1. **Process Monitor**

**Introduction**

***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*, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more.**

**Function:** Captures file system, registry, and process activity in real-time.

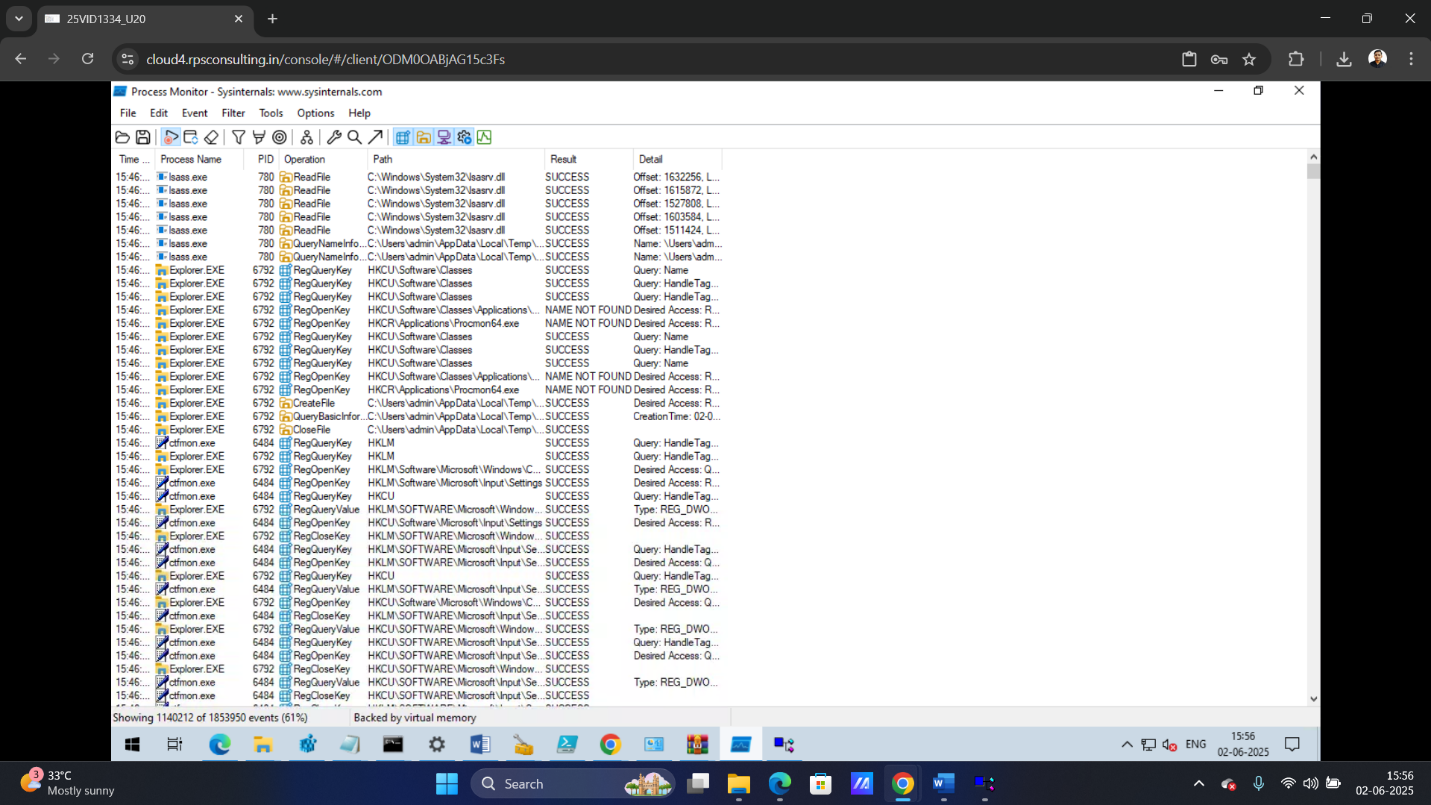
**Benefits:**

**•** Offers a detailed view of system interactions

• Helping to diagnose application startup issues

• File access problems

**Usage:** Use filters to narrow down the captured events to specific processes or operations. Monitor file access, registry keys and process behavior to pinpoint issues.

