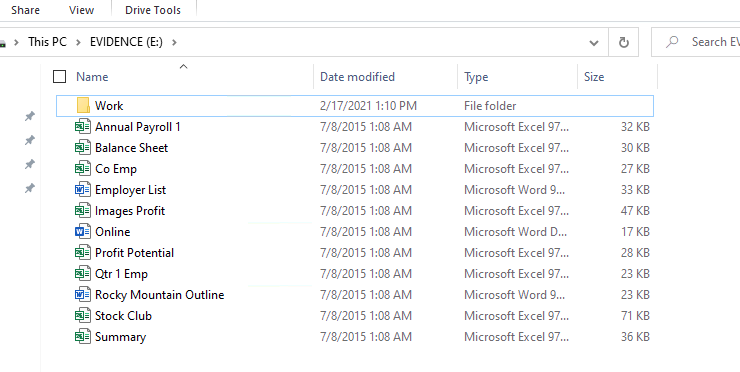
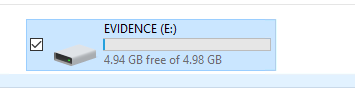
# Digital Forensics labs

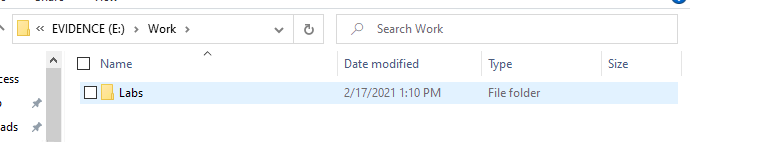
Lab 1:

I Logged into my VM and inserted a USB drive containing files I don’t need. I Right clicked on the Pro Discover icon and clicked Run as Administrator. I Clicked Yes on the User Account Control (UAC) message box. Next, I Clicked the “Don’t show this dialogue in the future” box and then clicked Cancel to close it. I Clicked Tools then Secure Wipe from the Menu, then Clicked the Disk to Wipe list arrow and clicked the drive letter corresponding to the USB drive. I Double checked before I proceeded that I had the correct drive selected to prevent accidental erasure. In the number of passes box, I typed 7 and then clicked Start to begin. The Securely Deleting file message was displayed in the lower left corner to indicate the process had begun. This took me at least 60mins for it to finish. A message was displayed when the process was completed. I Clicked NTFS in the file system list box and typed "EVIDENCE” in the volume label text box. And then I Clicked Start to format the USB drive. When the format was finished, I clicked OK and closed the dialogue box. After the dialogue box closed, I Copied the 11 files from the C2Proj1 folder onto the USB stick. The device was labeled, and no further files were copied to it and all windows were closed.



Lab 2:

I Inserted the USB drive containing the Evidence that I prepared in Lab 1, I then Created a folder called Work and created a subfolder called Labs and inside labs I Created subfolders Cases, Data and Evidence. After that I then Opened Pro Discover, Clicked Action, Capture Image from the Menu. In the Capture Dialogue box, I clicked the Source Drive list arrow and then clicked the drive letter of the USB. Then used Work\Labs\Evidence folder for my destination folder. In the Save as box I type C2Proj2 in the filename text box and clicked Save. In the Capture Image Dialogue box, I typed my full name in the technician box and C2Proj2 in the Image Number text box. When the imaging finished I went to the evidence folder to see if the files was successfully created.



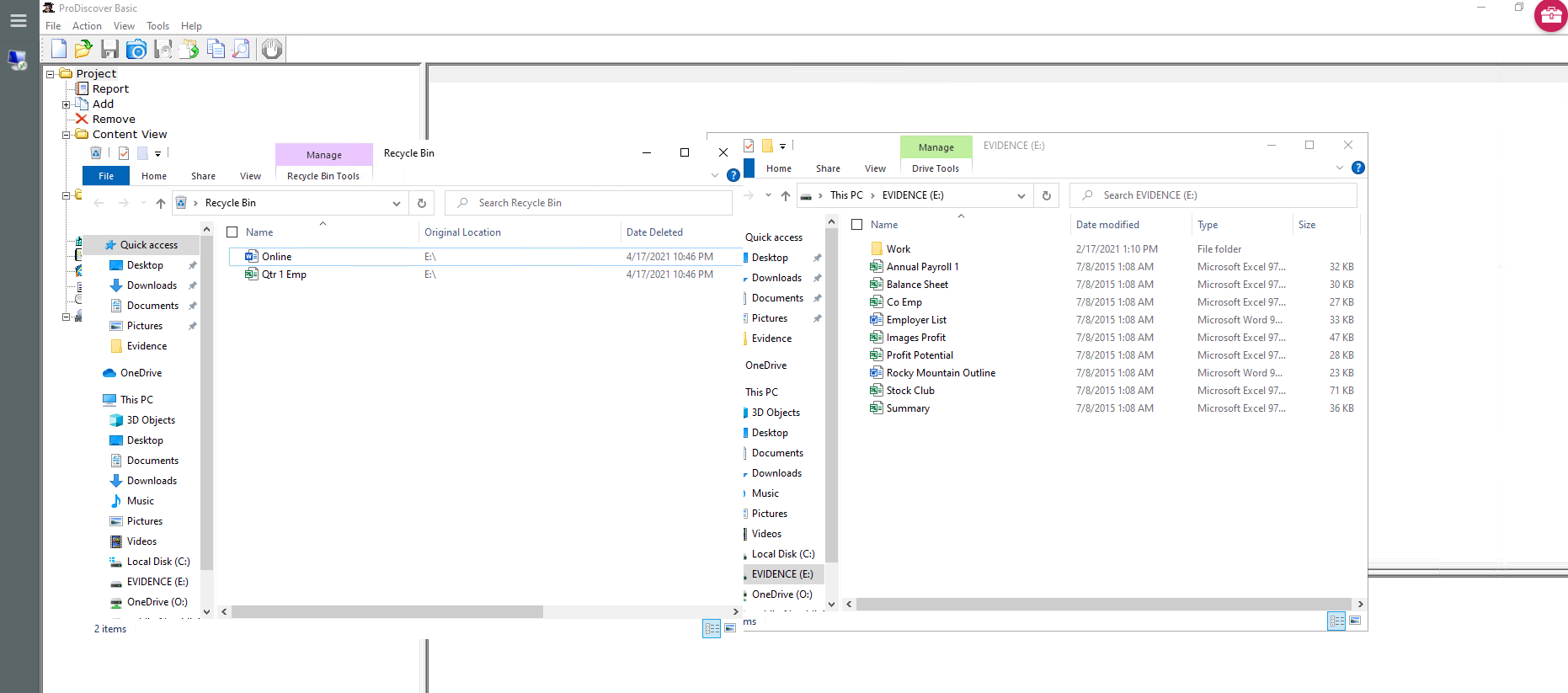
Lab 3:

