Difference between User, Admin and System Context.

In MSI, context refers to the level of access a process or component has within windows operating system.

User Context

- Runs under currently login user.
- Can only access files and settings of user profile.
- Best for task that does not requires system-wide changes.
- It has limited access to user's profile.

System Context

- Runs with elevated privileges often as system user with full wide access.
- Can access all files and system resources.
- Best where full system control is needed.
- It has full system-wide access.

Admin Context

- It has full access of system but is not the owner.
- These installations require to have admin privileges to run MSI and perform system changes.
- Best for installations that modify system files, services or other resources that requires elevated permissions.
- It requires admin privileges for system-wide changes.

Logon scripts to populate user profile data.

Logon script is a script that automatically runs soon after the user logs in.

These are the ways:

1. **Leverage Active Setup**
   Active Setup allows you to run specific actions like copying files, updating registry keys, or executing scripts during the user's logon process.
   we can include Active Setup within your MSI package to trigger these actions whenever a user logs in. Active Setup to copy configuration files from a machine location into the user's AppData folder during logon.
2. **Create and Assign Logon Script**
   These scripts can be batch files, PowerShell scripts, or other scripting languages like VBScript. A script might copy user-specific files from a shared network location to the user's profile directory during logon. Logon scripts can be assigned to individual user accounts or to groups of users via Group Policy
3. **Consider Deployment Strategies**
   we can deploy logon scripts using Group Policy, assigning them to specific organizational units (OU) or user accounts. Choose a scripting language suitable for your needs. Batch files are simpler, while PowerShell offers more advanced capabilities

4. **Example Copying User setting files**
   The application needs to store user-specific settings files in the user's AppData folder, but these files need to be available immediately upon logon
   Solutions
   - MSI Package- Include an Active Setup entry that triggers a logon script during user logon
   - Logon script- Create a script that copies settings files from the shared network to the user's AppData folder
   - Deployment- Deploy the MSI package and the associated logon script using Group Policy.
5. **Best Practices**
   - Error handling - incorporate error handling in logon script to prevent potential issues.
   - Security - ensure scripts are secure, especially while dealing with sensitive data.
   - Testing - check the test script and deployment process to ensure that they work as expected.
   - Documentation - document your script, deployment procedures, and other configurations for troubleshooting and easy maintenance.

Windows 11 Benefits

- Improved User Interface
- Enhanced Security
- Performance improvement
- Integrated AI assistant
- Improved Multi-tasking
- Enhanced Gaming Experience

Windows 10 Benefits

- Familiar Interface
- Wide Compatibility
- Stability
- Cost-Effective

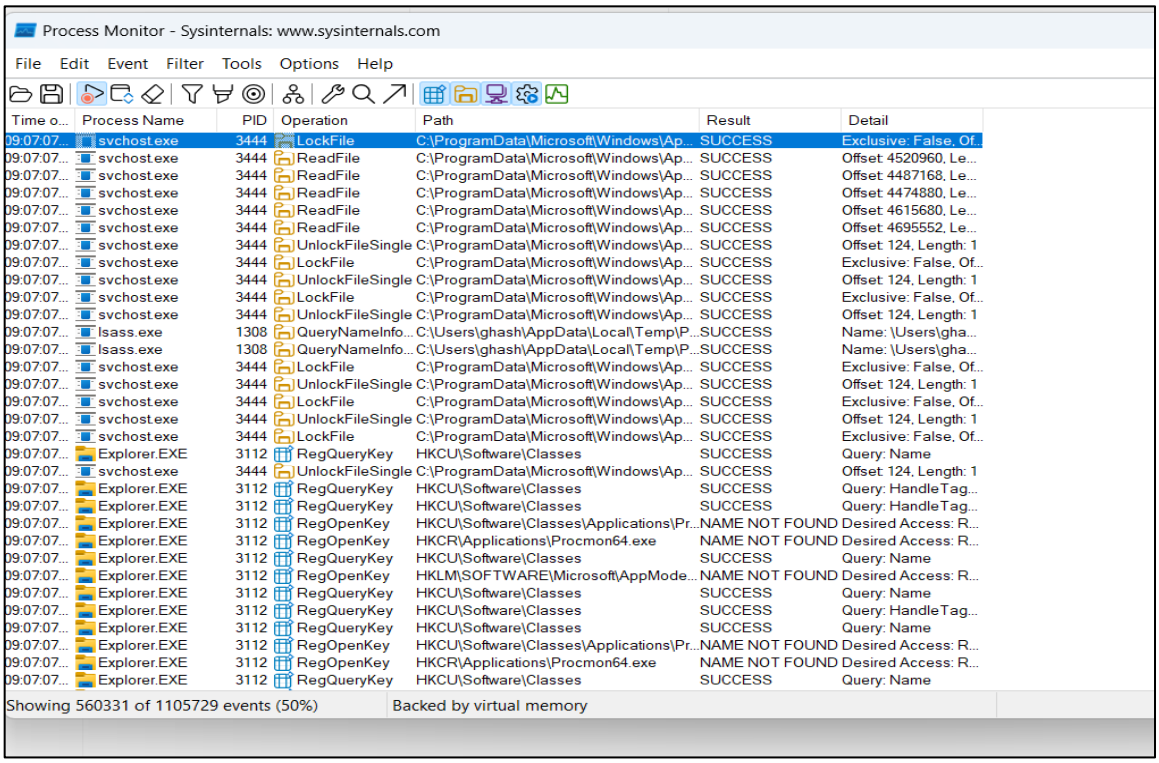
Considerations for an "App Pack"

