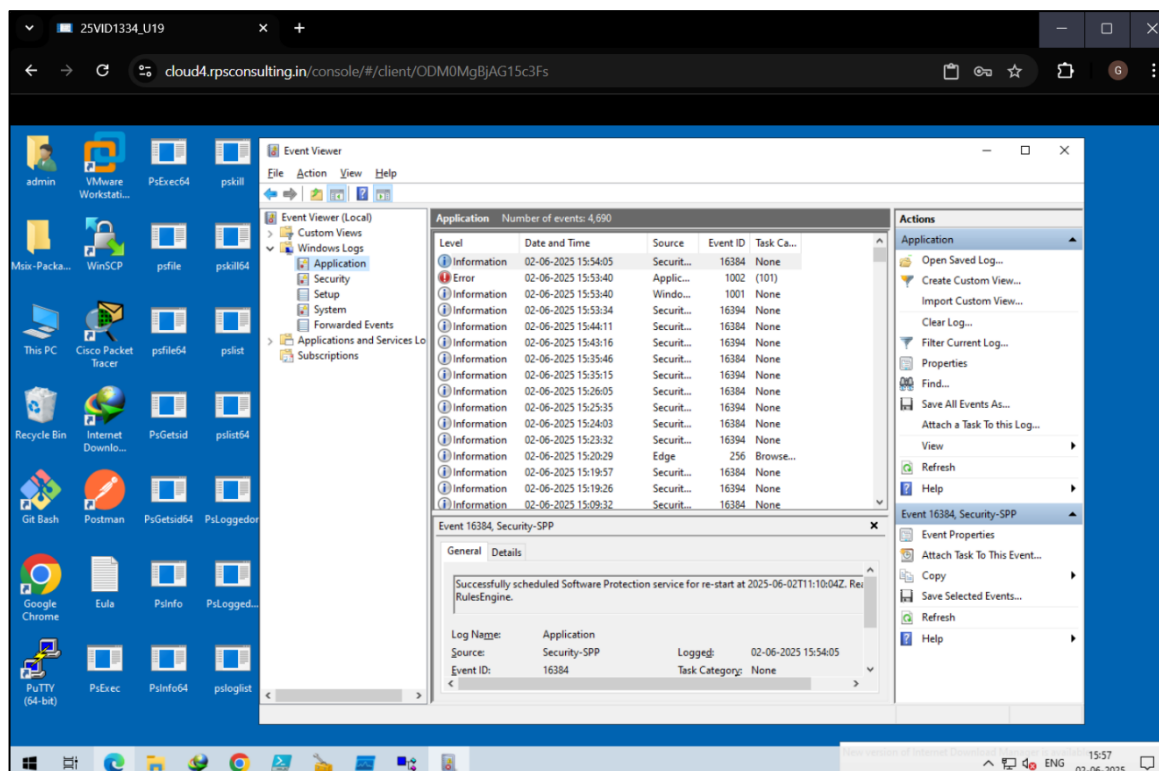
Event Viewer

- Event Viewer is used to **identify** the **System-Level Errors** related to the installation.
- It's used for **troubleshooting** problems, monitoring security events, diagnosing system or application errors, and more.
- Its **functions** are to log system events including errors, warnings and information messages.
- It searches for relevant error messages, warnings or event IDs to understand the nature of the problem.
- It provides a historical record of system activity, helping to identify recurring problems and pinpoint the source of errors.

