Live Forensics

This week we are working with digital evidence and the proper procedures that are used to collect electronic data. The lab is made to tech how to collect the relevant evidence and retrieve data without altering the evidence.

The first thing we do after logging in is head to the file explorer where we follow the path, Desktop > Toolbox > deft-8.2-002 then we open dart.exe found within. After clicking yes at the warning, we will see browse for folder where we go to evidence repository and make new folder named FOR\_LAB\_003. Inside that folder we make a new folder called DART\_LOGS and click on it then ok. In dart we will click on the Incident Resp. category. In the folders we go into the system info and click on DriveMan then start as admin to open the drive manager where we click disk info. After reviewing the information, we will close the drive manager information and move back to the dart homepage where we click on acquire. At the files, we click the plus by Image then click on FTK Imager and start as admin. We will in FTK Imager, hit file, add evidence item, choose physical drive at select source then next. At select drive we will choose PHYSICALDRIVE0 from the menu and hit finish. At the FTK Imager main window we will hit the plus next to the drive we chose, hit the plus next to basic data partition 2, then the one next to NONAME [NTFS], then expanding root, users, and finally administrator, before we close out of FTK Imager. Back at dark home page, we hit go back to incident resp. and expand the system info then click on treesizefree and start as admin. Once it loads, we will hit scan, choose the local disk c and let it run. After, we will click the arrow next to users, administrator and look at downloads before we close out of treesizefree. Back at the dart screen, we will hit incident resp. then winauditu and start as admin. Here, we click on options, apply, and then hit audit back at the main window. Once the audit is completed, we will look at the system overview, then choose installed software under categories to the left. We look it over then hit save, follow the folder path back to FOR\_LAB\_003, and create a new folder named FOR\_LAB\_003\_Audit, and saving a file inside setting it as an HTML file and then hitting save, then winaudit can be closed. At dart, we choose forensics, then browsinghistoryview 64-bit, and hit start as admin. At advanced options we choose ok then look over the browsing history, hitting edit, select all, file, and save selected items. Back into the FOR\_LAB\_003 folder, we add a new folder named FOR\_LAB\_003\_BrowsingHistory, saving the file inside as a html file named FOR\_LAB\_003-BrowsingHistory, then hitting save and ending the lab.

When it comes to gathering evidence, we need to be careful as it is quite easy to alter digital data. There are many ways to go about getting the desired evidence. The lab helped show how to get the data and information without the risk of altering it. The lab was very informative and helpful with learning about forensic evidence gathering.

Section 2 step 4

Graphical user interface

Description automatically generated

Section 3 step 10

A screenshot of a computer

Description automatically generated

Section 4 step 6

A screenshot of a computer

Description automatically generated

Section 5 step 10

A screenshot of a computer

Description automatically generated

Section 6 step 3

A screenshot of a computer

Description automatically generated

File Hashing and Hash Analysis

This lab focuses on file hashing and its importance with digital forensics. It is to help with the verification and validation of digital data and can help with proving evidence has not been tampered with.

After logging in, we access FTK Imager through the start menu or on the desktop. After launch, we then go to file, add evidence item, opening the select source window. We choose image file then hit next, then browse for source path. We follow the path   
This PC > Desktop> Toolbox > Datasets > Lab20 > Lab20 Hashset, choosing the file Lab20\_hashset.ad1 then hitting open and finish. In the evidence tree we move to, Lab20\_hashet.ad1 > Files for hashset\F:\LABS\FOR\_LAB\_020\Files for hashset [AD1] using the plus symbol. After looking through the file list, we right click on Files for hashset\F:\LABS\FOR\_LAB\_020\Files for hashset [AD1] and hit export file hash list. In the save as menu, we move into evidence repository e and create a new folder named FOR\_LAB\_020, then adding a folder in our new folder named, file hash list, then click open where we save the file as Lab20 file hash list and hit save. Moving to the file explorer we follow the path, This PC > Evidence Files > FOR\_LAB\_020 > File Hash List and double click the file, Lab20 file hash list to open it, followed by clicking ok on the text import window. After checking the file out, we move back to the file explorer and go to Desktop > Toolbox > hasher and launch hasher.exe. We go to tools then options where we check boxes, SHA-1 Base 16, SHA-256, SHA-512, and RipeMD-256, then hit save. Next, we go to file, select folder, following the path, Desktop > Toolbox > Datasets > Lab20 > Lab20 Files for Hasher and click ok. We move on to file, save results, to excel, then use the browse for folder window to find the file hash list from the prior steps and hit ok, then ok, and then we minimize hasher. Now, we go back to the file explorer and follow the path, ThisPC > Evidence Repository (E:) > FOR\_LAB\_020 > File Hash List, right clicking on the file, \*-HasherResults.xlsx, and open with LibreOffice, then ok. After comparing, we move on and head back to the start menu opening the folder autopsy and choosing Autopsy 4.15.0, clicking new case. The case is then named, FOR\_LAB\_020 and we open browse by the base directory. We locate the FOR\_LAB\_020 folder and create a new folder inside named Autopsy, then click select, then next. We enter in the case number and examiner information and click finish. At add data source we chose disk image or vm file, and hit next, then browse at the path. We follow the path, ThisPC > Evidence Repository 2 (H:) > Forensic Evidence Files > FOR\_LAB\_020 > FEF and click on the file called Lab20\_FEF.E01, then open. We change the time zone to (GMT+0:00) UTC, hit next, and deselect all at the configure ingest modules , then click hash lookup and move to global settings. Here, we will hit new hash set, naming it, Lab20Hashset, and clicking save as. Following the path, ThisPC > Evidence Repository (E:) > FOR\_LAB\_020 > Autopsy > FOR\_LAB\_020, we create a new folder named hash sets then hit open, save, ok, and then add hashes to hash set. We follow the path, ThisPC > Evidence Repository (E:) > FOR\_LAB\_020 > File Hash List and open the lab20 file hash list with double clicks, highlighting all of the MD5 hashes, right click, select copy. We move back to add hashes to hash set and click paste from clipboard and hit ok, ok, ok, then finish. We can now expand hashset hits and click lab20hashset, looking at the different files before finishing.

Hashing is a topic that tends to come up a lot in security, being able to see it in action was interesting as we had different ways to reach our desired outcome. As we went over in class, the hash of the files is quite important in showing that evidence has not been altered. It is an interesting topic and I am glad to have seen the hashing put in action.

Section 1 step 14

A screenshot of a computer

Description automatically generated

Section 2 step 10

A screenshot of a computer

Description automatically generated

Section 3 step 25

A screenshot of a computer

Description automatically generated