Lab – Analyzing the Windows Registry for Evidence

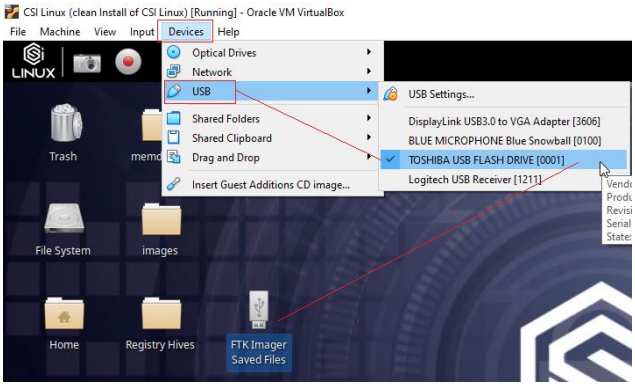
Overview

In this lab, you will learn how to perform a forensics analysis of the Windows registry for finding forensic information relevant to a criminal investigation. Forensic investigators frequently utilize Windows registry data when performing forensic analysis of computer networks as part of incident response and compromise assessment missions. Many different data types are present in the registry that can provide evidence of program execution, application settings, malware persistence, and other valuable artifacts.

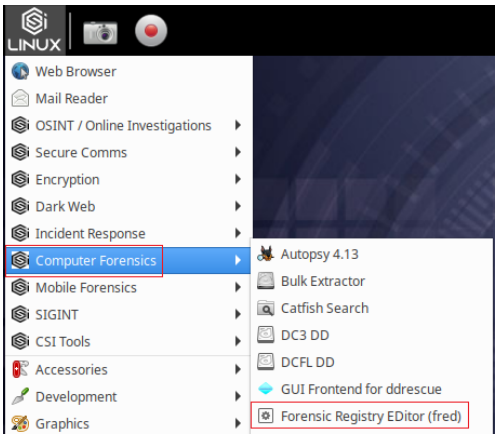
Lab Requirements

- Completion of the following lab
  - Lab – Acquiring a Forensic Copy of the Windows Registry
- An installation of VirtualBox
- One virtual install of CSI Linux

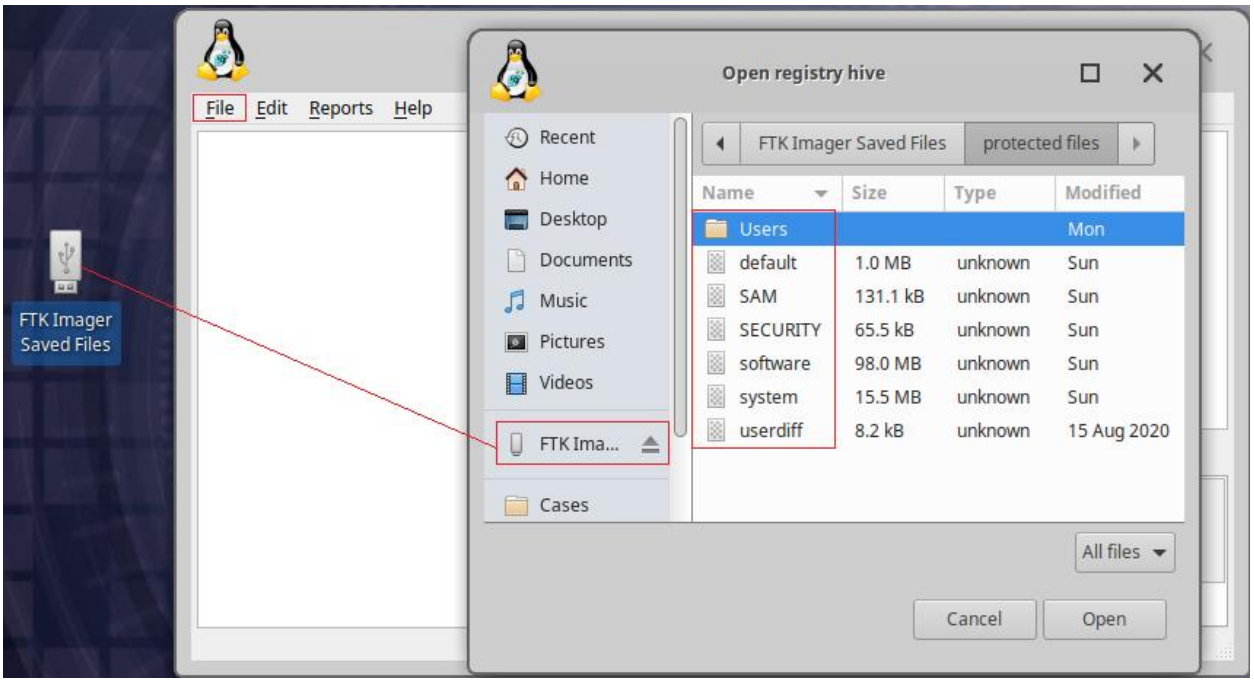
In our previous lab, **Acquiring a Forensic Copy of the Windows Registry**, we used a USB install of FTK Imager to create a live Windows 10 registry for a forensic copy. We saved the registry files to the same USB drive and then mounted the USB drive inside our virtual install of CSI Linux. We will have access to the registry files once the USB drive has been mounted.