STEPS OF EVENT VIEWER

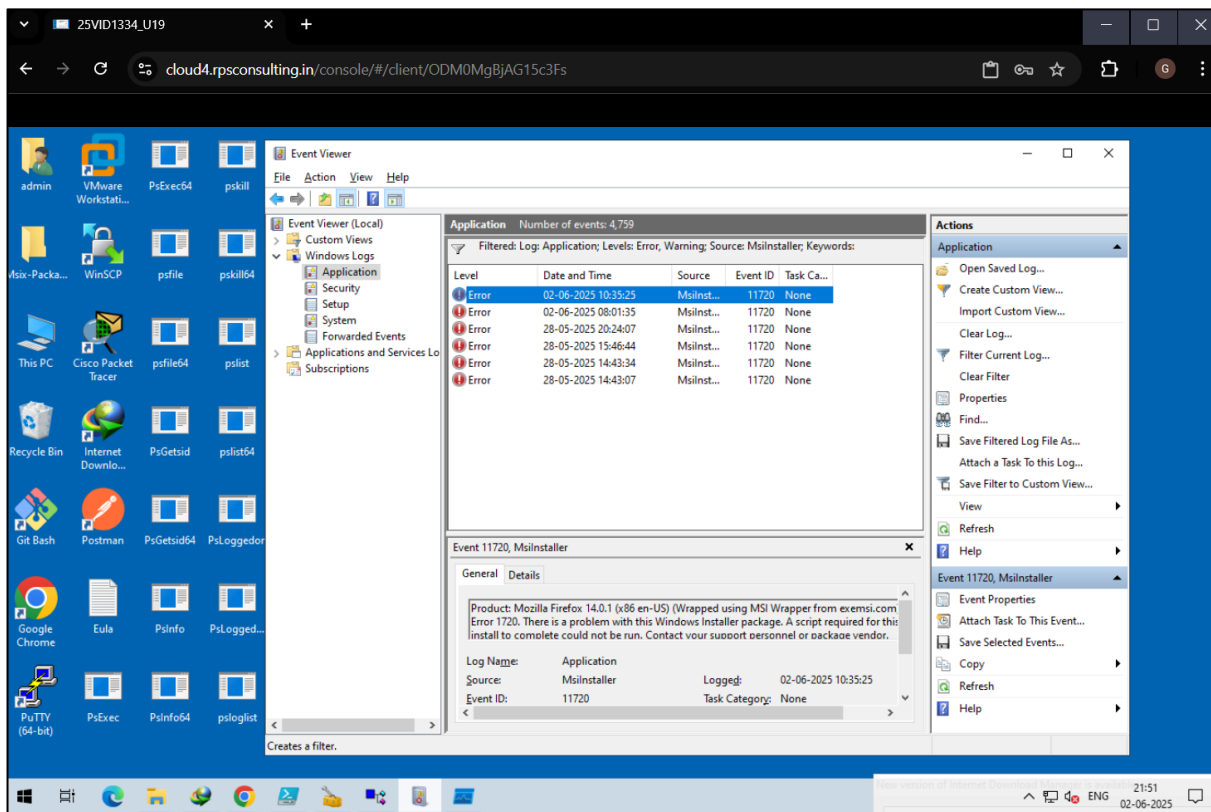
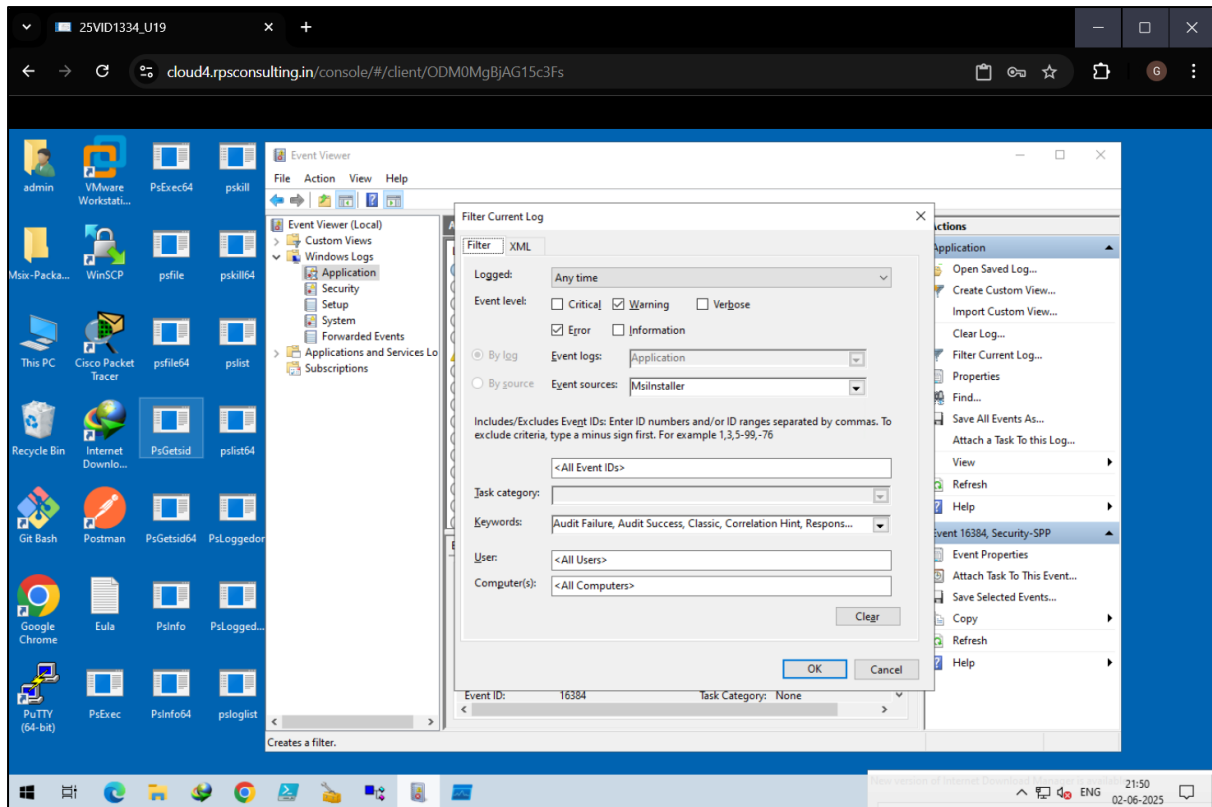
Step 1: Open Event Viewer from the Start Menu.

