

## Lab 2: Data Acquisition and Basic Forensic Analysis

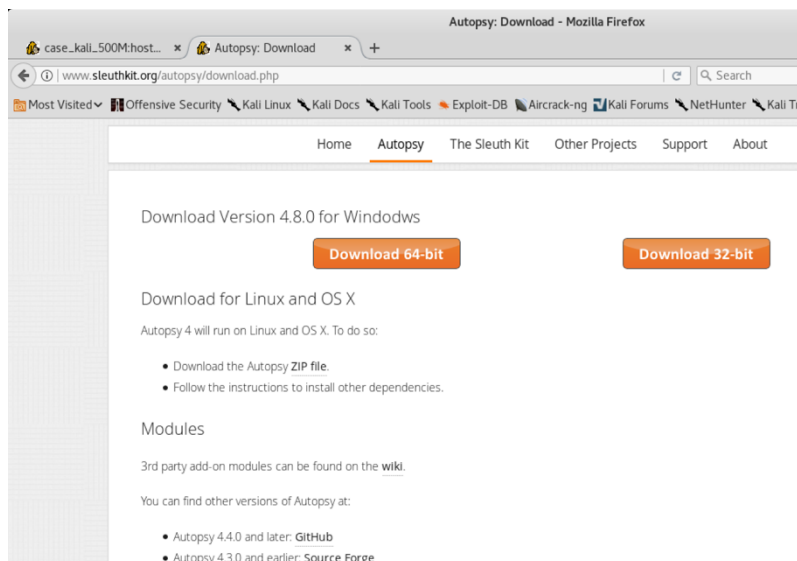
### Objectives

- Perform Data Acquisition using FTK imager and Linux dd, dcflddd commands
- Learn to use Windows version Autopsy
- Locate deleted/hidden files
- Perform a dirty word search
- Create a case report with any evidence you find
- Understand the difference between disk formatting in Windows and zero-out

### Tasks

#### Task 1. Software Preparation.

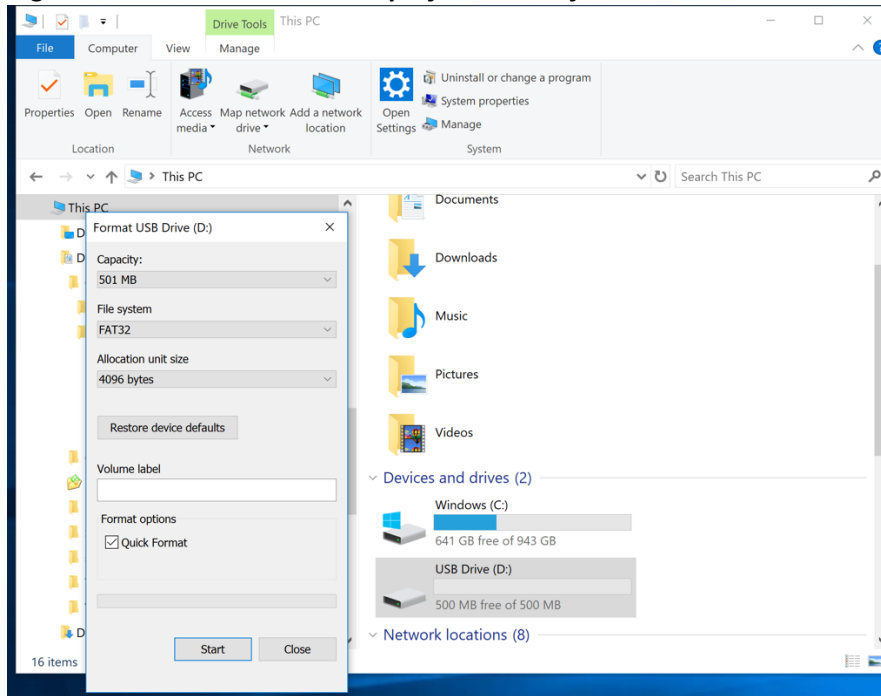
1. Download and Install FTK Imager on your windows machine. The download page for FTK Imager is  
<https://accessdata.com/product-download/ftk-imager-version-4.2.0>
2. Download and install Autopsy windows version on your windows machine. The download page for Autopsy is  
<https://www.sleuthkit.org/autopsy/download.php>



3. Install a CAINE or Kali Linux virtual machine following the instructions of our in-class activity 1. You may skip this step if you decide to use the lab machines in RVR2009 to perform the steps involving Linux.

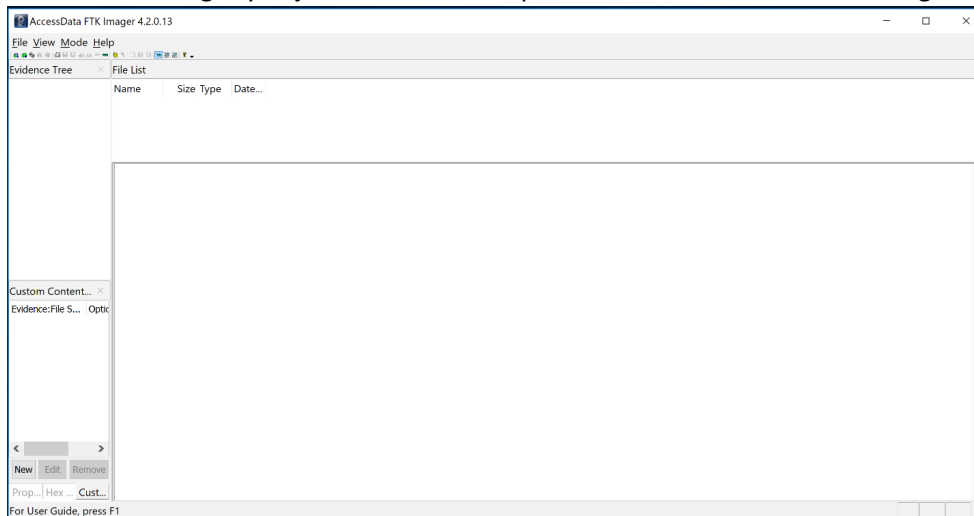
## Task 2. Prepare a suspect drive.

