Registry Forensics

In this lab we are finding forensic artifacts that are in the windows operating system. The registry hives contain user settings and configuration data of installed software while the registry files can be used to determine user activity. The file data can then be compared to collected evidence and source data to help check the activity. The lab goes over the most common registry hives and how we can locate them.

The lab starts with going to AccessData on the start menu and clicking FTK Imager. Once it loads, we go to file, add evidence item, choosing image file for the select source, then hitting next. At select file we hit browse and follow the path, This PC > Desktop > Toolbox > Datasets > Lab4 and choosing the FEF called C Drive.E01, then we hit open, then finish. At evidence tree we will hit the plus beside C Drive.E01, NONAME [NTFS], root, Documents and Settings, and click on the folder named, IEUser. We then go into the file list and highlight with Ctrl and left-click, the NTUSER.DAT file and the NTUSER.DAT.LOG file, then right-click and choose export files. In the Browse For Folder, we choose Evidence Repository (E:), Make New Folder, and name it FOR\_LAB\_004, make a new folder in that one called, Registry\_Files, then another called IEUser, and finally hit ok twice. Back at the evidence tree we follow the path, Documents and Settings> IEUser > Local Settings > Application Data > Microsoft > Windows and export the UsrClass.dat file and UsrClass.dat.LOG file similar to the last export. We then follow the path, FOR\_LAB\_004 > Registry\_Files > IEUser and make a new folder called, UsrClass, then hit ok. Back at the tree we hit the plus for Windows and System32, then click on the config folder. We then highlight, the files, SAM, SECURITY, SYSTEM, and SOFTWARE, with their respective log files and export them. We follow the path, Evidence Repository (E:) > FOR\_LAB\_004 > Registry\_Files, and make a new folder named Config\_Registry\_Files, and hit ok. Back at FTK Imager, we hit file, Obtain Protected Files, select Password recovery and all registry files, then cancel and fully close FTK Imager. Now we go to the folder, Toolbox and double click RegRipper2.8-master and right click rr.exe and run as administrator. Now we click the Windows File Explorer icon, view, and check hidden items, then close. Back at RegRipper, we hit browse next to hive file and follow the path, Evidence Repository (E:) > FOR\_LAB\_004 > Registry\_Files > IEUser and click open on NTUSER.DAT and open. We click the browse next to report file and create a new folder in the FOR\_LAB\_004 folder and call it, Registry\_Reports, then hit open and enter NT\_User\_report in the file name and hit save. In profile we choose ntuser then hit rip it. We complete the RegRipper steps for the files, SAM, SYSTEM, SOFTWARE, SECURITY, and UsrClass.dat, then close RegRipper. To check over the files we first go to Evidence Repository (E:) > FOR\_LAB\_004 > Registry\_Reports and open NT\_User\_report.txt in notepad. We hit edit, find, and type in comdlg32, hitting find next. Now we type in RecentDocs into the find term box and hit find next. We repeat this with the term TypedURLs and UserAssist then hit close. Back at Registry\_Reports, we open SAM\_report.txt in notepad and look through it then hit close. We repeat the process with System\_report.txt and use file find with the terms, Computername, Network Key, Shutdowntime, and USBStor then hit close. Now we repeat this with Software\_report.txt hitting file, find, and using the terms default browser check, Systemrestore, and Winnt\_cv before closing out and finishing the lab.

The lab took us through familiar paths like FTK Imager and unfamiliar like RegRipper. It was interesting with having to repeat certain steps and seeing the information we could get just from the first section. Most of the sections cover looking over the files and what they contain so I find it nice that it was not quite difficult and was to the point.

