Dependency Walker

Dependency Walker is a utility that scans Windows modules (EXE, DLL, SYS, etc.) to display:

- All DLL dependencies
- Missing or mismatched DLLs
- Exported/imported functions
- Potential compatibility issues

Step-by-Step Execution of Dependency Walker

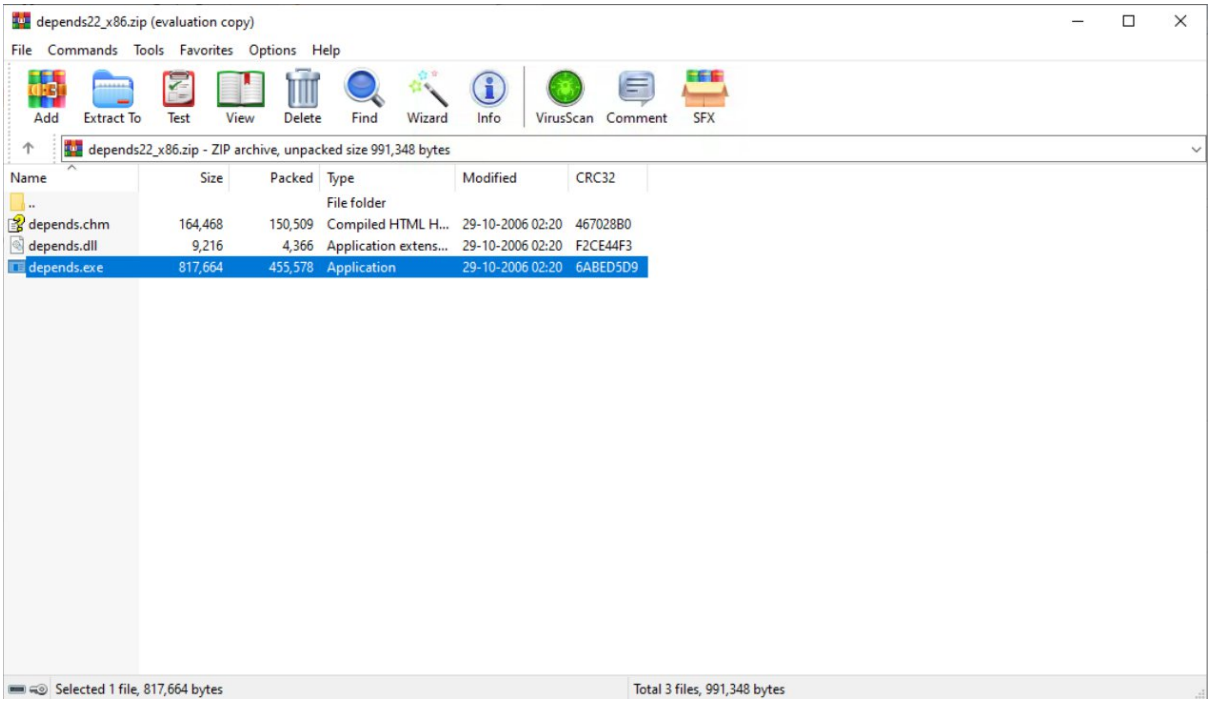
Step1: Download and Install Dependency Walker

1. Visit the official website: http://www.dependencywalker.com/

2. Download the appropriate version for your system (usually x86 or x64).

3. Extract the ZIP file or install if it's an installer.

4. Launch depends.exe.



Step 2: Open the Target

1. In Dependency Walker, click on File → Open... or press Ctrl + O.
2. Browse to the .exe, .dll, or other module you want to inspect.
3. Select it and click **Open**.

Step 3: Analyze Dependencies

Once opened:

- Dependency Walker will parse the file and list:
  - All immediate (static) dependencies.
  - Functions imported/exported.
  - Any missing or unresolved dependencies.
- The tree view shows modules loaded by your target.
  - Missing modules are highlighted in red.
  - Potential issues are shown in yellow.

