Experiment No:6

**Aim:** Case study on Windows Registry.

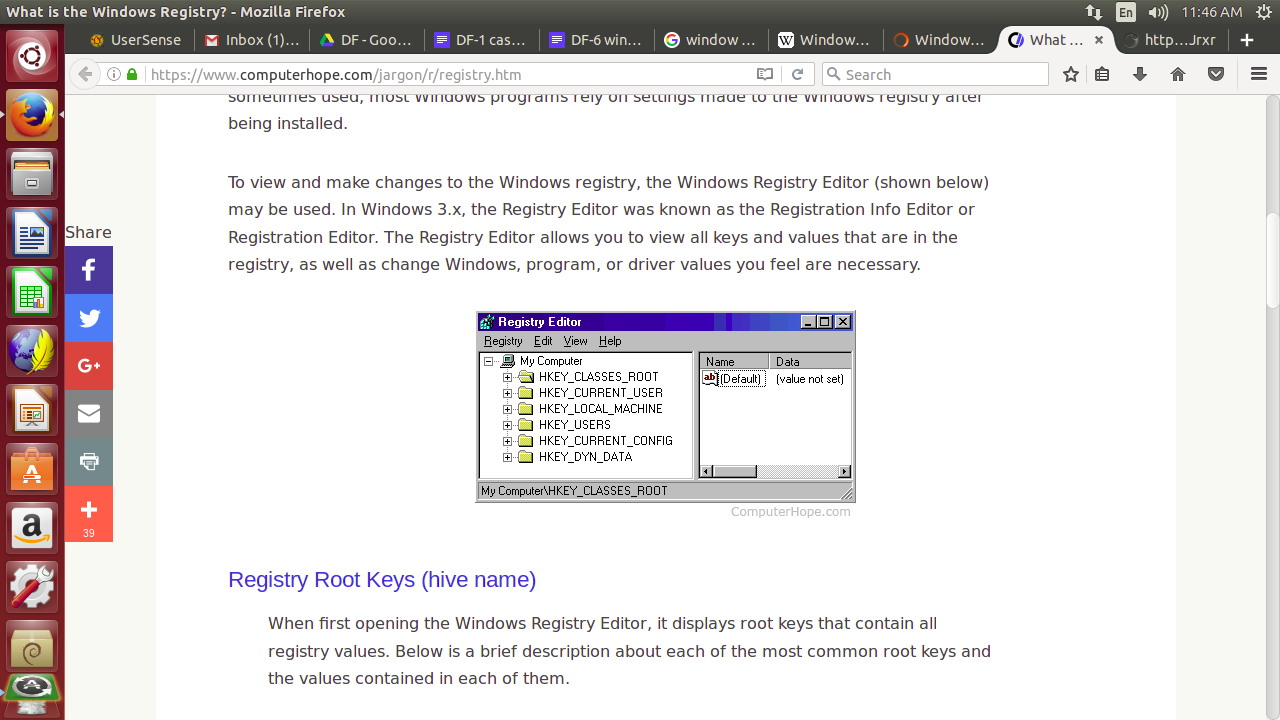
**Theory:**

**What is Windows Registry?**

The **registry** or **Windows registry** contains information, settings, options, and other values for programs and hardware installed on all versions of Microsoft Windows operating systems. For example, when a program is installed, a new subkey contains settings like a program's location, it's version, and how to start the program, are all added to the Windows registry. To view and make changes to the Windows registry, the Windows Registry Editor (shown below) may be used. In Windows 3.x, the Registry Editor was known as the Registration Info Editor or Registration Editor. The Registry Editor allows you to view all keys and values that are in the registry, as well as change Windows, program, or driver values you feel are necessary.

**To open the Windows registry, follow the steps below.**

1. Click the Start button.
2. In the Start Menu, either in the Run Box or the Search box, type **regedit** and press Enter. In Windows 8, you can type **regedit** on the Start screen and select the *regedit* option in the search results. In Windows 10, type **regedit** in the Search box on the taskbar and press Enter.
3. If prompted by User Account Control, click **Yes** to open the Registry Editor.
4. The Windows Registry Editor window should open and look similar to the example shown below.



## **How to edit a Windows registry value**

To edit a registry value, double-click the name of the value you want to edit. For example, if we were to double-click the 'IntelliPoint' value in the example above, a new window would appear that would allow us to change the value of the Data. In this case, we could change the file path of where the "ipoint.exe" file is located for the IntelliPoint driver.

