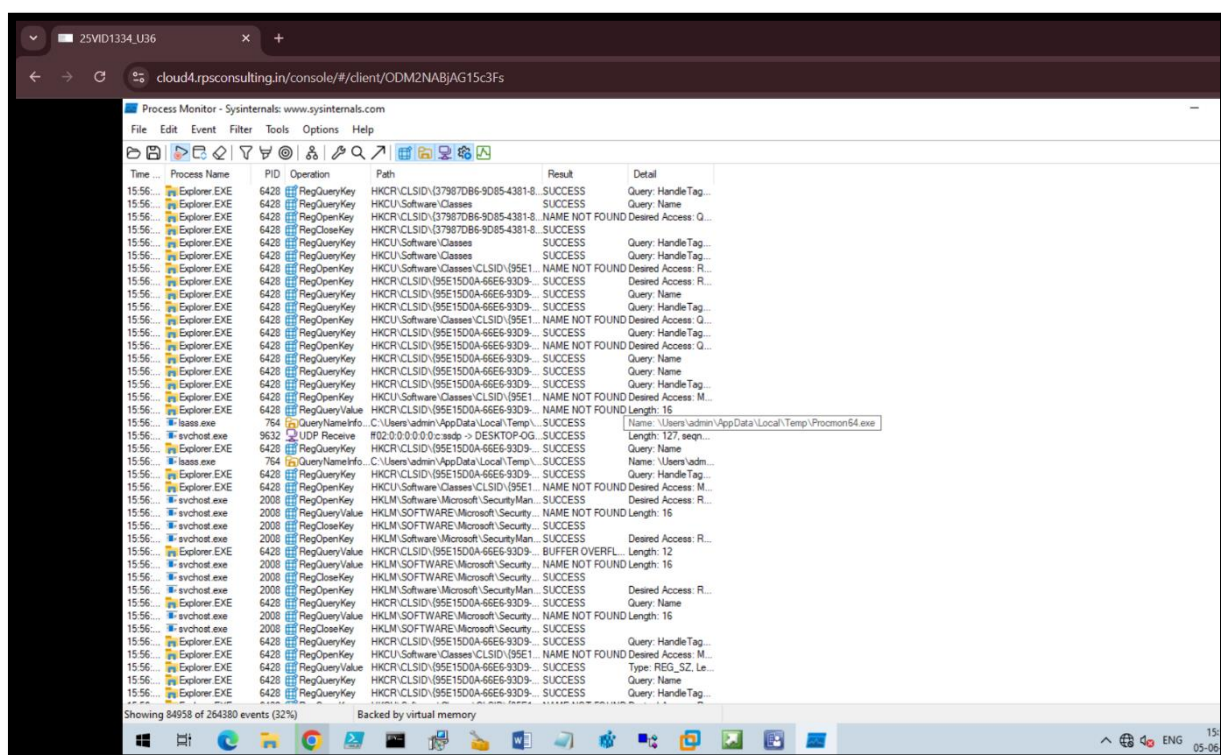


Step-by-Step Process

Process Monitor, Dependency Walker, Event Viewer and ACT (Application Compatibility Toolkit)

A. Process Monitor

- It 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.
- It 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.