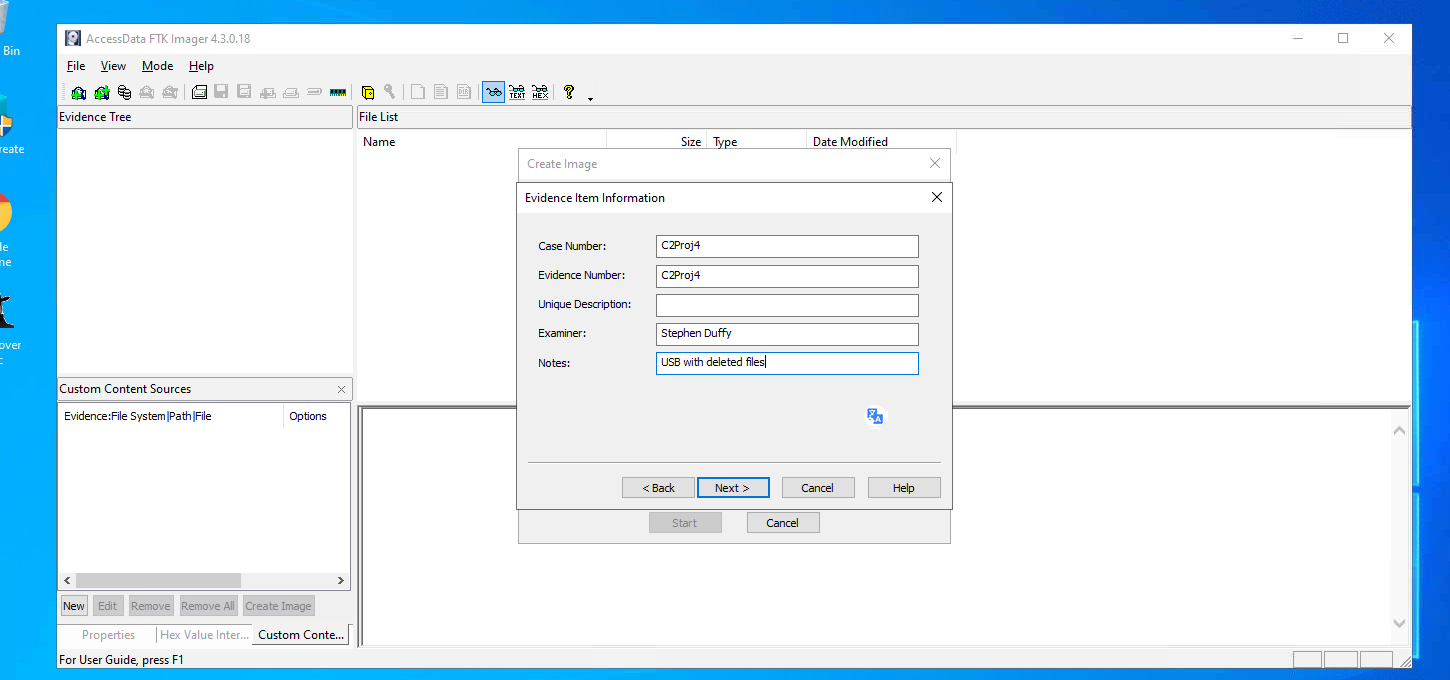
I Opened Pro Discover then went to the tools menu, I used the convert pro discover image tool to navigate to the evidence folder and convert C2Proj 2 into C2Proj.dd, The image file was approximate the size of the storage device.

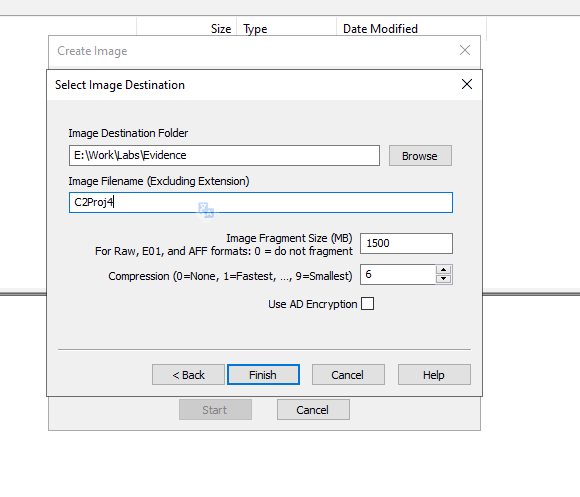
Lab 4:

First, I deleted files qtr 1 emp.xls and online docx files on the usb drive, I then opened the ftk imager as admin and created a disk image from the menu, I selected logical drive as my option in the menu and selected evidence ntfs as my source drive in the drop-down box at the top. In the next tab I clicked add and selected the image type as the E01 option, the case number and evidence number were C2Proj4.

I entered my full name in the examiners box and typed “usb image with deleted files” in the notes text box, I clicked next to continue. In the image destination box, I located to work/labs/evidence in my E Drive (usb) and clicked ok, naming the image file C2Proj4.