- Find a USB drive with the size of 500MB-2GB to work as the suspect drive.
- Connect the USB drive to your windows machine. Create a word file named “test.doc” (or “test.docx”) on the USB drive. Type a message into the file: “Life does not provide Warranties and Guarantees it only provides possibilities and opportunities for those who there to make best use of it!”
- Right click on the USB drive and **perform a disk format** towards the USB drive.

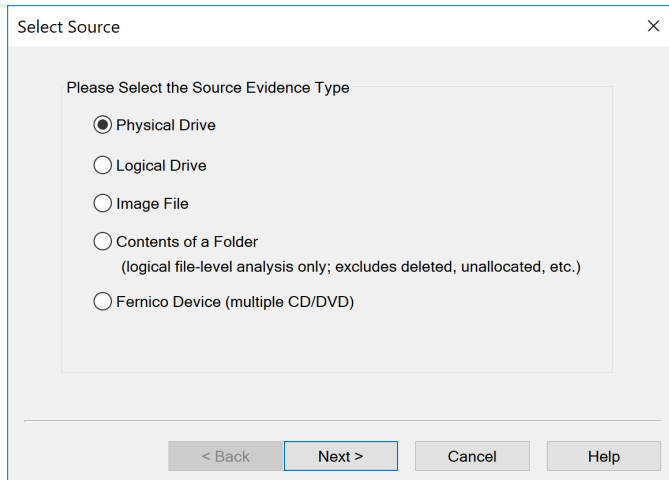


## Task 3. Perform a data acquisition with FTK Imager.

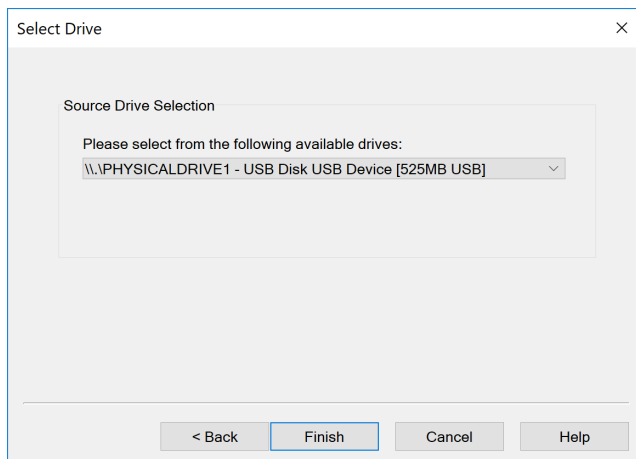
- Click on FTK Imager you just installed in Step 1. Choose File->Create Disk Image.



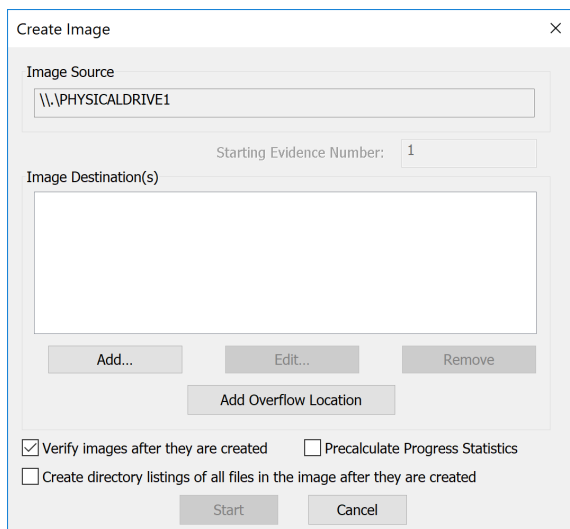
- In the Select Source dialog box, click the Physical Drive option, and then click Next.

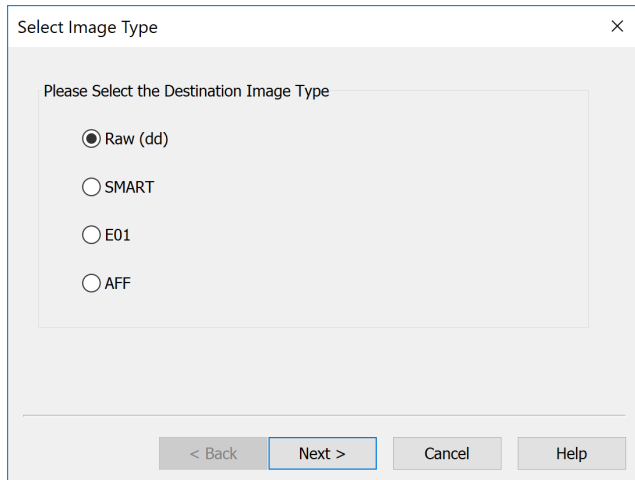


9. In the Select Drive dialog box, click the Source Drive Selection list arrow, click on suspect drive, and then click Finish.



10. In the Create Image dialog box, select “Verify images after they are created”, and then click “Add”. Then select “Raw” as the Destination Image Type.