Step 4: Examine the Output

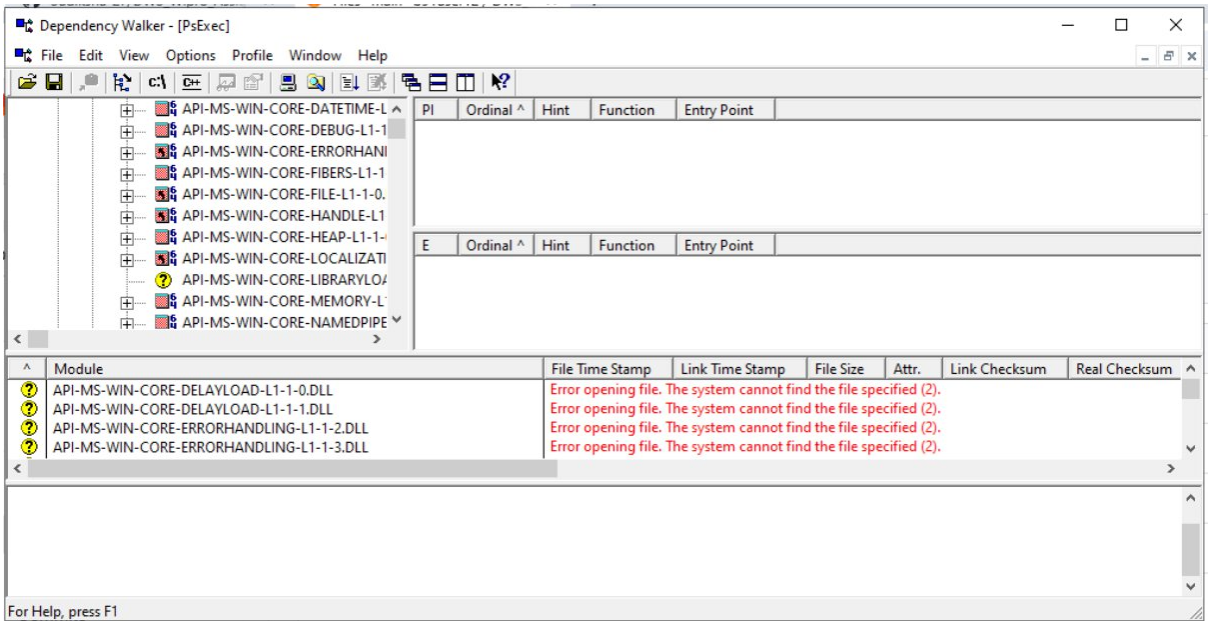
Module List: Lists all modules with load status and full paths.

Functions: Lists imported/exported functions.

Errors/Warnings: Highlight missing DLLs, incorrect versions, or functions not found

Step 5: Close the Application

When you're done, close the project or exit the application.