Step 2: Navigate to the **Windows Logs**, expand the Windows Logs in that **Application, Security, Setup, System** are available select one in that events will be present (Here in the Application - 4690 Events are present)



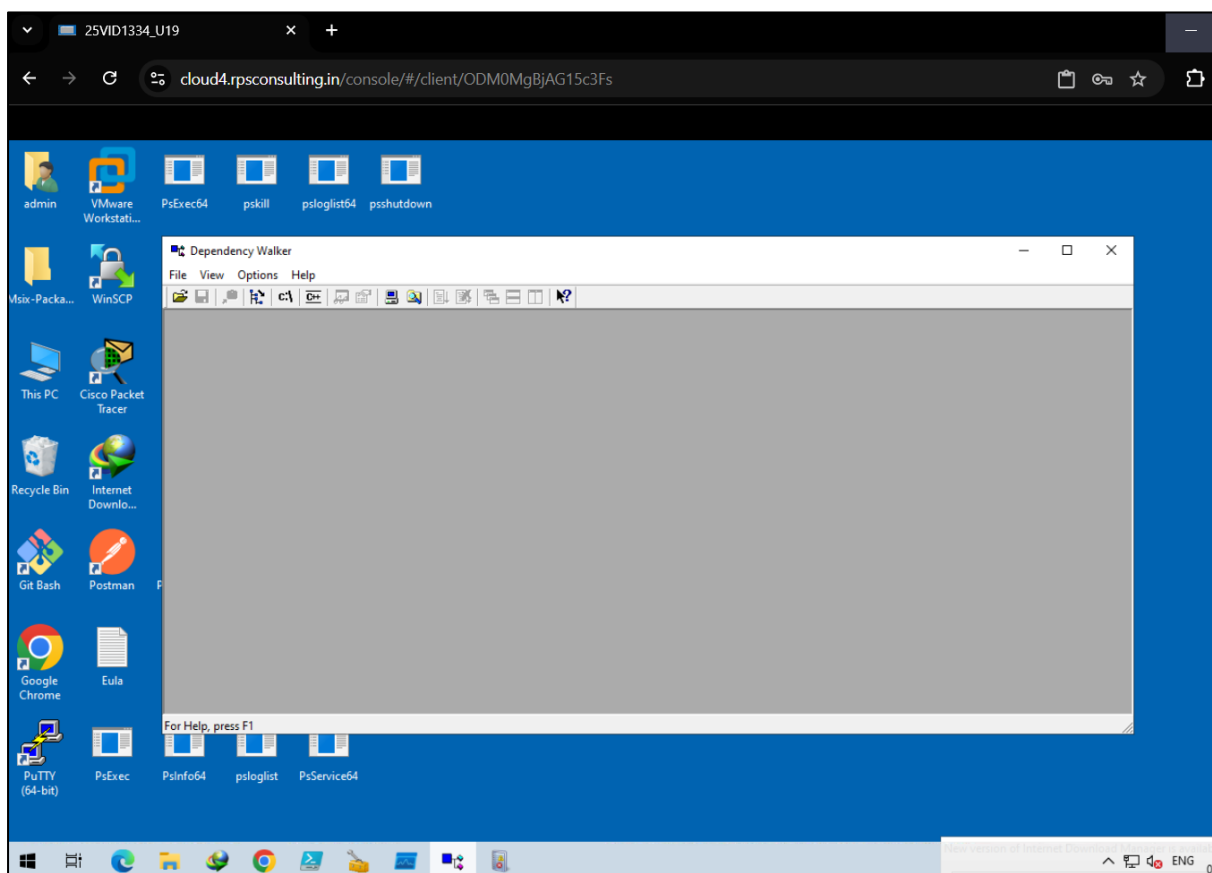
Step 3: In the **Actions** pane (right side), click **Filter Current Log**. In the filter window, under **Event sources**, select **MsiInstaller**. You can also filter by **Event level** (e.g., Error, Warning) to narrow down the results. Click **OK** to apply the filter

Step 4: Analyze the Event to identify the cause of MSI installation error(In the bottom pane).