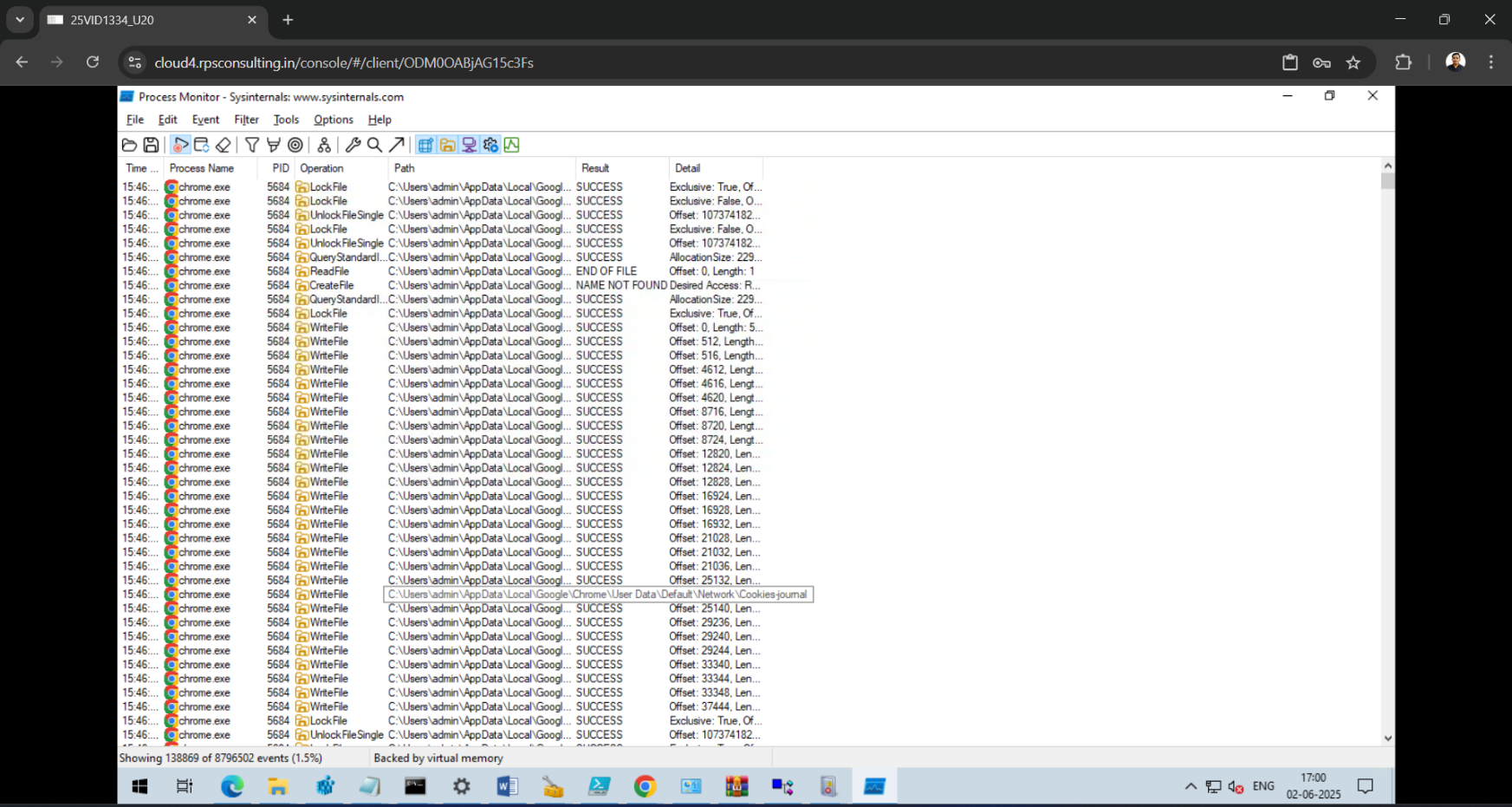
****

**Process Monitor (ProcMon) – Step-by-Step Process**

**A real-time monitoring tool for file system, registry, and process/thread activity.**

**Steps:**

* Download and run ProcMon.exe (no installation required).
* Accept the EULA when starting for the first time.
* Start capturing events (default is ON).
* Use Filter > Filter... to add filters (e.g., Process Name contains “app.exe”).
* Observe file, registry, and process activities.
* Pause or stop capture for analysis.
* Use Highlight to mark specific events.



