DFSC1316: Digital Forensic and Information Assurance I

Lab 6 Windows Operating System Forensics

This lab will give you hands-on experience of conducting forensics investigation of the Windows operating system.

Lab 6.1: Metadata investigation

Metadata was introduced in the class. Essentially, metadata is the data (information) regarding the files stored in the operating system.

As a specific example, we have looked at the EXIF information of image files, and you have found that a mere jpeg file can contain incredible information regarding the file itself, the person and the device that created the file.

During the class, you have examined the big-name websites such as Facebook and Twitter, and found that these websites will remove the EXIF information before it upload users' photo. In this question, you will explore more websites and see if all websites follow the same practice.

What to submit: choose at least 5 social medial websites that you are familiar with (preferably have an account registered), such as a blog, a forum, etc. Inspect the photos posted either by yourself, or by other users, and find out whether EXIF information still remains.

For each website you have investigated, you will attach screenshots, alone with a brief description, to explain what you have done, and what your conclusion is. Note that it is NOT necessary to eventually find a website that retains EXIF information.

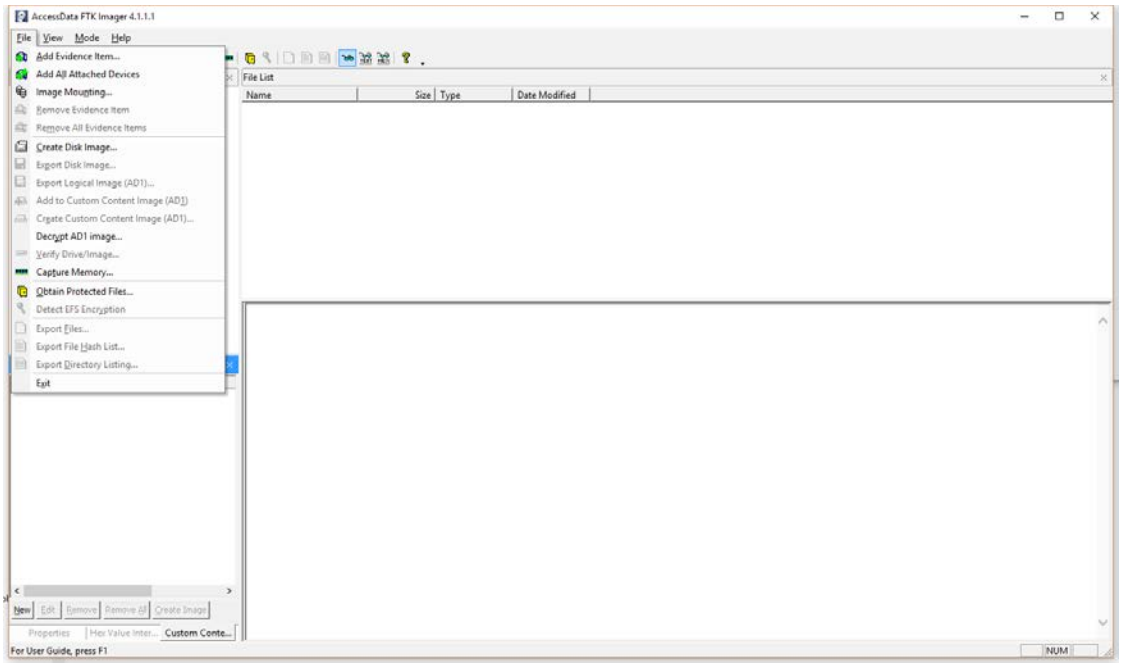
Lab 6.2 Windows Registry Forensic

As has been introduced in class, the registry is the central database on the Windows operating system that contains information of the operation system and system users. In this lab, you will use automated tools to investigate the registry of a forensic image, and identify some useful evidences.

To start with, follow the steps below.