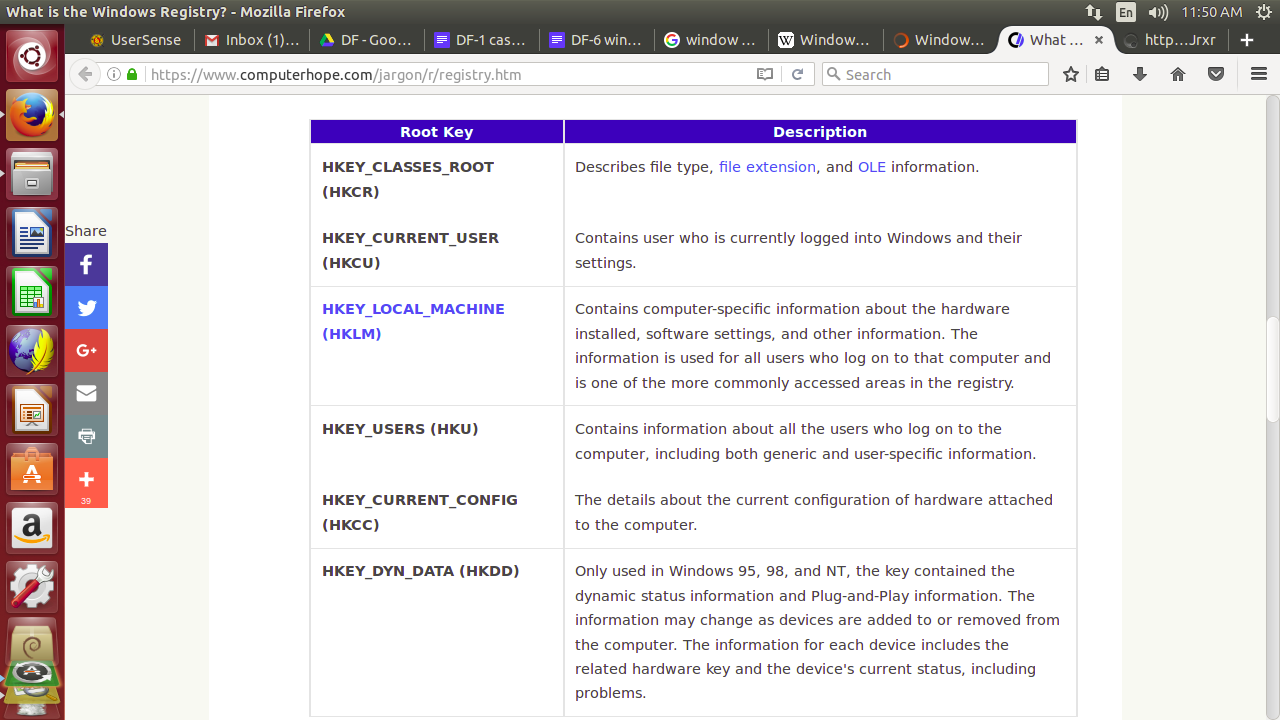
## **How do I delete a Windows registry value**

To delete a registry value, highlight any registry Name and then press the delete key on the keyboard. For example, if we did not want the IntelliPoint program to load each time Windows starts, we could highlight IntelliPoint and then press the delete key.