For analysis of the Windows 10 registry, we'll be using the free registry analysis tool, Forensic Registry Editor (fred).



Once you launch the Forensic Registry Editor, you click on the file; find your mounted USB drive or the Registry Hives directory from the left windowpane. Open and from the right windowpane, select the registry hive to load. You will do this each time as you look for evidence with each hive.



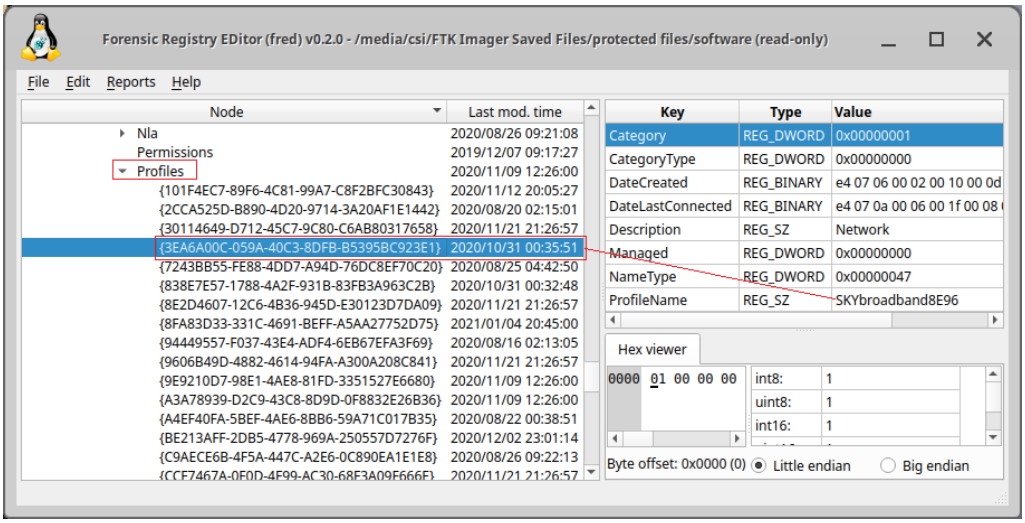
Wireless Evidence in the Registry

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. To find what the device has accessed wireless networks, we examine the following key.

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

Under Profiles, you will find a list of GUIDs of wireless access points the machine was last connected to. When you click on one, it reveals information, including the SSID name and the date last connected in hexadecimal.

You can see in this screenshot below showing the perpetrator had connected to the "SKYbroadband8E96" SSID 10/31/2020 at 00:35.51.



