### ****Windows Registry Hives****

|  |  |  |  |
| --- | --- | --- | --- |
| **Registry Hive** | **Path** | **Associated Files** | **Description / Contents** |
| **HKEY\_CLASSES\_ROOT** | N/A | Merged view from HKLM\Software\Classes and HKCU\Software\Classes | Stores information about registered applications, file associations, and COM objects. |
| **HKEY\_CURRENT\_USER** | %SystemRoot%\Users\<username>\NTUSER.DAT | Ntuser.dat, Ntuser.dat.log | Contains configuration for the currently logged-in user (desktop, environment, network, applications). |
| **HKEY\_LOCAL\_MACHINE\SAM** | %SystemRoot%\System32\Config\SAM | Sam, Sam.log, Sam.sav | Stores Security Accounts Manager (SAM) information – user names and hashed passwords. |
| **HKEY\_LOCAL\_MACHINE\SECURITY** | %SystemRoot%\System32\Config\Security | Security, Security.log, Security.sav | Contains local security policy, access control, and auditing settings. |
| **HKEY\_LOCAL\_MACHINE\SOFTWARE** | %SystemRoot%\System32\Config\Software | Software, Software.log, Software.sav | Stores software configuration, including OS and application settings. |
| **HKEY\_LOCAL\_MACHINE\SYSTEM** | %SystemRoot%\System32\Config\System | System, System.alt, System.log, System.sav | Stores system configuration including drivers, services, and startup settings. |
| **HKEY\_LOCAL\_MACHINE\HARDWARE** | N/A (volatile) | Not stored on disk | Recreated at boot, contains hardware information detected by Windows at startup. |
| **HKEY\_USERS** | %SystemRoot%\System32\Config\Default  (for .DEFAULT) | Default, Default.log, Default.sav | Contains user-specific settings for all users on the system. Subkeys include .DEFAULT and individual user SIDs. |
| **HKEY\_CURRENT\_CONFIG** | Linked to HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current | System, System.alt, System.log, System.sav | Provides runtime hardware configuration used at system startup. |
| **HKEY\_USERS.DEFAULT** | %SystemRoot%\System32\Config\Default | Default, Default.log, Default.sav | Default user profile used when no user is logged in (like at login screen). |

### ****Additional Notes on Registry Hives:****

* **Volatile Hives** (not stored on disk):
  + HKEY\_LOCAL\_MACHINE\Hardware
  + HKEY\_LOCAL\_MACHINE\System\CurrentControlSet
  + HKEY\_CURRENT\_USER
* **Hive Files Storage Directory**:
  + %SystemRoot%\System32\Config
* **File Types in Registry**:
  + .dat, .log, .sav — used to store, update, and back up registry data.

**Registry File Locations (Quick View)**:

|  |  |
| --- | --- |
| **File** | **Path** |
| NTUSER.DAT | %SystemRoot%\Users\<username>\ |
| SAM, SECURITY, SOFTWARE, SYSTEM, DEFAULT | %SystemRoot%\System32\Config\ |

!