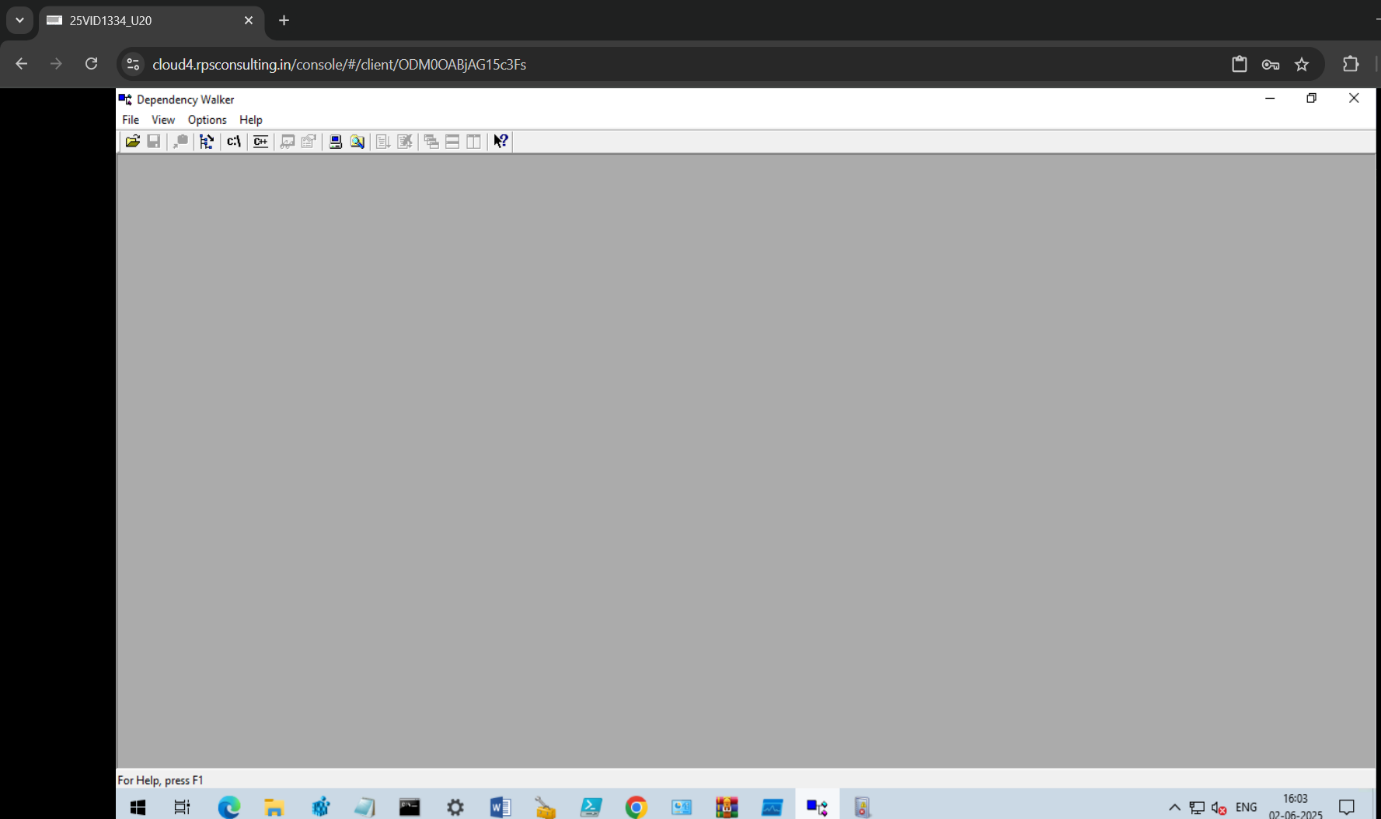
1. **Dependency Walker**

Dependency Walker is a free utility that scans any 32-bit or 64-bit Windows module (exe, dll, ocx, sys, etc.) 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. Another view displays the minimum set of required files, along with detailed information about each file including a full path to the file, base address, version numbers, machine type, debug information, and more.  
  