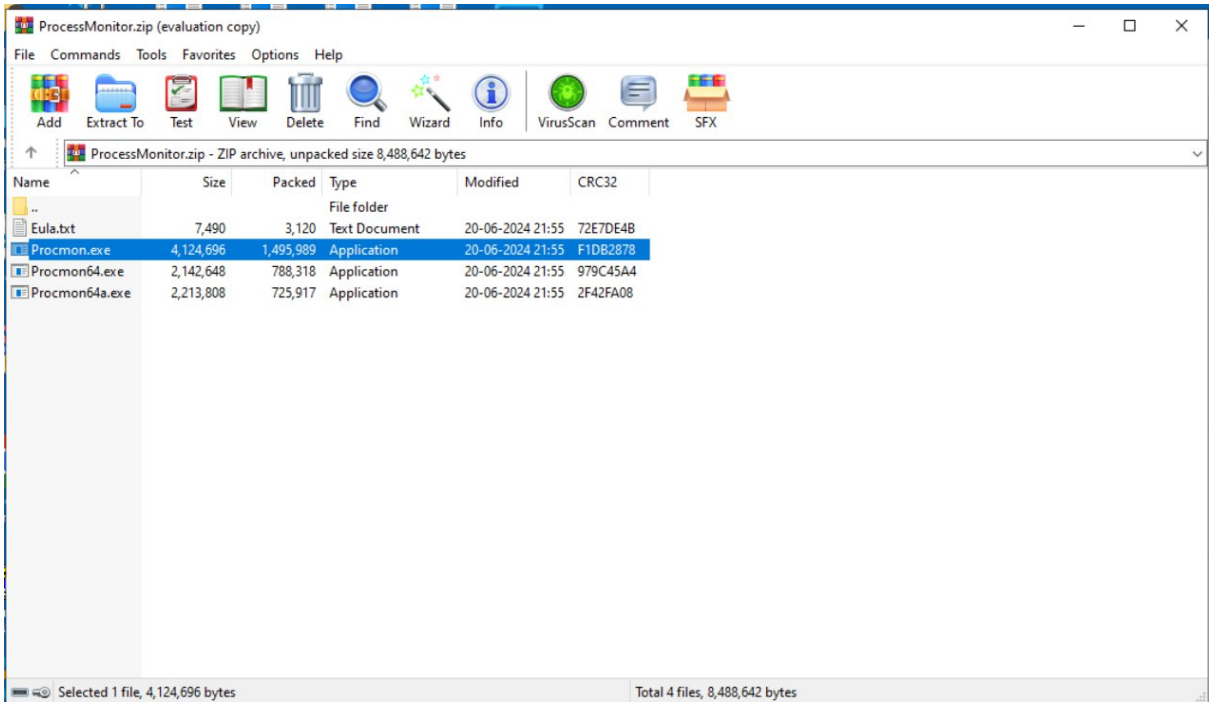


Step by step execution of Process Monitor

Step 1: Download Process Monitor

1.Go to the official Sysinternals website :
https://learn.microsoft.com/sysinternals/downloads/procmon
2.Download the **Procmon.zip** file.