Dependency Walker

- **Dependency Walker** is a free utility that scans any 32-bit or 64-bit Windows module (exe, dll, ocx, sys) and builds a hierarchical tree diagram of all dependent modules.
- For each module found it lists all the functions that are **exported** by that module and which of those functions are actually being **called** by other modules.
- It identifies missing or incorrect dependencies such as DLLs.
- Dependency Walker is also very useful for troubleshooting system errors related to loading and executing modules.
- It helps resolve problems caused by missing or corrupted dependencies ensuring that applications function correctly.
- It runs on Windows 95, 98, Me, NT, 2000, XP, 2003, Vista, 7, and 8



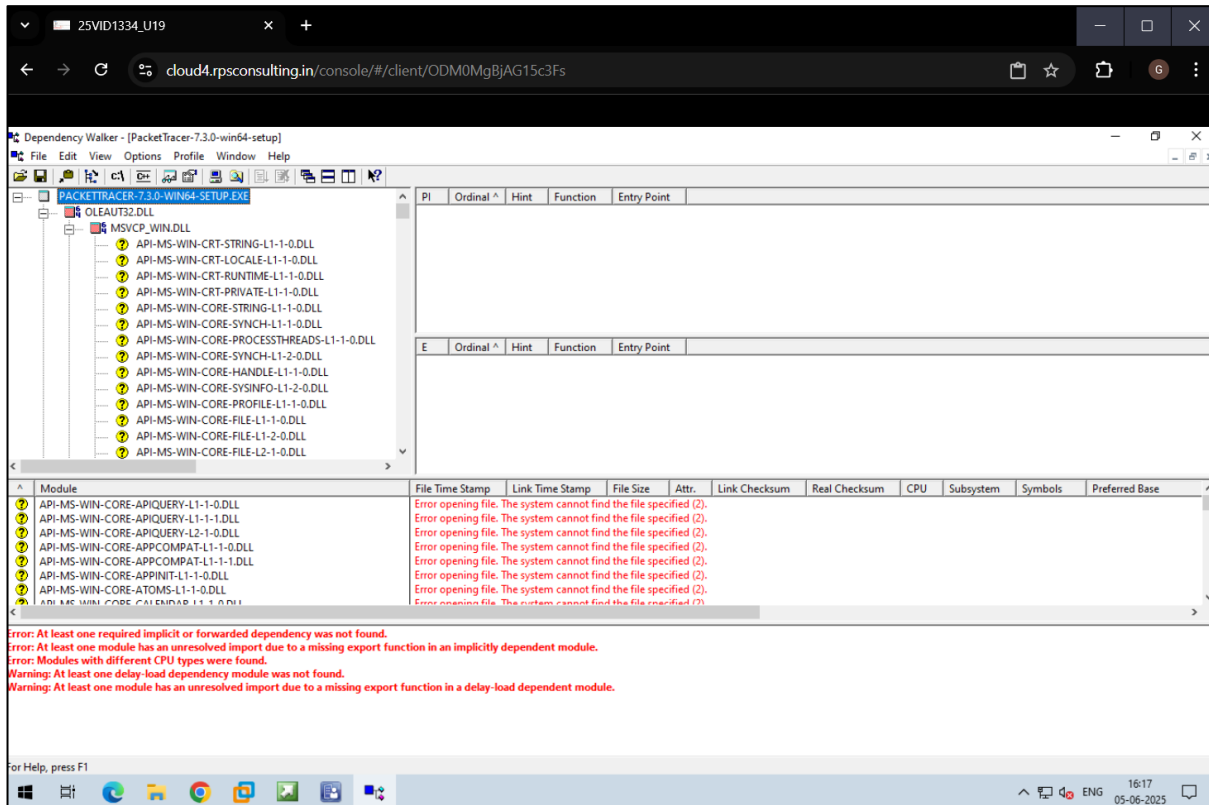
STEPS OF DEPENDENCY WALKER

Step 1: Download the **Dependency Walker** from the link (<http://dependencywalker.com/>)

Step 2: Extract the **depends22_x64.zip** file and run the **depends.exe** file.

Step 3: Click **File** and then click **Open** and select any .exe file.