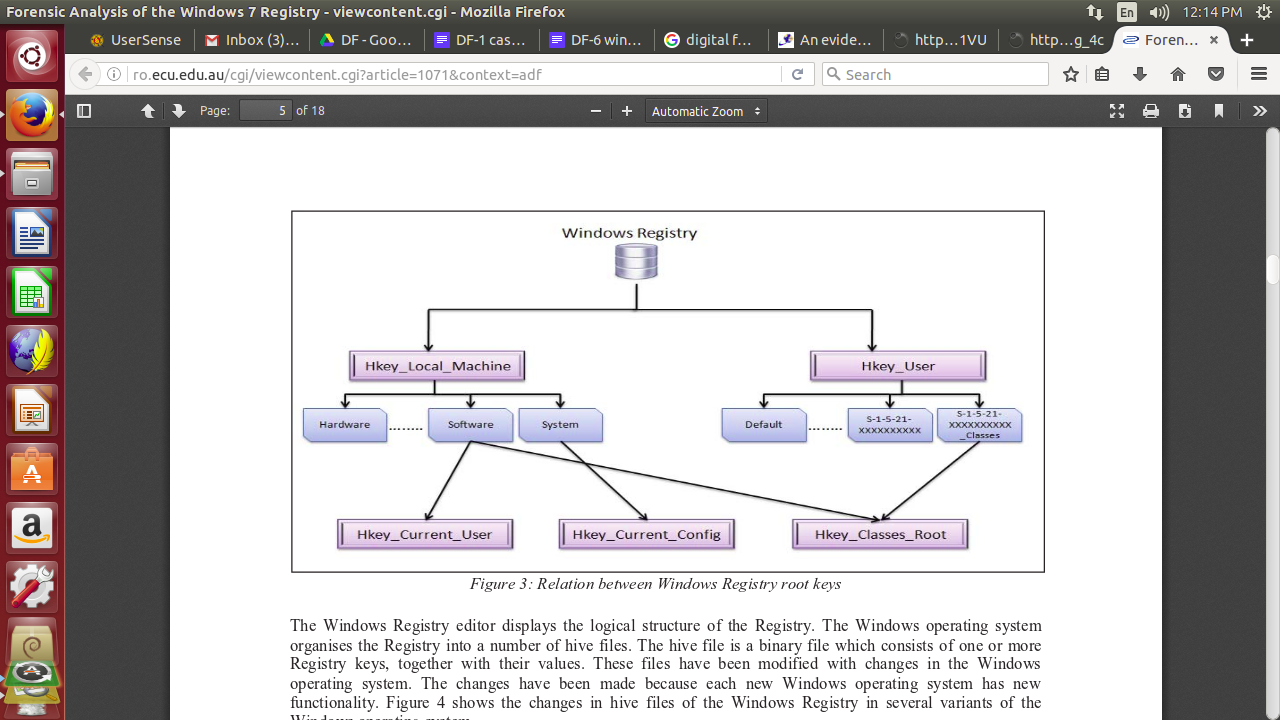
## 

## **Registry Root Keys (hive name)**

When first opening the Windows Registry Editor, it displays root keys that contain all registry values. Below is a brief description about each of the most common root keys and the values contained in each of them.



Like other files and services in Windows, all registry keys may be restricted by access control lists (ACLs), depending on user privileges, or on security tokens acquired by applications, or on system security policies enforced by the system (these restrictions may be predefined by the system itself, and configured by local system administrators or by domain administrators). Different users, programs, services or remote systems may only see some parts of the hierarchy or distinct hierarchies from the same root keys.



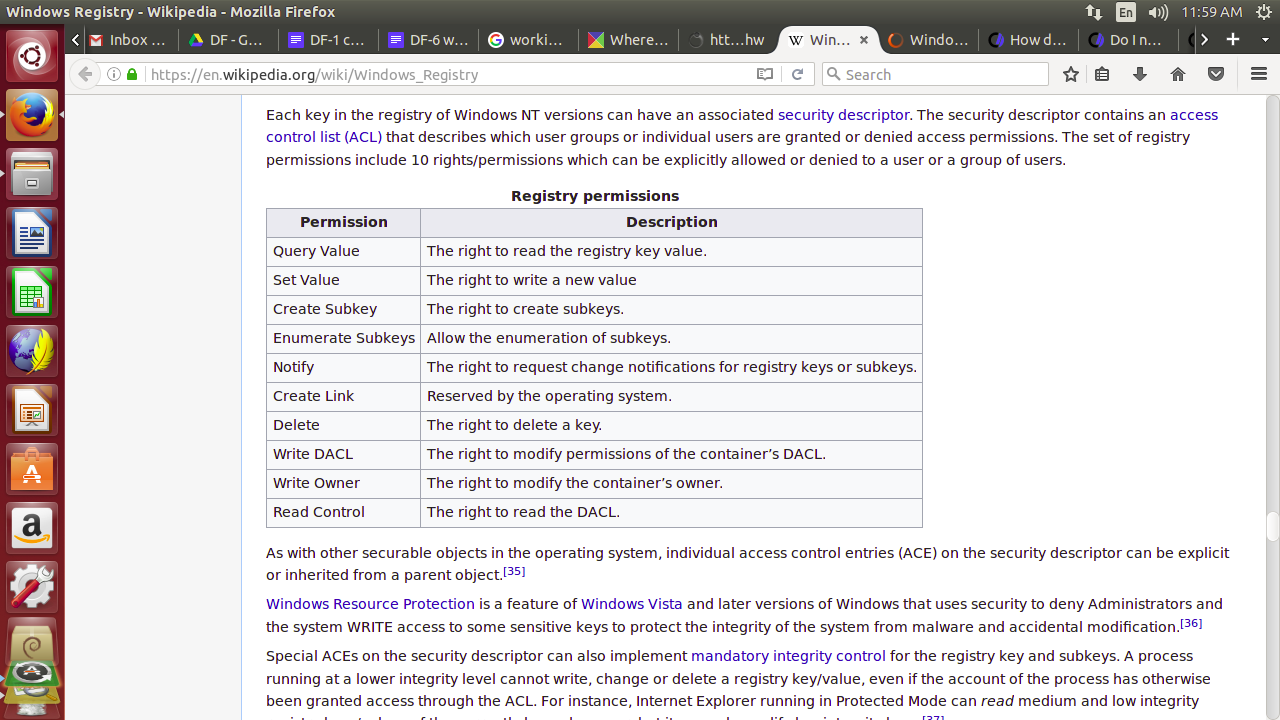
**Fig: Relation between Windows Registry root keys**