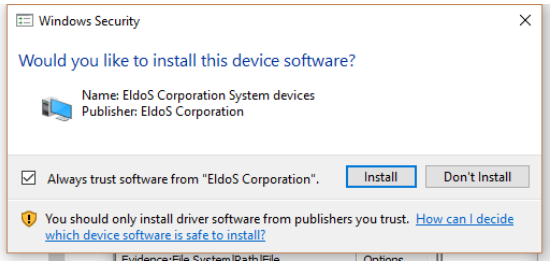
1. Download the forensic image from the following link. The image is 600+ MB, so the downloading can take a while. As you may notice, this file has extension .E01, this format is the default format used by the software EnCase. But it can also be opened by other mainstream forensic software such as FTK Imager and Autopsy.
   https://myshsu-my.sharepoint.com/personal/mxw032_shsu_edu/_layouts/15/guestaccess.aspx?docid=1b5d90c8efda34c85926f75a0703cf085&authkey=AWz__EuIJarrdjrdp9X_iRI&e=47c1b8e695ba42f386d775df6a65484e

2. Open FTK Imager that you have used in Lab 5. From inside FTK Imager, select File → Image Mounting. Under the context of operating systems, "mount" is a verb that describes the action that to "hook" a drive to the operating system, such that the operating system can see, and access this drive.

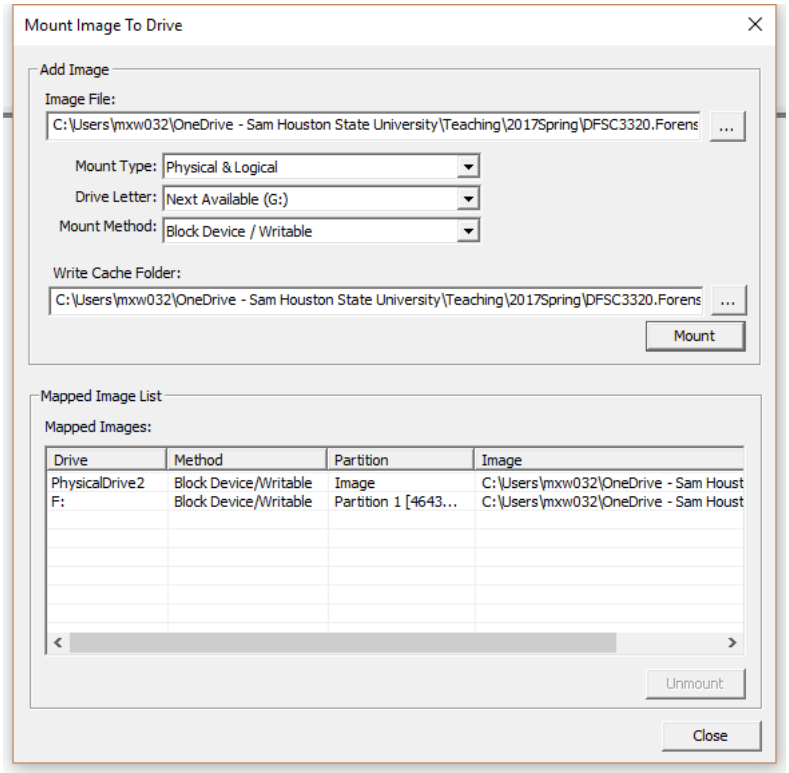


3. In the Image File blank, navigate to the path where your downloaded image is stored.
    a. Mount Type can be left unchanged as “physical & Logical”.
    b. Driver Letter can be left unchanged, but you can also choose another letter if you prefer. This only affects the name of the drive, e.g., drive F:, or drive E:.
    c. Mount Method: we will choose Block Device/Writable. Beware: this option will allow us to modify the content the image. In case we only want to browse the image, choose Read Only.
    d. Write Cache Folder can be left unchanged.
    e. Click “Mount” button.

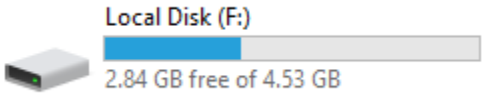
You may be prompted with some security alerts, such as the one below, click Install to proceed.



