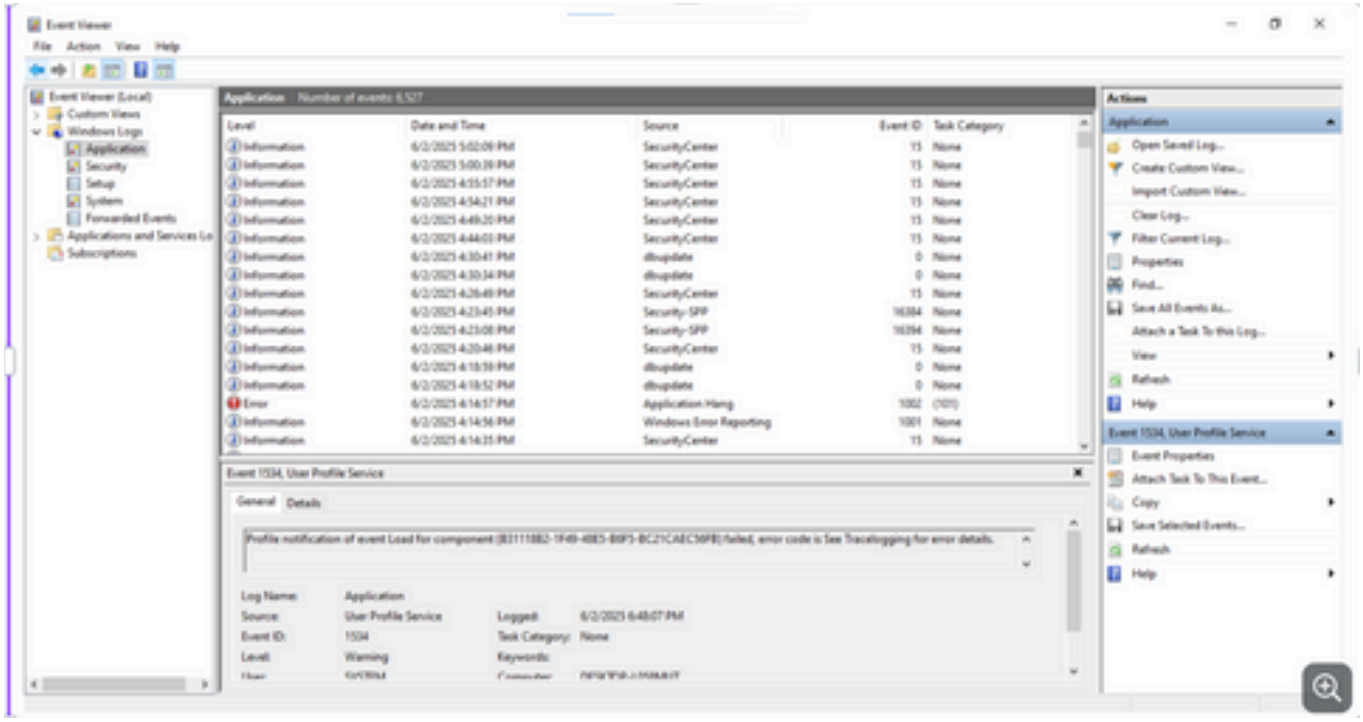
Event Viewer, Process Monitor and Dependency Walker