Select Image Type

Please Select the Destination Image Type

☒ Raw (dd)

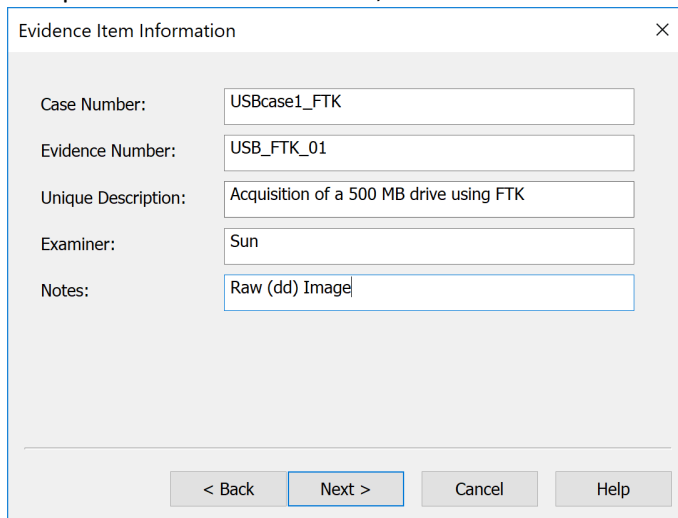
☐ SMART

☐ E01

☐ AFF

< Back   Next >   Cancel   Help

11. Complete the case information, and then click Next.



Evidence Item Information

Case Number: USBcase1\_FTK

Evidence Number: USB\_FTK\_01

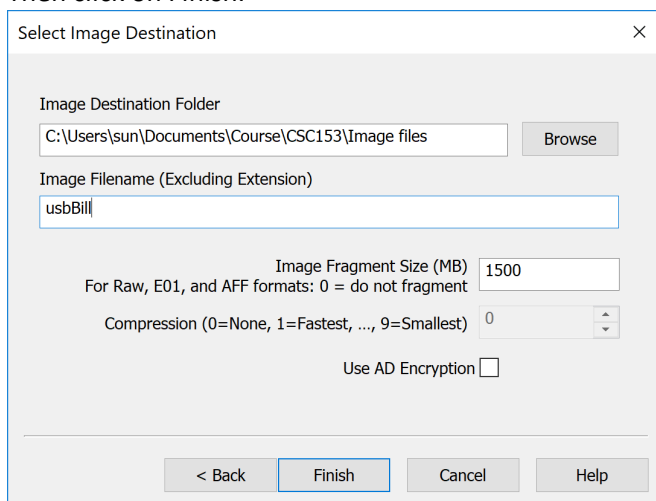
Unique Description: Acquisition of a 500 MB drive using FTK

Examiner: Sun

Notes: Raw (dd) Image

< Back   Next >   Cancel   Help

12. In the Select Image Destination dialog box, click Browse and specify the location you want to store the image. Type in the Image Filename. Click to clear the Use AD Encryption check box. Then click on Finish.



Select Image Destination

Image Destination Folder

C:\Users\sun\Documents\Course\CSC153\Image files   Browse

Image Filename (Excluding Extension)

usbBill

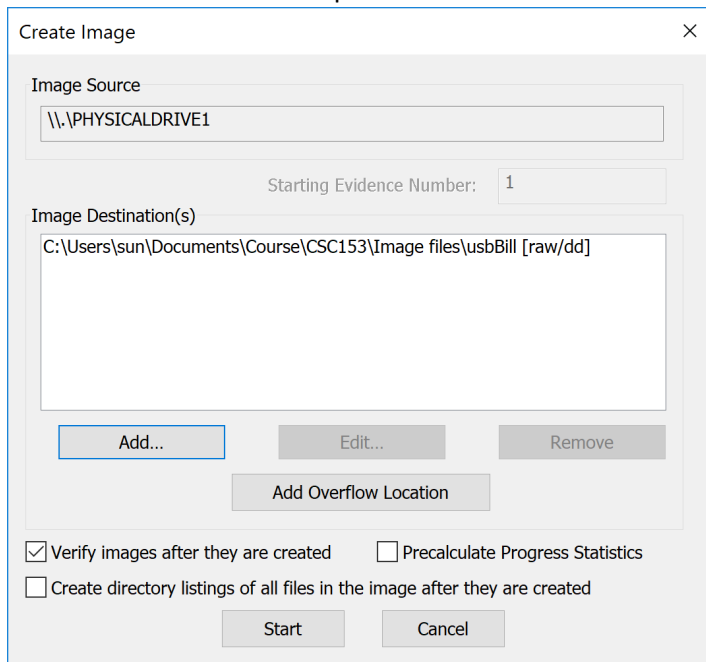
Image Fragment Size (MB) 1500  
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 0

Use AD Encryption ☐

< Back   Finish   Cancel   Help

13. Click start to initiate the acquisition.



The 'Create Image' dialog box is shown. It has a title bar with a close button. The 'Image Source' field contains '\\.\PHYSICALDRIVE1'. The 'Starting Evidence Number' is set to 1. The 'Image Destination(s)' list contains 'C:\Users\sun\Documents\Course\CSC153\Image files\usbBill [raw/dd]'. Below the list are buttons for 'Add...', 'Edit...', and 'Remove'. There is also an 'Add Overflow Location' button. At the bottom, there are three checkboxes: 'Verify images after they are created' (checked), 'Precalculate Progress Statistics' (unchecked), and 'Create directory listings of all files in the image after they are created' (unchecked). 'Start' and 'Cancel' buttons are at the bottom right.