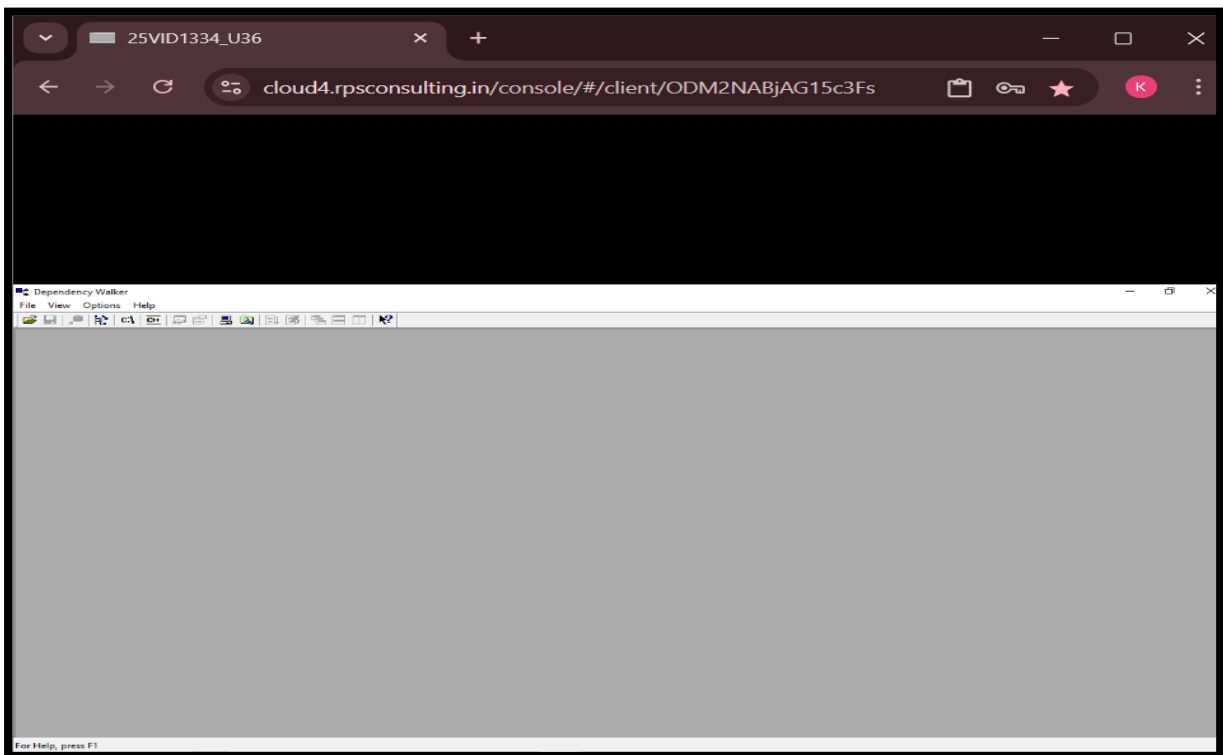


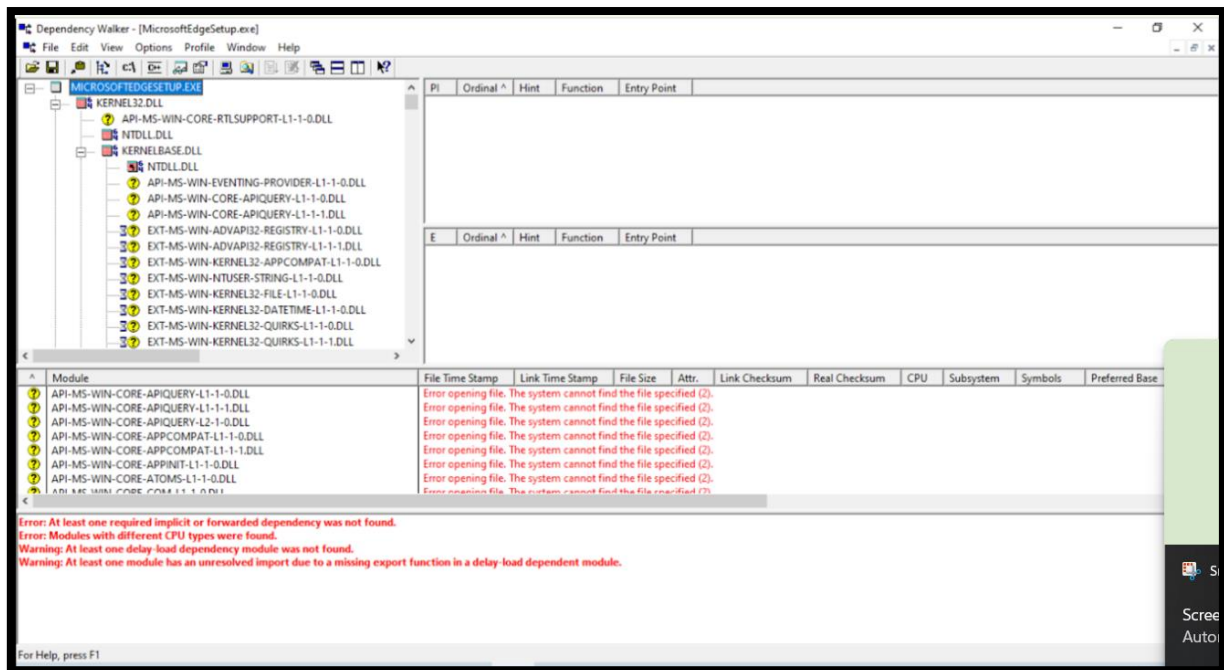
Steps:

- Download the Process Monitor from the link <https://learn.microsoft.com/en-us/sysinternals/downloads/procmon>
- Extract the zip files and run the Procmon.exe file.
- To filter the processes click on the Filter option (or use Ctrl+L) and then a window will appear, in that select the appropriate parameters for filtering. Example: PID in first dropdown, is in second dropdown, 752 in third dropdown, Include in fourth dropdown, then press OK.
- Then a dialog box comes asking You did not add the item you were editing. Add it now? So press Yes.
- All the processes which are filtered will be shown (Here, for example all the processes with PID as 752 are shown).