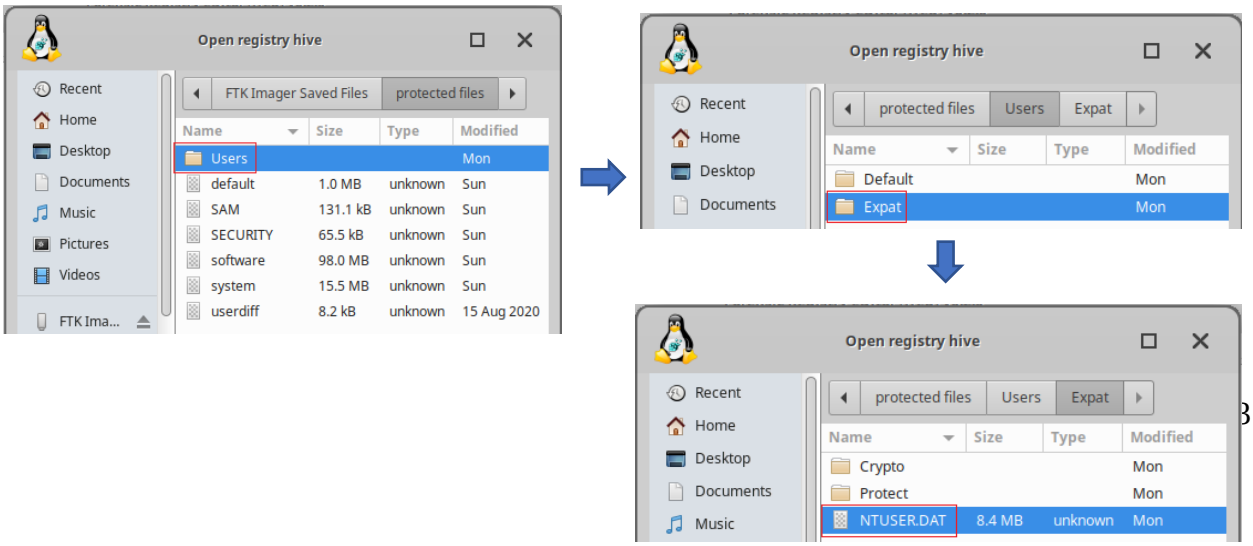
The RecentDocs Key

The Windows registry tracks so much information about the user's activities. In most cases, these registry keys are designed to make Windows run more efficiently and smoothly. As a forensic investigator, these keys are like a road map of the user or attacker's activities.

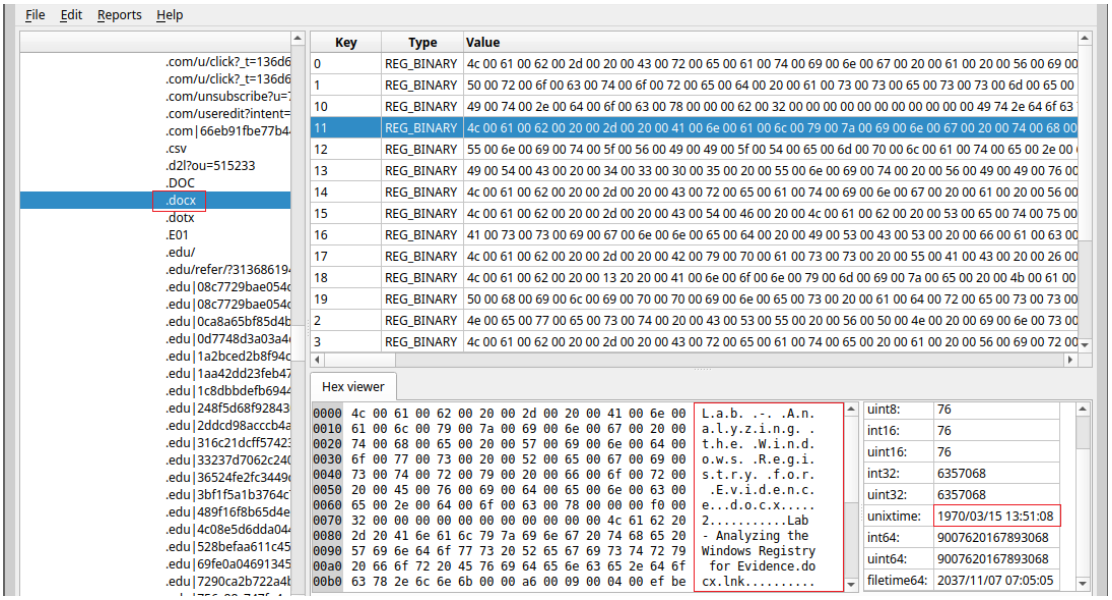
One of those keys is the "RecentDocs" key. It tracks the most recent documents used or opened on the system by file extension. It can be found at:

- **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs**

We need to access the Users folder and the individual's profile we are investigating to access this key. Inside the user's profile, we load the NTUSER.DAT



For instance, the most recently used Word documents would be found under .doc or the .docx extension depending upon the version of Word they were created in (each key can hold up to the last 10 documents). If we go to the .docx extension, we see the previous 10 Word documents listed under this key.