Step 4: Analyze the errors shown in the logs window.



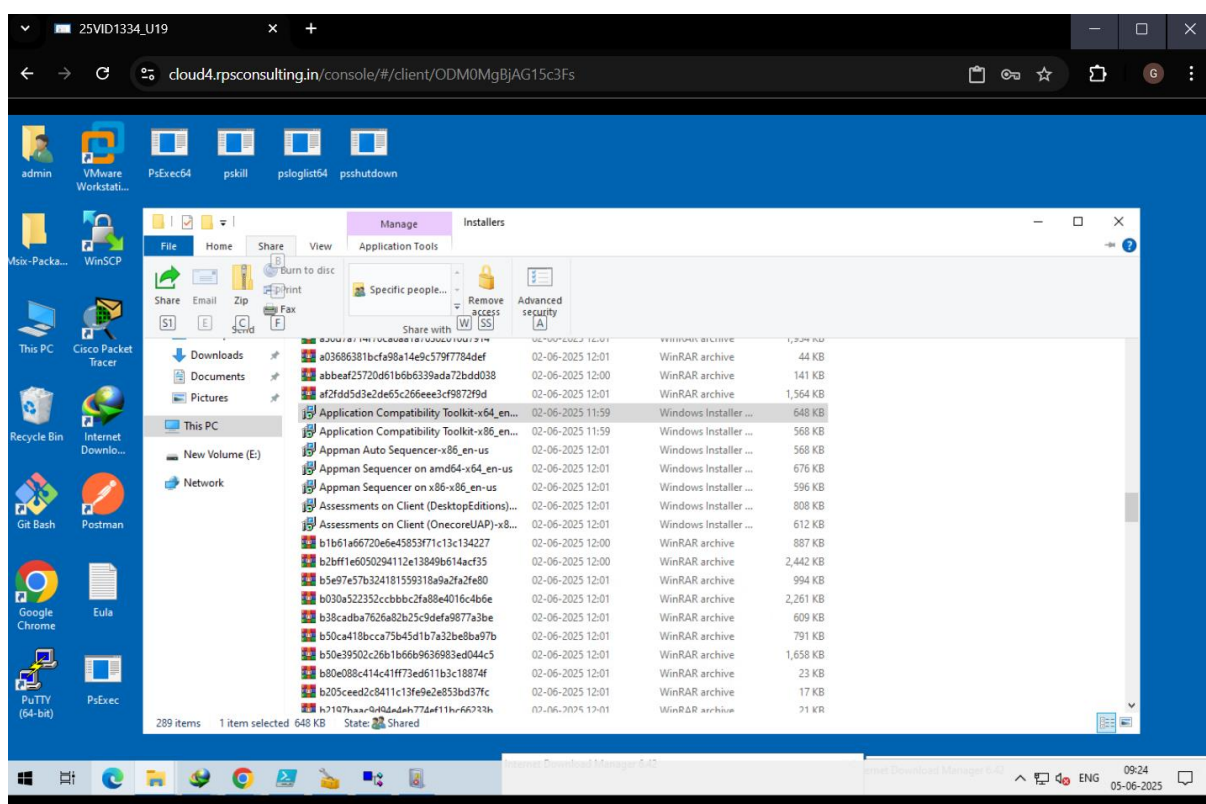
Application Compatibility Toolkit (ACT)

The **Application Compatibility Toolkit (ACT)** is a set of tools provided by **Microsoft** to help **test and fix compatibility issues** when deploying **new versions of Windows** in enterprise environments.

