Digital Forensics for the Aspiring Hacker, Part 5 (Windows Registry Forensics)

- By **occupytheweb**
- Forensics

Welcome back, my aspiring hackers!

As I mentioned in earlier posts, the best hackers (or at least those not behind bars) have a keen understanding of digital forensics. If I am tasked to intrude upon an enemy's file server to retrieve war plans, such as in this tutorial, it is essential to my country's (and my own) well-being that it not be traced back to me. Understanding digital forensics helps us to leave without a trace and never have a trail back to us or our employer.

Although nearly all Microsoft Windows users are aware that their system has a registry, few understand what it does, and even fewer understand how to manipulate it for their purposes. As a forensic analyst, the registry can be a treasure trove of evidence of what, where, when, and how something occurred on the system.

In this post, I want to help you to understand how the Windows registry works and what evidence it leaves behind when someone uses the system for good or ill.

What Is the Registry?

The registry is a database of stored configuration information about the users, hardware, and software on a Windows system. Although the registry was designed to configure the system, to do so, it tracks such a plethora of information about the user's activities, the devices connected to system, what software was used and when, etc. All of this can be useful for the forensic investigator in tracking the who, what, where, and when of a forensic investigation. The key is just knowing where to look.

Hives

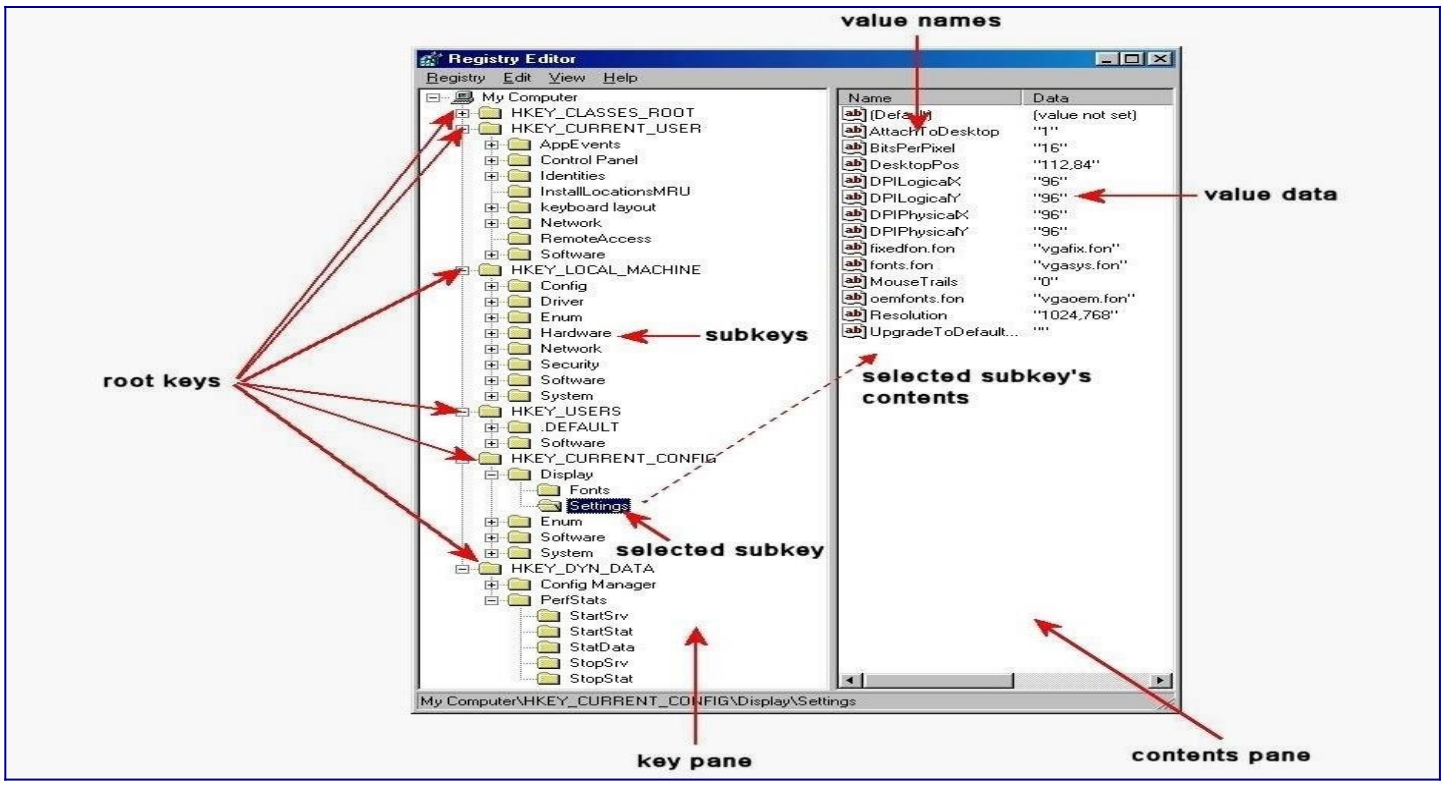
Inside the registry, there are root folders. These root folders are referred to as hives. There are five (5) registry hives.