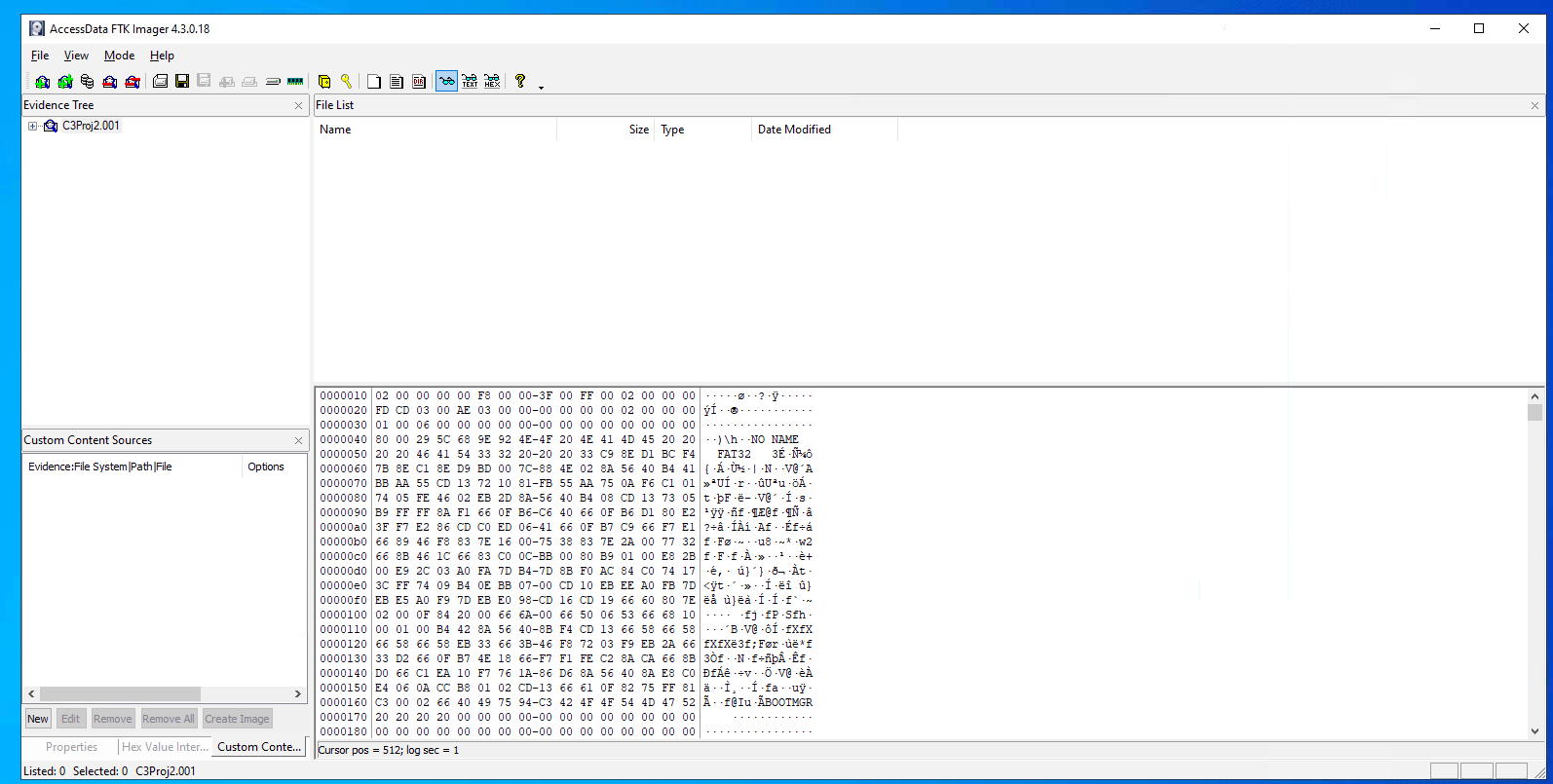


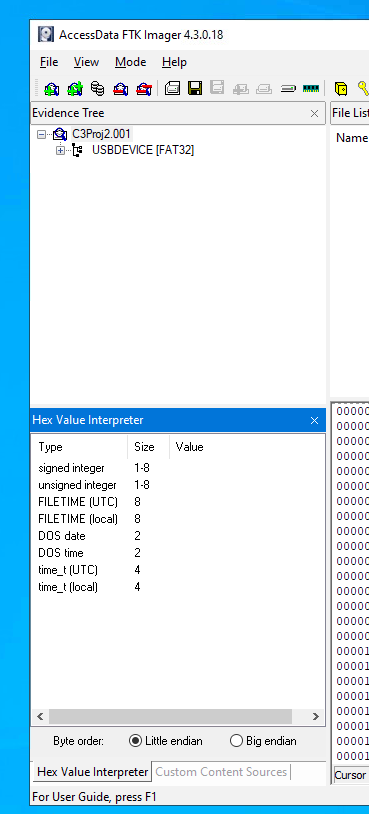


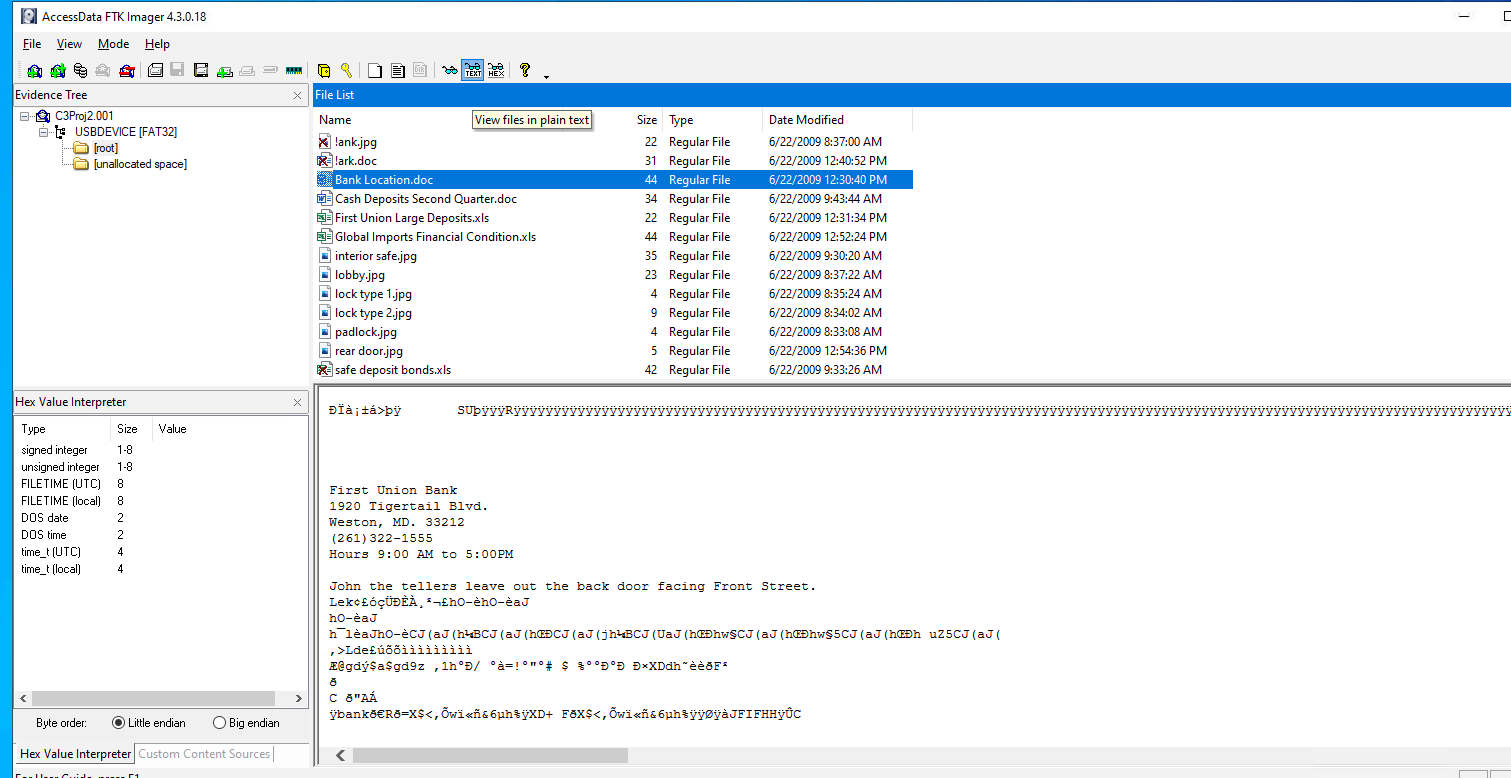
Lab 5:

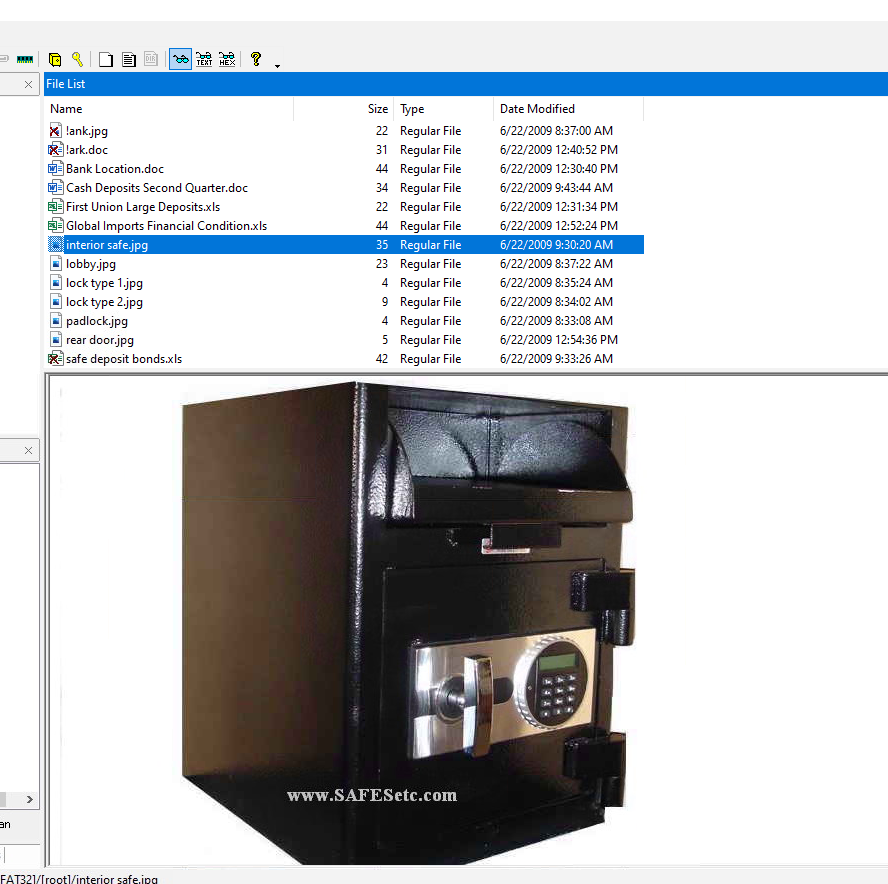
I opened ftk imager as admin and clicked “file”” and “add evidence item” from the menu, I clicked the image file option button and then clicked next. I clicked browse and went to work/labs/evidence and clicked the C2Projj4.e01 file that we made in labs 4 and clicked open, then finish. I expanded the file in the evidence tree pain to find the deleted files were recovered from the usb drive, I CTRL clicked these files and exported them to the evidence folder.