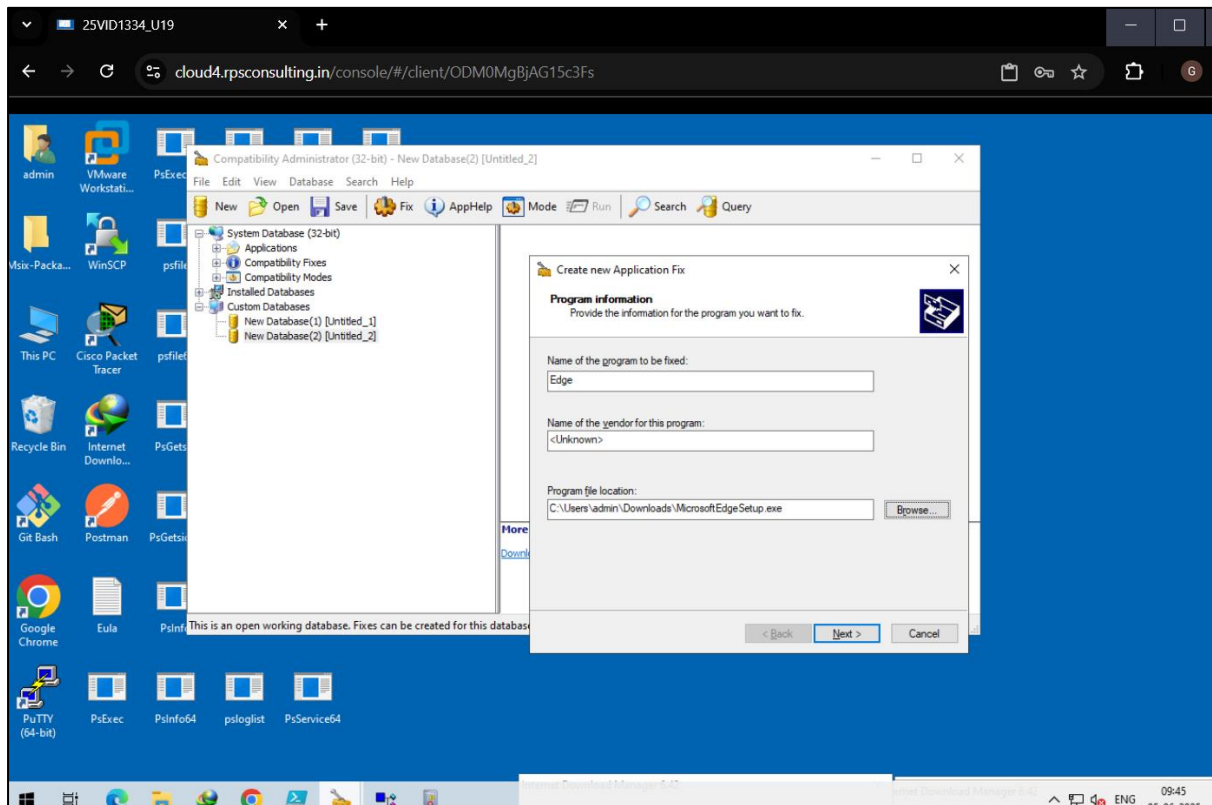
- The Microsoft Application Compatibility Toolkit (ACT) is a tool that assists in identifying and managing your overall application, reducing the cost and time involved in resolving application compatibility issues and helping us quickly to deploy Windows and Windows updates.
- With ACT we can analyze applications, websites and computers.
- We can manage compatibility of applications and configuration settings.
- It prioritizes application compatibility with filtered reporting.
- It is used to add and manage issues and solutions for our enterprise-computing environment.
- It is used to send and receive compatibility information from the Microsoft Compatibility Exchange
- Shims, registry edits, and virtualization are techniques used to enhance application compatibility and persistence on Windows systems.

Step 1: Download the ACT from the link (<https://learn.microsoft.com/en-us/windows-hardware/get-started/adk-install#download-the-adk-101261002454-december-2024>)