- **HKEY_USERS**: contains all the loaded user profiles
- **HKEYCURRENT_USER**: profile of the currently logged-on user
- **HKEYCLASSES_ROOT**: configuration information on the application used to open files
- **HKEYCURRENT_CONFIG**: hardware profile of the system at startup
- **HKEYLOCAL_MACHINE**: configuration information including hardware and software settings

Registry Structure

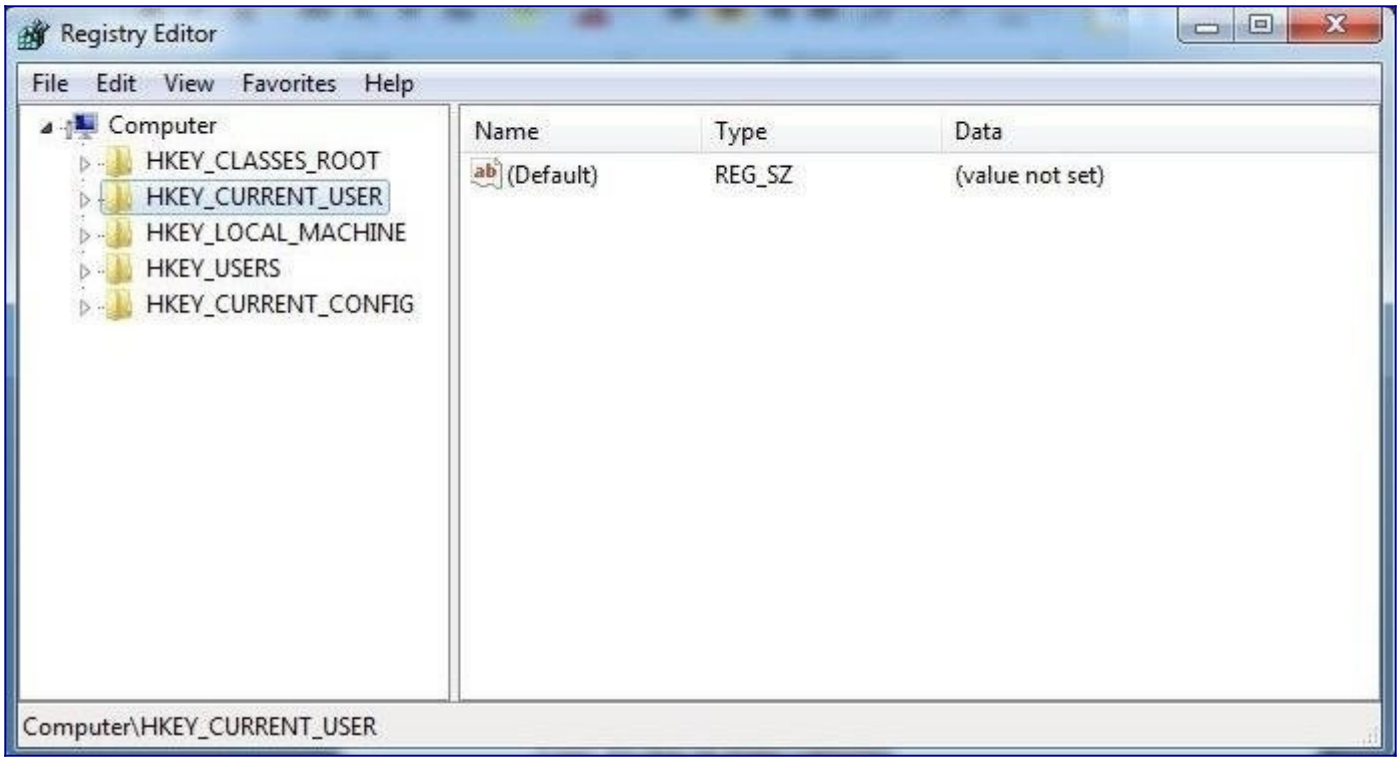
The registry is structured very similarly to the Windows directory/subdirectory structure. You have the five root keys or hives and then subkeys. In some cases, you have sub-subkeys. These subkeys

then have descriptions and values that are displayed in the contents pane. Very often, the values are simply 0 or 1, meaning on or off, but also can contain more complex information usually displayed in hexadecimal.



Accessing the Registry

On our own system—not in a forensic mode—we can access the registry by using the **regedit** utility built into Windows. Simply type regedit in the search window and then click on it to open the registry editor like that below.