- App Compatibility
- Performance
- Security

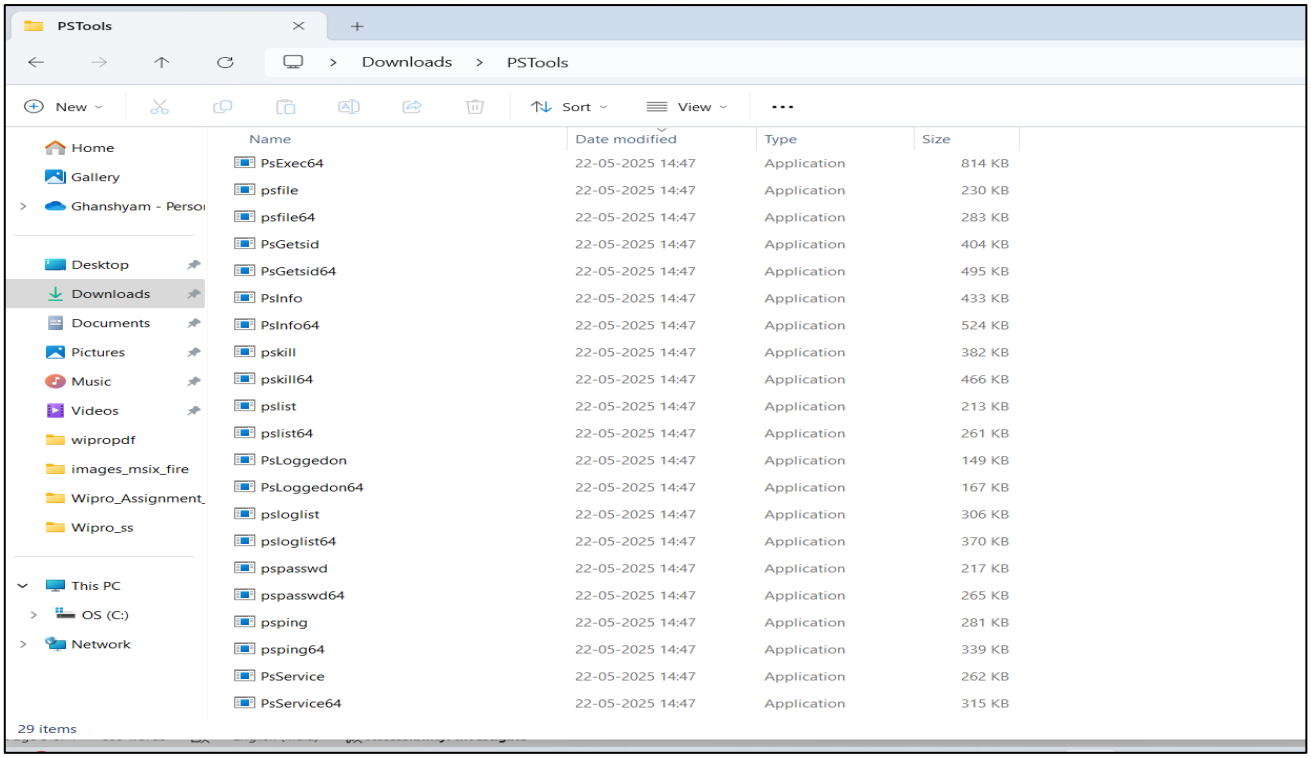
Sysinternal tools for troubleshooting and security

1. **Autologon –**
    - It automates user login process.
    - It's a GUI tool that configures the Windows registry to automatically log on a specified user with provided credentials.
    - Useful for headless systems or automated testing environments.

