Picture File Analysis

For this lab, we are looking into how photos can have additional information that can give us evidence and location. We are looking at the EXIF data from the picture files as they can contain helpful information.

We start with launching the DEFT Linux virtual machine and using the provided login. Once there we open the LXTerminal on the desktop. We navigate to the picture files with the command, cd Evidence\_Files/FOR\_LAB\_011/Pics and hit enter. We use ls to look in the folder. We start with an image by extracting it with the Exiftool, exiftool IMG\_001.jpg and hit enter. We now write the data into a text file using exiftool IMG\_001.jpg -w txt in the command box. Then we look at it with gedit IMG\_001.txt. Now we can look at the metadata of the file and then exit the exiftool once we are done.

Now we are using the windows virtual machine and opening HxD from the desktop. Now, we go to file, open and browse for Evidence Repository (E:) > FOR\_LAB\_011 > DB\_File and clicking the file called Thumbs.db and open. Now we use control f and look at the following search entries in the Hex-values tab, FF D8 FF E0 AND FF D9, then use control e to open the select block. We enter the start as A18, and the end as 6E38 hit ok then choose file save selection. We make a new folder called Exported Files in the E drive in FOR\_LAB\_011. We click into that folder and save the file as pic1.jpg and hit save then we can use file explorer to double check.

The saying a picture is worth a thousand words never felt truer than these labs. A lot of the labs can take images and find all sorts of information about them and hidden within. I found I quite enjoyed this lab as we were able to use pictures even more for evidence gathering.

