Creating a Forensic Image

This lab is designed to help teach how to maintain the integrity of the evidence by use of images. The evidence is important to any case which is why we want to keep it as safe as possible. The imaging helps with making a court-admissible forensic image.

The first thing we do is access the FTK Imager through the Start Menu and AccessData. After looking through the different menus, we move on to file create disk image where we select the source evidence type as physical drive. Next, we select the drive we are using and hit finish. From there, at create image, we are adding the image source and only check marking the verify images after they are created box. At select image type, we choose E01 then move on to the evidence item information page where we fill in the needed information, then continue. Next, we move to choosing the image destination folder which we call FOR\_LAB\_001 under this pc and evidence repository. Then, we name the image and hit finish, being sent back to the create image screen which we double check is set up like prior, then we hit start. Once the imaging finishes, we are sent to drive/image verify results which we look over then hit close and then close the creating image box behind it.

From there, we move on to the logical forensic image so we go back to file, create disk image, and choose logical drive in the source evidence type. We select the drive then hit add at create image choosing the E01 image type and filling in the evidence item information. At select image destination we will browse and go to this pc, evidence repository, and make a new folder called FOR\_LAB\_OO1A and hit ok. After naming the image we hit finish and double check that only the verify images after they are created box is checked, then we hit start. After this, we can close the results and the creating image window.

The next step is to review the image reports so we start by going to the FOR-LAB-001 folder in the evidence repository. We look at 1GB\_Seagate\_SN954321.E01.txt in notepad then we do the same for the picture in FOR-LAB-001A. Back at FTK Imager, we go to file, add evidence item, select source opens and we choose image file then take the location of the txt files from prior and set that as the source path. We look through the evidence tree then repeat the process for the second image once we determine that the image was successfully created.

Images can be quite important evidence in a lot of cases so seeing how we work with them was quite interesting. The lab ran through each type of image so we can see how it differs for each type. The evidence tree was interesting as we are able to look at the different files that are made with the images. This lab was quite fun to work through and I was able to learn a lot about the forensic imaging.

Section 2 step 18

A screenshot of a computer

Description automatically generated

Section 3 step 14

A screenshot of a computer

Description automatically generated

Section 4 step 3

A screenshot of a computer

Description automatically generated

Section 5 step 6

A screenshot of a computer

Description automatically generated

Metadata and Link File Analysis

This lab is set up to introduce us to metadata and the importance of determining when a file was accessed. The lab goes over how to get the metadata and what data link files are. It is just as important to know when something happened as what happened.

We start by launching the FTK Imager, found through the start menu and access data. Then we go to file, add evidence item, and select source image file before hitting next. In the source path, we are setting it to Desktop, Toolbox, Datasets, Lab8, Lab8-1 and then the file Lab8-1.E01, hitting open. Hitting finish on the select file, we turn to the evidence tree hitting the plus next to the Lab8-1.E01 item, then hitting the plus next to partition 1. Moving on, we expand the NONAME [NTFS] folder then the root folder. We move down to expand the Documents and Settings, Mr. Evil, and then Recent folder before clicking on the yng13.lnk file, then the priorities tab where we will find our metadata. We then turn back to the file list and select all of the link files before doing right click, export files which will bring us to the browse for folder window. From here, we go to evidence repository and make a new folder called FOR\_LAB\_008, and another folder inside that one called Link\_Files before hitting ok and then ok again.