When we click on one of those keys, it reveals information about the document, as seen below. We can view the document data in both in hex to the left and ASCII to the right. In this case, it shows the document we are currently viewing.

In some cases, an attacker will upload a .tar file, so that is a good place to look for breach evidence. In general, you will not see a .tar file extension on a Windows machine, so the presence of an entry here would be something that needs further investigation. Check the files in the .tar key and see what they might reveal about the attack or attacker.

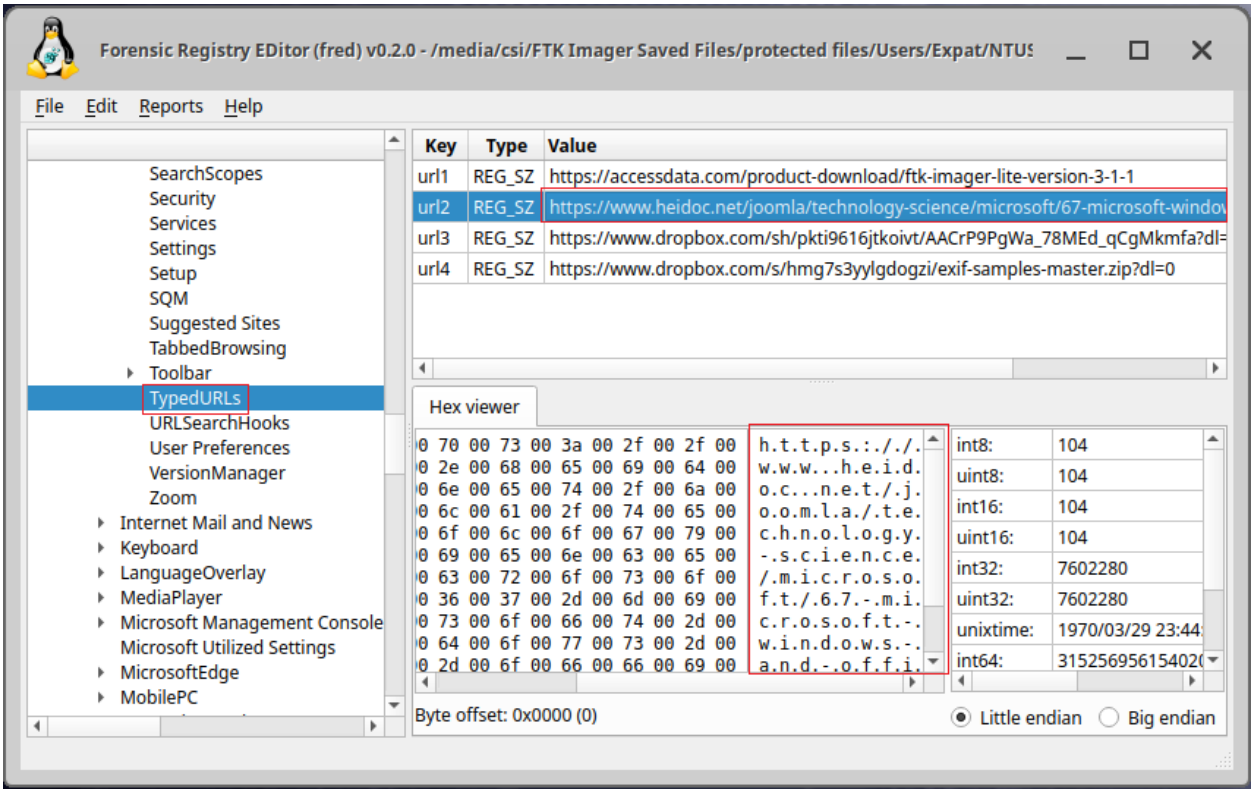
In civil or policy violation investigations, evidence might be found in the various graphic file extensions such as .jpg, .gif, or .png. (pornography would be an example.)

