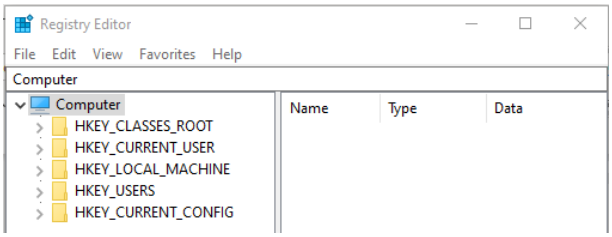
Lab – Acquiring a Forensic Copy of the Windows Registry

Overview

In this lab, you will learn how to create a forensic copy of the Windows registry. When considering computer forensics, registry forensics plays a massive role because of the amount of evidence it stores. The extraction of this data is critical when conducting a forensic investigation.

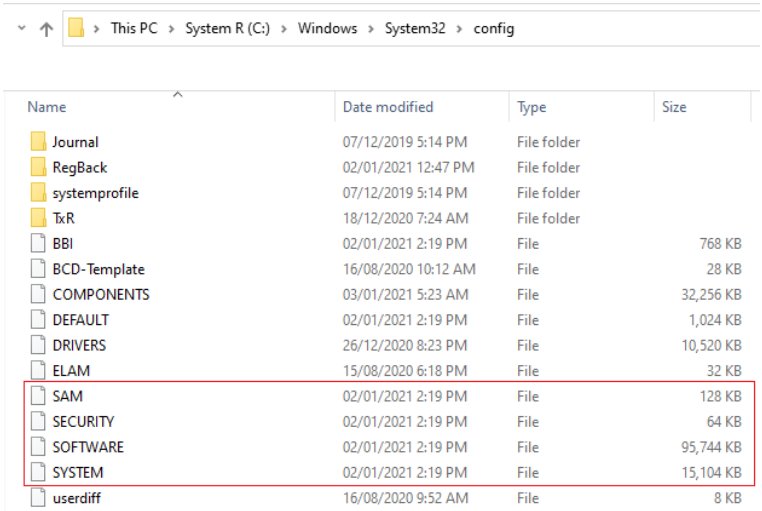
Because of the registry file format (.REG), extracting information is challenging for investigators. Registry files typically store data under unique values called "Keys." One challenge that investigators face is the lack of knowledge about Registry Keys and the Keys' data.

Inside the registry, there are five root folders. These root folders are also referred to as hives. There are five (5) registry hives in a Windows operating system.

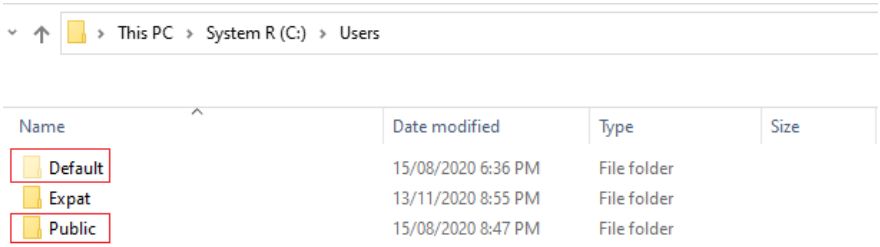


- HKEY_CLASSES_ROOT: configuration information on the application used to open files
- HKEY_CURRENT_USER: profile of the currently logged-on user
- HKEY_LOCAL_MACHINE: configuration information including hardware and software settings
- HKEY_USERS: contains all the loaded user profiles
- HKEY_CURRENT_CONFIG: hardware profile of the system at startup

The registry hive files are in the **`Windows\system32\config`** folder.