Section 4 Step 8

Graphical user interface, application

Description automatically generated

Section 5 Step 9

A screenshot of a computer

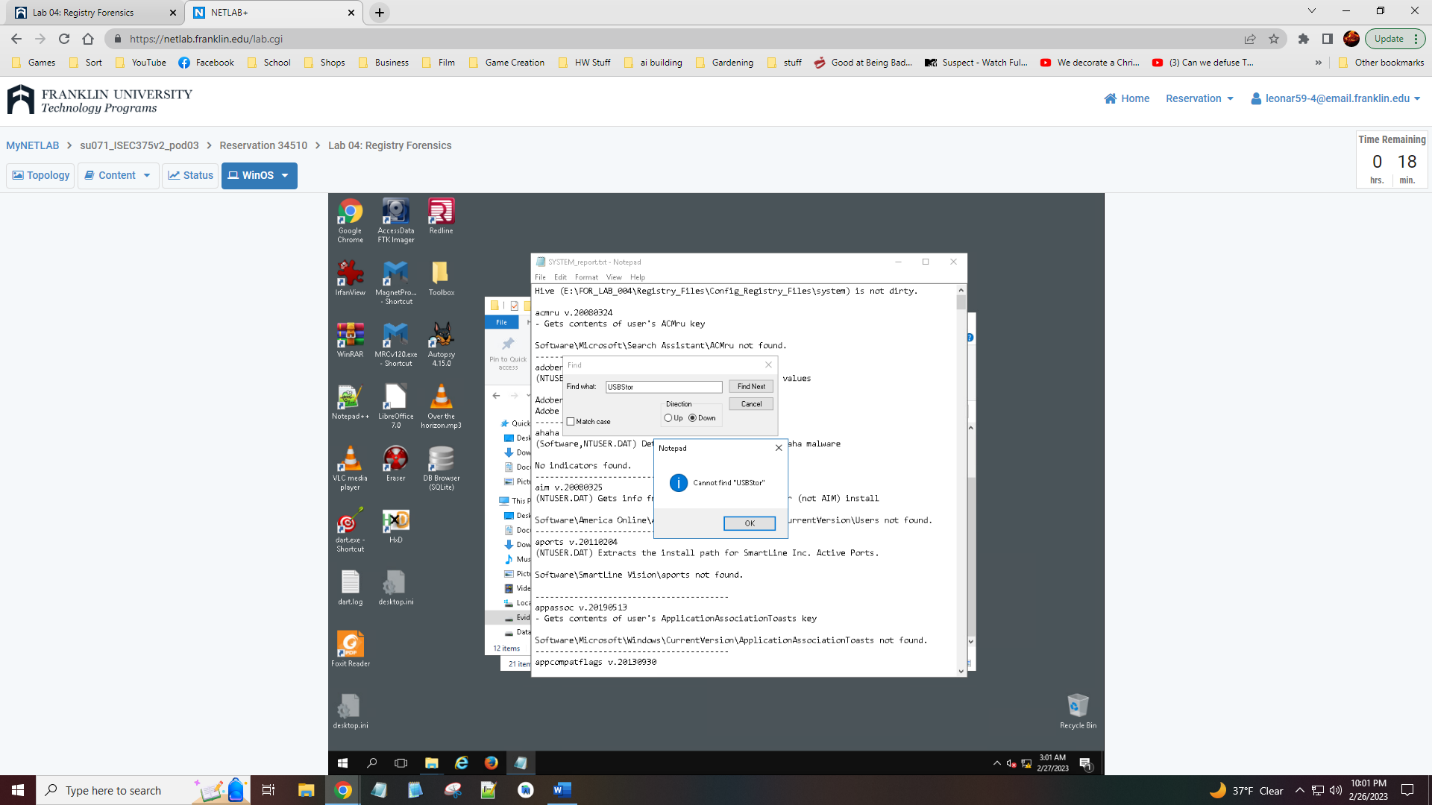
Description automatically generated

Section 6 Step 4

A screenshot of a computer

Description automatically generated

Section 7 Step 11



Section 8 Step 8

A screenshot of a computer

Description automatically generated

File System

The purpose of this lab is to introduce file systems and how we can identify the differences between them and the limitations they have. We learn about partitions and how to access them with the Hex Editor.

The first step is to hit the Start Menu and click on HxD Hex Editor and open HxD. Then we go to view, toolbars, and data inspector. In tools we click open disk image and follow the path Toolbox > Datasets > Lab5, select the file NDG FAT Lab5.001 and click open and ok. Now we go to view, offset base, and select decimal. In search we hit go to enter 446 in the text box, choose dec, and hit ok. We repeat this using the offsets 32256, 32277, 32288, 32295, 32310 and then move on clicking tools, open disk image, this time choosing NDG NTFS Lab5.001, repeating the view, offset base, and decimal step. Now we go to search go to and enter the offsets 446, 32256, 32296, 32304, and 32328 then we repeat the previous steps to open the file NDG exFAT Lab5.001. We repeat the prior steps with the view and the search and enter the offsets 446, 32256, 32328, 32356, 32364, and then we finish the lab.

This lab was a lot of repeating steps with most of them being to search for specific terms. The Hex Editor seems like an interesting tool and I can see how it can be quite useful when looking at partitions and the file systems.