TypedURLs Key

When the user types a URL in Internet Explorer, this value is stored in the registry at:

- **HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs**
-

When we open that key in the registry, it lists the last URLs that the user visited with IE. This could reveal the source of malicious malware used in the breach or civil or policy violation types of investigations, may reveal what the user was looking for.



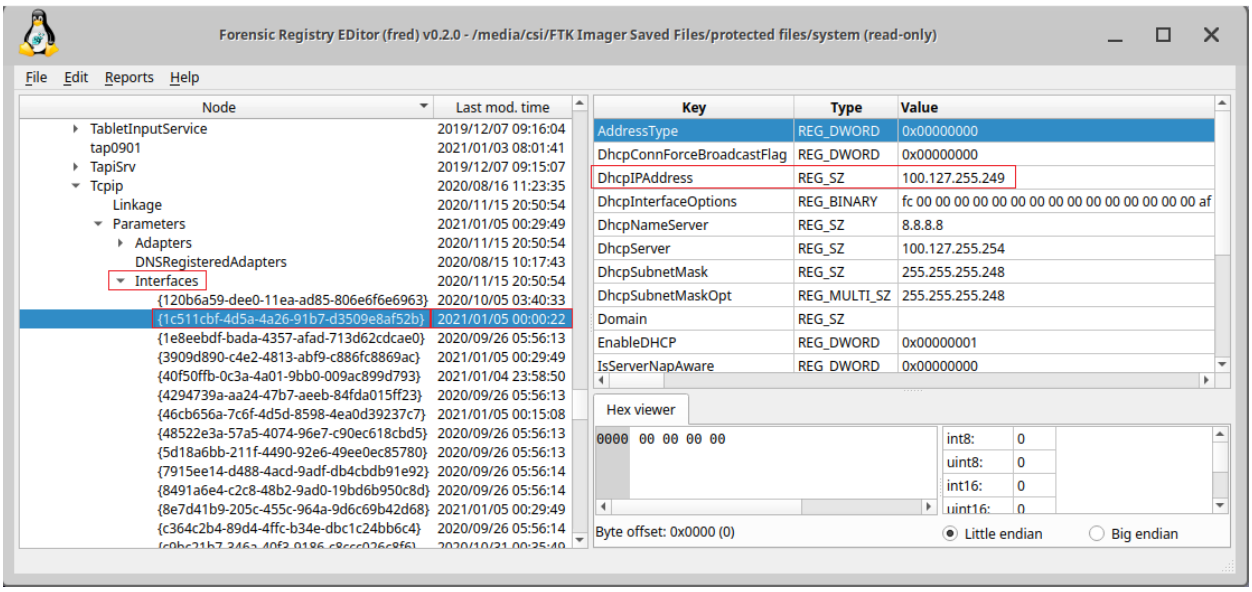
The values will run from urI1 (the most recent) to urI25 (the oldest).

IP Addresses

The registry also tracks the IP addresses of the user interfaces. Note that there may be numerous interfaces, and this registry key tracks each interface's IP address and related information.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Tcpip\Parameters\Interfaces

As we can see below, we can find the IP address assigned to the interface, the subnet mask, and the time when the DHCP server leased the IP. In this way, we can tell whether the suspect was using that particular IP at the intrusion or crime time.

