**Windows Registry**

The Registry is a various levelled or we can say a hierarchical database that stores low-level settings and other information for the Microsoft Windows Operating System and for applications that pick to utilize the registry. From the point of installation of operating system, registries are used. Kernel, Device Driver settings to the Hardware and User Interface all settings are stored in the windows registry.

When Programs and Applications are installed in the system their configurations and default values are stored in the registry although there are some applications which do not utilize windows registry. For example, .NET framework applications use XML files for configuration, Portable applications usually keep their configuration data within files in the directory/folder where the application executable resides.

**Importance of Registry in Windows Forensics**

For a Forensic analyst, the Registry is a treasure box of information. It is the database that contains the default settings, user, and system defined settings in windows computer. Registry serves as repository, monitoring, observing and recording the activities performed by the user in the computer. The Data is stored in the main folders in a Tree like structure which is called Hive and its subfolders are called KEYS and SUBKEYS where each component’s configuration is stored called VALUES. Some Important aspects of Windows Registry are:

1. Windows Registry can be considered as a gold mine of forensic evidence.
2. We can create new registries manually or we can modify the ones that already exist.
3. Original files that contain registry values are stored in the system directory itself.
4. Registry files are system protected and can not be accessed by any user unless administration access is provided.
5. For the investigation purpose, the forensic investigator analyzes registry files via tools such as Registry Viewer, Regshot, Registry Browser etc..
6. Trojans and Malware information can be found in the registries.

**Main Registry Hives**

* HKEY\_CLASSES\_ROOT
* HKEY\_CURRENT\_USER
* HKEY\_LOCAL\_MACHINE/SAM
* HKEY\_LOCAL\_MACHINE/SOFTWARE
* HKEY\_LOCAL\_MACHINE/SECURITY
* HKEY\_LOCAL\_MACHINE/SYSTEM
* HKEY\_USERS
* HKEY\_CURRENT\_CONFIG

Link - <https://medium.com/@lucideus/windows-registry-forensic-analysis-part-1-windows-forensics-manual-2018-2cb4da210125>

Link - <https://gbhackers.com/windows-registry-analysis-tracking-everything-you-do-on-the-system/>