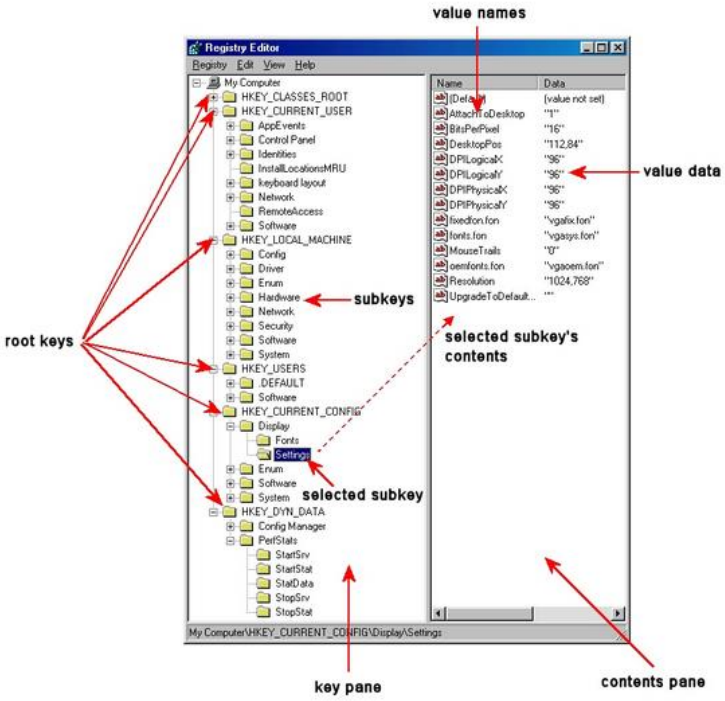


Inside the folder C:/*Users*, we can find two additional folders, *default* and *public*, containing an **NTUSER.DAT** file, which stores all user's registry settings (**HKEY_CURRENT_USER**).



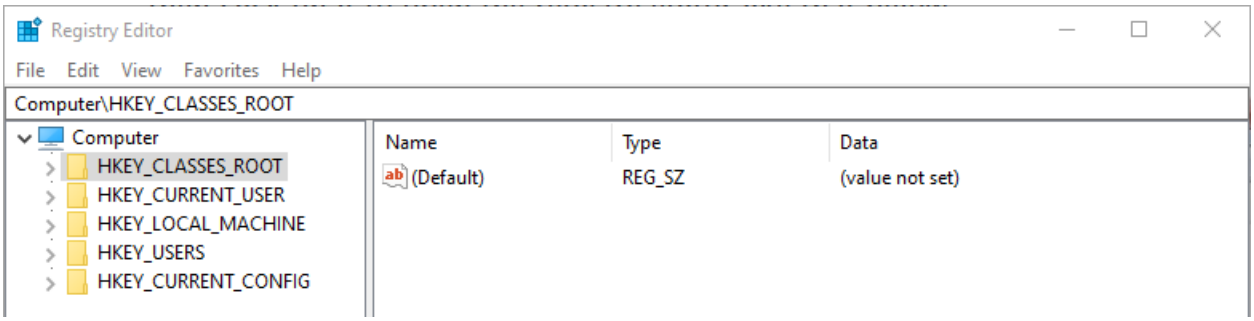
Registry Structure

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. The values are often 0 or 1, meaning on or off, and can contain more complex information usually displayed in hexadecimal.



Accessing the Registry

On any Windows system—not in a forensic mode—we can access the registry using the **regedit** utility built into Windows. 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.

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 of any searches done on the system
- And much, much more

Creating a forensic Copy of a Windows 10 Registry

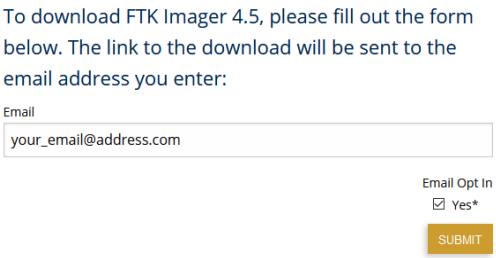
To create a forensic image of the windows registry, you can export registry hives using FTK Imager, a free tool by AccessData. FTK Imager is primarily used for forensics imaging and file-system analysis but is fully capable of extracting a wealth of information from running systems or from forensic images.

To extract registry hives from a running system, you can install and use FTK Imager (full version) from a USB drive. This will prevent you from making any changes to the target machine. FTK Imager is used to conduct forensics imaging with the least possible interaction with the running machines. The stand-alone capabilities of FTK Imager also make it great for acquisitions from a server.

This will take you to the download page for the FTK Imager.

https://accessdata.com/product-download/ftk-imager-version-4-5

Once you register using your email address and you opt-in to receive email notifications, you should receive an email with the download links for both the FTK Imager Lite and the full version. Concern yourself with just the full version as the lite version has an invalid certificate and will launch on a Windows 10 machine.



If you do not receive the email, please send an email to info@accessdata.com, which I had to do. Here is their email response.