2. **Process Explorer –**
    - A powerful tool for viewing and managing running processes.
    - It Provides detailed information about processes, including memory usage, handles, and open files.
    - Essential for troubleshooting process-related issues, investigating malware, etc.



3. **PsExec –**
    - A powerful tool for remote execution of commands and programs.
    - It allows administrators to run applications on a remote computer as if they were running locally.
    - Useful for remote system management, patching, and troubleshooting
4. **PSTools –**
    - A collection of command-line tools for system administration and troubleshooting.
    - Includes tools like PsLoggedOn, PsFile, and PsList, among others.
    - It provides a wide range of administrative capabilities for local and remote systems.



5. **RegMon –**
    - Monitors registry access and changes in real-time.
    - It tracks all registry activity, including reads, writes, and deletes.
    - It also helps troubleshoot registry-related issues, investigate security vulnerabilities.
6. **Sysmon –**
    - A Windows system service and driver that monitors and logs system activity(provides system level monitoring).
    - It provides detailed information about process creations, network connections, and file access changes.
    - Essential for security monitoring, intrusion detection, and forensic analysis
7. **Whois –**
    - A command-line tool (though not directly from Sysinternals) used to retrieve information about domain names and IP addresses.
    - It queries a Whois database to retrieve registration details.
    - Useful for network troubleshooting, identifying domain owners, and checking domain availability

Active Setup Versioning to ensure it runs each time during Fresh Install

To ensure Active Setup runs during a fresh install, increment the "Version" value in the HKLM (HKEY_LOCAL_MACHINE) registry key. This forces the Active Setup process to compare the HKLM version with the HKCU (HKEY_CURRENT_USER) version and execute the "StubPath" command when a user logs in.

1. **Active Setup and Versioning**

- Active Setup is a Windows mechanism that allows an application to perform user-specific configuration upon user login.
- It works by comparing versions in the HKLM and HKCU registry hives.

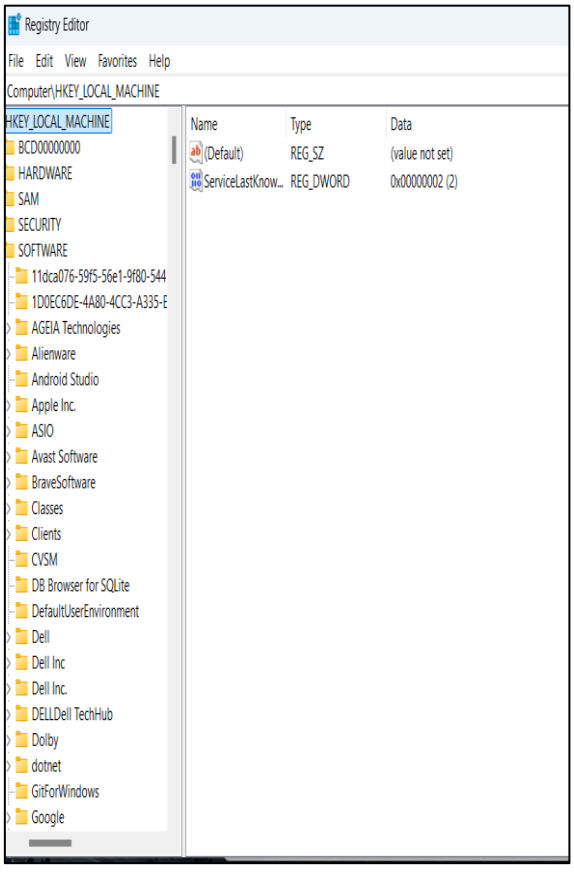
2. **HKLM vs HKCU**

- **HKLM**: Stores the master Active Setup data such as application name, StubPath and Version.
- **HKCU**: Stores the user-specific Active Setup data which is populated based on the HKLM data during logon.

3. **Incrementing the Version**

- If the version in HKLM is higher than the version in HKCU, Active Setup will execute the command specified in the "StubPath" value and update the HKCU version.

HKLM



HKCU