 **Application Logs** – events from installed software.

 **System Logs** – events from Windows system components (drivers, services).

 **Security Logs** – login attempts, access control (success/failure audits).

 **Setup & Forwarded Events** – installation/configuration-related log

 **HKEY\_CLASSES\_ROOT (HKCR)** → Info about file types & associations.

 **HKEY\_CURRENT\_USER (HKCU)** → Settings of the current logged-in user.

 **HKEY\_LOCAL\_MACHINE (HKLM)** → System-wide settings for all users.

 **HKEY\_USERS (HKU)** → Profiles of all user accounts.

 **HKEY\_CURRENT\_CONFIG (HKCC)** → Hardware configuration at startup.

**CMD – Why it is used?**

👉 *“CMD is used for running basic commands, troubleshooting, and supporting older applications or scripts.”*

**PowerShell – Why it is used?**

👉 *“PowerShell is used for automation, advanced administration, and deployment tasks because it’s more powerful and supports scripting with cmdlets.”*

* **File Permissions (NTFS**)
* Read – View content.
* Write – Add or modify content.
* Execute – Run programs.
* Modify – Read, write, delete.
* Full Control – All actions, including permission changes.

whois

* A Whois is a **command-line tool** used to query information about a domain name or IP address.
* Provides ownership and technical information about domains and IP addresses.
* Symon
* Sysmon helps track detailed system activities like processes, file changes, and network connections, which is useful for monitoring and troubleshooting in packaging
* Data Preparation – Clean, filter, and organize raw data.
* Data Analysis – Discover trends, patterns, and insights.
* Visualization – Create professional charts and dashboards.
* Get → Retrieve information
* Set → Modify something
* New → Create something
* Remove → Delete something

“Intune is a cloud-based tool used by organizations to manage devices, apps, and security policies remotely.