Hi Cliff,

Sorry about that! Below are the links to the downloads you requested:

https://ad-zip.s3.amazonaws.com/Imager_Lite_3.1.1.zip

https://ad-exe.s3.amazonaws.com/AccessData_FTK_Imager_4.5.0_%28x64%29.exe

Have a great day!

Again, no need to worry about using the lite version. Install the full version and follow the instructions for creating a lite version using the full installer.

How to run FTK Imager from a portable drive

Procedure:

1. On a machine other than the system to be imaged, install FTK Imager
2. Insert a flash drive formatted with either the FAT32 or NTFS file system
3. Copy the entire "FTK Imager" installation folder (typically "C:\Program Files\AccessData\FTK Imager" or "C:\Program Files (x86)\AccessData\FTK Imager") to your flash drive
4. Insert the flash drive in the system to be imaged
5. Navigate to the folder you created on the flash drive
6. Run **FTK Imager.exe** (as Administrator) and use Imager as you normally would

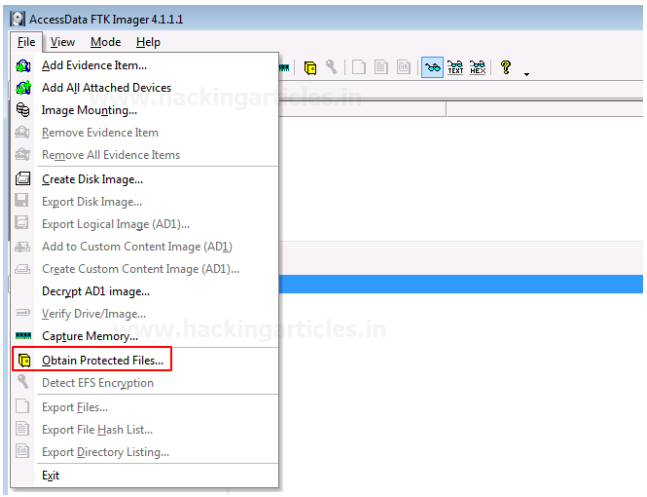
This will allow a user to create a portable “Imager Lite” from the FTK Imager full install.

You do not need a USB drive to run FTK Imager for this lab. Download it and run it as an installed program from your local machine but, to be in Forensic Mode, you must mount a flash drive onto the target machine, access the USB drive, and launch the FTK Imager.exe as administrator.

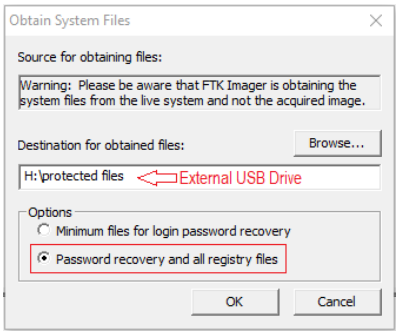
Pay attention to the fact that this procedure can only extract the registry from the machine you are working on, not on forensic images or remote machines.

Launch FTK Imager

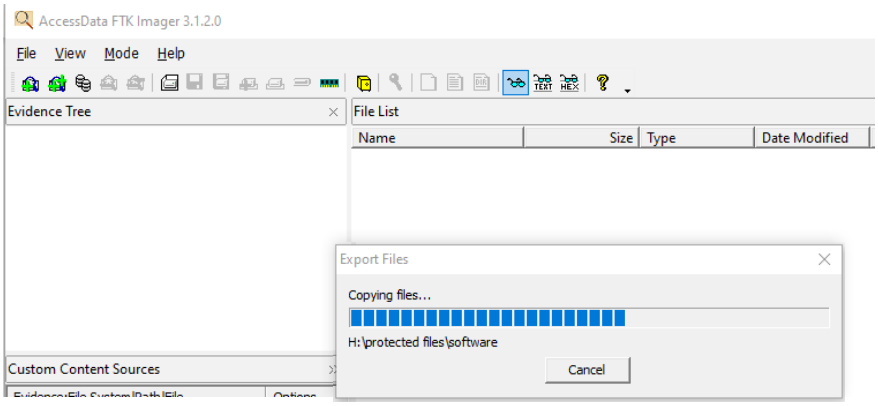
Once you have downloaded and install the FTK Imager, you can launch it. Once the program is up and running, click on **File** and select, Obtain Protected files from the context menu.