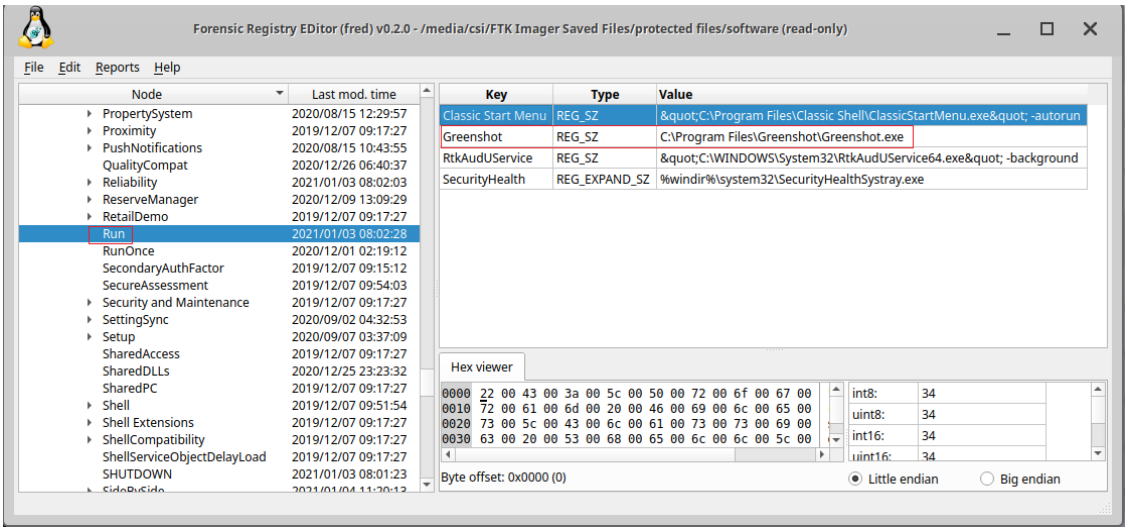


Start-Up Locations in the Registry

As a forensic investigator, we often need to find what applications or services were set to start when the system starts. Malware is usually set to start each time the system restarts to keep the attacker connected. This information can be in the registry in literally tens of locations. We will look at a few of the most common keys.

Probably the most used location is:

- **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run**



Any software/locations designated in these subkeys will start every time the system starts. Rootkits and other malicious software can often be found here, and they will start each time the system starts.

RunOnce Startup

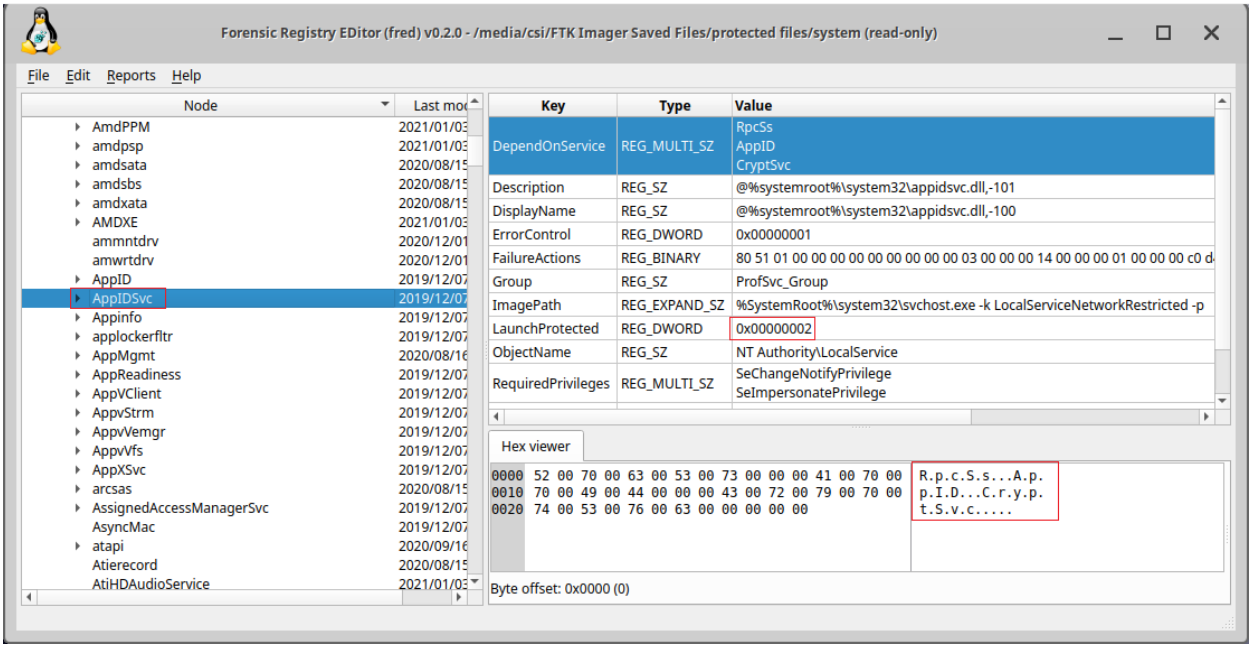
If the hacker just wanted the software to run once at start-up, the subkey may be set here.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