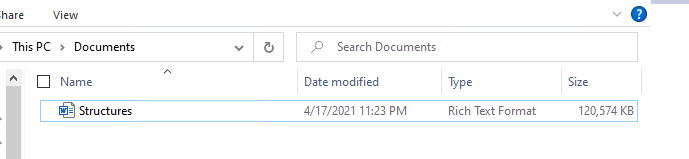
Lab 6: I coped the file c3proj2.001 from the data files to my work/labs folder and opened ftk imager. I added the file as an evidence item and loaded the file c3proj2.001. I expanded the file and looked around and studied the structure of the file. I used the hex toolbar button to see the hex values of the file. II looked at the interior safe jpg file and used the eyeglass toolbar to see the full image and lastly, I saved the contents of usb device to a WordPad document called “structures.”





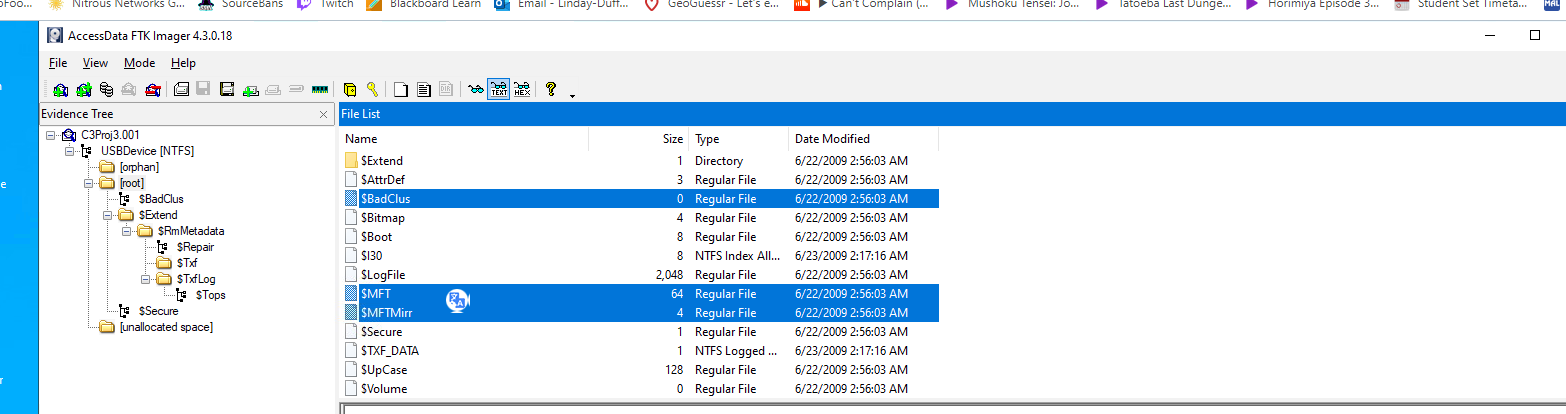


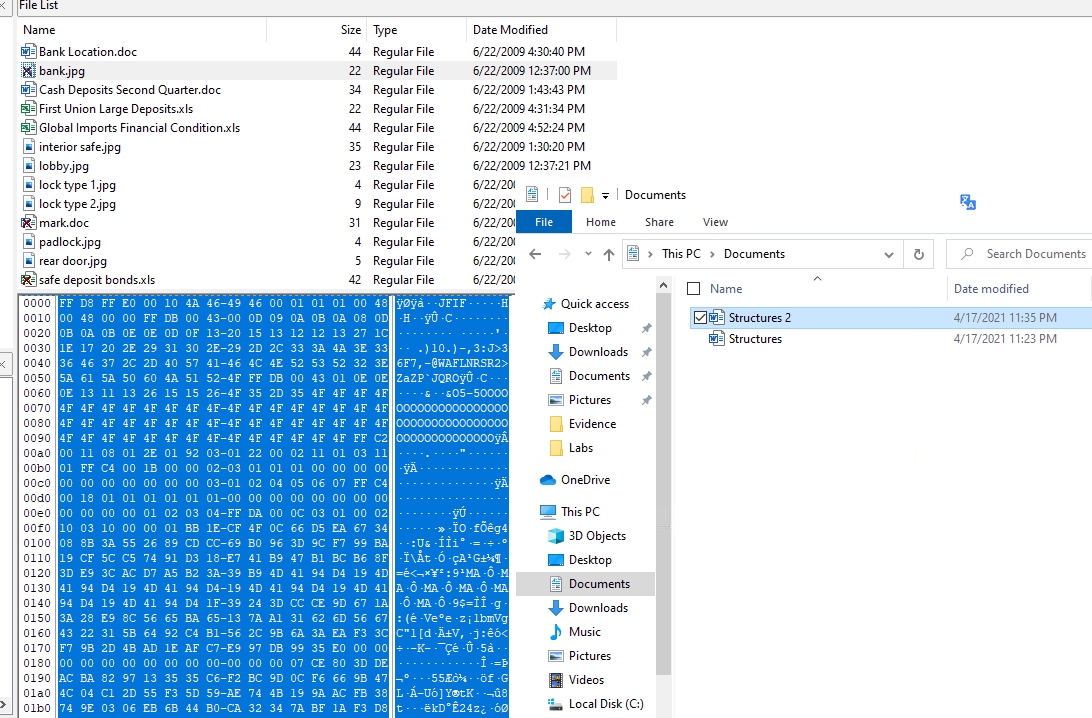




Lab 7:

