WINDOWS REGISTRY,SOME BASIC UNDERSTANDING

For the peoples who use Windows, 'Windows Registry' is not a new word at all. The registry is a central database of all configuration settings for most of the applications installed on the computer. Windows stores all its settings in this 'Registry' itself. The 'Windows Registry Editor' allows us to configure many hidden settings for windows and other applications installed, which are not accessible by the interface of the particular software itself. You can easily manipulate and modify the values of registry and improve the PC's performance. However, do it carefully, because modify the right setting and your computer gets a boost, modify the wrong one and you end up with a non-booting system. In my previous post I wrote about 'Autoruns', it can also manipulate registry. (Read here)

To edit registry, we can use 'Windows Registry Editor', which is preinstalled in Windows itself. It can be launched by using the command 'regedit' in the 'RUN' dialog box, which can be launched by pressing "Windows key+R". On start-up, 'Windows Registry' will show up the following five root entries.

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

All the settings given above are not stored in a single file. They are spread across multiple files in logical groups called 'hives'. The combination of hives makes 'Windows Registry'. . The values are stored here in binary format. That means only "1" and "0" is used here. "1" means "yes", whereas the value "0" represents "no". Let us look into the details of these settings.

1. **HKEY_CLASSES_ROOT**: It is abbreviated as HKCR. This part of registry is used for storing file associations and information about the applications registered for handling different data types.
2. **HKEY_CURRENT_USER:** This is abbreviated as HKCU. This sub-tree contains the user profile for the user who is currently logged on. This profile contains environment variables, personal program groups, desktop settings, network connection, application preference etc. a new HKEY_CURRENT_USER sub-tree is created each time a user logs on. The data for this sub-tree comes from the profile of current user. This sub-tree provides easier access to the data. The values can be viewed and changed accordingly to your desire.
3. **HKEY_LOCAL_MACHINE:** It is abbreviated as KHLM. This sub-tree contains information about local computer system, including hardware and operating system info, such as "bus type, system memory, device driver etc..". The settings in this section are arranged as "Company/Product/Version" format. Thus settings for Microsoft's own applications will be found in 'HKLM-Software-Microsoft'. The settings can be modified accordingly.
4. **HKEY_USERS:** This key contains the configuration of each user. It has one sub-key for each user after the user's "Security ID"(SID).
5. **HKEY_CURRENT_CONFIG:** This part of Registry contains the information that is generated during the runtime.

Apart from the command 'regedit', advanced registry modification can be done using the 'Microsoft Management Console', which can be launched by using the command "mmc" in Run dialog box. In addition, you can launch 'Group Policy Editor' by using the command 'gpedit.mmc'. This allows you to configure your computer's "policies" such as password strength restriction etc.

At last I would like to say that Windows Registry is a very vast database. Do not modify or manipulate anything, if you exactly don't know what you are doing!

Source: http://alltech360.wordpress.com/2012/05/05/windows-registrysome-basic-understanding/