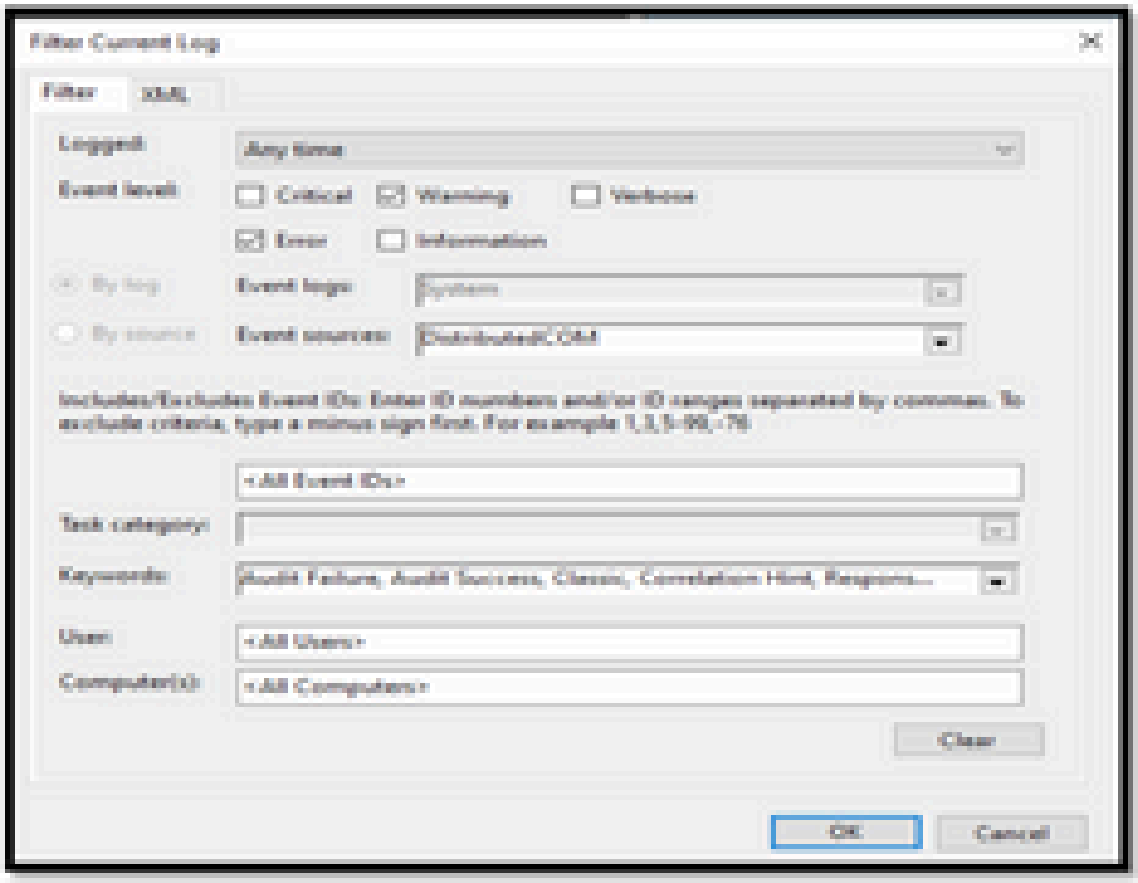
Event Viewer, Process Monitor (ProcMon), and Dependency Walker are valuable tools for troubleshooting a variety of issues, including application failures, system errors, and dependency problems.