Section 2 Step 25

A screenshot of a computer

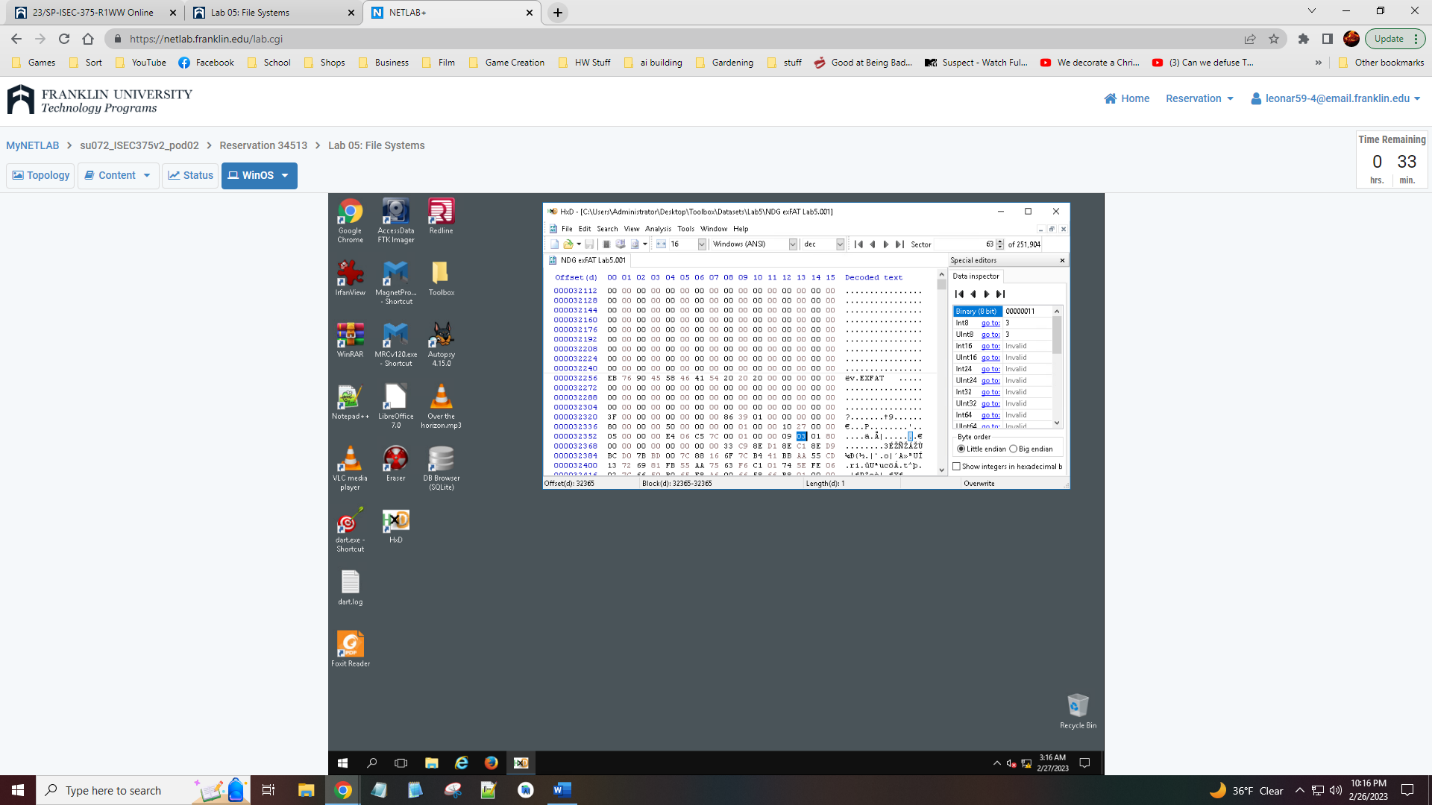
Description automatically generated

Section 3 Step 17

A screenshot of a computer

Description automatically generated

Section 4 Step 15



Steganography and Alternate Data Streams

This lab is going over commonly reviewed data hiding techniques and how we can make sure nothing is missed or looked over. We are looking at the techniques, steganography and alternative data streams and how they are used to hide potential evidence in files that seem unimportant.

We start by opening windows file explorer and following the path, This PC > Evidence Repository (E:) > FOR\_LAB\_010 > Steganography Files, and opening both files we find, PlanC.jpg and WhatsApp-Encryption.jpg. Now we follow the path, Start Menu > HxD Hex Editor > HxD and open HxD. We click file, open, and navigate back to the Steganography Files folder choosing the WhatsApp-Encryption.jpg file. Now we go to the end of the file and click the last value, entering the message, steganography is a great way to share secrets, or any message we want. At the size change prompt, we click the box for do not ask this question again and hit ok, then finish the message. Now we hit file and save or ctrl S and move back to the file explorer and open the Steganography Files folder and opening the WhatsApp-Encryption.jpg file. Moving back to HxD, we hit file, open and we choose the other file in Steganography Files called PlanC.jpg and hit open. Now we hit search, find, hex-values, and type in 89 50 4E 47 0D 0A 1A 0A, and hit ok. We repeat this with searching 49 45 4E 44 AE 42 60 82. Then we click edit, select block, and set the offsets to 191F9, and 1A025 and hit ok. Then we go to file, save selection, and make a new folder in Steganography Files named Exported Files where we then save the file as Exported picture.png and hit save. Using the file explorer, we locate our new file and open it to see the message. Now we move on and open the start menu and clicking run, typing in cmd, and hitting ok. Now we type in the command E: to change the drive and then change the directory using cd FOR\_LAB\_010\ADS\Exercise1. Now we type in dir and hit enter then we run the command Type legitimate\_program.exe > Legitimate\_program.exe:secret.txt to make a file. Now we open this file with the command Notepad legitimate\_program.exe:secret.txt and then hit file and save inside the notepad. Now we type in Dir /r and hit enter then review and finish the lab.

It is quite interesting to think about the types of messages that can be hidden within files and images. This makes me think of how some games will hide pieces of lore within its files and how there could be information easily missed.

Section 3 Step 9

Graphical user interface, application

Description automatically generated