Dependency Walker is also very useful for troubleshooting system errors related to loading and executing modules. Dependency Walker detects many common application problems such as missing modules, invalid modules, import/export mismatches, circular dependency errors, mismatched machine types of modules, and module initialization failures.

**Function:** Analyzes the dependencies of Windows modules (EXE, DLL, etc.).

**Usage:** Identifies missing or incorrect dependencies, such as DLLs.

**Benefit:** Helps resolve problems caused by missing or corrupted dependencies, ensuring that applications function correctly.

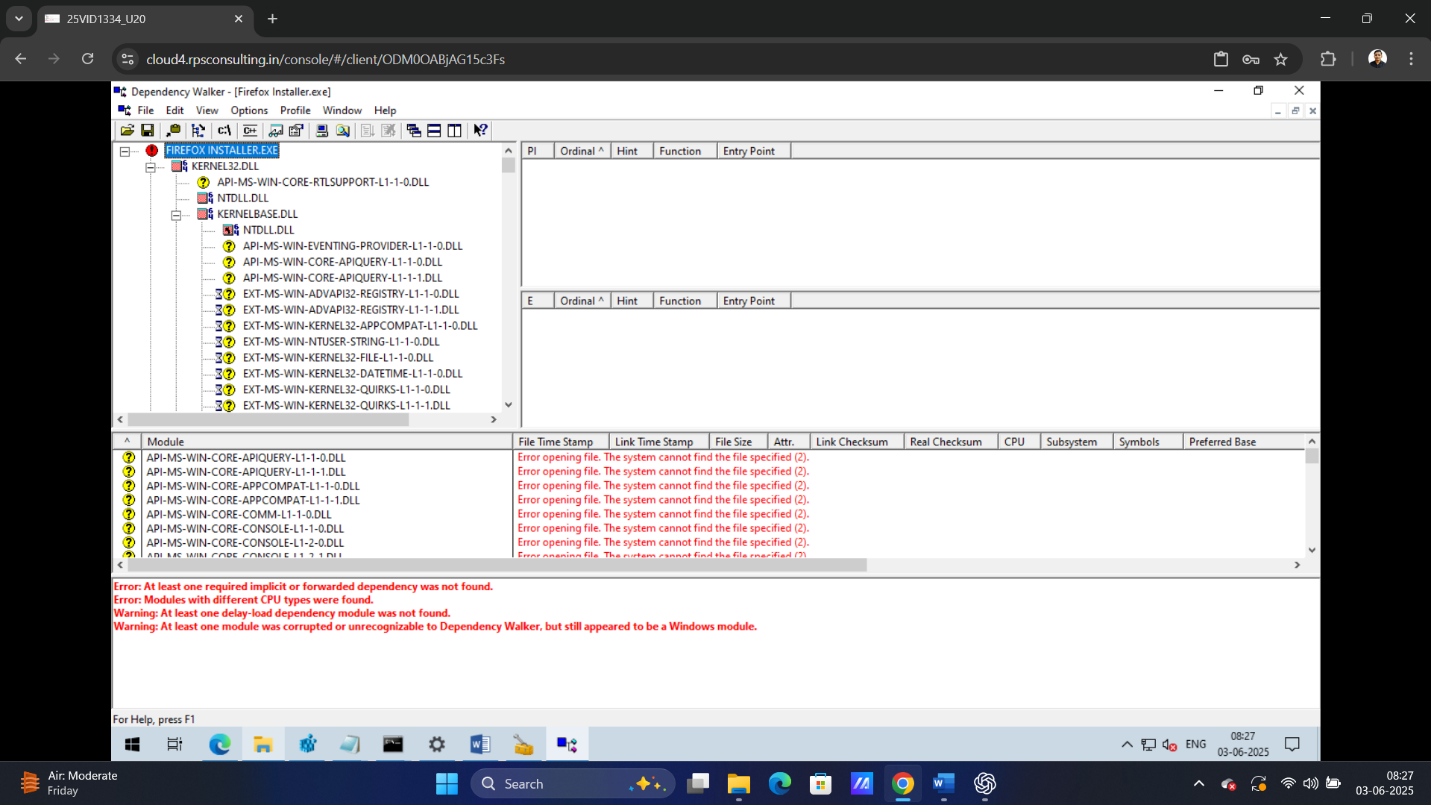


**What is Dependency Walker?**

**Dependency Walker (depends.exe) is a tool that shows all the DLL files required by a program and checks for missing or incompatible modules. It's often used for troubleshooting application startup issues.**

**Step-by-Step to Use Dependency Walker**

* 🔹 Step 1: Open Dependency Walker
* 1. Go to Start Menu or folder where it's installed (e.g., C:\Program Files (x86)\Dependency Walker).
* 2. Double-click depends.exe to open it.
* 🔹 Step 2: Open the Application You Want to Analyze
* 1. Click on File > Open...
* 2. Browse and select the .exe file of your application (e.g., firefox.exe, myapp.exe).
* 3. Click Open.
* 🔹 Step 3: Wait for the Analysis
* The tool will load and scan all dependencies.
* This may take a few seconds to a minute depending on the application.
* 🔹 Step 4: Read the Dependency Tree
* Top pane: Hierarchical list of dependent DLLs.
* Bottom pane: Details like functions imported/exported.
* 🔹 Step 5: Look for Errors or Warnings
* Look out for:
* Missing DLL
* Potential issue (e.g., delay-load failure)
* Module not loaded yet
* 🔹 Step 6: Diagnose the Problem
* Missing DLLs? → You need to install those or add them to the system path.
* Mismatched architecture (x86 vs x64)? → Use the correct version of the application or DLL.
* 🔹 Step 7 (Optional): Use Profile Mode
* To analyze runtime loading:
* 1. Go to Profile > Start Profiling...
* 2. Check options (e.g., "Log LoadLibrary calls").
* 3. Click OK.
* It will launch the app and show dynamic dependencies as they load.

****

1. **Event Viewer**

**🔹 Definition**

Event Viewer is a built-in Windows tool that allows users to view and manage event logs on a local or remote system. These logs contain information about system events, application behavior, and security activities.

