Summary of MSI Contexts in Windows Installer:

In Windows Installer (MSI), context refers to the level of access during installation or execution:

- **User Context**: Runs under the logged-in user's profile. It has access to user-specific files/settings but lacks full system access. Best for user-specific tasks and applications.
- **System Context**: Runs with elevated privileges (as SYSTEM), allowing full system-wide access. Suitable for system-wide installations and critical changes.
- **Admin Context**: Not a separate context, but some actions require admin rights. Used when installations modify system files or need elevated permissions.

Summary of Logon Scripts :

1. **Active Setup in MSI Packages**:

   Triggers actions (e.g., file copies, registry updates) during user logon.

   Ensures user-specific data is initialized, like copying config files to %AppData%.

2. **Creating and Assigning Logon Scripts**:

   Use scripting languages like batch, PowerShell, or VBScript.

   Scripts can copy files from shared locations to user profiles.

   Assign via Group Policy to users or groups.

3. **Deployment Strategies**:

   Use Group Policy to assign logon scripts or deploy MSI packages.

   Select scripting tools based on complexity—PowerShell for advanced logic.

4. **Example Scenario**:

   An app needs settings in %AppData% upon user logon.

   Active Setup triggers a logon script to copy settings .

   Deploy the MSI and script using Group Policy or Software Distribution.

Summary of Sysinternals Tools:

Sysinternals tools are essential for Windows system troubleshooting and security analysis:

1. **Autologon** – Automates user login via registry settings; ideal for testing or headless systems.
2. **Process Explorer** – Offers deep insight into running processes, memory usage, and handles; vital for diagnosing system and malware issues.
3. **PsExec** – Enables remote execution of commands; useful for remote administration and troubleshooting.
4. **PSTools** – A suite of command-line tools (e.g., PsList, PsFile) for managing local and remote systems.
5. **RegMon** – Monitors real-time registry activity; helps in diagnosing registry issues and detecting malicious changes.
6. **Sysmon** – Logs detailed system events like process creation and network activity; key for security monitoring and forensics.
7. **Whois** – Retrieves domain/IP registration details; helpful for network troubleshooting and identifying domain owners.