B. Dependency Walker

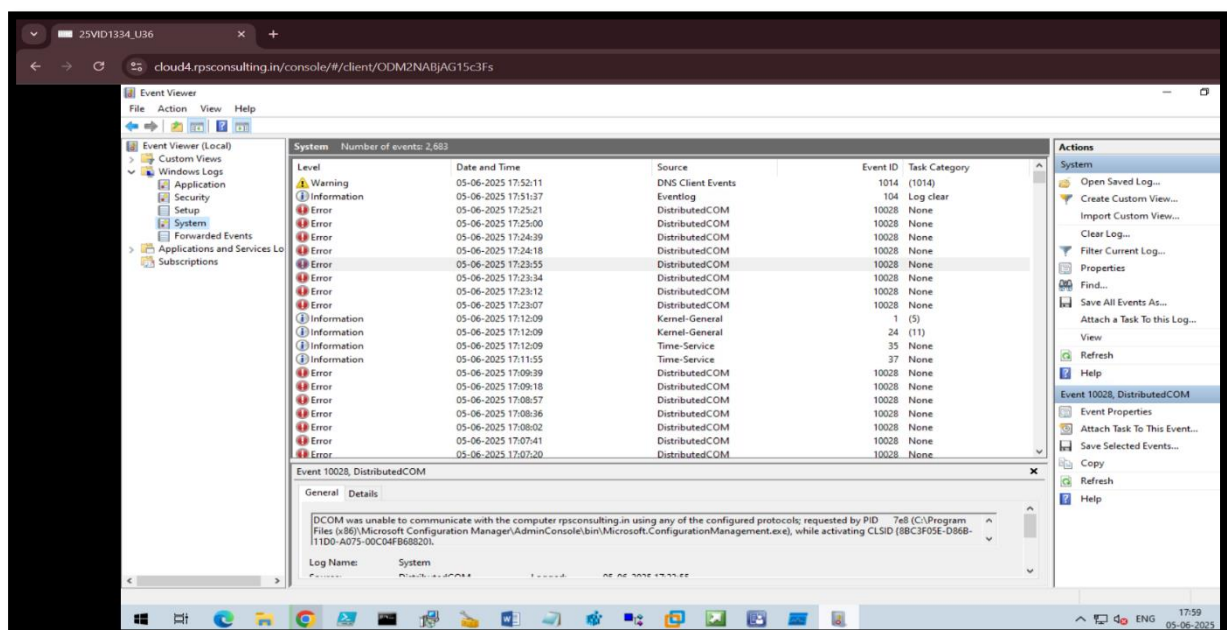
- Dependency Walker is a free utility that scans any 32-bit or 64-bit Windows module (exe, dll, ocx, sys) and builds a hierarchical tree diagram of all dependent modules.
- For each module found it lists all the functions that are exported by that module and which of those functions are actually being 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.