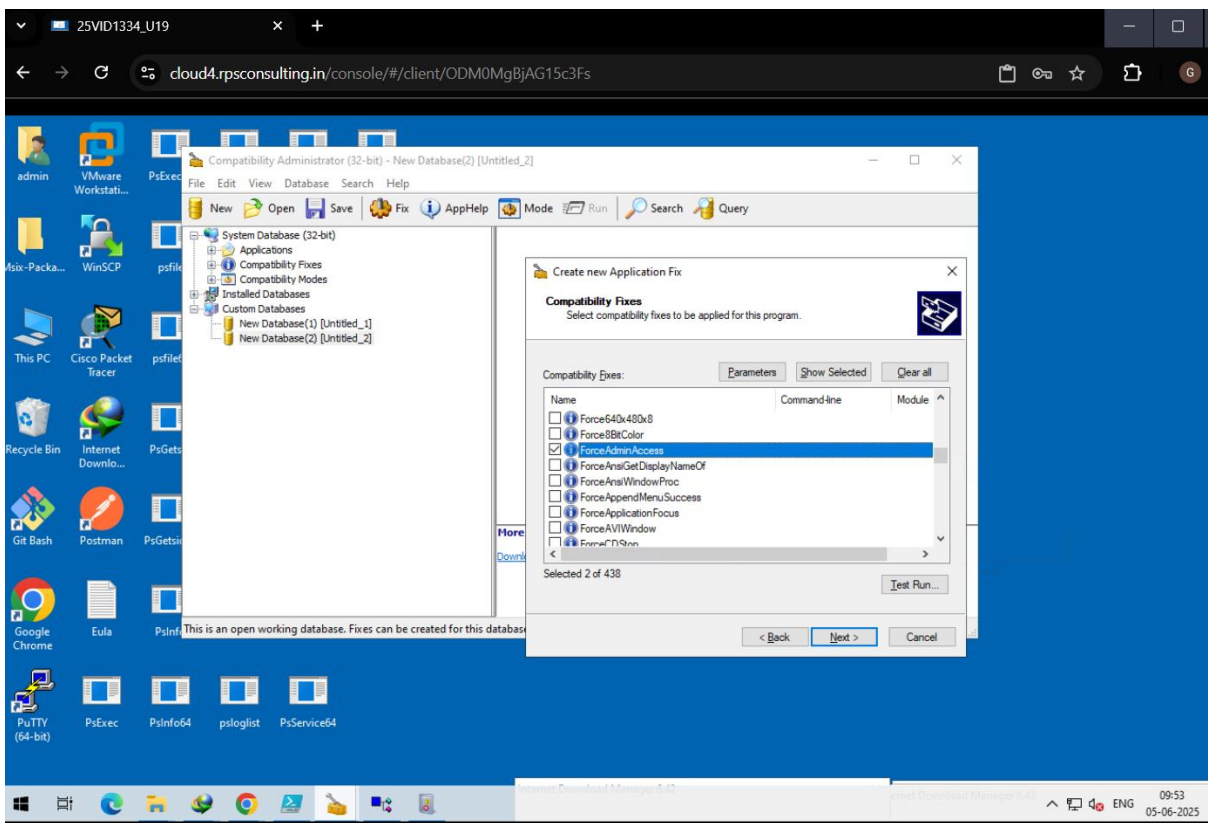
Step 2: Run the **adksetup.exe** and it will create a folder **Windows Kits** -> Navigate to **Windows Kits\10\ADK\Installers** and search for **Application Compatibility Toolkit x64**-> Open it and then it will download and in Start Menu search for **Compatibility Administrator 32/64**



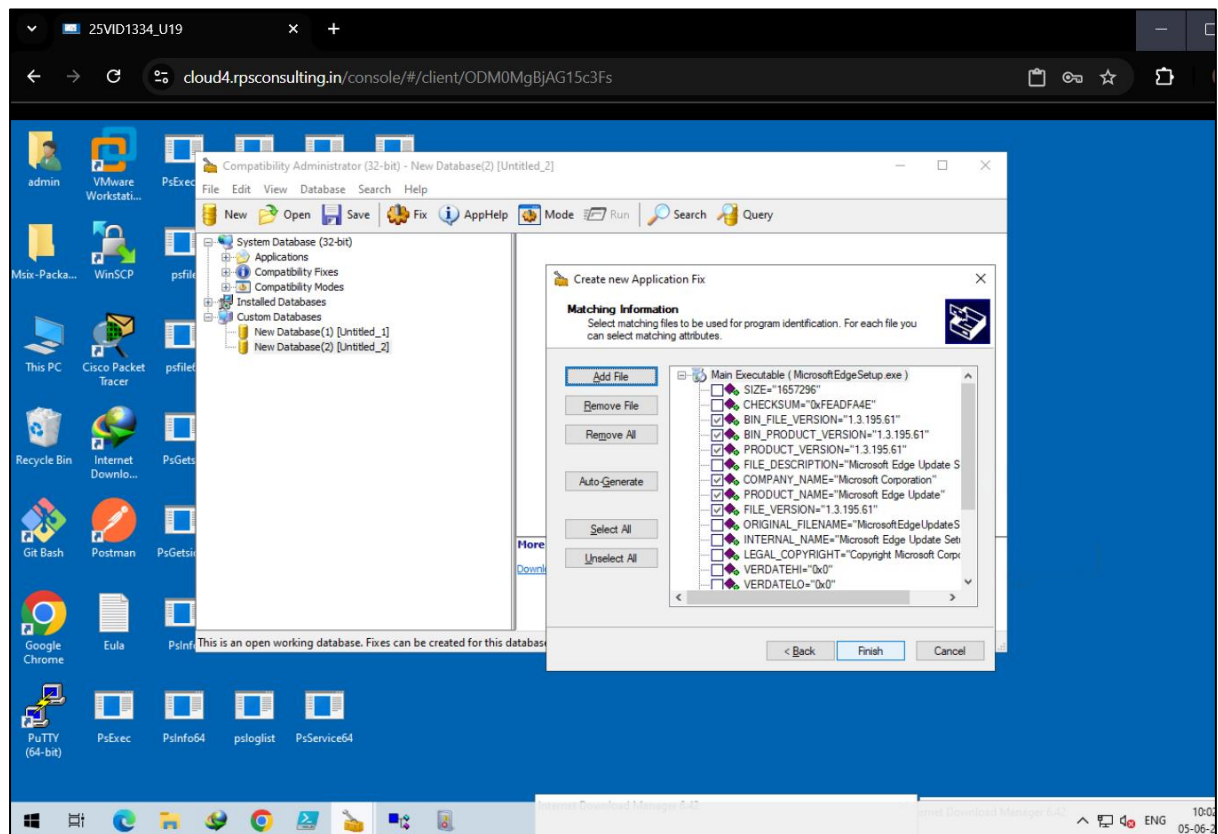
Step 3: Click on **new** -> in Custom Database Right click **New Database -> Create New-> Application Fix** then Enter the name and browser for **.exe file -> Next** then **In Compatibility Modes -> Next**