Create Image

Image Source  
\\.\PHYSICALDRIVE1

Starting Evidence Number: 1

Image Destination(s)  
C:\Users\sun\Documents\Course\CSC153\Image files\usbBill [raw/dd]

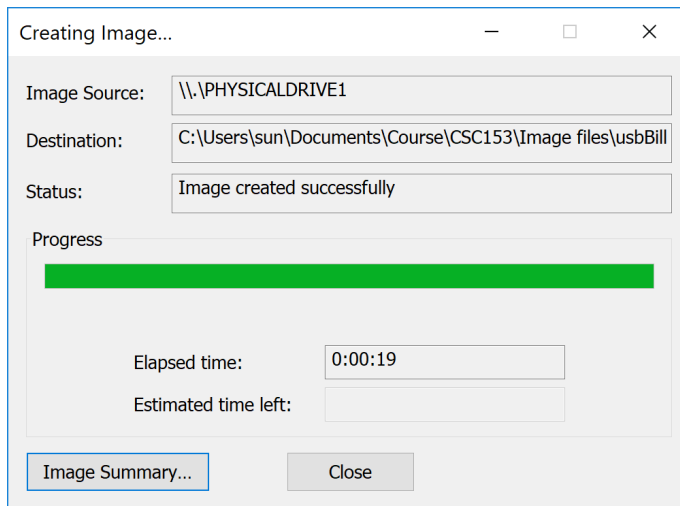
Add... Edit... Remove

Add Overflow Location

☒ Verify images after they are created ☐ Precalculate Progress Statistics  
☐ Create directory listings of all files in the image after they are created

Start Cancel

14. Review the information in the Drive/Image Verify Results dialog box, and then click Close. Close again in the Creating Image dialog box.



The 'Creating Image...' dialog box is shown. It has a title bar with minimize, maximize, and close buttons. The 'Image Source' field contains '\\.\PHYSICALDRIVE1'. The 'Destination' field contains 'C:\Users\sun\Documents\Course\CSC153\Image files\usbBill'. The 'Status' field contains 'Image created successfully'. Below this is a 'Progress' section with a green progress bar. At the bottom, there are fields for 'Elapsed time' (0:00:19) and 'Estimated time left'. At the very bottom are 'Image Summary...' and 'Close' buttons.

Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\sun\Documents\Course\CSC153\Image files\usbBill

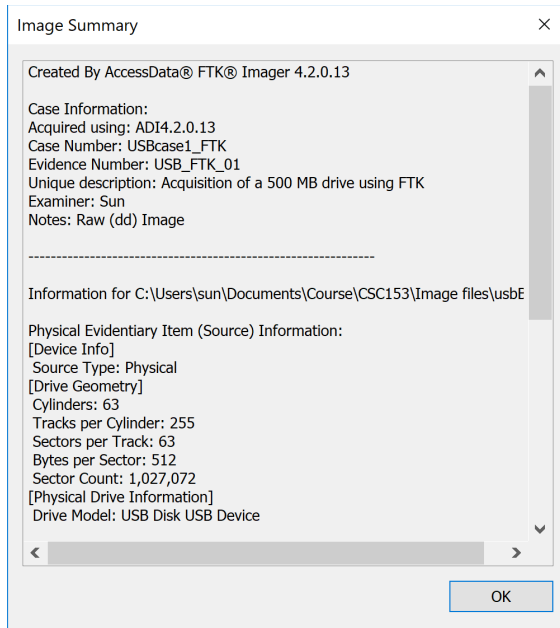
Status: Image created successfully

Progress

Elapsed time: 0:00:19

Estimated time left:

Image Summary... Close

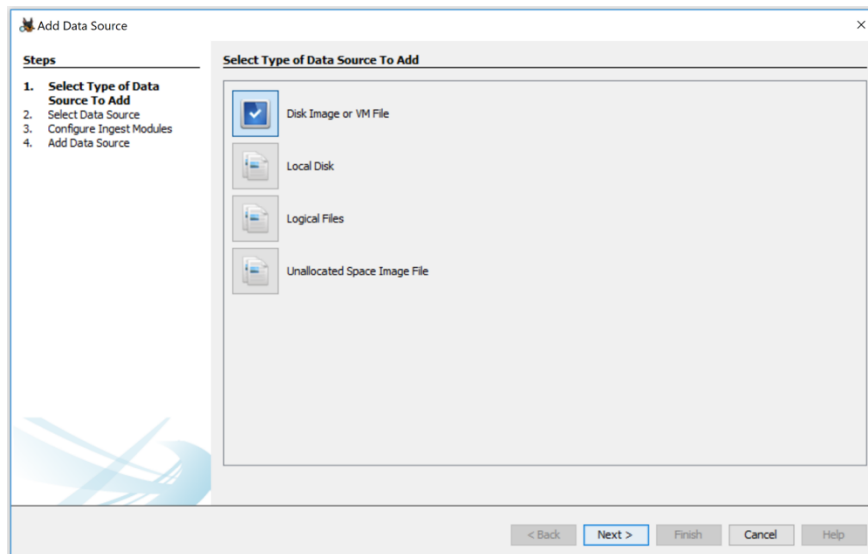


#### Task 4. Perform a data acquisition with Linux dd/dcfldd command.

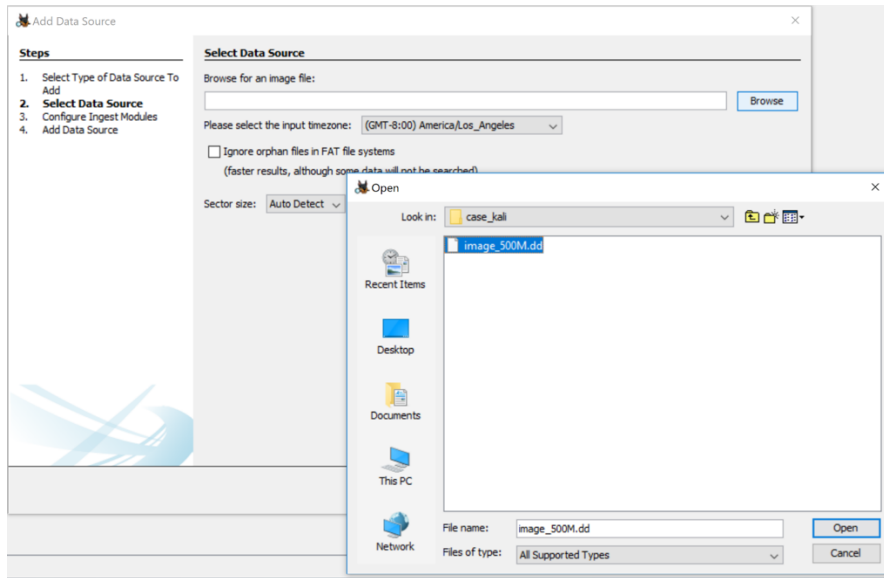
15. Open the CAINE or Kali Linux virtual machine, follow the instructions of in-class activity 3 to perform data acquisition of the USB drive using Linux dd/dcfldd commands.

#### Task 5. Analyze the acquired data.

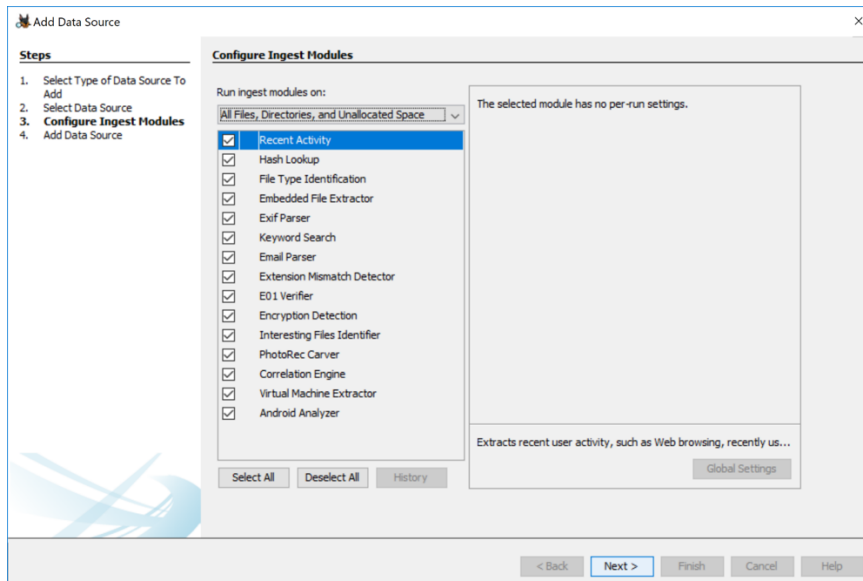
16. Open Windows version Autopsy that you installed in Task 1.
17. Create a new case and add the image by choosing Disk Image or VM File.



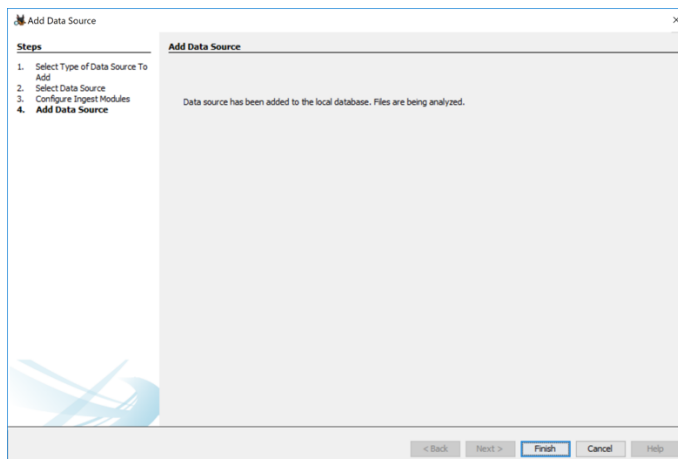
18. Choose the raw image you acquired in step 15.



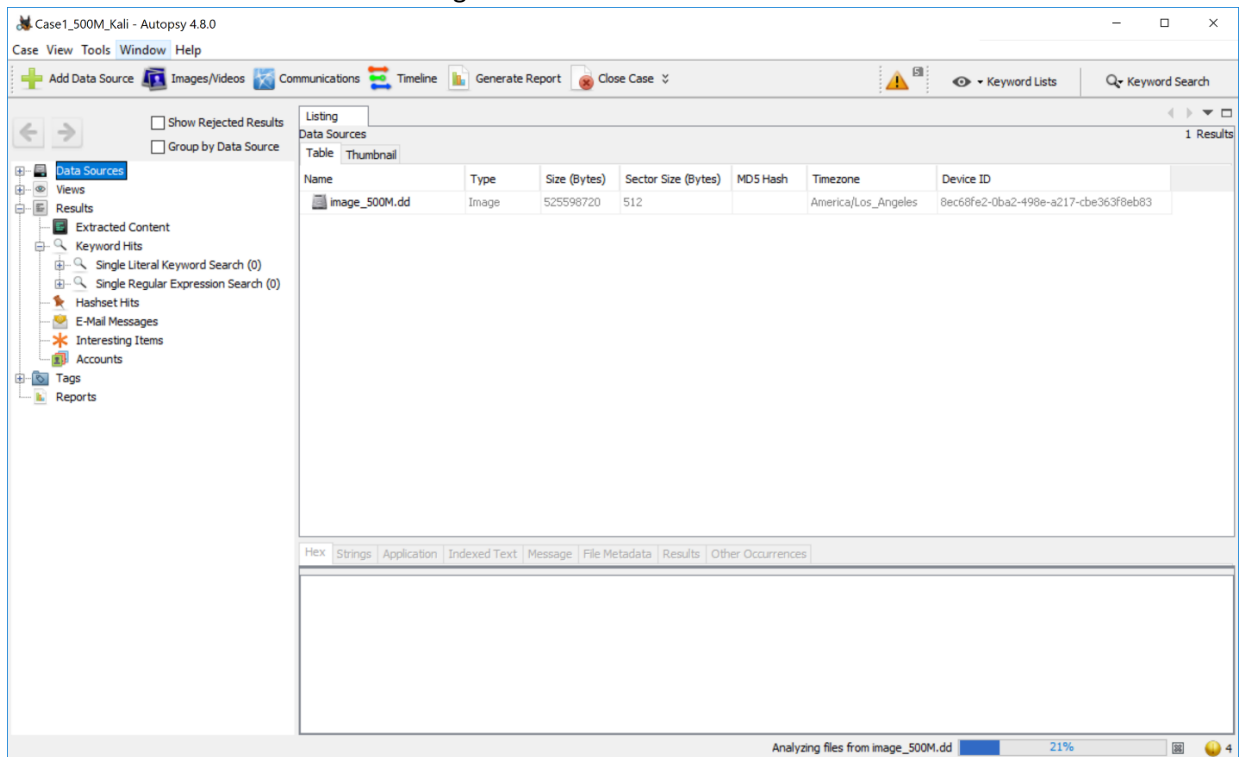
19. Select all, and click on Next.