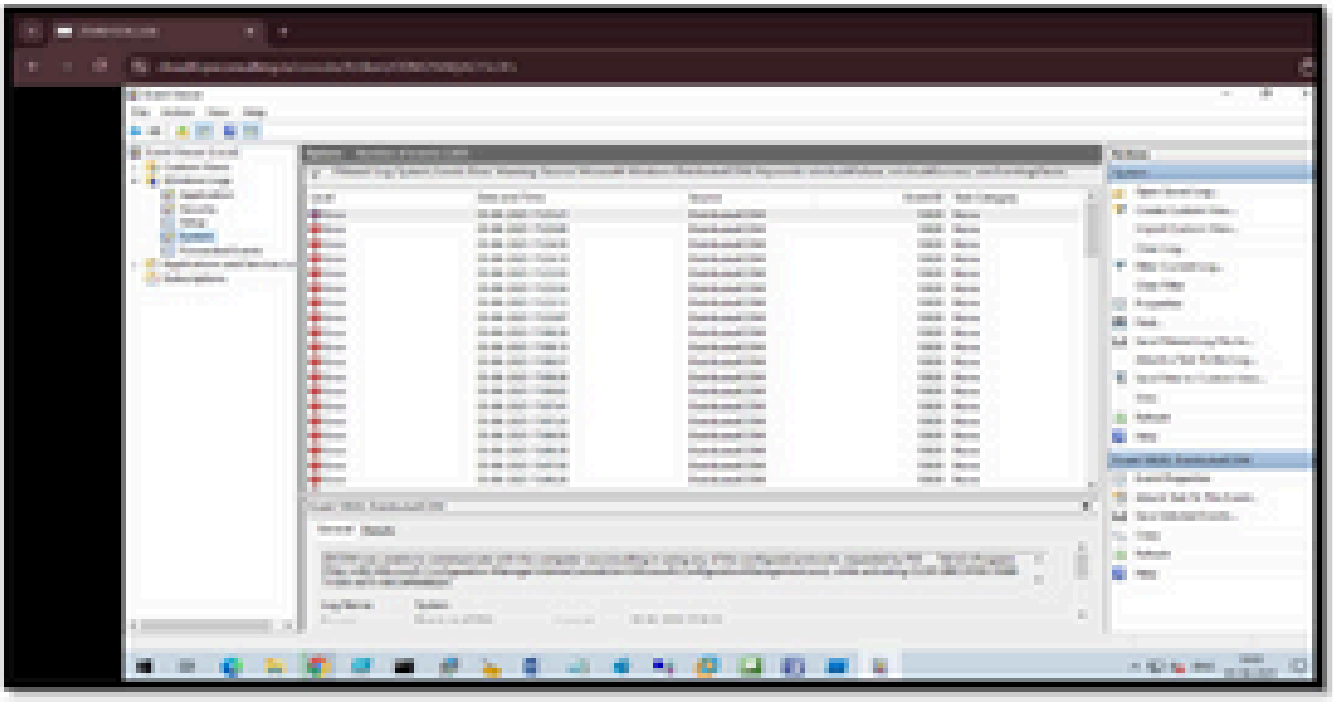
Event Viewer: Logs system events, including errors, warnings, and information messages

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.**


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Application and Services Lo
Subscriptions
Application Number of events: 6,527
Level Date and Time Source Event ID Task Category
Information 6/2/2025 5:02:09 PM SecurityCenter 15 None
Information 6/2/2025 5:00:39 PM SecurityCenter 15 None
Information 6/2/2025 4:55:57 PM SecurityCenter 15 None
Information 6/2/2025 4:54:21 PM SecurityCenter 15 None
Information 6/2/2025 4:49:20 PM SecurityCenter 15 None
Information 6/2/2025 4:44:03 PM SecurityCenter 15 None
Information 6/2/2025 4:30:41 PM dbupdate 0 None
Information 6/2/2025 4:30:34 PM dbupdate 0 None
Information 6/2/2025 4:26:49 PM SecurityCenter 15 None
Information 6/2/2025 4:23:45 PM Security-SPP 16384 None
Information 6/2/2025 4:23:08 PM Security-SPP 16394 None
Information 6/2/2025 4:20:48 PM SecurityCenter 15 None
Information 6/2/2025 4:18:59 PM dbupdate 0 None
Information 6/2/2025 4:18:52 PM dbupdate 0 None
Error 6/2/2025 4:16:57 PM Application Hang 1002 (101)
Information 6/2/2025 4:14:56 PM Windows Error Reporting 1001 None
Information 6/2/2025 4:14:35 PM SecurityCenter 15 None
Event 1534, User Profile Service
General Details
Profile notification of event Load for component {B3111BB2-1F49-40E5-B6F5-BC21CAEC56FB} failed, error code is See Tracelogging for error details.
Log Name: Application
Source: User Profile Service
Logged: 6/2/2025 6:48:07 PM
Event ID: 1534
Task Category: None
Level: Warning
Keywords:
Actions
Application
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 1534, User Profile Service
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help