Information in the Registry with Forensic Value

As a forensic investigator, the registry can prove to be a treasure trove of information on who, what, where, and when something took place on a system that can directly link the perpetrator to the actions being called into question. As a hacker, the registry can provide that evidence necessary to put you away in prison for quite awhile.

Information that can be found in the registry includes:

- Users and the time they last used the system
- Most recently used software
- Any devices mounted to the system including unique identifiers of flash drives, hard drives, phones, tablets, etc.
- When the system connected to a specific wireless access point
- What and when files were accessed
- A list any searches done on the system
- And much, much more

Wireless Evidence in the Registry

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.

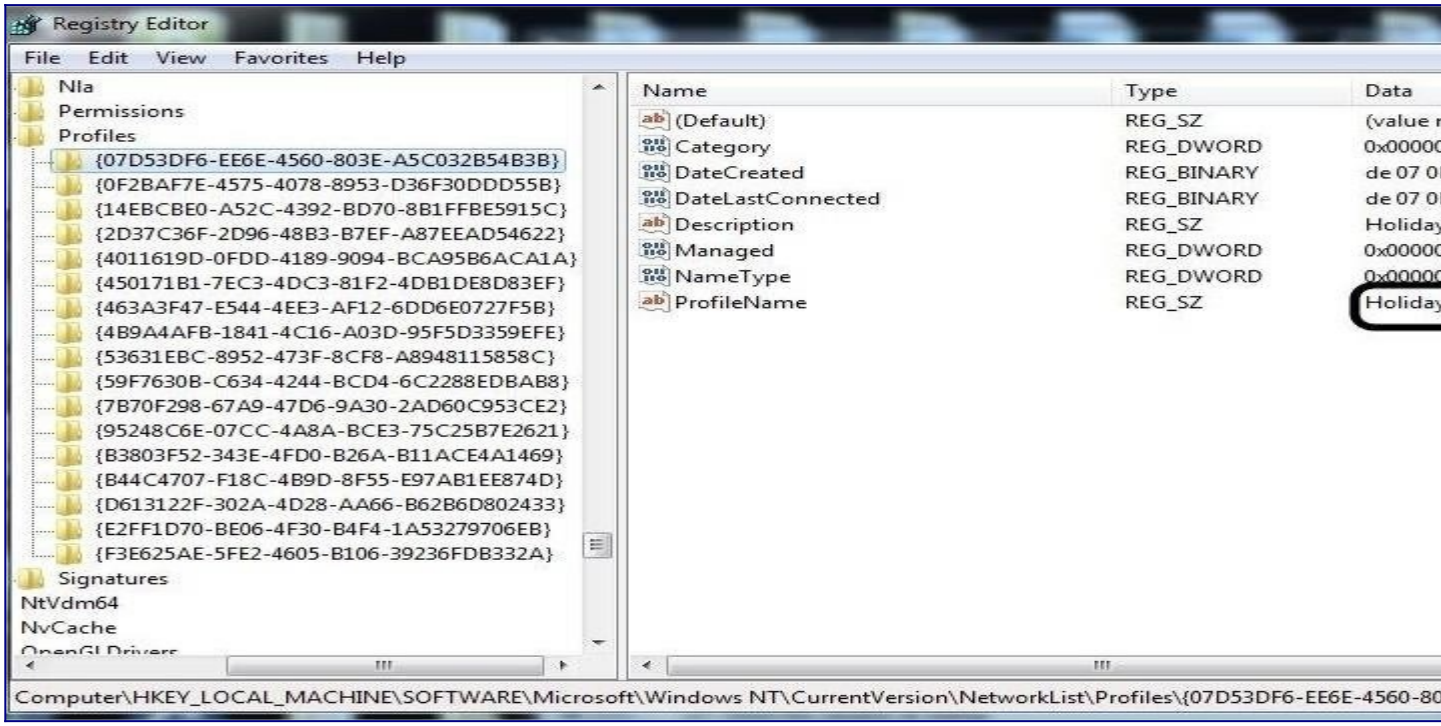
Eventually, the FBI was able to find the suspect through various investigation techniques, mostly low-tech, exhaustive, detective work. It helped that John Borrell had bragged on Twitter of his success as a hacker. Eventually, Mr. Borrell was convicted and sentenced to two years in Federal prison.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

There, you will find a list of GUIDs of wireless access points the machine has been connected to. When you click on one, it reveals information including the SSID name and the date last connected in hexadecimal. So, although Mr. Borrell initially denied his involvement with this hack, this evidence was conclusive and he eventually plead guilty.

You can see in this screenshot below showing the perpetrator had connected to the "HolidayInnColumbia" SSID in November 2014.



We will further explore how the registry can be used in digital forensics in future tutorials, so keep coming back, my aspiring hackers, as we further explore the science and art of digital forensics! And if you want to start putting some of these tasks to work, make sure to check out my digital forensics series for Kali, too.