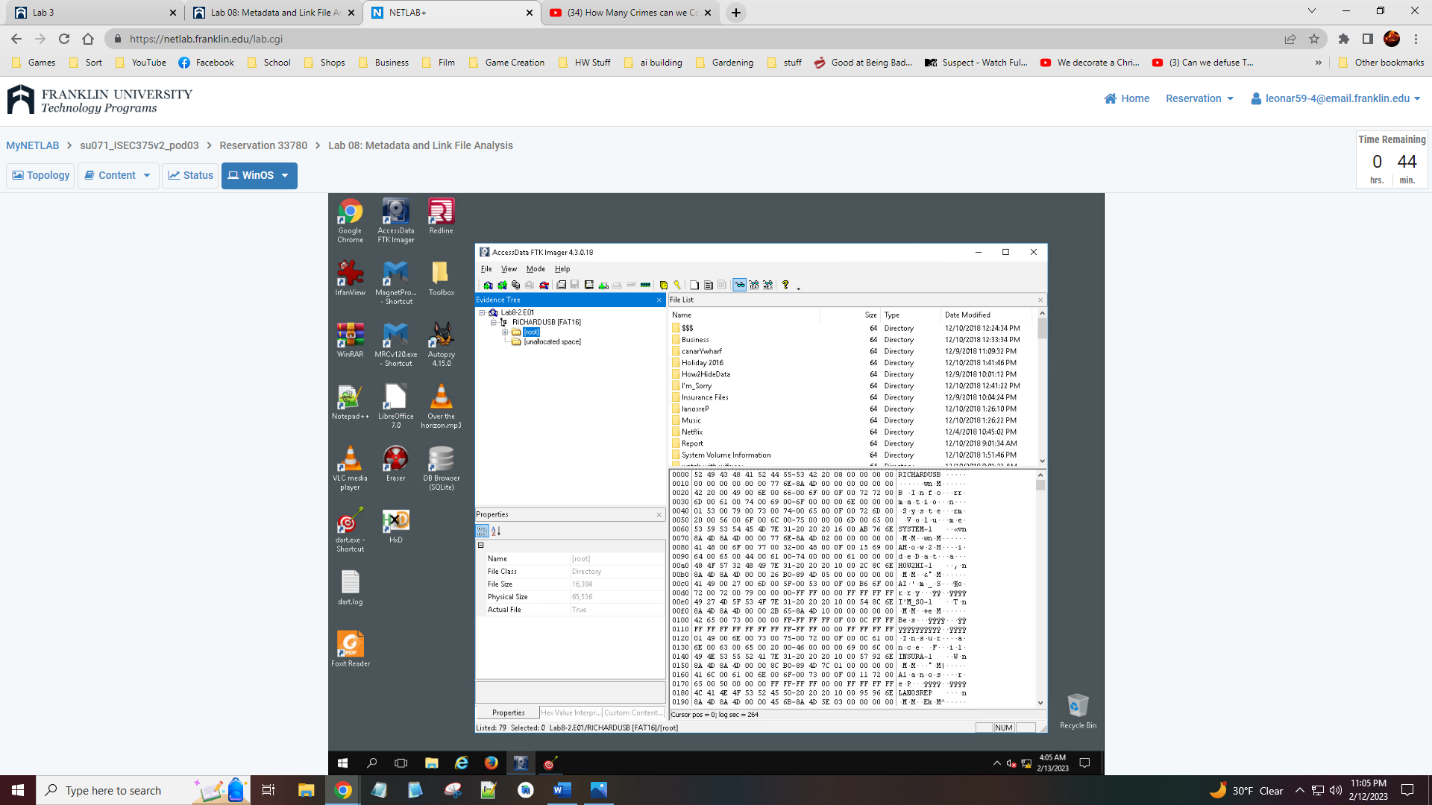
Now we go to the Windows File Explorer and go to this pc, desktop, toolbox, and then double click deft-8.2-002 and then dart.exe. After clicking yes at the warning, we will be in browse for folder where we go to evidence repository, FOR\_LAB\_008, and make a new folder named DART 2.0. At the main window, we click on forensics and then the plus by windows forensics where we click on Lnk Examiner and finally, START AS ADMIN. At the Lnk Examiner, we click on process then folder where we follow the browse for folder path back to the Link\_Files that we made earlier and hit ok. After looking through the different columns, we then export and save as CSV file where we save in a new folder under FOR\_LAB\_008 called Lnk\_Report and then enter it to save the folder, Exported Lnk Metadata.

Back at the FTK Imager, we go to file, remove all evidence items, then hit add evidence item. We pick the image file and go back to Lab8 and then into Lab8-2 and Lab8-2.E01, hitting open, then finish. Now we move on to clicking the plus next to the Lab8-2.E01, then the RICHARDUSB [FAT16], and then clicking on root. Then we select the files: 19861-sc-clients-national.xls, Ar17\_en.pdf, Kaczynski2.pdf, Kpmg-feature-sep-2010.pdf, LBTH\_Tall\_Buildings\_Report\_24\_07\_17.pdf, Only Death Pablo Neruda.docs, TuringComputing.pdf. Then we right click and export files, making a new folder in FOR\_LAB\_008 called Metadata\_Analysis, hitting ok twice then closing all of the windows we have up.

Next, we go to This PC, Desktop, Toolbox, and MetaExtractor where we double click MetaExtractor.exe. Then we his the open folder and selecting the folder called Metadata\_Analysis, then select folder. After scrolling through the columns, we click Save to CSV and make a new folder in FOR\_LAB\_008 called Metadata\_Report and a new folder in that one called Exported File Metadata, hitting save and the closing everything.

This lab was interesting as we worked through the metadata and what information is being saved with the files themselves. Metadata is a term that we hear a lot of today so looking more into it was quite nice. I was worried since the page count was 52 but it did not take too long to complete.

Section 4 Step 9



Section 6 Step 8

A screenshot of a computer

Description automatically generated

Section 6 Step 10

A screenshot of a computer

Description automatically generated