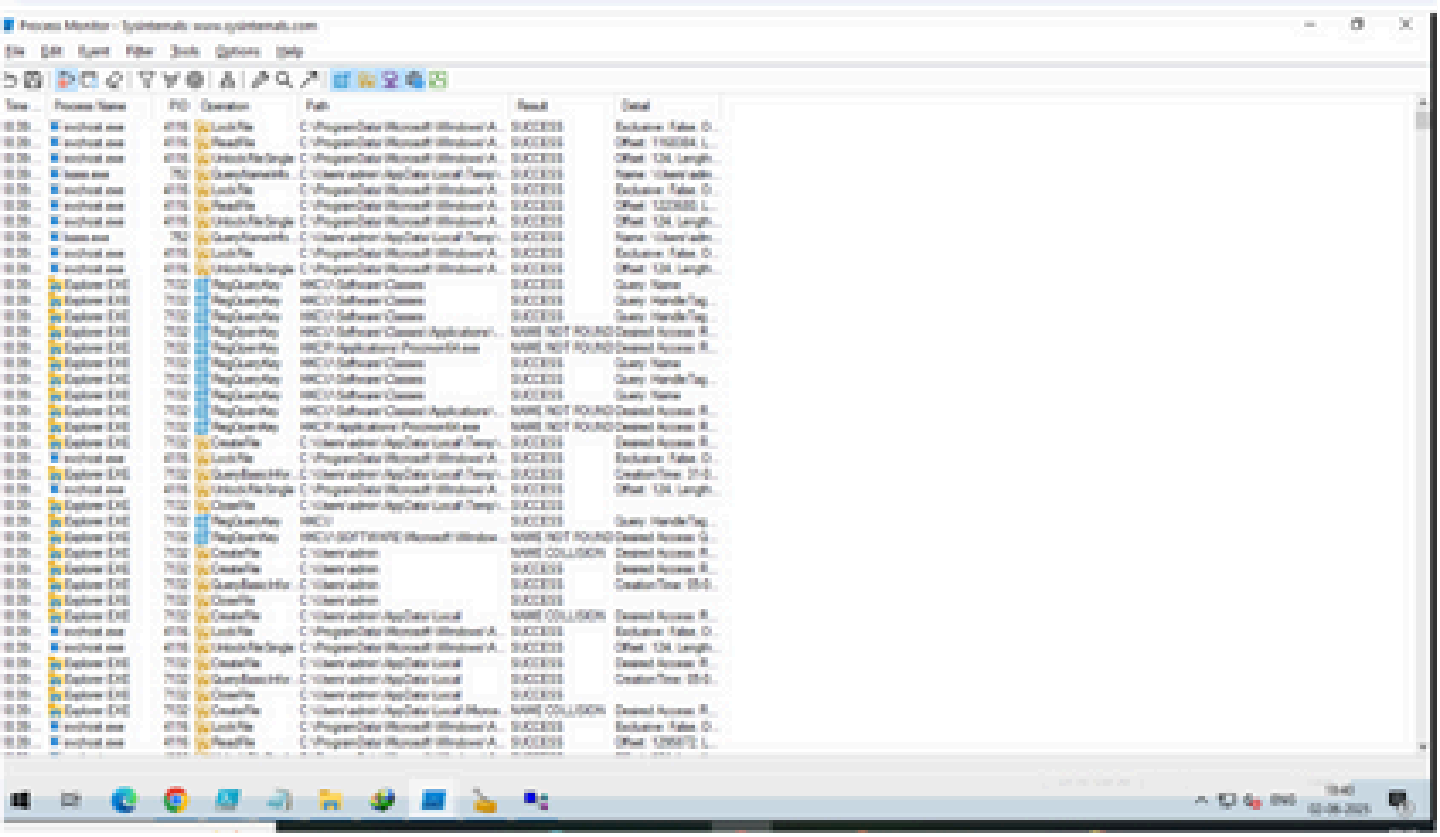
Process Monitor (ProcMon):

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry, and process/thread activity.

Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

Process Monitor includes powerful monitoring and filtering capabilities, including:

- *More data captured for operation input and output parameters*
- *Non-destructive filters allow you to set filters without losing data*
- *Configurable and moveable columns for any event property*
- *Cancellable search*
- *Boot time logging of all operations*

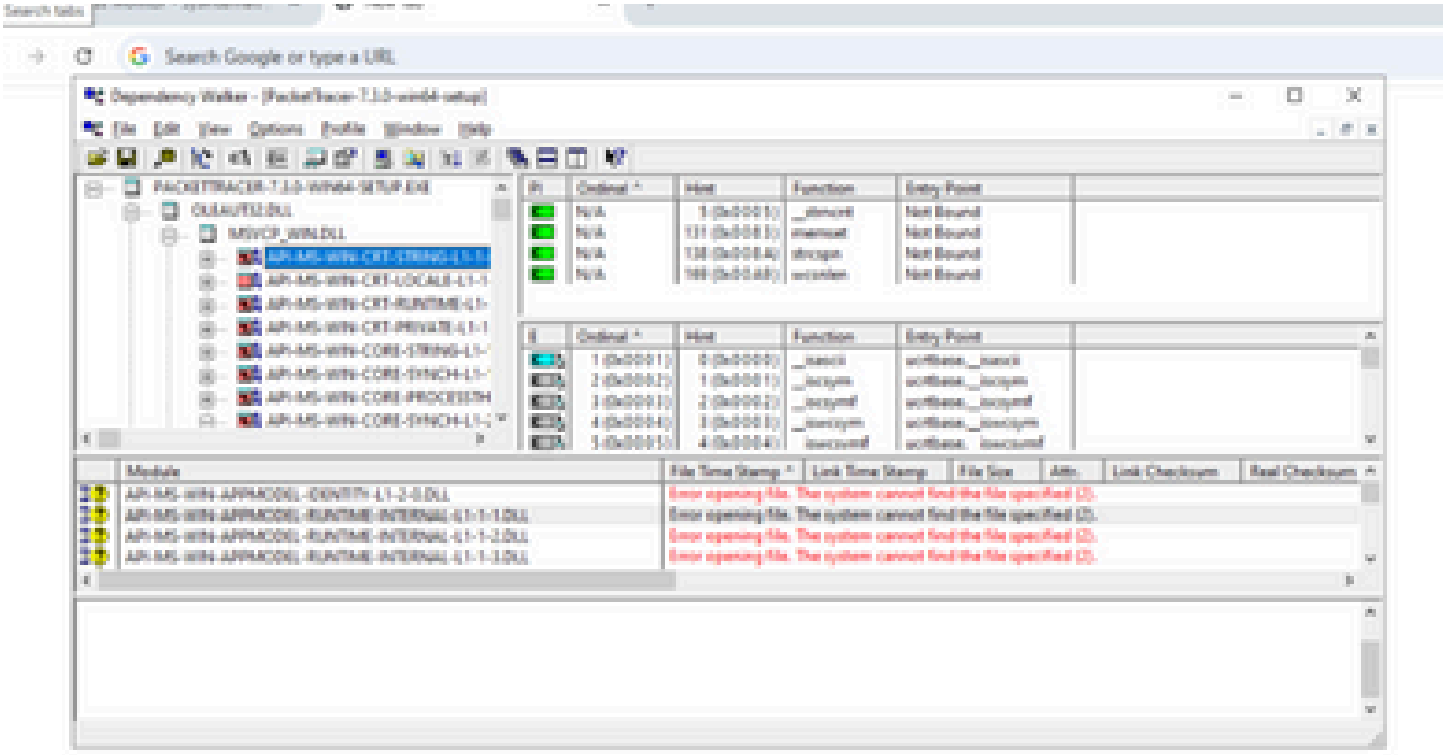


Dependency Walker:

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

- *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.*
- *t 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 to evaluate your application compatibility using application compatibility toolkit:

- Collect – Create your data collection package
- Analyze – Rationalize, categorize, prioritize, filter your compatibility data

- Test and Mitigate – Use the test tools to understand compatibility issues to develop a plan for mitigation