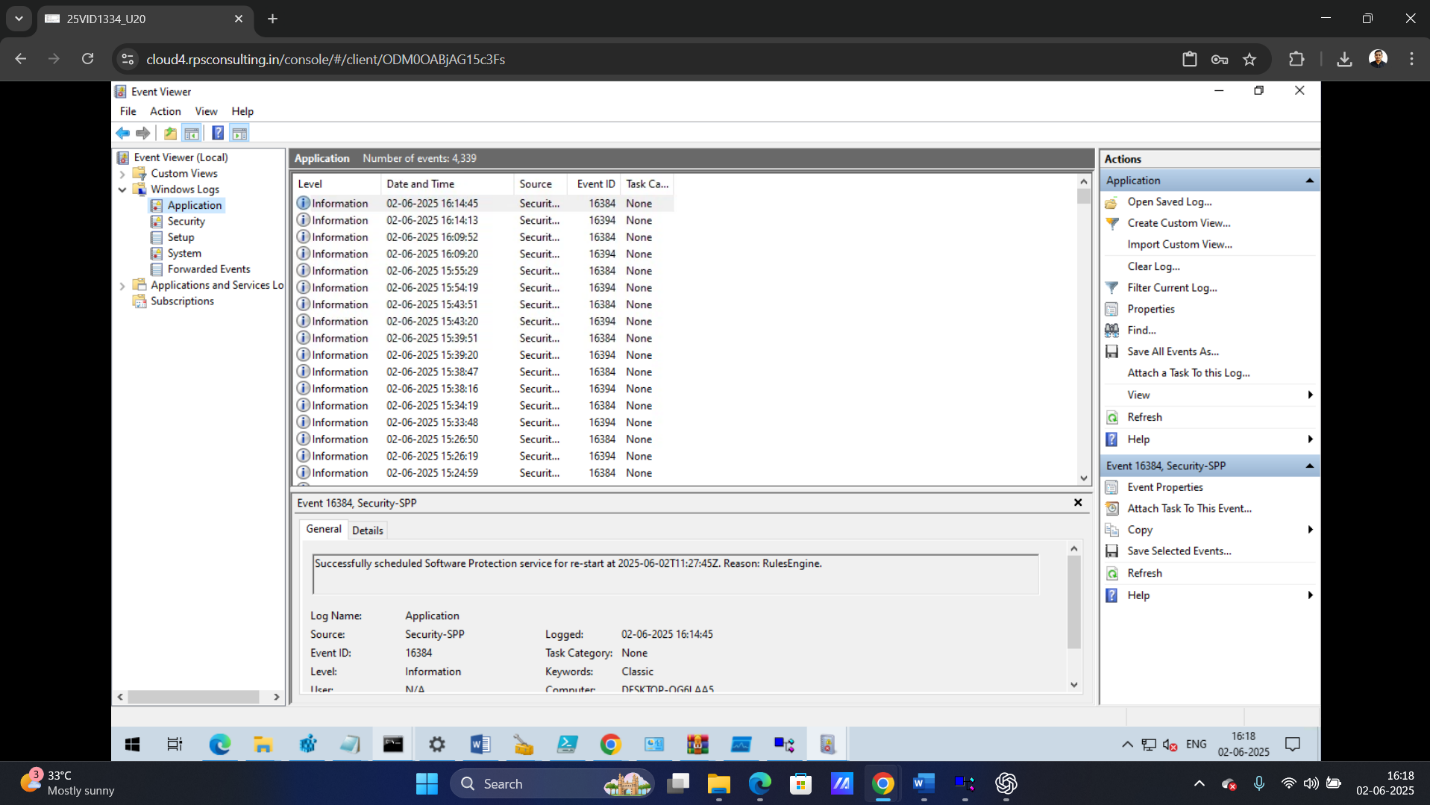
**Purpose**

* Helps in monitoring and troubleshooting system performance and security.
* Provides an audit trail of system operations and user activities

**Function:** Logs system events, including errors, warnings, and information messages.

**Usage:** Search for relevant error messages, warnings, or event IDs to understand the nature of the problem.

**Benefit:** Provides a historical record of system activity, helping to identify recurring problems and pinpoint the source of errors.