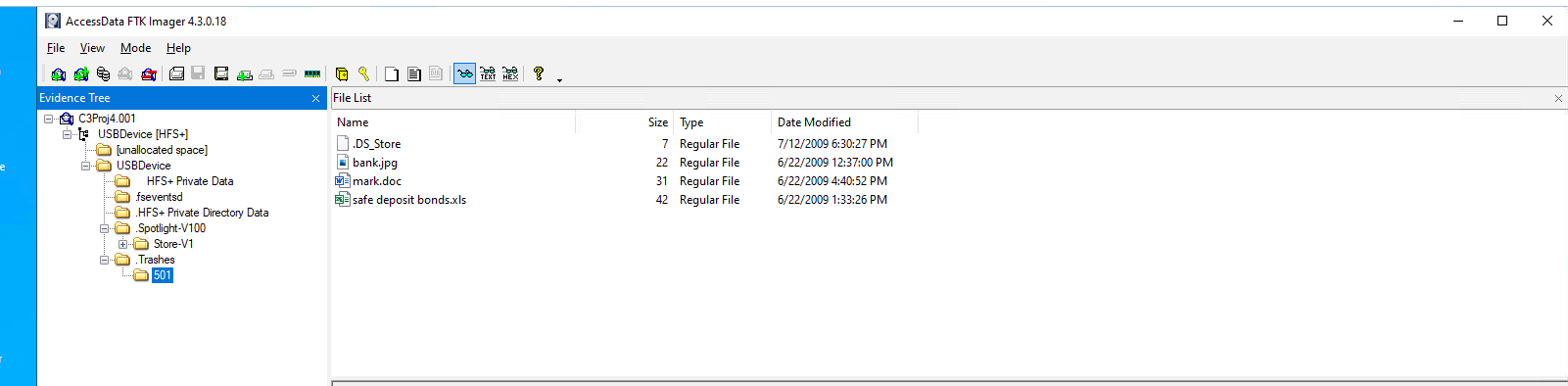
I coped the file c3proj3.001 from the data files to my work/labs folder and opened ftk imager. I added the file as an evidence item and loaded the file c3proj3.001, the file system is identified as ntfs. I studied the file and observed its hidden files, noticing $badclus, $mft and $mftmrr. I checked the hex value for each file and copy and pasted the roots hex values into a WordPad file called “structures 2”





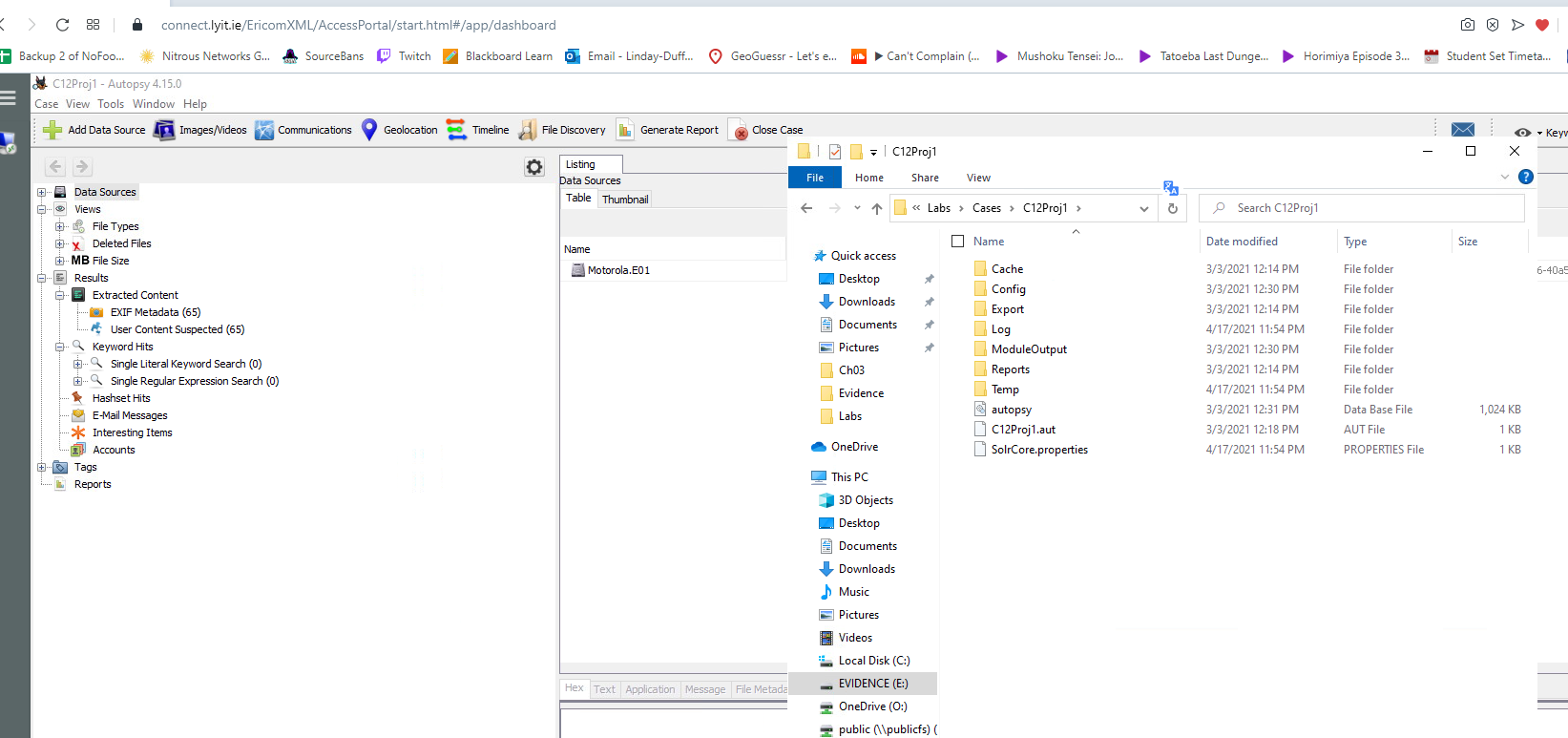
Lab 8:

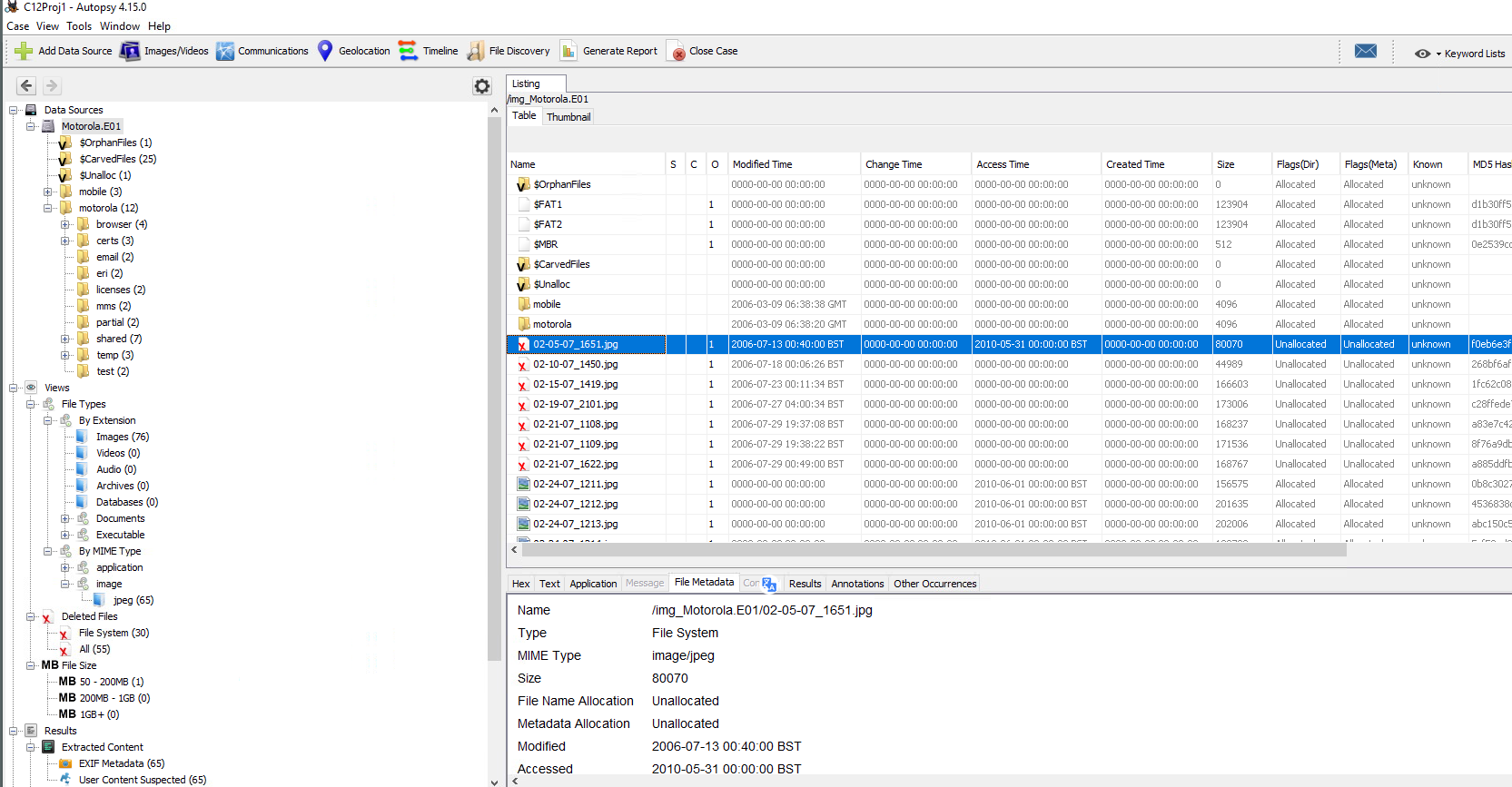
I coped the file c3proj4.001 from the data files to my work/labs folder and opened ftk imager. I added the file as an evidence item and loaded the file c3proj4.001, The first thing I noticed was that there was no root file/folder. I examined the hidden folders as they were used for journaling file transactions. I expanded the .trashes folder and clicked the 501 folder. I saw the same deleted files as before, but they weren’t indicated as deleted. I viewed each files properties and security attributes. I saved the hex values the same was as I did in the last 2 labs.