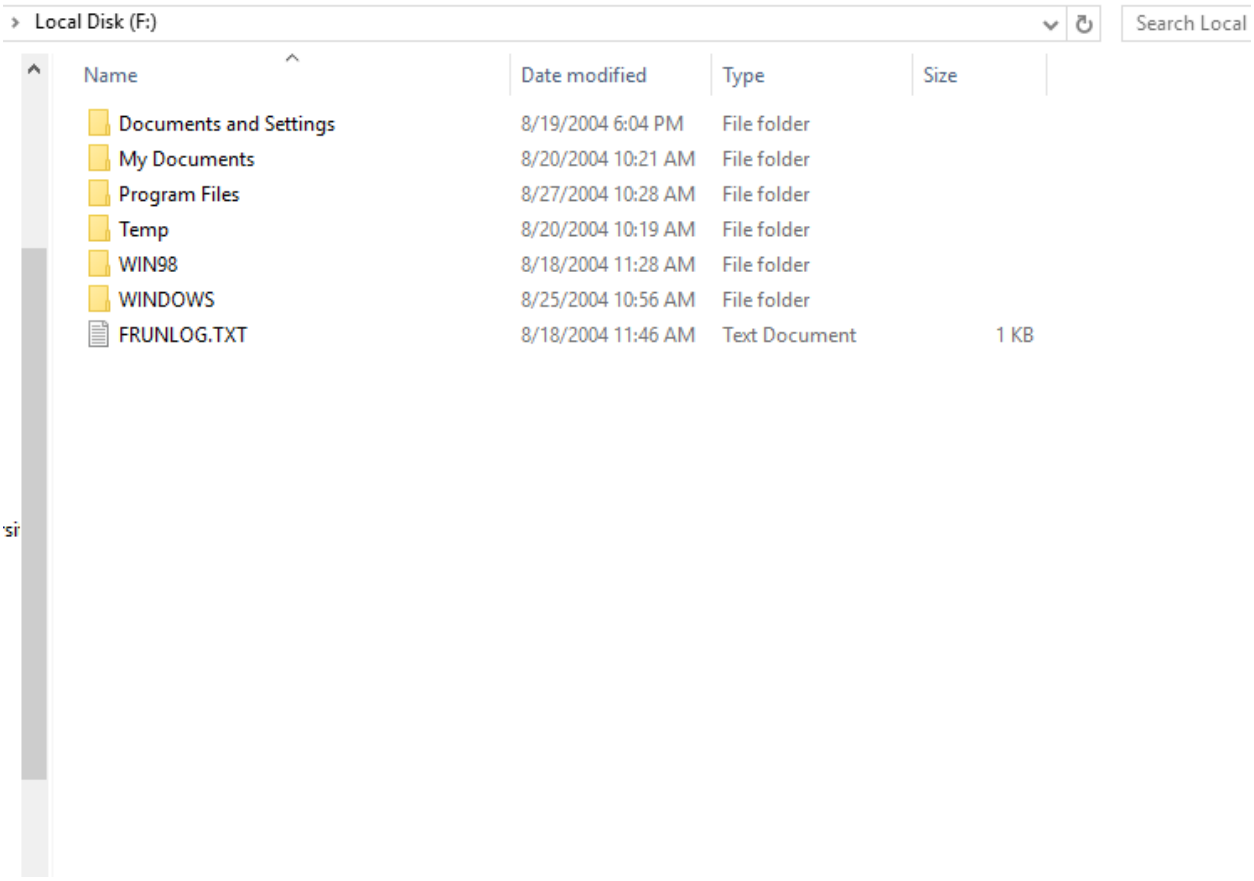
When this step is done, you should see the bottom half of the windows shows a drive letter. In my case, it is drive F. You can leave this window open, since we'll "unmount" the drive at the end of the lab.



4. Open "My Computer", you should now see a new drive shows in the file browser, it has the letter you have assigned (F in my case), and it has the size "2.84 GB free of 4.53 GB".