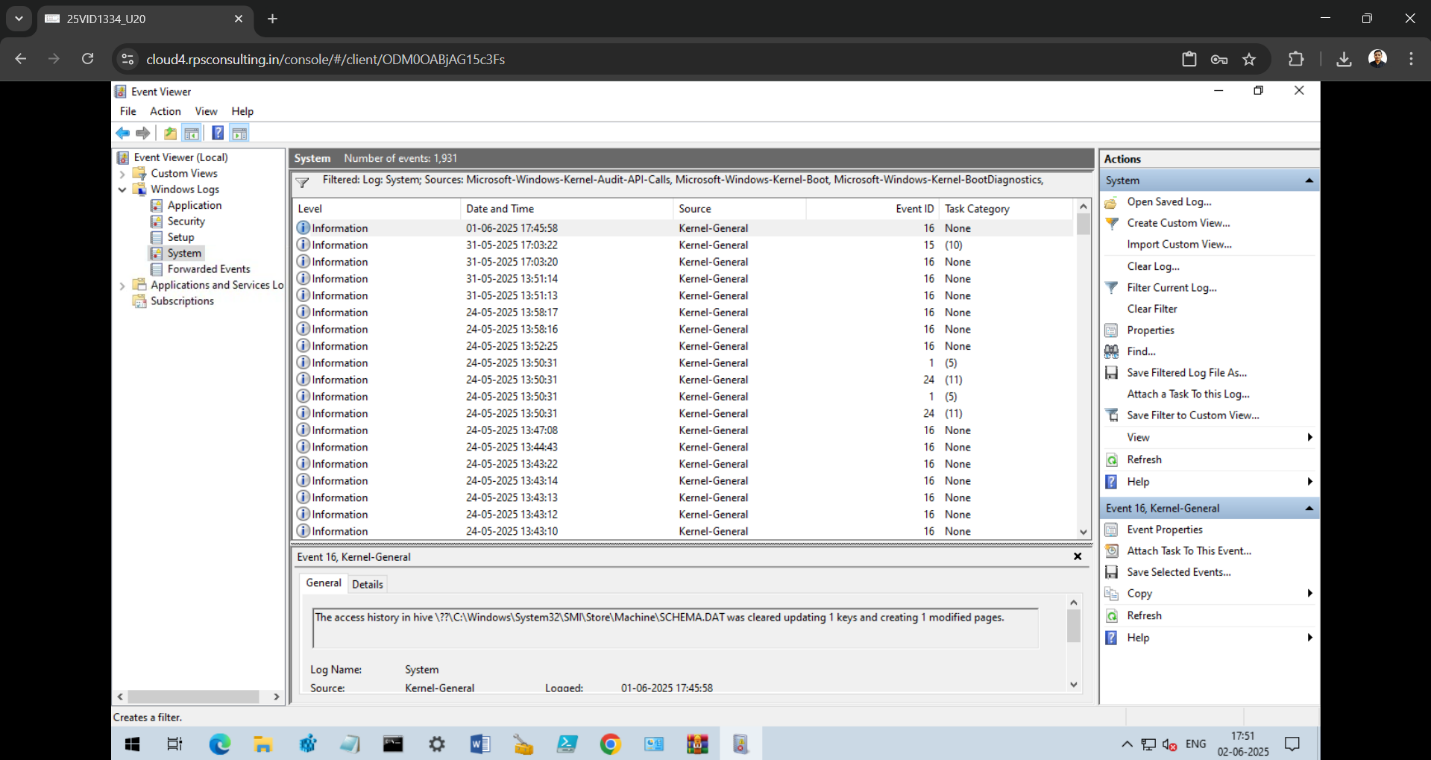


**Event Viewer – Step-by-Step Process**

**Used to log and analyze system events like errors, warnings, and information messages.**

**Steps:**

* Press Windows + R, type eventvwr, and hit Enter.
* Expand Windows Logs > choose Application or System.
* Click an event to view details like Event ID, Source, and Description.
* Use the Filter Current Log option to narrow down events.
* Use Event ID and Description to troubleshoot the issue.
* Optionally, export logs using Save All Events As for sharing



1. **Application Compatibility Toolkit (ACT)**

**What is ACT?**

The **Application Compatibility Toolkit (ACT)** is a **Microsoft tool** that helps you:

* **Find and fix problems** that older applications may have when running on **newer versions of Windows**.
* **Test and analyze** how well applications work after a Windows upgrade.
* Make sure important apps keep working during **Windows migrations**.

**What does ACT do?**

* **Scans** your applications.
* **Detects compatibility issues** (like old code or settings that don't work on new Windows).
* **Applies fixes (shims)** to help those apps run properly.
* Lets you create and install **custom fixes** for apps using a tool called **Compatibility Administrator**.

**Why use ACT?**

* To **avoid problems** when upgrading Windows.
* To **save time** instead of replacing or rewriting old software.
* To **keep business apps working** without major changes.

**Main Tools in ACT:**

* **Compatibility Administrator** – Create and apply fixes for apps.
* **Standard User Analyzer** – Find issues apps may have running without admin rights.
* **ACT Log Processing Tools** – Analyze reports from app testing.