Section 1 step 7

A screenshot of a computer

Description automatically generatedSection 2 step 16

A screenshot of a computer

Description automatically generated

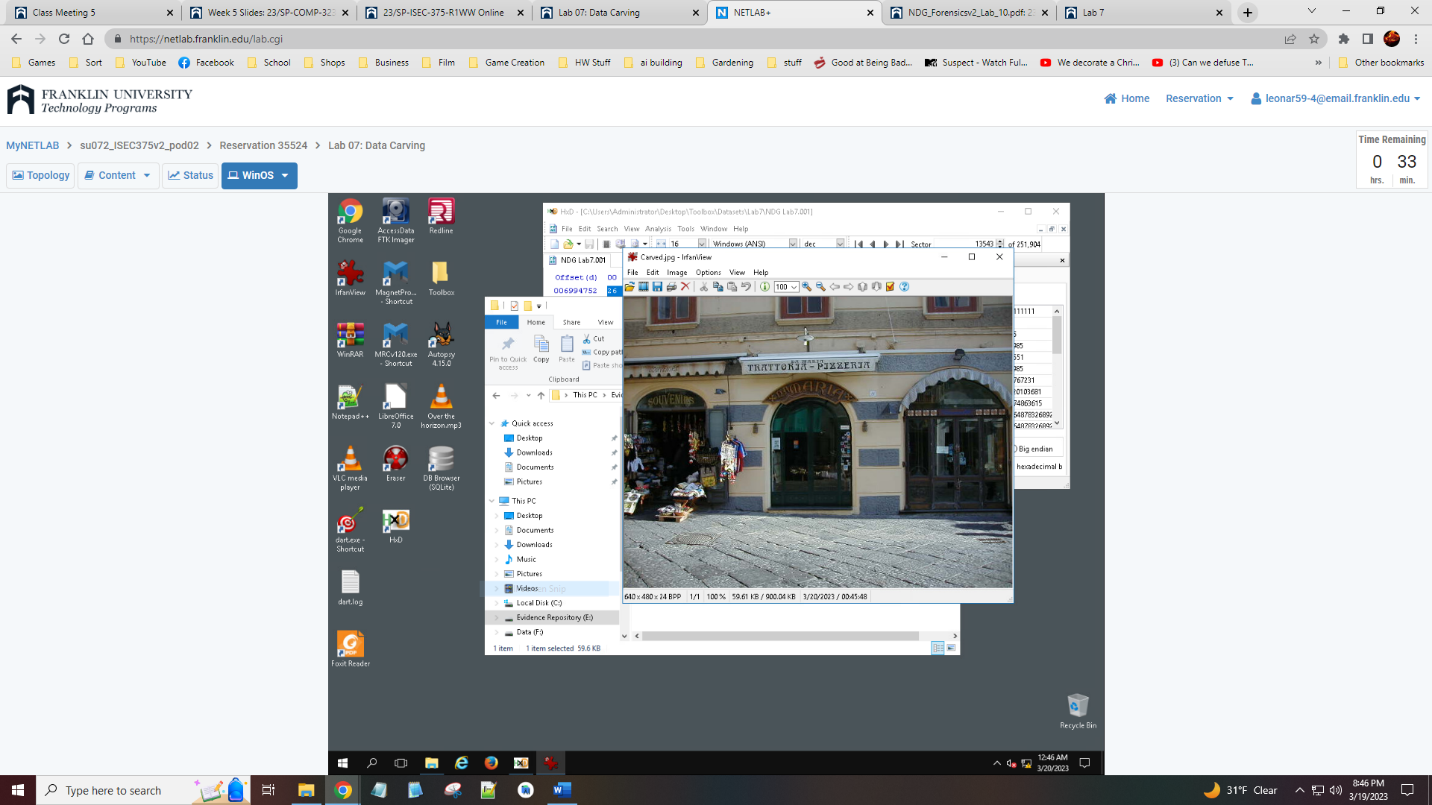
Data Carving

This lab looks at data recovery and how we can identify file through their signatures. We are learning how to do data carving and identify characters. We are looking at file signatures and carving JPG files only.

We start with the Windows virtual machine and opening HxD from the desktop. Going to view, toolbars, and data inspector within HxD. Now we go to tools and choose open disk image. We follow the path, This pc, desktop, toolbox, Datasets, Lab7, and choose the file Lab007.001 and open. At sector size we choose, 512 (hard disks/floppy disks), and hit ok. We go to view offset base and choose decimal. We ctrl and f and choose the hex-values typing in, FF D8 FF E0, selecting forward search direction and hit ok. Next, we search for FF D9 and hit ok. Then we repeat with FF D9. We hit ctrl and c setting the start to 6934016 and end to 6995053 hitting dec then ok. Then we go to file, save selection, follow the path, ThisPC > Evidence Repository > FOR\_LAB\_007 > Exported\_Files and save the file as Carved.jpg and hit save. We now use file explorer to find our saved image, Carved.jpg and open it.

The lab was interesting to work through as we were dealing with more pictures and able to turn a block of the data into an image. I find it fascinating how much can be done with the hex-values and how we can take a long file and find an image inside of it.

Section 4 Step 12



Steganography and Alternate Data Streams

We are back at this lab to work through how a message can be created within a file and how we can find and extract a file that is inside another. The plan is to be able to gather data that is hidden within files.

We start by clicking file explorer and following the path, This PC > Evidence Repository (E:) > FOR\_LAB\_010 > Steganography Files so we can look at the images. Now we open HxD once more with a double click on the desktop icon and go to file open. We travel the path prior and choose the file named, WhatsApp-Encryption.jpg and hit open. We hit search, go to, and select the end(backwards) then hit ok. We will enter the empty square at the bottom and type in a message, we hit the checkbox for do not ask this question again and hit ok should the pop up window appear. We hit ctrl and s to save and use file explorer to go back to the images and open and check the image did not change. We now go back to HxD and hit file and open so we can select the other image called PlanC.jpg and hit open. We click ctrl and f and choose hex-values entering into the search bar, 89 50 4E 47 0D 0A 1A 0A, and hitting ok. Next, we look at 49 45 4E 44 AE 42 60 82 in the search. Now we hit ctrl and e and set the start to 191F9 and end to 1A025 and hit ok. Now we hit file, save, and go back to the folder, Steganography Files and create a new folder called Exported Files and open that saving the file with the name, Exported picture.png and hit save. Now we can use the file explorer to get to our new folder and double click our file to see the message.

Section 1 Step 10

A screenshot of a computer

Description automatically generated

Section 2 Step 15

A screenshot of a computer

Description automatically generated