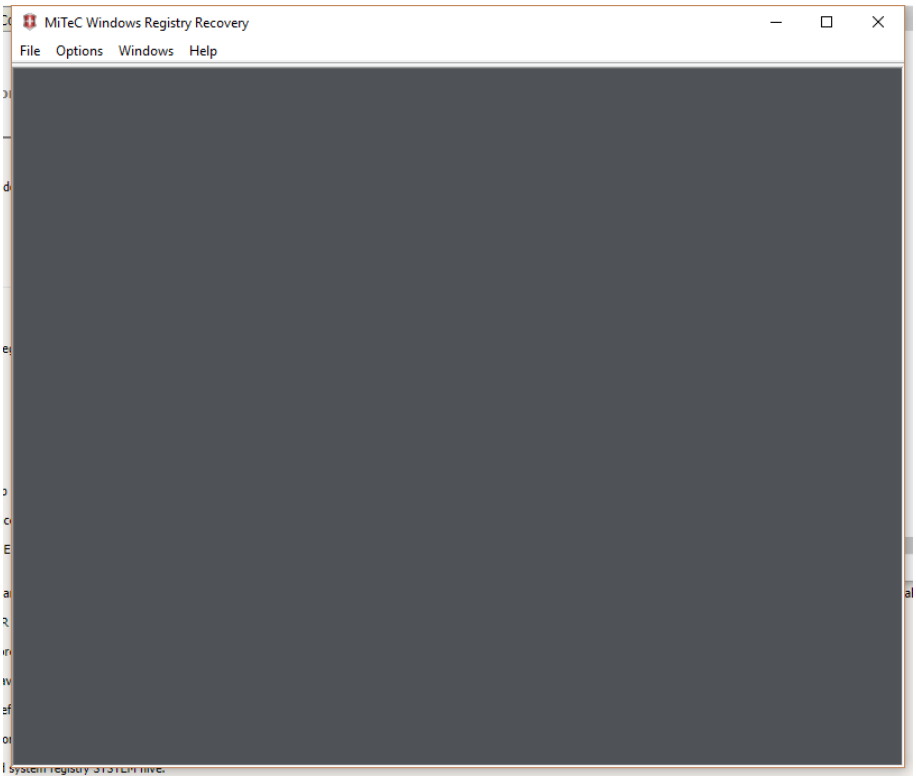


5. Double click to open this drive. You should now see many folders same as the following.

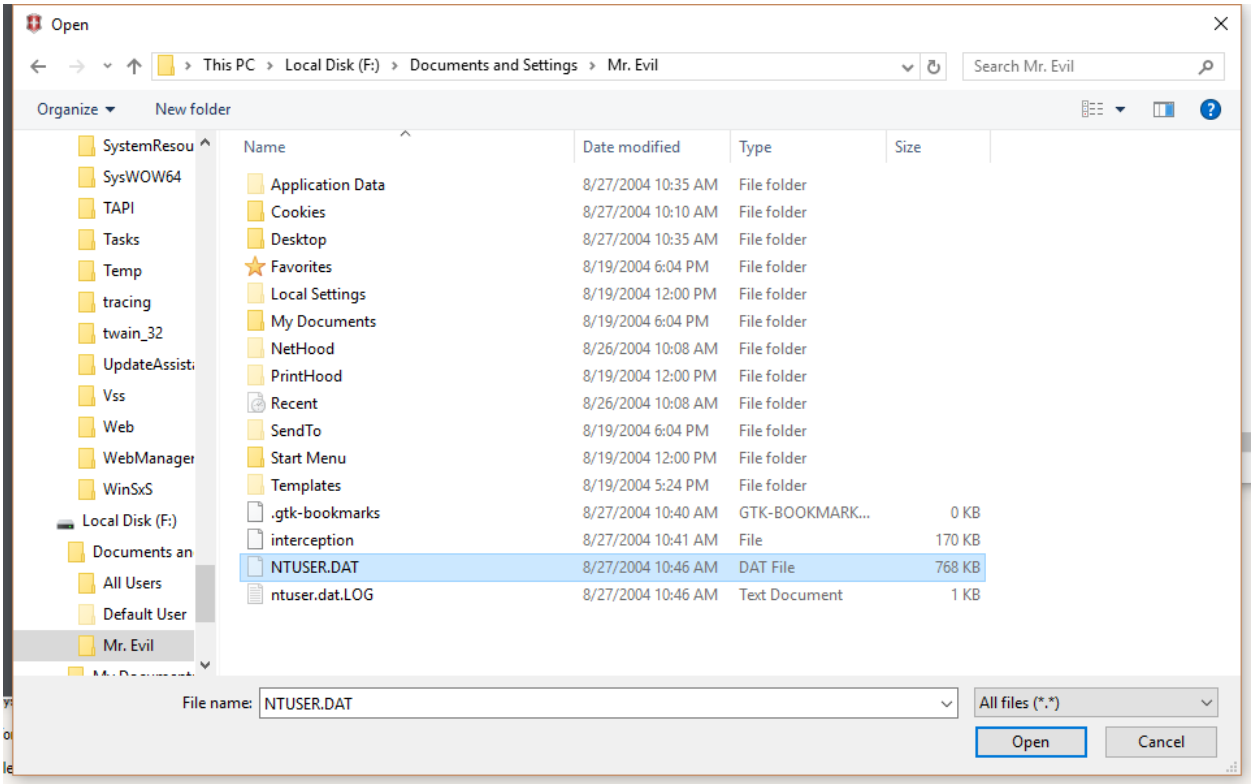


6. What you have seen here is the C: drive of the machine from where the Image is taken. If you are not familiar with Windows operating system, the operating system is