Lab: 11

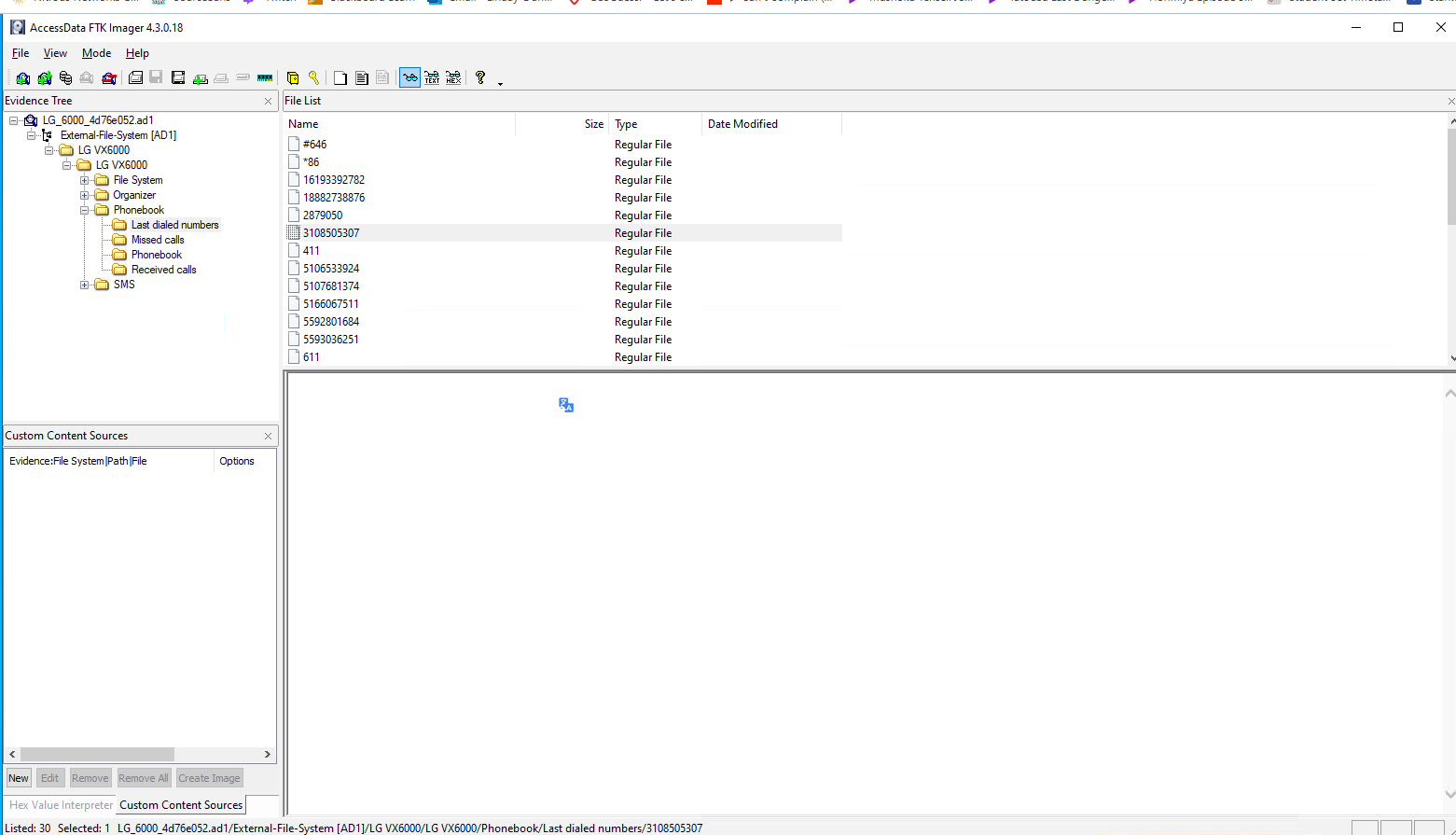
I started off by copying the Motorola file from the data files to my evidence folder and opening it in autopsy, I opened it as a new case and called it C12Proj1, I added it as a file data source. I viewed the files OS folders and MicroSD storage and looked at the metadata tab. I checked the recovered jpg files and looked at the master boot record that contains information needed to mount the storage device. The device was manufactured by San Disk, this information was giving to us as it was named SANVOL. I expanded the extracted content and clicked exif metadata to see the exif information, by scrolling through this information I could see the photos taken by the camera phone.