3. Extract the contents to a folder.

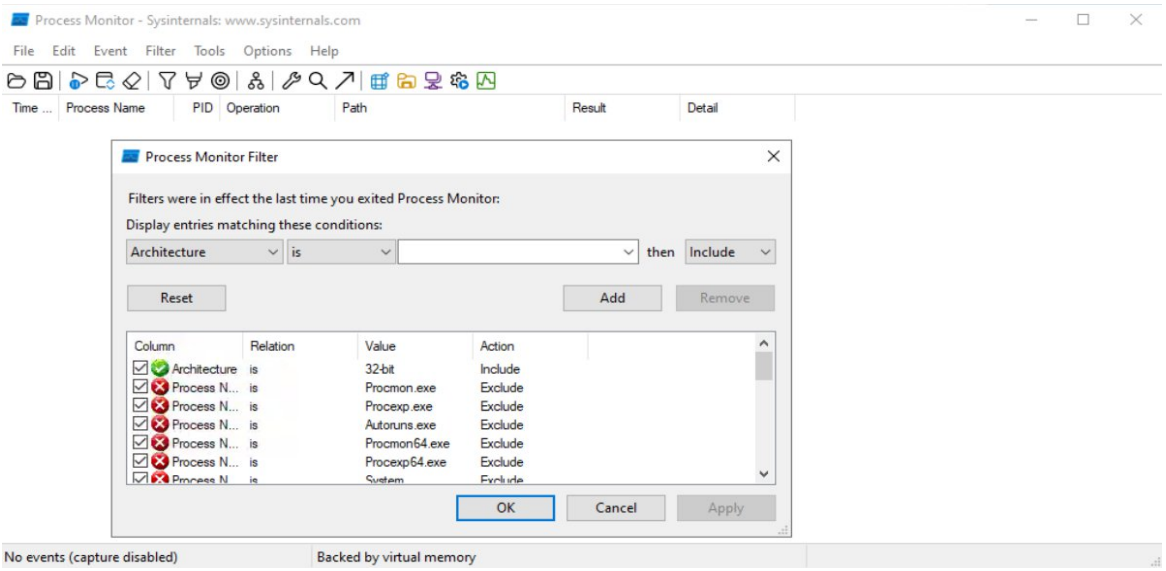


Step 2: Launch Process Monitor

1. Open the extracted folder.

2. Run Procmon.exe (you may need to **Run as Administrator** for full access).

3. Accept the **EULA (End User License Agreement)** on first launch.



Step 3: Initial Capture Starts Automatically

1. Process Monitor begins **capturing events immediately** when it opens.

2. You'll see a stream of events related to file system, registry, network, and process activity.

Step 4: Stop the Capture

1. Click the **Magnifying Glass icon** (🔍) or press **Ctrl + E** to **pause** capturing.

2. This prevents overload while setting filters.

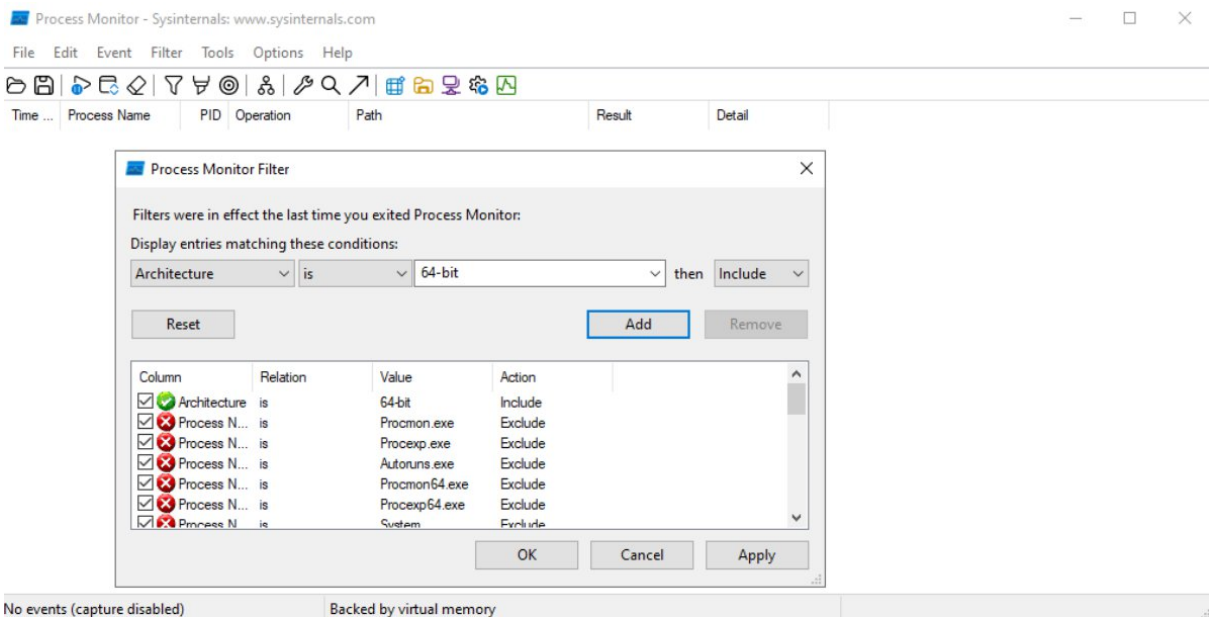
Step 5: Apply Filters

1. Click on **Filter > Filter...** from the top menu.

2. Set filters to narrow down events:

    - E.g., Process Name is not explorer.exe then Exclude
    - Use filters like:
        - Process Name
        - Operation
        - Path
        - Result