installed on the C drive by default, most of the operating system related files are stored in “Program Files” and “Windows” folder, and most user related files are stored in “Documents and Settings” and “My Documents” folder. And, of course, the registry data is also stored on the C drive.

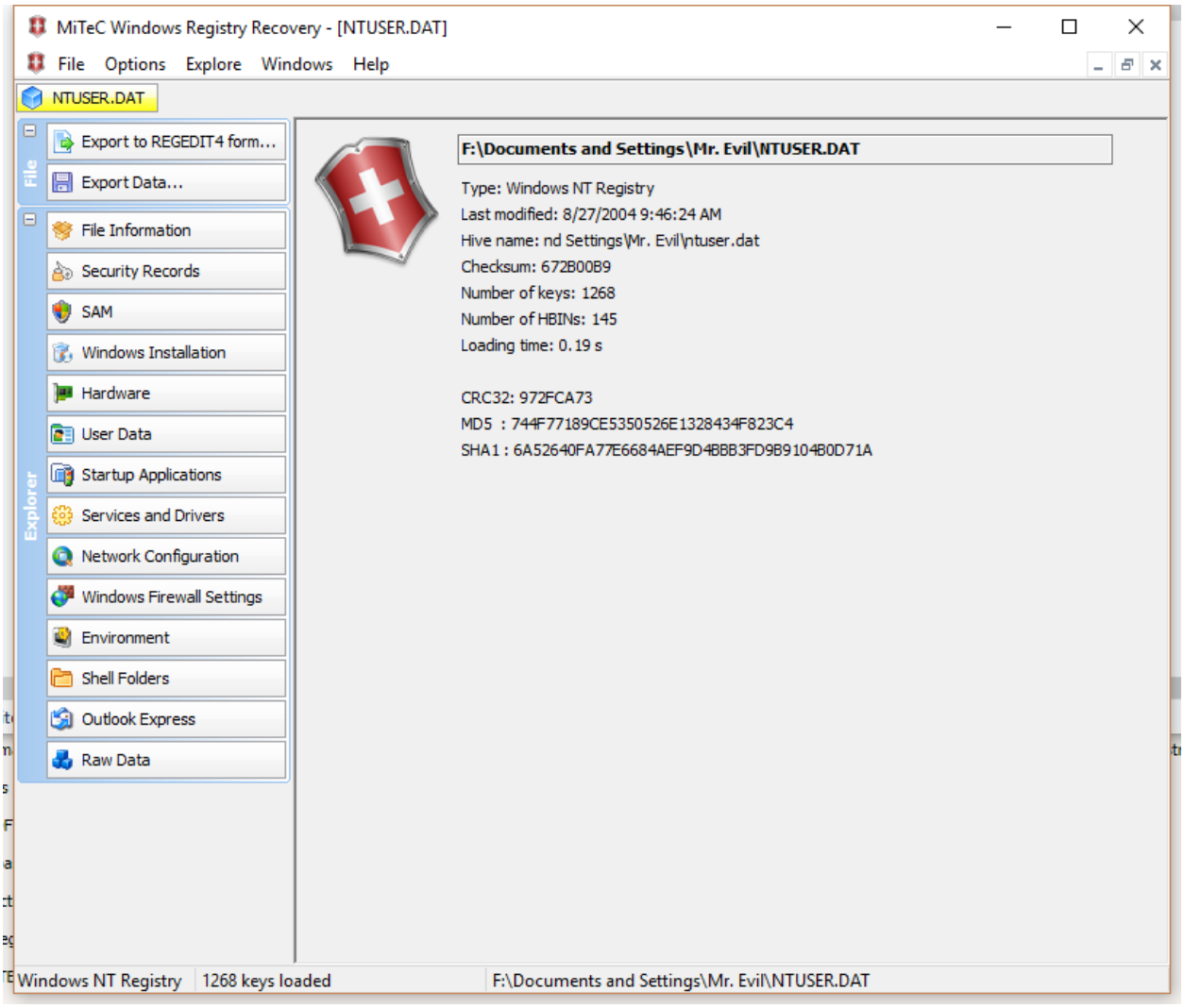
7. Go to http://www.mitec.cz/wrr.html and download the “Windows Registry Recovery”, which is an automated tool that helps you investigate Windows Registry.
   The WRR is a “green” application, which means you do not need to install it, you can directly use it after download.
   Double click wrr.exe to bring it up. And you’ll see the application like below.