**Application Compatibility Toolkit (ACT) –**

**Step-by-Step Process**

**ACT is used to identify and mitigate application compatibility issues on Windows.**

Steps:

1. Install ACT (part of Windows Assessment and Deployment Kit - ADK).

2. Open Compatibility Administrator tool.

3. Select New Database (32-bit or 64-bit) based on the application.

4. Click on File > Create New Application Fix.

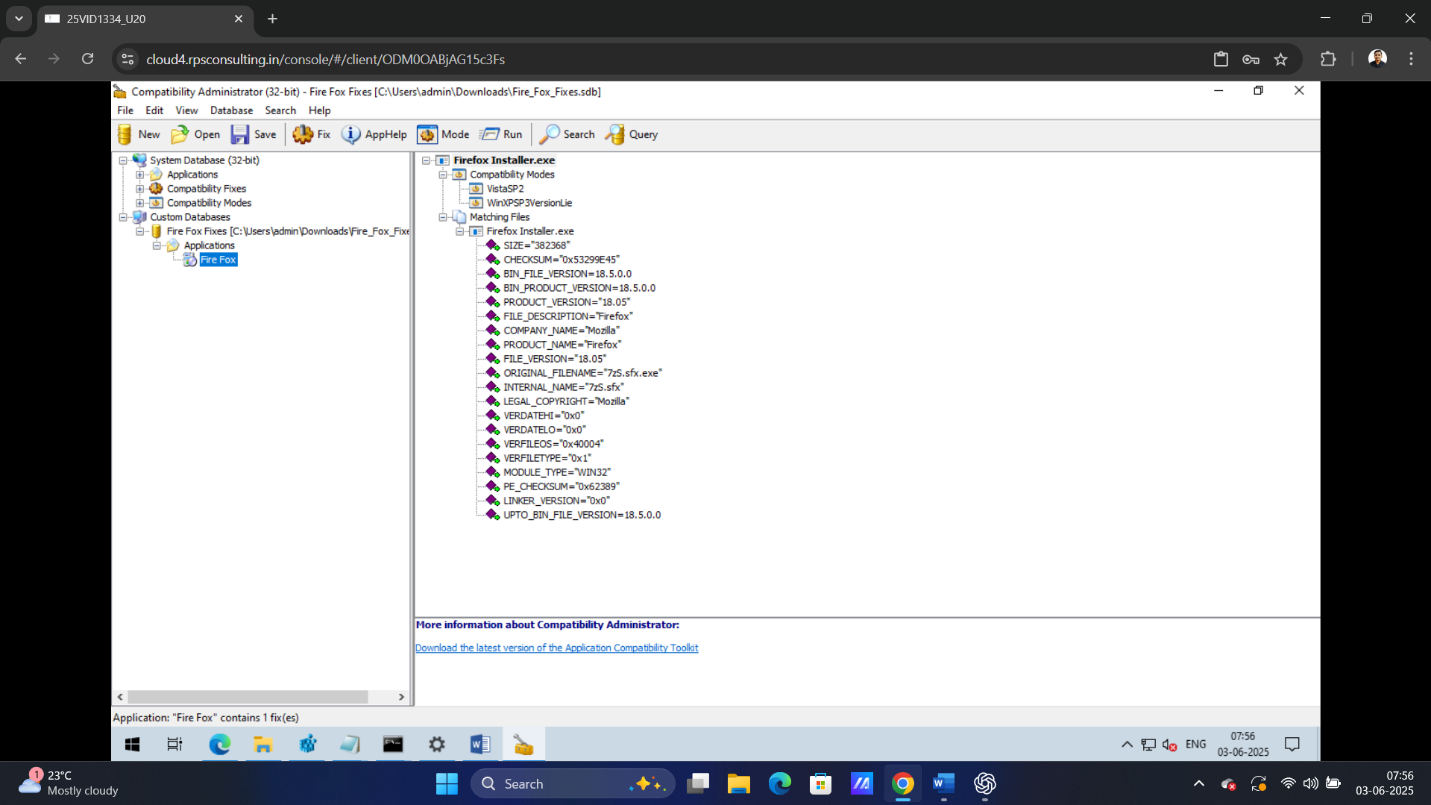
5. Enter the application name, vendor, and path to executable.

6. Select compatibility modes or click Next.

7. Select compatibility fixes and click Next.

8. Enter the matching information to identify the application.

9. Click Finish.

10. Save the database and install the fix using sdbinst.exe

