Philip Herman

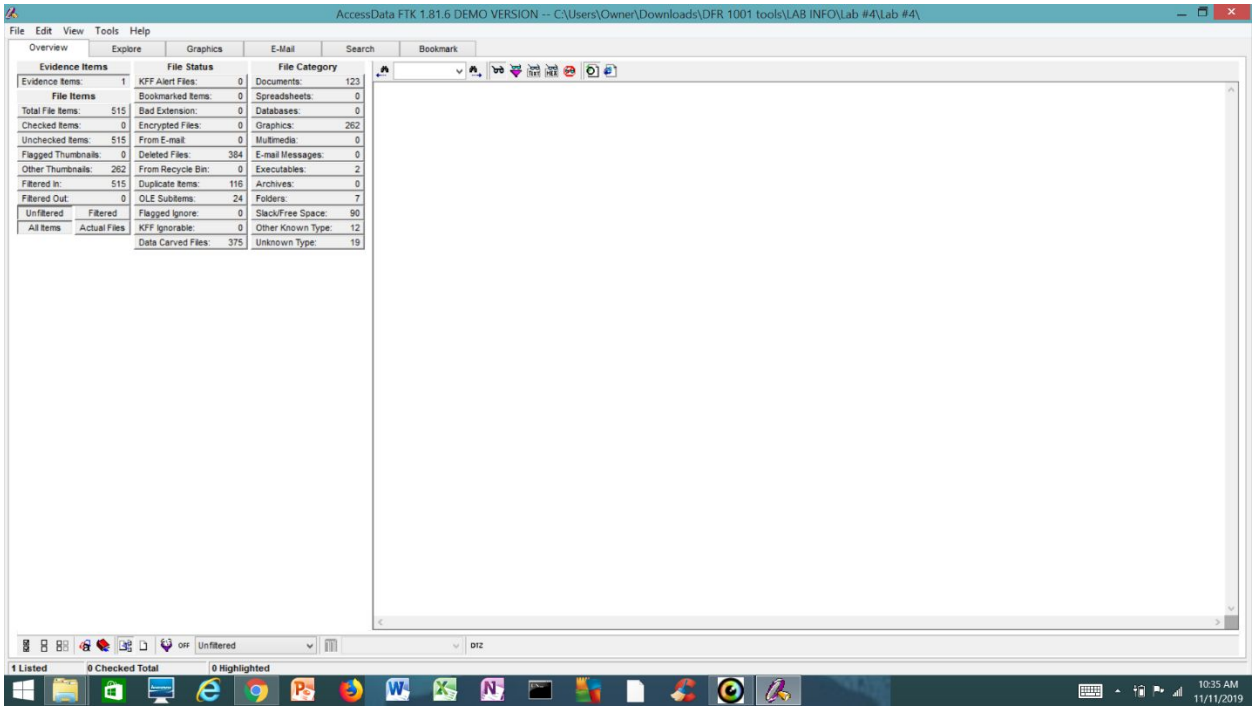
DFR 1001

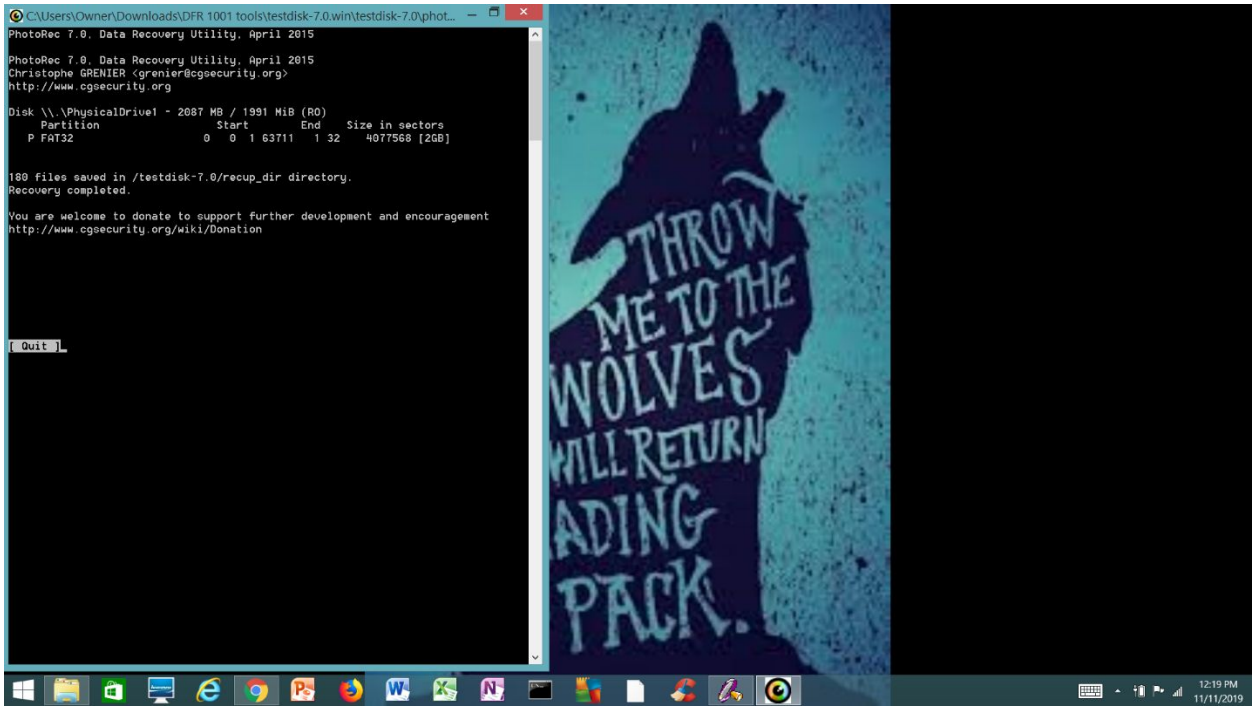
11/12/2019

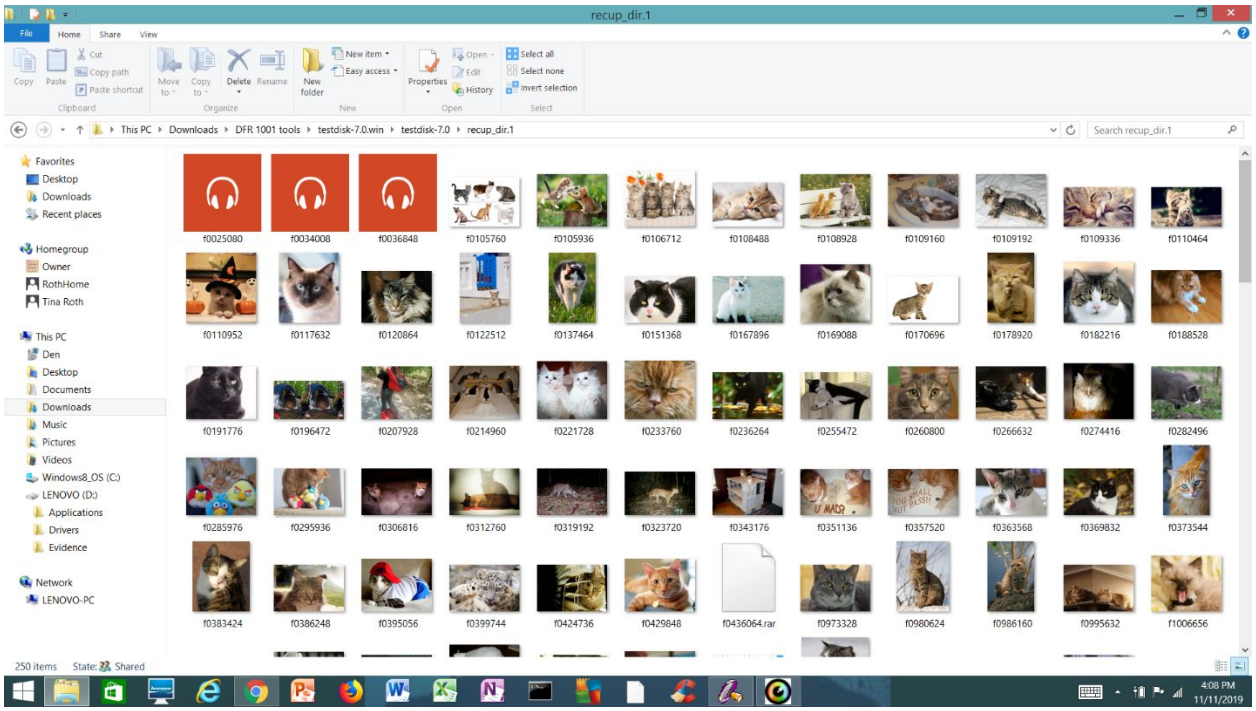
Lab #4

The purpose of this lab was to recover images using both FTK and PhotoRec and compare the results of the two programs. To start this process, I opened up FTK and started a new case and made sure the destination file was set to the right folder. I kept all of the settings as the default and imported the E01 file from the "Evidence" folder provided on Blackboard. From there I was able to process the files and use the data carving tool to come up with a total of five hundred and fifteen files; two hundred and sixty two other thumbnails, three hundred and eighty four deleted items, one hundred and sixteen duplicate items, twenty-four OLE subitems, three hundred and seventy five data carved items, one hundred and twenty three documents, two hundred and sixty two graphics, two executables, seven folders, ninety free space, twelve known type and nineteen unknown type files. Before I could start the PhotoRec part of this lab, I had to open up FTK imager and mount the file so that it would appear on a separate drive. Without doing that, PhotoRec won't be able to find the file. Once the file was mounted I opened up PhotoRec and ran it as an administrator. From there I opened