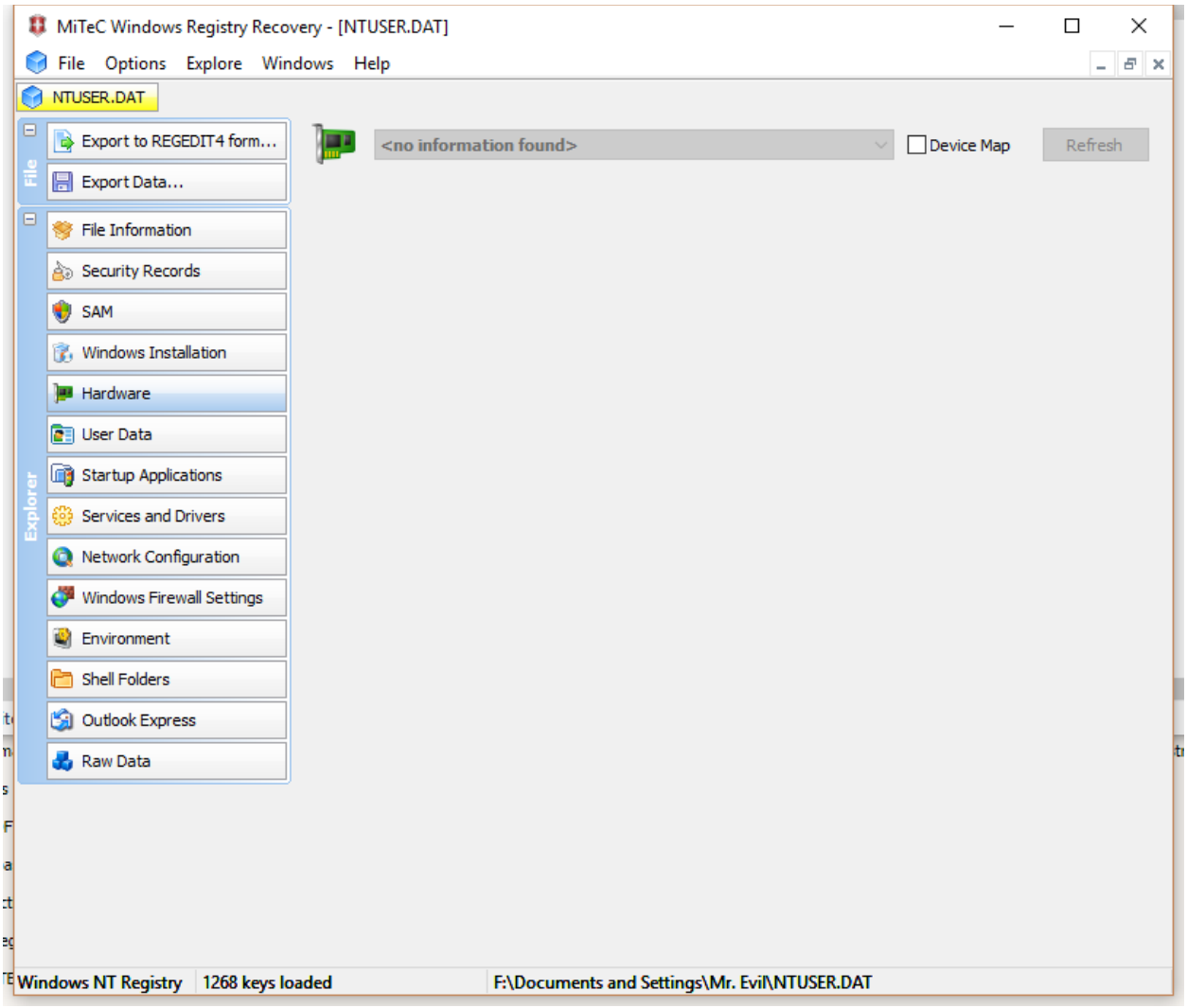
8. Click on File → Open. Navigate to the NTUSER.DAT file as shown below. Choose the file NTUSER.DAT, and click open.