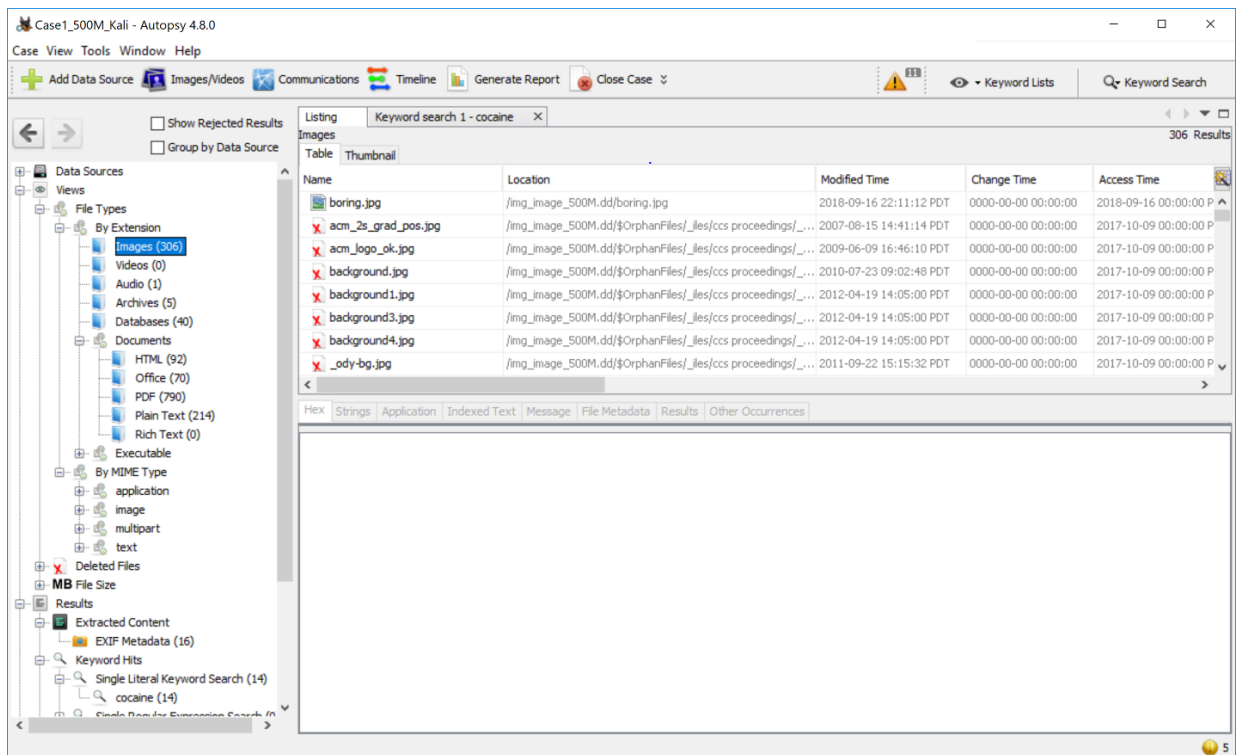
20. Click on Finish.