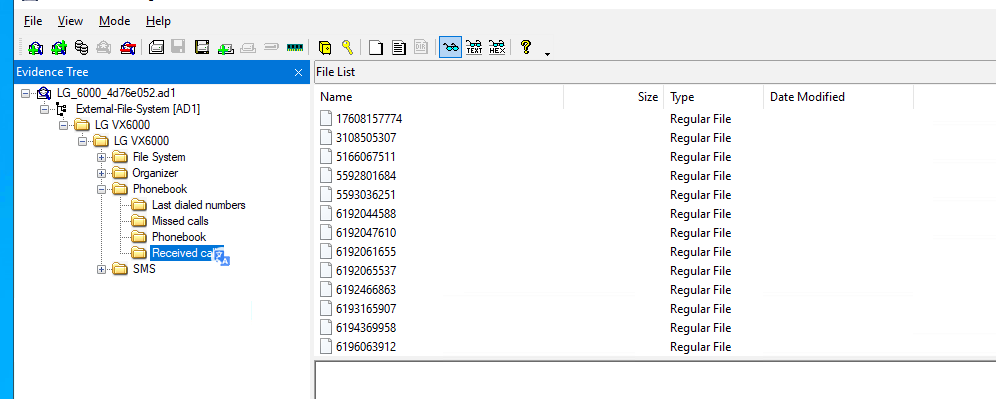


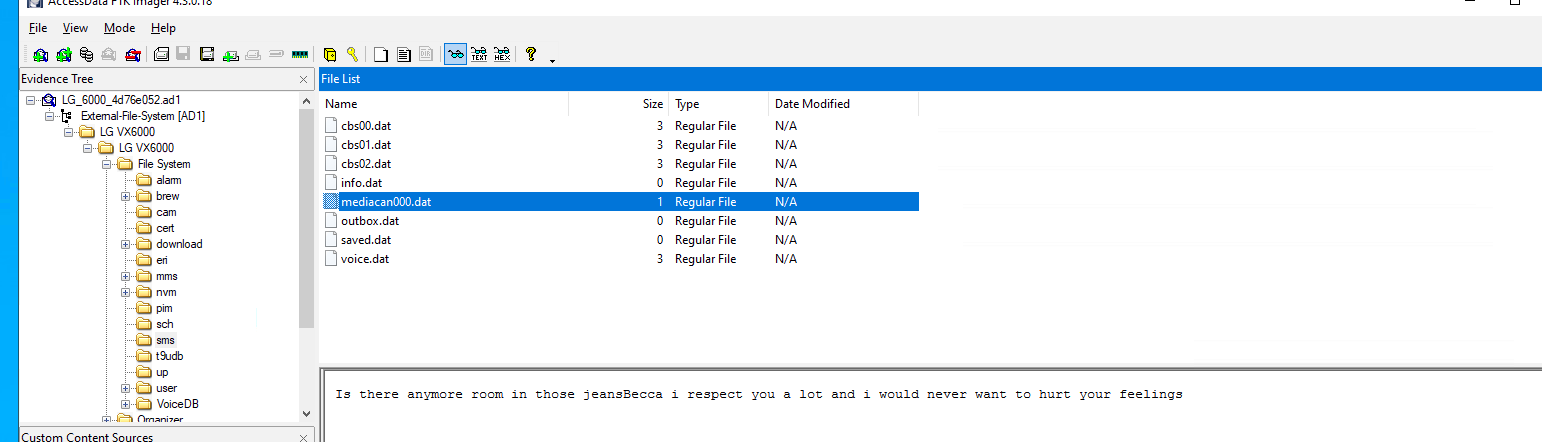


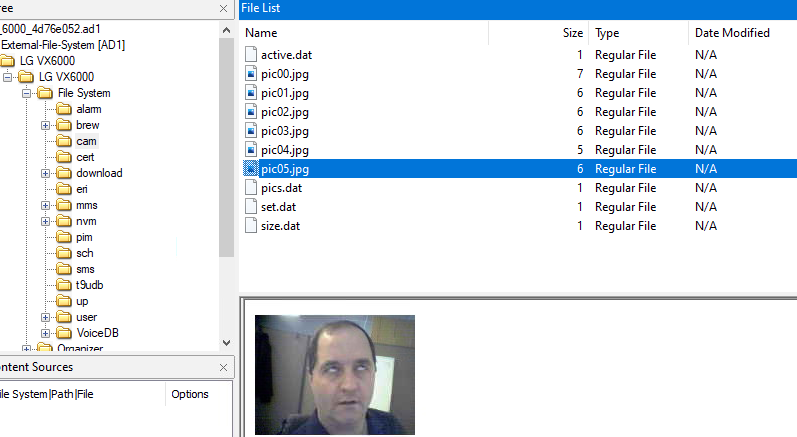
Lab 12:

Opened the LG\_6000\_4d76e52.adl file, added it as evidence as an image file in FTK. Browsed the phonebook folder and checked missed and inbound calls as well as text messages and photos.