up the drive it was in and selected the FAT32 file and carved the portion of the file with unallocated space by selecting "free" from the next prompt. From there I selected the next directory which was the drwxxx file with two dots at the end and started the recovery process which saved to the folder it was directed to in the beginning. The biggest difference between the two is that upon completion it didn't break down which file was for which. It just stated that one hundred and eighty files were saved in the folder to be viewed. Upon opening that folder all the files were visible, some were audio, some were pictures and some were text files. Both programs show you what is in the files, however it is done in very different ways. I think FTK is better, personally, because it catches more information and filters it a little better than PhotoRec did.

FTK even caught the deleted files which was good in case someone tried to discard evidence, it can be retraced. Overall I liked this lab and thought it was a great way to expand into new tools and show that even though two tools are marked to do the same job, they don't always do them as thoroughly and as well as others can.




C:\Users\Owner\Downloads\DFR 1001 tools\testdisk-7.0.win\testdisk-7.0\phot...
PhotoRec 7.0, Data Recovery Utility, April 2015
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
Disk \\.\PhysicalDrive1 - 2087 MB / 1991 MiB (RO)
Partition Start End Size in sectors
P FAT32 0 0 1 63711 1 32 4077568 [2GB]
180 files saved in /testdisk-7.0/recup_dir directory.
Recovery completed.
You are welcome to donate to support further development and encouragement
http://www.cgsecurity.org/wiki/Donation
[Quit]
THROW ME TO THE WOLVES WILL RETURN ADING PACK.
12:19 PM
11/11/2019


recup_dir.1
File Home Share View
This PC ▸ Downloads ▸ DFR 1001 tools ▸ testdisk-7.0.win ▸ testdisk-7.0 ▸ recup_dir.1
Search recup_dir.1
Favorites
Desktop
Downloads
Recent places
Homegroup
Owner
RothHome
Tina Roth
This PC
Den
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows8_OS (C:)
LENOVO (D:)
Applications
Drivers
Evidence
Network
LENOVO-PC
f0025080 f0034008 f0036848 f0105760 f0105936 f0106712 f0108488 f0108928 f0109160 f0109192 f0109336 f0110464
f0110952 f0117632 f0120864 f0122512 f0137464 f0151368 f0167896 f0169088 f0170696 f0178920 f0182216 f0188528
f0191776 f0196472 f0207928 f0214960 f0221728 f0233760 f0236264 f0255472 f0260800 f0266632 f0274416 f0282496
f0285976 f0295936 f0306816 f0312760 f0319192 f0323720 f0343176 f0351136 f0357520 f0363568 f0369832 f0373544
f0383424 f0386248 f0395056 f0399744 f0424736 f0429848 f0436064.rar f0973328 f0980624 f0986160 f0995632 f1006656
250 items State: Shared
4:08 PM
11/11/2019