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. Virtualization creates isolated environments for applications, allowing them to run in a different context without interfering with the host system. [1, 2, 3, 3, 4, 4, 5, 6, 7, 8, 9, 10, 11, 12]

1. Shims:

- **Purpose:** Shims are designed to address application compatibility issues by providing a layer of compatibility between applications and the Windows operating system. [1, 1, 2, 2, 6, 13]
- **Mechanism:** They intercept API calls made by applications and redirect them to compatible versions of the OS or modify the application's behavior directly. [1, 1, 13, 13, 14, 15, 16]
- **Examples:**
- Redirecting API calls: A shim might intercept calls to the OpenFileDialog API and redirect them to a version compatible with the application's target Windows version. [13, 13]
- Modifying application behavior: A shim might modify an application's behavior to work around compatibility issues with the underlying OS, such as changing the way it handles file paths. [4, 13, 13, 17]

- **Persistence:** Shims can be used to achieve persistence by being invoked repeatedly by applications that require them. [13, 13, 18, 18]

2. Registry Edits:

- **Purpose:** The Windows registry is a database that stores system settings and configuration information. Modifying the registry can be used to change system behavior, install software, or bypass security features. [2, 3, 3, 4, 19, 19, 20, 21, 22]
- **Mechanism:** Registry edits involve changing key-value pairs in the registry, which can be done manually using the Registry Editor or through automated scripts. [3, 3, 23, 23]
- **Examples:**
- Enabling or disabling features: Registry edits can be used to enable or disable specific features in Windows or other software. [3, 19, 24, 25]
- Bypassing security controls: Registry edits can be used to bypass security controls, such

as User Account Control (UAC). [4, 4, 13, 13]
- Installing software: Registry edits are often used as part of the installation process for software, adding entries to the registry to indicate that the software is installed. [1, 26]

- **Security Risks:** Modifying the registry can have unintended consequences and can be exploited by malicious actors to compromise system integrity. [4, 4, 13, 13]

3. Virtualization:

- **Purpose:** Virtualization creates isolated environments for applications, allowing them to run in a different context without interfering with the host system. [5, 5, 6, 6, 27, 28, 29]
- **Mechanism:** Virtualization techniques, such as application virtualization (App-V), create virtual environments where applications can run as if they were installed on a different OS. [6, 6, 30, 31, 32]
- **Examples:**
- App-V: App-V allows applications to be deployed and run on a virtual environment without being installed on the host operating system. [6, 33, 34, 35]
- Sandbox: Sandboxes create isolated environments for applications, allowing them to run without impacting the host system or other applications. [36, 37, 38, 39]

- **Benefits:** Virtualization helps improve application compatibility, reduce conflicts between different applications, and improve security by isolating applications from the host system. [6, 6, 36, 36, 40, 41, 42]

In summary, shims, registry edits, and virtualization are powerful tools for managing application compatibility and persistence on Windows systems. However, they can also be used for malicious purposes, so it's important to understand the potential risks and security implications of using these techniques. [4]