9. You should now see a window like the following. As you can see, the left part of the window gives you the option to view all kinds of information regarding the operating system (such as Hardware), and the user (such as User Data). Click on each tab, and check what information you can see.

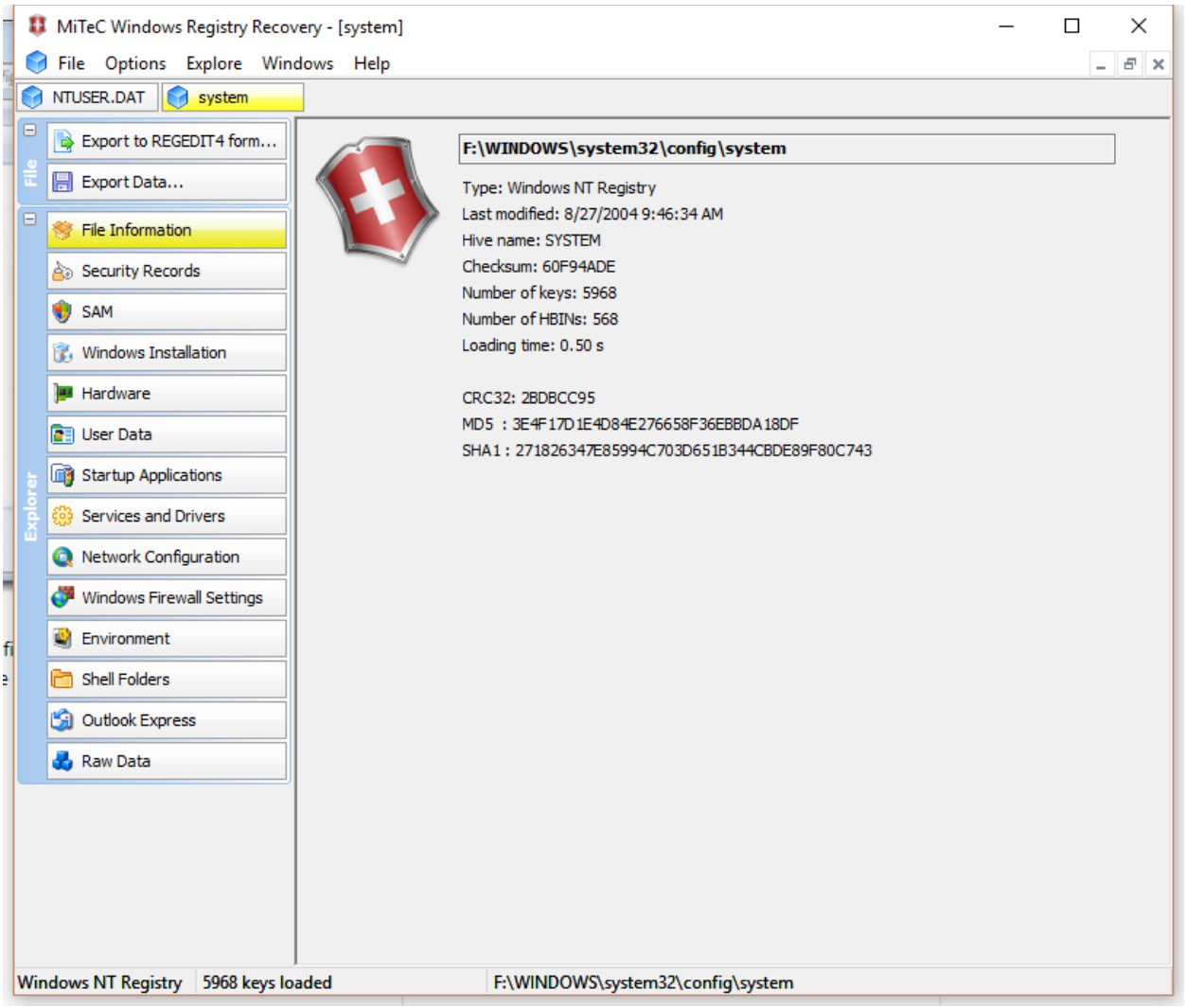


10. If you have clicked on each tab, you should notice that some tab does not give any information, such as the “hardware” tab as following. This is because, the registry data is not stored in only one file. The NTUSER.DAT file only contains part of the registry that relates to the specific user, in our case, Mr. Evil.



11. Question: find out where HKEY_LOCAL_MACHINE is stored. If other words, the information related to the root key HKEY_LOCAL_MACHINE is stored in a file that locates somewhere in the C drive. You will do some online search, and find out what the file name is, and where it is located. Hint: the file name is “system”, it locates somewhere under the “windows” folder.

12. After you find this “system” file, you can repeat step 7 and 8 to load the “system” file, or the HKEY_LOCAL_MACHINE, into WRR. You will see a screen like the following. Notice now I have two tabs on the top, one is NTUSER.DAT, another is system.



13. This “system” file contains the information related to HKEY_LOCAL_MACHINA, as the name indicates, it gives information of the machine from which the image is taken.
    Click to select the “system” tab, and then click the tabs on the left, you’ll find some information that was not available in “NTUSER.DAT” is now available, such as “Hardware”.

14. This is the end of this lab. If you are interested, you can do further search and find out information for all the 5 root keys.

15. After you have finished the following questions, get back to FTK Imager, select the drive letter, and “unmount” it. Then you can close FTK Imager.

Questions to answer (25 points each question):

1. Answer the question in step 11, where is the “system” file located in the C drive?

2. In order Windows versions, such as Win98/XP, and Win7, when you press the “Windows” key, you will have the “Start menu” pops up. In the start menu contains many shortcuts from where you can quickly and conveniently start a program. Find out what program is contained in the “start menu” of the machine under investigation. Make a screen copy to answer this question.

3. What is Mr. Evil’s email address?

4. What is the manufacture/brand of the DVD drive of this machine?