### **Windows Registry Availability**

The Windows Registry and the Microsoft Registry Editor program are available in nearly every Microsoft Windows version including Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000, Windows NT, Windows 98, Windows 95, and more.

## **Security**

Each key in the registry of Windows NT versions can have an associated security descriptor. The security descriptor contains an access control list (ACL) that describes which user groups or individual users are granted or denied access permissions. The set of registry permissions include 10 rights/permissions which can be explicitly allowed or denied to a user or a group of users.



# **POWELIKS: Malware Hides In Windows Registry**

We spotted a malware that hides all its malicious codes in the Windows Registry. The said tactic provides evasion and stealth mechanisms to the malware, which Trend Micro detects as TROJ\_POWELIKS.A. When executed, TROJ\_POWELIKS.A downloads files, which can cause further system infection. Systems affected by this malware risk being infected by other malware, thus causing further system infection. In addition, it has the capability to steal system information, which may be used by cybercriminals to launch other attacks.

**Case:**

Many hackers crack a local wireless access point and use it for their intrusions. In this way, if the IP address is traced, it will lead back to the neighbor's or other wireless AP and not them. For example, back in January 2012, an Anonymous member, John Borrell III, hacked into the computer systems of the Salt Lake City police department and the Utah Chiefs of Police. The FBI was called in to investigate and they traced the hacker back to the IP address of Blessed Sacrament Church's Wi-Fi AP in Toledo, Ohio. The hacker had apparently cracked the password of the church's wireless AP and was using it to hack "anonymously" on the Internet.

Eventually, the FBI was able to find the suspect through various investigation techniques, mostly low-tech, exhaustive, detective work. It helped that John Borrell had bragged on Twitter of his success as a hacker. Eventually, Mr. Borrell was convicted and sentenced to two years in Federal prison. When the FBI tracked down Mr. Borrell and seized his computer, they were able to prove he had been connected to the church AP by examining his registry. The forensic investigator simply had to look in the registry at this location:

**Backups and recovery**

Different editions of Windows have supported a number of different methods to backup and restore the registry over the years, some of which are now deprecated:

* **System Restore** can backup the registry and restore it as long as Windows is bootable, or from the Windows Recovery Environment (starting with Windows Vista).
* **NTBackup** can back up the registry as part of the *System State* and restore it. Automated System Recovery in Windows XP can also restore the registry.
* On Windows NT, the *Last Known Good Configuration* option in startup menu relinks the HKLM\SYSTEM\CurrentControlSet key, which stores hardware and device driver information.
* Windows 98 and Windows Me include command line (Scanreg.exe) and GUI (Scanregw.exe) registry checker tools to check and fix the integrity of the registry, create up to five automatic regular backups by default and restore them manually or whenever corruption is detected. The registry checker tool backs up the registry, by default, to %Windir%\Sysbckup Scanreg.exe can also run from MS-DOS.
* The Windows 95 CD-ROM included an Emergency Recovery Utility (ERU.exe) and a Configuration Backup Tool (Cfgback.exe) to back up and restore the registry. Additionally Windows 95 backs up the registry to the files system.da0 and user.da0 on every successful boot.
* **Windows NT 4.0** included RDISK.EXE, a utility to backup and restore the entire registry.
* **Windows 2000 Resource Kit** contained an unsupported pair of utilities called Regback.exe and RegRet.exe for backup and recovery of the registry.

**Conclusion:** Given the popularity of the Windows operating system - in homes and businesses - it is important for computer forensic experts to understand the complexity of the Windows Registry. The information and potential evidence that reside in the Registry make it a significant forensic resource; uncovering this data can be crucial to any computer related investigation. By understanding the fundamentals of the Registry from a forensics standpoint, an examiner can develop a more precise account on what actions occurred on the given machine.