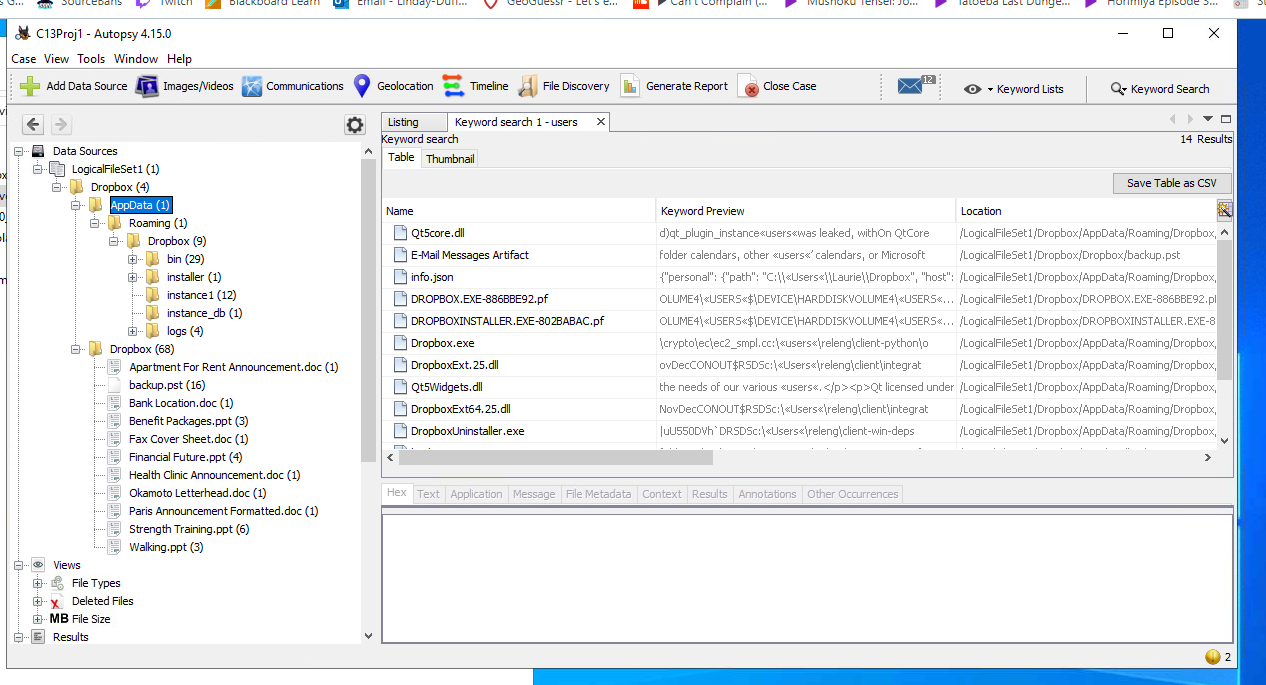


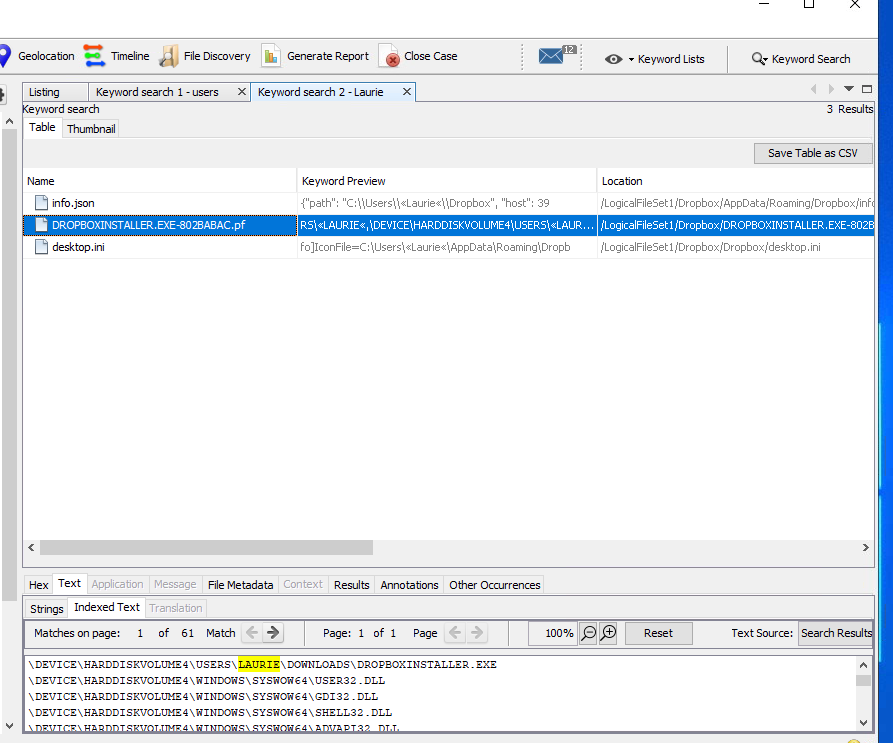


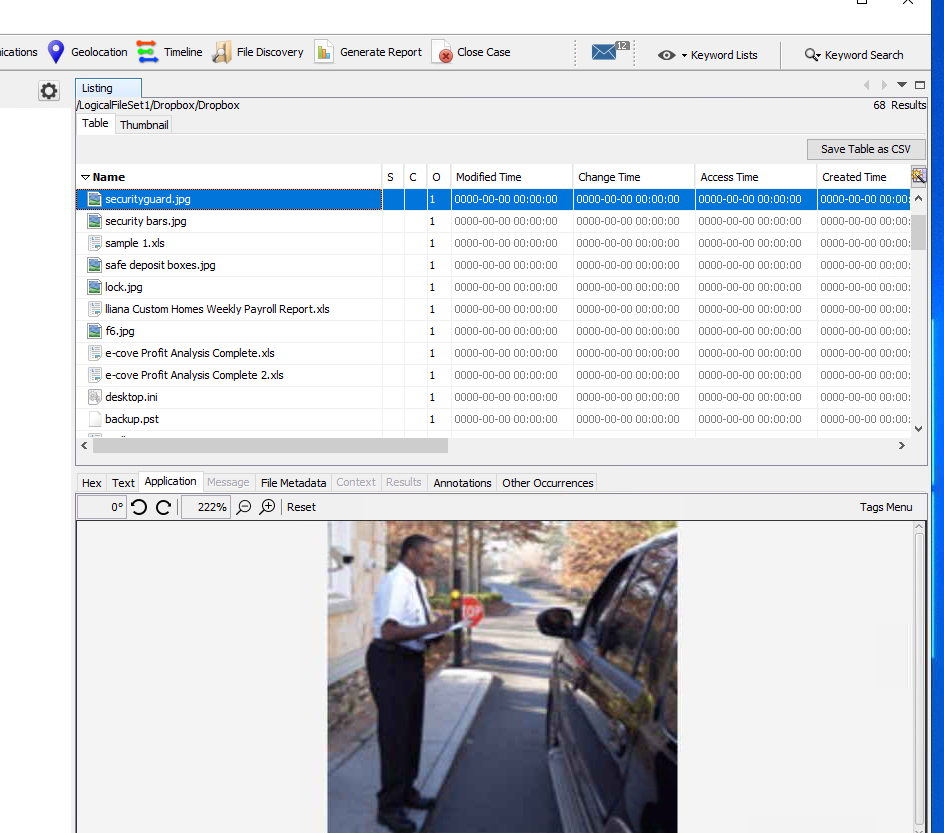


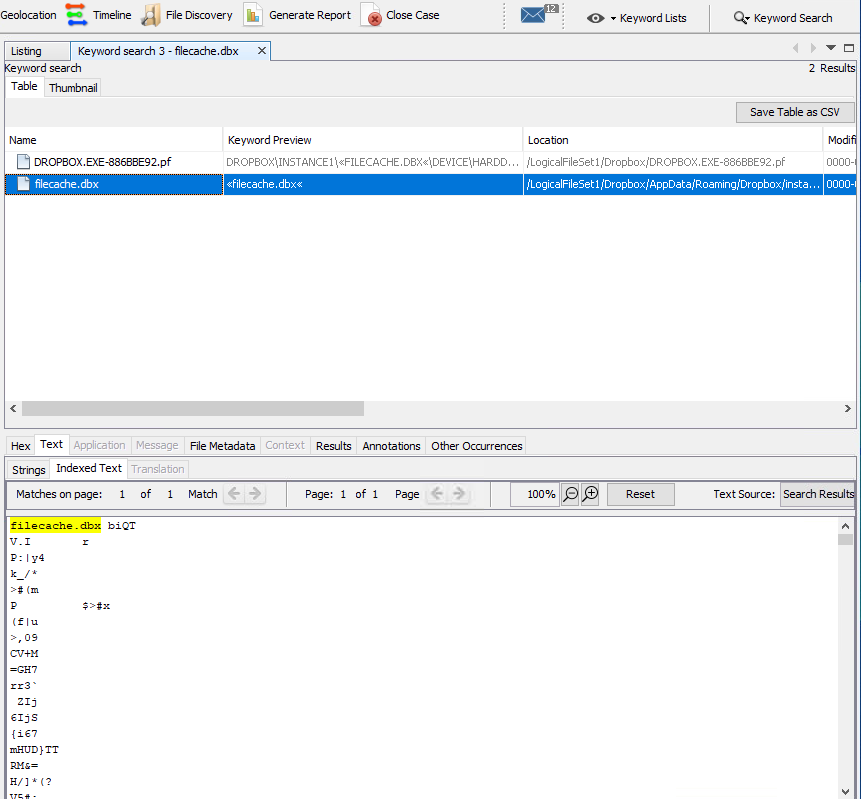
Lab 15:

I copied the drop box file from ch13 to the evidence folder and then started autopsy. I created a new case and called it C13Proj1. I added the source to the location of the drop box folder. I let autopsy scan the file and I use the keyword search function to search “users”. I clicked the DROPBOXINSTALLER.EXE-802BABAC.pf file and I can see the name Laurie in the lower pane. I used this information and searched for the keyword “Laurie” to see what information I could find on the user. I checked the files linked with cloud storage in the drop box folder under App data.









Lab 16:

I copied the OneDrive folder from the chapter 13 data files folder to my evidence folder and loaded the file up in Autopsy. I named the case/number C13Proj2 and put my initials in the examiners box and continued. I added the folder as a logical file source and searched for users as I did in lab 15. I clicked on the 42-f7a03bfblc86c703.ini file that was found in the right pane and viewed the username for the one drive account. I clicked keyword search again and searched for SyncDiagnostics.log.

And checked the table tab to see the metadata about the folder transactions associated with the OneDrive account.