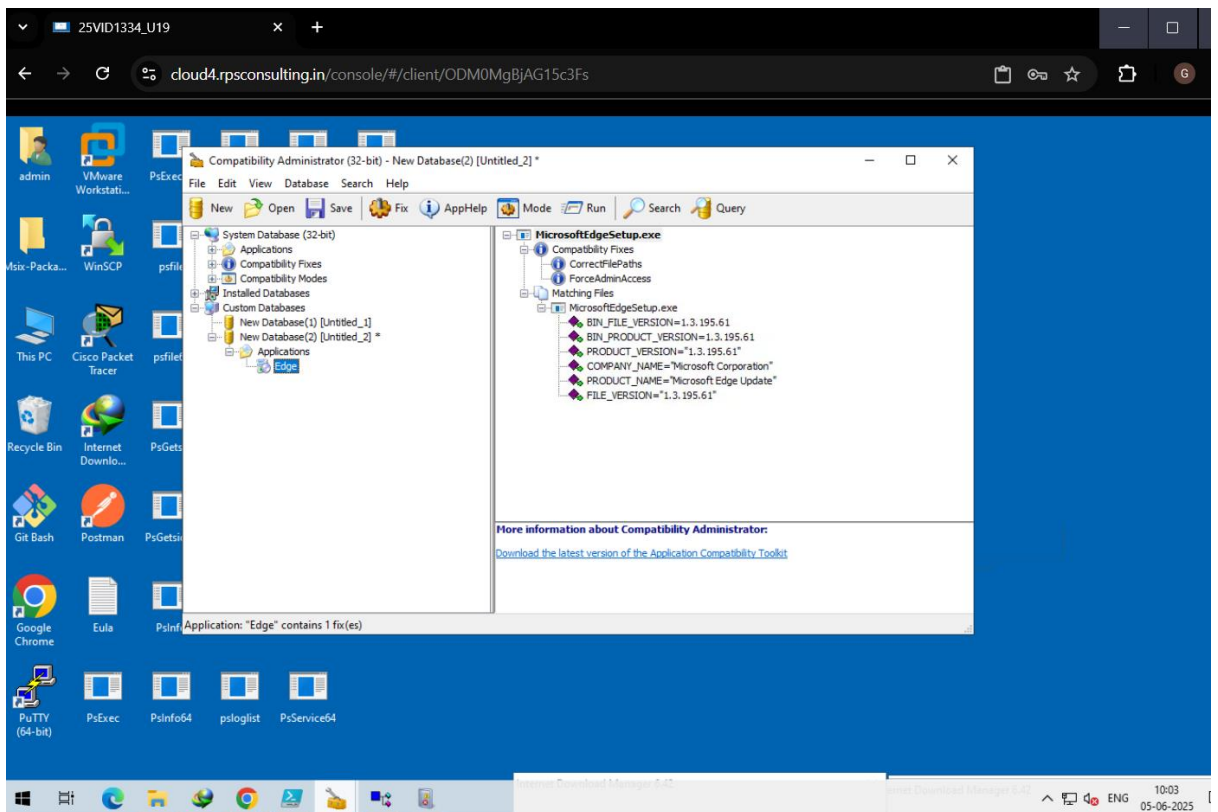
Step 4: In Compabatlity Fixes select **ForceAdminAccess, CorrectFilesPaths, etc -> Next**



Step 5: In Matching Information -> Finish



Step 6: Save this .sdb file



Step 7: Open **Command Prompt as Administrator** and run **sdbinst "C:\Path\MyFixes.sdb"**

