Windows Registry

The Windows Registry is used to store much of the information and settings for software programs, hardware devices, user preferences, operating system configurations, and much more.

In the registry, there are 'hives' that correspond to several files. Hives are a collection of keys, subkeys and values that contain the configurations for the operating system and programs.

In the registry, there are 5 default hive groups:

- `HKEY_CLASSES_ROOT` – Contains technical information that enables applications to exchange information with one another
- `HKEY_CURRENT_USER` – Contains personal settings for the currently logged-in user
- `HKEY_LOCAL_MACHINE` – Contains system-wide settings that apply regardless of who's logged in
- `HKEY_USERS` – Stores the personal settings of all registered users, including special system accounts that are used for administrative tasks
- `HKEY_CURRENT_CONFIG` – Contains information about which hardware and drivers are installed and running at the moment

For the corresponding hives, you will see several types of extensions:

- No Extension: The complete registry hive
- .alt: An alternate copy of the registry hive
- .log: A log of changes that have occurred within the registry hive
- .sav: A backup created from when a setup or program installation occurs.

Registry Hive Locations and Supporting Files

Registry Hive Name	Location	Supporting Files
HKEY_LOCAL_MACHINE \SYSTEM	%SystemRoot%\system32\config\system	System, System.alt, System.log, System.sav
HKEY_LOCAL_MACHINE \SAM	%SystemRoot%\system32\config\sam	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE \SECURITY	%SystemRoot%\system32\config\security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE \SOFTWARE	%SystemRoot%\system32\config\software	Software, Software.log, Software.sav
HKEY_USERS \UserProfileSID	%SystemRoot%\winnt\profiles\username	
HKEY_USERS.DEFAULT	%SystemRoot%\system32\config\default	Default, Default.log, Default.sav
HKEY_CURRENT_CONFIG	%SystemRoot%\System32\Config	System, System.alt, System.log, System.sav, Ntuser.dat, Ntuser.dat.log

Useful Registry Locations

- **USB Device Registry Entries - Find USB device information after it enumerates**
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB`
- **Find a list of User Profile SID's**
  - `\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\`
  - **Or Use wmic Command:** `wmic useraccount get name,sid`