Choose your destination folder for the copying of the files. In this example, I am using an attached USB thumb drive. Make sure wherever you save the files that you first create a storage directory. Click OK.

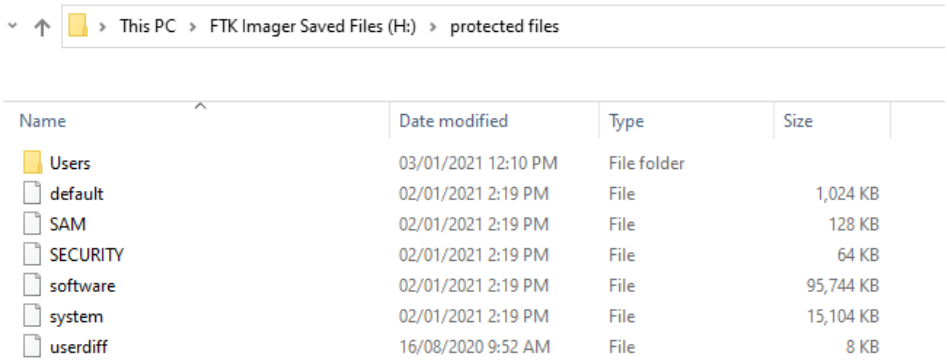


The copying process begins.



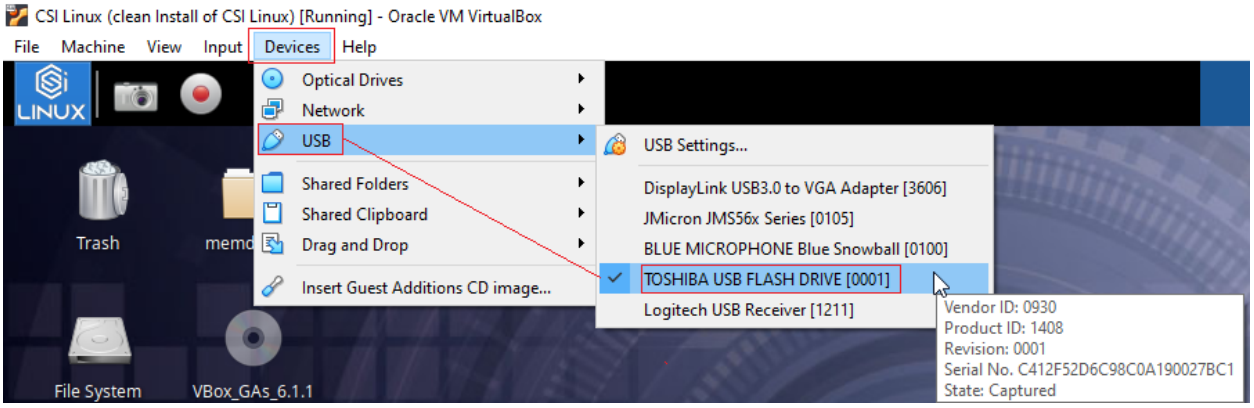
Once the copying process has been completed, you can open the destination folder to examine the contents.

And here are acquired protected files.

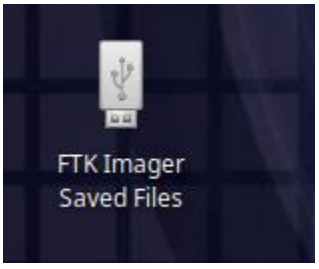


Now that we acquired our registry files, we are ready to analyze the suspects' registry for key forensic information.

Since I am using a USB stick, I can attach the USB drive inside my CSI Linux virtual machine by just clicking on Devices, go to USB, and then select the USB storage device to mount.



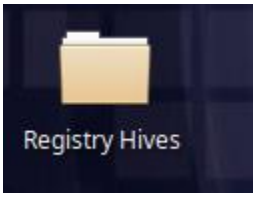
Once you mount the device, the contents will open, or you can access the mounted drive using the USB shortcut added to your CIS Linux desktop.



Alternative for Acquiring a copy of the Registry Files

Your other option is to open a browser and use the following link to download and use a copy of the same registry files saved to my Dropbox location.

Once you have the archive saved to your Download folder, extract the contents to your desktop.



End of the lab!

Summary –

In this lab, you learned how to create a forensic copy of the suspect's registry files. In our next lab, we will learn how to analyze the Windows registry to find critical pieces of evidence from a suspect's seized computer or laptop.