3. Click **Add**, then **OK**.

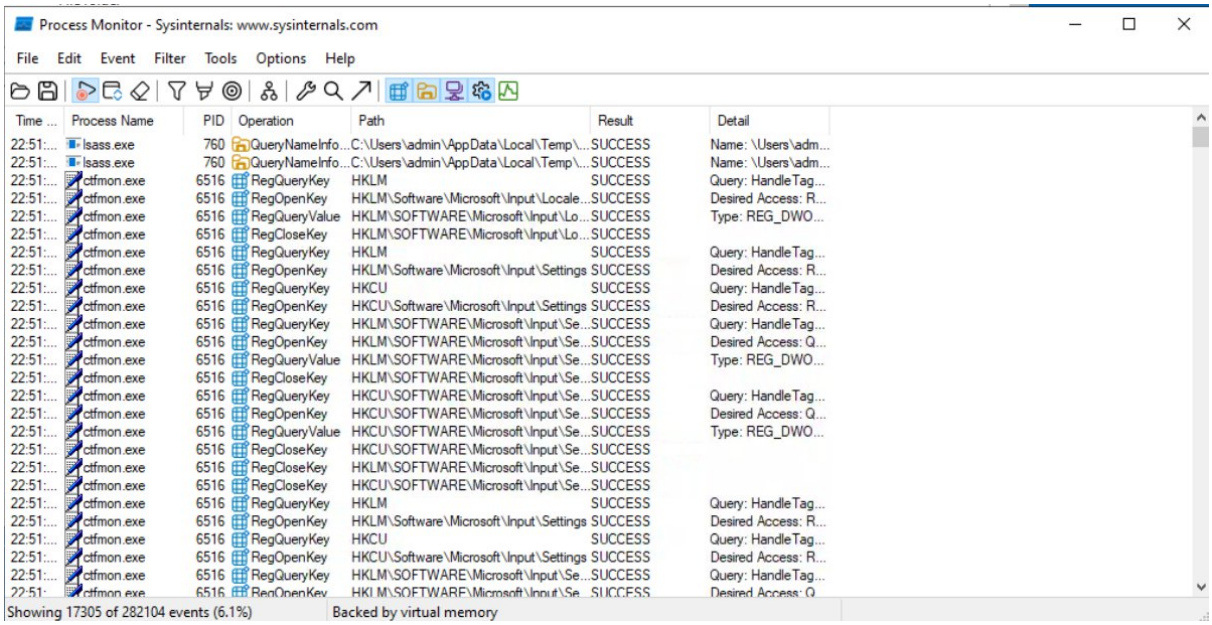


Step 6: Analyze Captured Data

1.View events in real time:

- **Time of Day** – Timestamp of the event
- **Process Name** – Executing process
- **Operation** – e.g., RegOpenKey, CreateFile, etc.
- **Path** – Registry key or file path
- **Result** – Success, Name Not Found, Access Denied, etc.

2.Double-click an event to see detailed information.

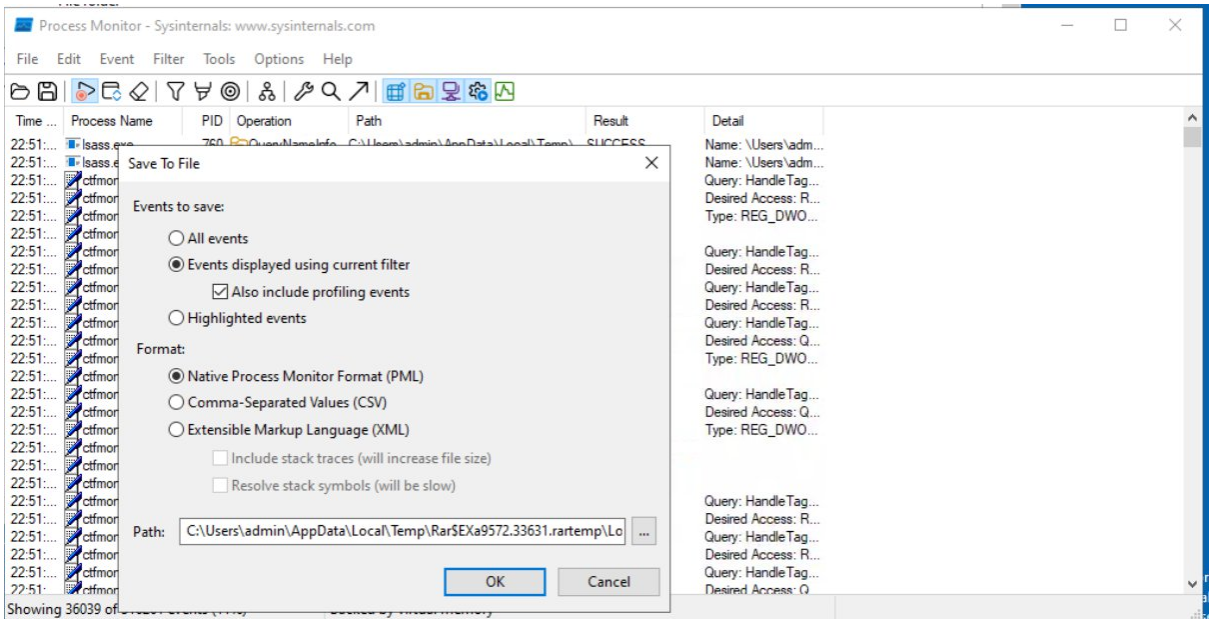


Step 7: Save or Export Logs

1.To save the captured data:

- Go to File > Save.
- Choose format (e.g., .PML, .CSV).

2.Useful for sharing or further analysis.



Step 8: Exit Process Monitor

1. Simply close the application.

2. Optionally clear the log before exiting via Edit > Clear Display**.**