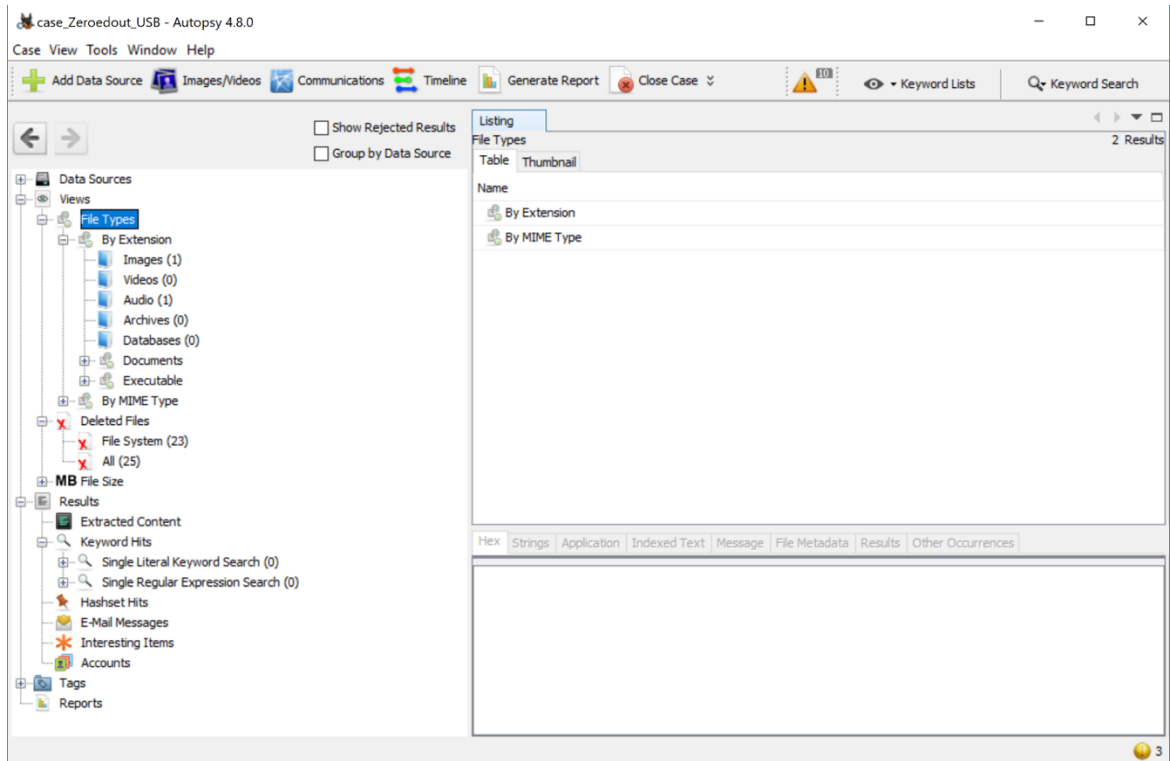
21. Click on Data Sources to view the image.



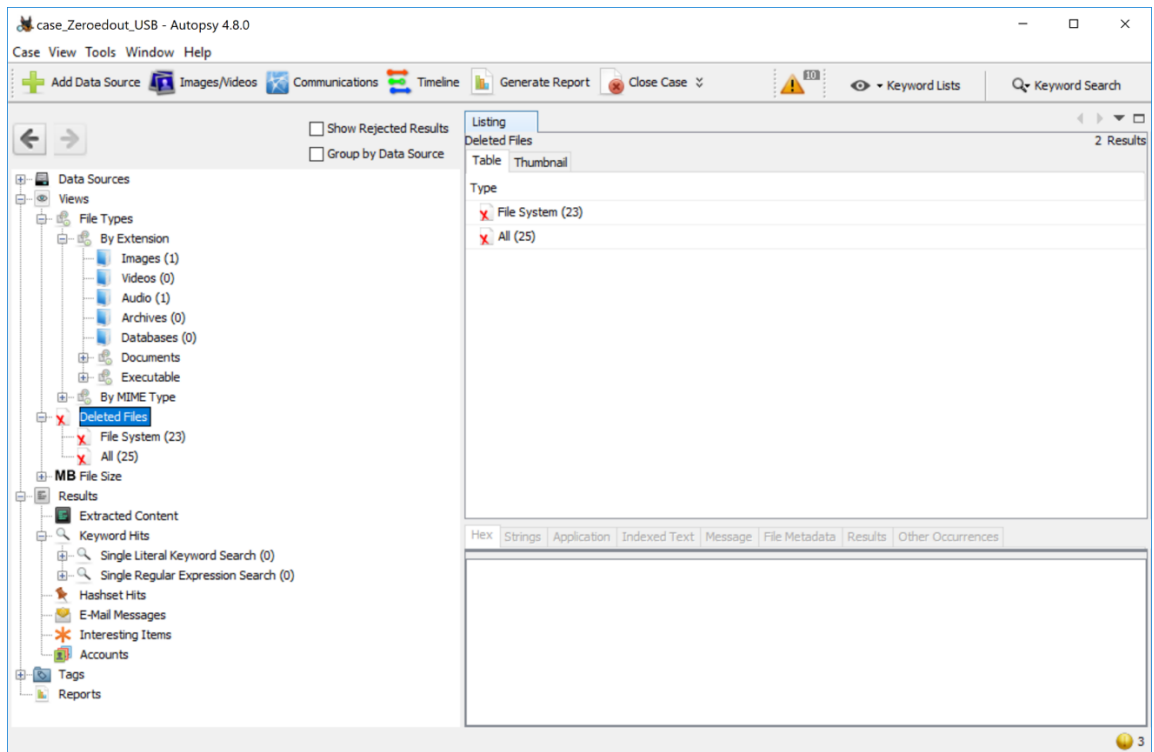
22. Click on the tabs under “Views” to check the files on this USB drive.