Start-Up Services

The key below lists all the services that are set to start at system start-up. If the key is set to 2, the service starts automatically; if it is set to 3, the service must be started manually; and if the key is set to 4, the service is disabled.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services



Start Legacy Applications

When legacy 16-bit applications are run, the program listed is run at:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\WOW

Start When a Particular User Logs On

In the following key, the values are run when the specific user logs in.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Storage Artifacts in the Registry

Often, the suspect will use a Flash drive or hard drive for their malicious activities and then remove them not to leave any evidence. The skilled forensic investigator can still find traces of evidence of those storage devices within the registry if they know where to look.

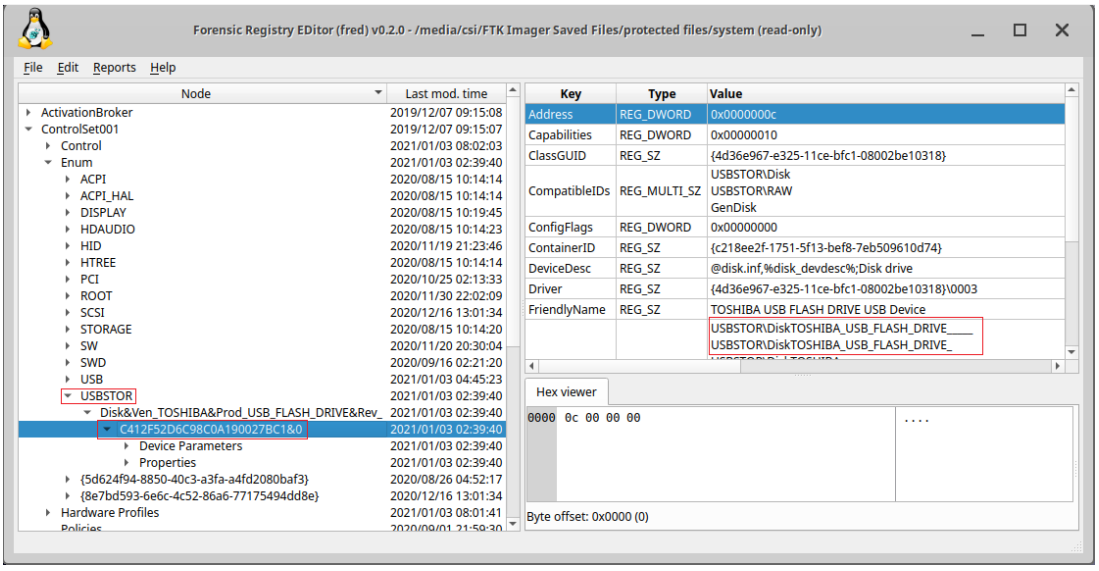
The registry on a Windows system varies a bit from version to version. A skilled, professional digital forensic investigator needs to work with nearly all versions of Windows and other operating systems. Since Windows 10 is now the most widely used operating system, I will demonstrate it by far. Keep in mind, though, that this will vary slightly between versions.

USB Storage Devices

Imagine a case where we suspect that someone installed a keylogger or removed confidential information with a USB drive. How would we find evidence that a USB storage device was inserted and used? To see proof of USB storage devices, we want to look at the following key.

HK_Local_Machine\System\ControlSet00x\Enum\USBSTOR

In this key, we will find evidence of any USB storage device that has ever been connected to this system. Expand USBSTOR to see a listing of every USB storage device ever connected to this system.



In the screenshot above, I have circled one suspicious-looking USB device. When we expand it, it reveals a unique identifier for that device. By clicking on this identifier, we can find much more information about the device.

As you can see in the screenshot above, when we click on the USB storage identifier, it reveals in the right-hand window the Global Unique Identifier (GUID), the user-friendly name, and the hardware ID, among other things. This may be exactly the evidence we need to tie the suspect to their activity on this system.

Summary –

The registry can provide a wealth of data for a forensic investigator. A complete picture of attacker activity can be assembled with numerous deleted and historical data sources during an investigation. As attackers continue to gain sophistication and improve their tradecraft, investigators will have to adapt to discover and defend against them.