**Summary on today’s Class:**  
User, System, and Admin contexts define the privilege level and scope under which processes run. The User Context is limited to user-specific resources, while the System Context runs with full machine-level privileges under the local system account. The Admin Context allows elevated operations typically used during software installation or configuration. Logon Scripts, run at user login, are useful for setting environment variables or mapping drives, whereas Active Setup in MSI packages enables per-user initialization tasks by comparing registry entries in HKLM and HKCU and running setup commands if needed. Windows 10 and 11 offer different benefits: Windows 10 ensures broader compatibility, while Windows 11 introduces enhanced security features (TPM 2.0, virtualization-based security) and productivity improvements. When packaging applications, considerations include installation scope (user vs system), silent install options, dependencies, and user-specific configurations, often handled through Active Setup or scheduled tasks. Scheduled Tasks allow actions to run on triggers like logon or time, under various privilege levels. For debugging and system management, Sysinternals tools such as Autologon, Process Explorer, PsExec, PSTools, SysMon, and Whois provide deep insight and control over system behavior. During a fresh install or update, Active Setup versioning ensures user configurations are reapplied if versions mismatch. Understanding the registry distinction between HKLM (system-wide) and HKCU (user-specific) is critical for proper configuration management.