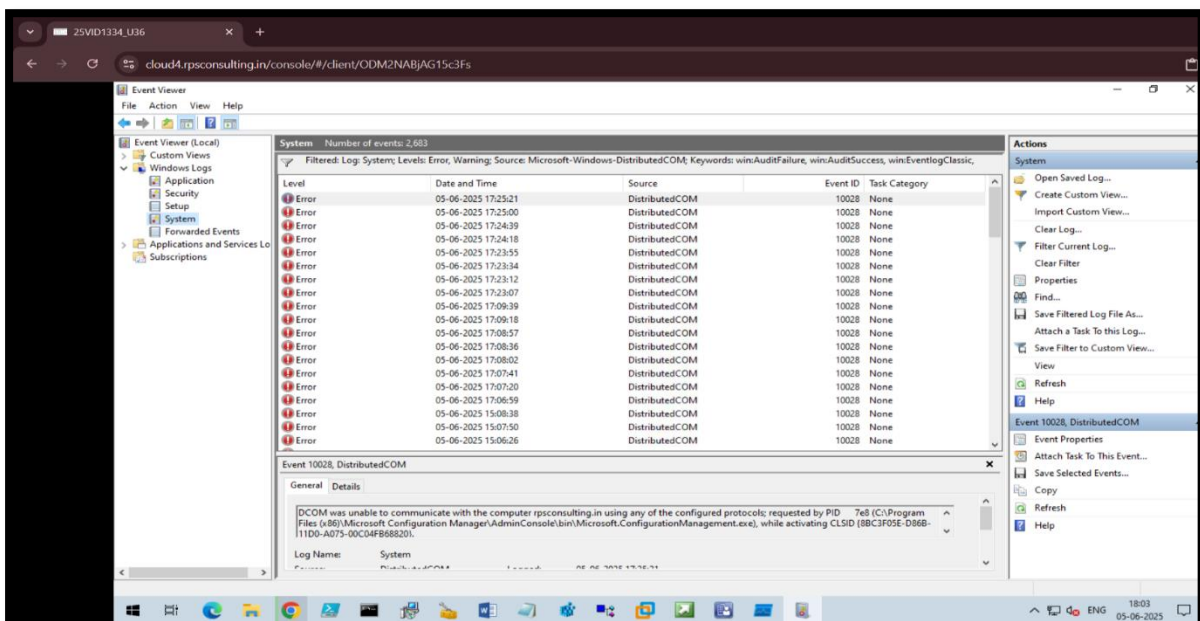
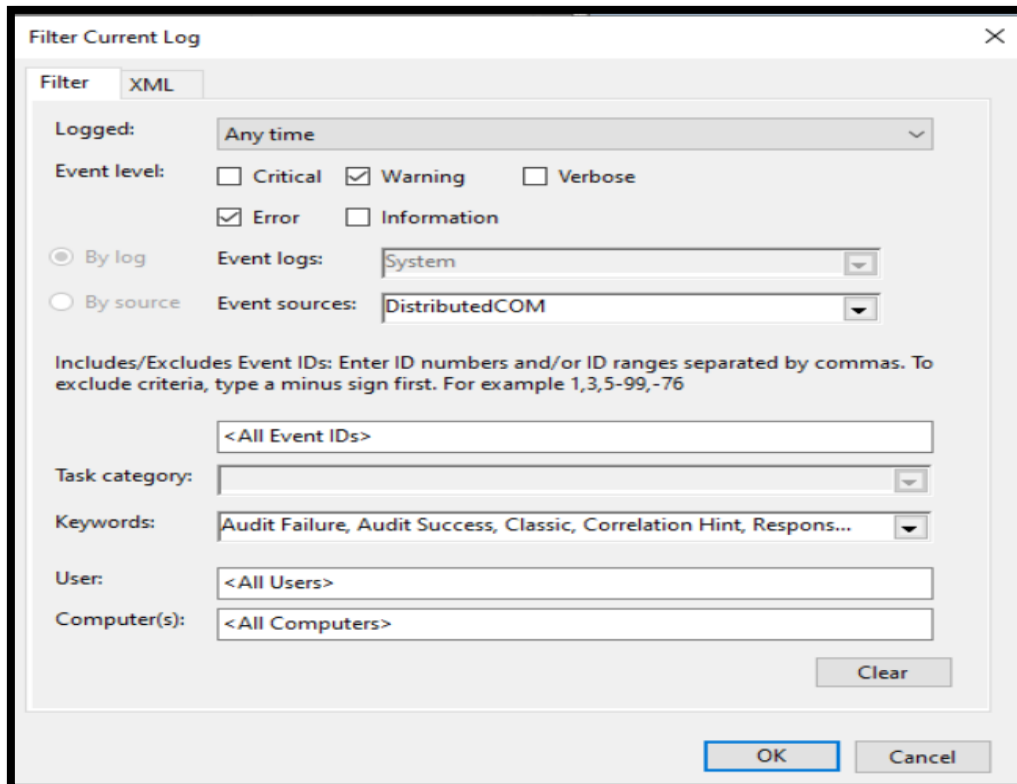
C. Event Viewer

- Event Viewer is used to identify the System-Level Errors related to the installation.
- It is 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.