---

Step by step process of ACT (Application Compatibility Toolkit):

Download the Application Compatibility Toolkit

Step 1: Download and Install ACT

- Go to Microsoft's official website or search for "**Microsoft Application Compatibility Toolkit download**" (it's part of the Windows ADK - Assessment and Deployment Kit).
- Install the toolkit by running the installer.
- During setup, ensure the following features are selected:

  o Application Compatibility Toolkit

  o Compatibility Administrator

  o Standard User Analyzer (optional)

Step 2: Launch the Compatibility Administrator

- 1. Open **Compatibility Administrator** (32-bit or 64-bit depending on your application).
- o Start > All Programs > Microsoft Application Compatibility Toolkit > Compatibility Administrator

Step 3: Create a New Database

1. In the left panel, right-click **Custom Databases** and select **New.**

2.Right-click your new database and choose **Create New > Application Fix.**

Step 4: Configure the Application Fix

1. **Name** your application.

2. **Browse** to select the executable (.exe) file for the app.

3. Click **Next.**

Step 5: Select Compatibility Modes

1. Choose from a list of predefined **compatibility modes** (e.g., Windows XP SP3, Windows 7, etc.).

2. Click **Next.**

Step 6: Select Compatibility Fixes

1. Check one or more **fixes** (shims) as needed.

2.You can also test them later to see which ones resolve the issue.

3. Click **Next.**

Step 7: Matching Information

1. Set criteria for when the fix should apply:

- Filename
- size
- Checksum, etc

2.Click **FINISH**

Step 8: Save and Install the Fix

1. Go to **File > Save As** to save the .sdb file.

2. Use **Command Prompt** (Admin) and run:

- nginx
- CopyEdit
- sdbinst yourfile.sdb

This installs the fix on the system.

Step 9: Test the Application

1.Run the application and verify that the compatibility fix resolves the issue.

2.Use tools like **Standard User Analyzer** if needed to test for UAC issues or permissions.

Step 10: Manage or Uninstall Fixes

- To remove a fix:

nginx

CopyEdit

sdbinst -u yourfile.sdb

- To view installed fixes, use Compatibility Administrator or check the registry path:

CopyEdit

`HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\AppCompatFlags`

To collect your software and hardware inventory

- 1. On the taskbar, click **Start**, point to **All Programs**, point to **Microsoft Application Compatibility Toolkit 5.6**, and then click **Application Compatibility Manager.**
- 2. On the **Collect** screen, click **File** from the toolbar, and then click **New**.

The New <DCP_Name> dialog box appears.

- 3. In the **Package Name box**, type **Inventory_Collection.**
- 4. In the **Evaluate compatibility when** area, click **Deploying a new Operating System or Service Pack.**
- 5. Click **Advanced.**

The Advanced Settings dialog box appears.

- *6. Clear the* **User Account Control Compatibility** *Evaluator and* ***Windows Compatibility Evaluators*** *check boxes, and then click* ***OK.***

The Advanced Setting dialog box closes.

- 7. In the **When to monitor application usage** area, do not change the default options, but change the **Duration** to **10 Minutes.**
- 8. In the **Output Location** box, do not change the default value, previously specified in the ACT Configuration Wizard.
- 9. On the **File** menu, click **Save and Create Data Collection Package.**
- 10. Save the compiled DCP to your desktop.
- 11. Determine which method you will use to deploy your DCP. For information about the various deployment options, see Deploying a Data Collection Package.
- 12. By using the method determined in the previous step, deploy the DCP to your specified client computers' desktops.
- 13. Double-click the packaged DCP from each identified client computer's desktop.

The DCP runs on the client computer.

Shims

Shims: Shims, registry edits, and virtualization are techniques used to enhance application compatibility and persistence on Windows systems.

Shims are compatibility layers that modify application behavior to run on different versions of Windows.

Registry edits, or modifying the Windows registry, can be used to configure software or bypass security features.

Shims are designed to address application compatibility issues by providing a layer of *compatibility between applications and the Windows operating system*.