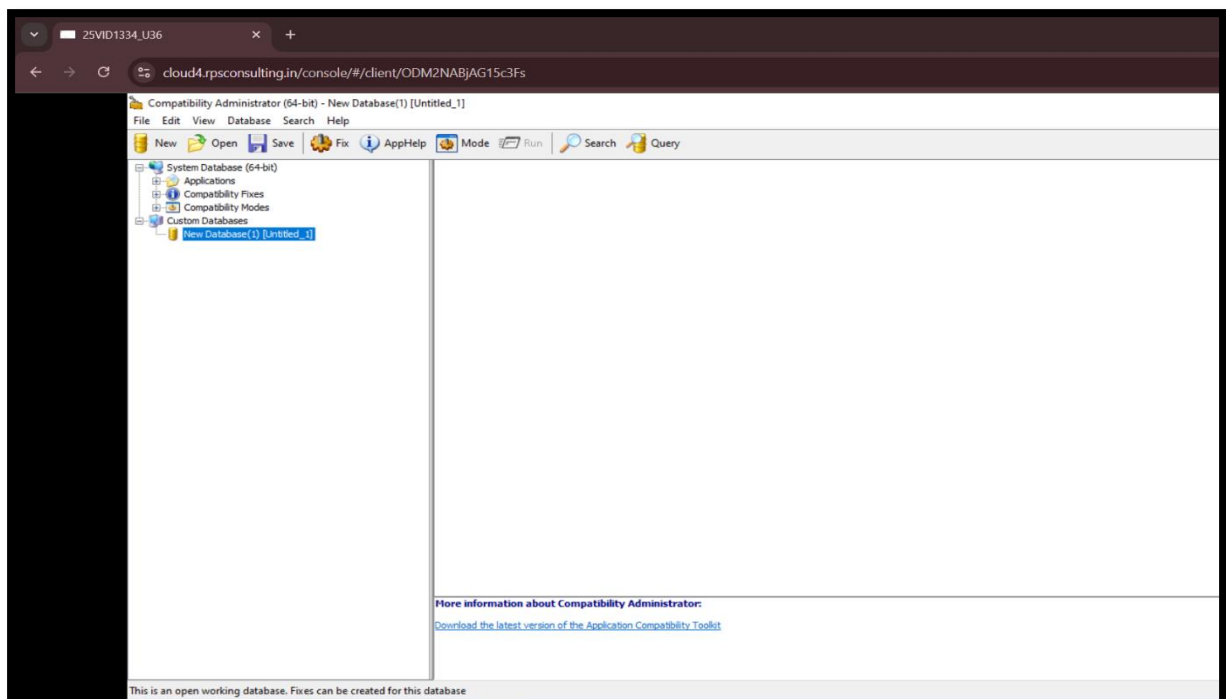
Steps:

- Open **Event Viewer** from the Start Menu.
- Navigate to the **Windows Logs** and expand it, in that **Application, Security, Setup** and **System** are available, so select the one where events will be present. For eg. in the Application, 4715 Events are present.
- In the **Actions** pane (right side), click **Filter Current Log**.
- In the **Filter Current Log** window, under **Event sources** select **Msiinstaller**. We can also filter by **Event level** for eg. **Error, Warning** to narrow down the results. Also under **Keywords** we can select **All keywords** and then click **OK** to apply the filter.
- Analyze the Event to identify the cause of MSI installation error (in the bottom pane). **Error! Filename not specified.**



D.ACT (Application Compatibility Toolkit)

- 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.



Steps:

- Download the **ACT** from the link learn.microsoft.com/en-us/windows-hardware/get-started/adk-install#download-the-adk-101261002454-december-2024
- Run the **adksetup.exe** file and it creates a folder named **Windows Kits**.
- Navigate to the path **Windows Kits\10\ADK\Installers** and after that search for **Application Compatibility Toolkit**.
- Install any one of them according to the configurations of the device.
- Open **Compatibility Administrator (32-bit)** or **Compatibility Administrator (64-bit)**.
- Click on **Database** then click **Create New** then click **Application Fix**.
- In **Program Information** give **Name of the program to be fixed** and browse our .exe file in the **Program file location** and click **Next**.
- In **Compatibility Modes** do nothing and click **Next**.
- In **Compatibility Fixes** select **ForceAdminAccess**, **CorrectFilePaths**, etc checkboxes and click **Next**.
- In **Matching Information** do nothing and click **Finish**.
- Save this database file by clicking **Save As** and write the **Database Name** and click **OK** and then save it using the file name **MyFixess.sdb**.

- Open **Command Prompt as Administrator** and in **system32** write the command **sdbinst** “C:\Users\admin\Downloads\MyFixess.sdb”