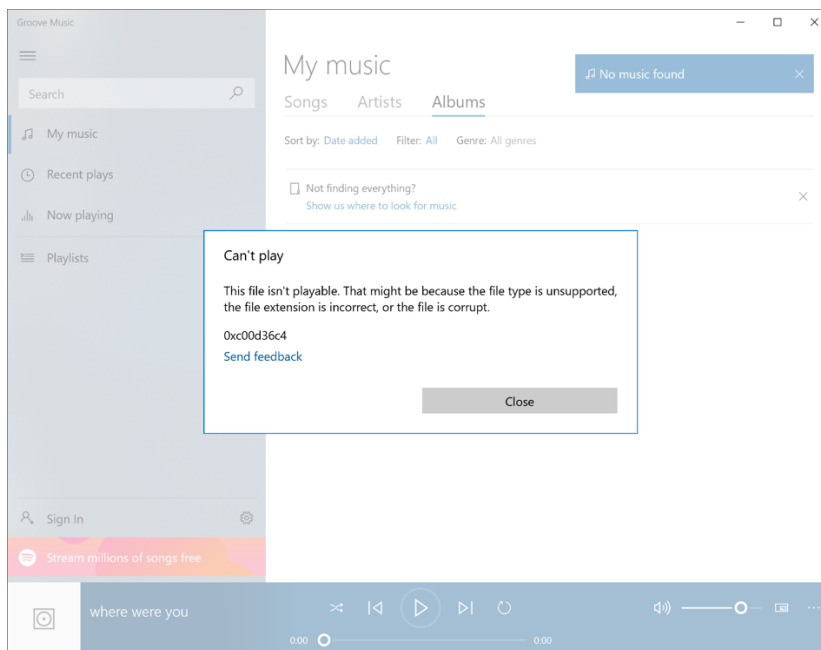
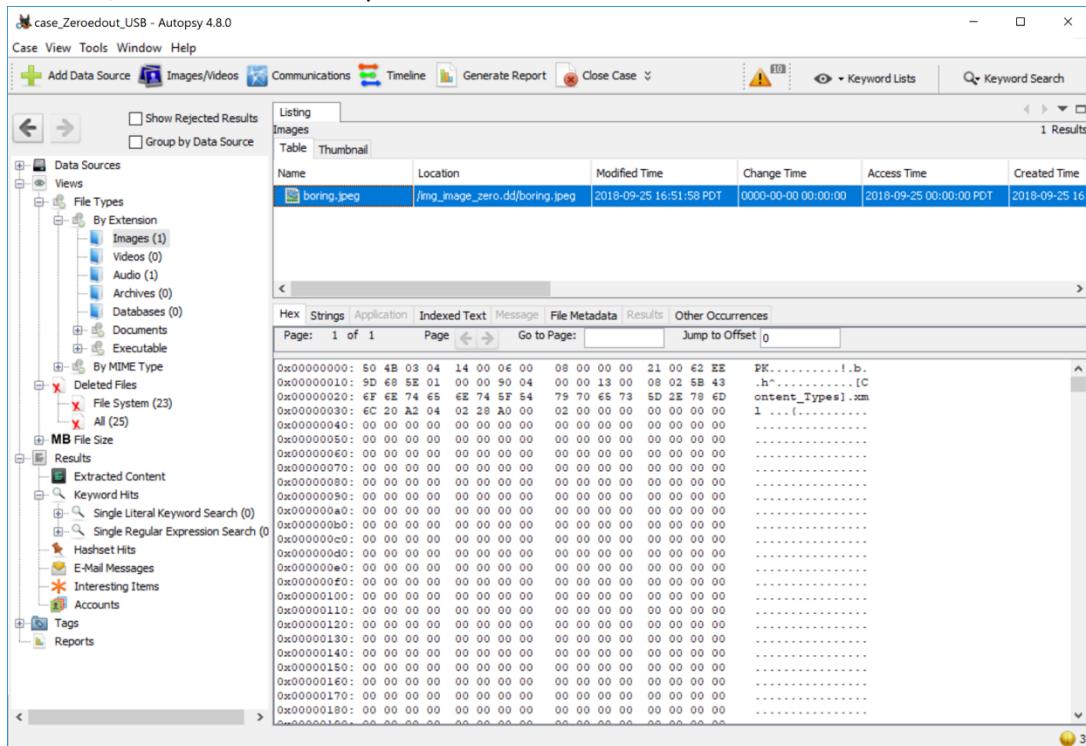


23. Click on deleted files to see the deleted files.



24. You may check the content for each file by clicking on that file. You can also *download* a file by right-click on the file, choose “Extract file”, and then save it to a directory. You can then try to

view the file on your machine. For example, I tried to open the “where were you.mp3” file in my machine, but found I cannot open it.



**Task 6. Perform a dirty word search.**

25. A dirty word search is a search through all of the bytes in the image looking for specific strings or words. Look at the information listed in the case summary, and consider what words a suspect might use. This search takes some time. Normally a forensic analyst would have a long list of dirty words ready. For demonstration, in this lab just use the “**Warranties**” as the key word.
26. Click on the “Keyword Search” button.
27. Ensure ASCII, and Case Insensitive are selected. Type in a dirty word from your list. Click the “Search” button.
28. When you get a hit, make a note of the sector the hit was in. You will be able to determine what file the hit was located in by comparing the sector the word was found in with the sectors listed in the file reports you made during the file analysis.

**Task 7. Zero-out the suspect USB drive.**

29. Connect the same suspect USB drive you used in this lab to the CAINE/Kali Linux again. ***Zero-out the suspect drive by following the instructions in our In-class Activity 3. This step is very important. Please don't skip this step.***

**Task 8. Repeat Task 4-6.**

30. Repeat the activities 4-6 towards the zeroed-out USB drive.

**Task 9. Answer the questions. *Please attach screenshots to prove your answers when necessary.***

1. In Task 4, the acquired image has an extension of “.dd”. In Task 3, what is the extension for the image file?
2. In Task 5, how many files are there on the USB drive? What are they? *Please attach screenshots to prove your answer.*
3. In Task 5, which file/files are deleted? *Please attach screenshots to prove your answer.*
4. In Task 6, are you able to find any hit when you search “**Warranties**” as the key word? In which file is the key word located? *Please attach screenshots to prove your answer.*
5. In Task 8, how many files are there on the USB drive? What are they? *Please attach screenshots to prove your answer.*
6. In Task 2, you performed a “disk format” operation towards the USB drive. Did this operation completely erase the “test.doc” (or “test.docx”) file in the USB drive? How do you know? *Please provide a screenshot to prove your answer.*
7. In Task 7, you performed a “zero out” operation towards the USB drive. Did this operation completely erase the “test.doc” (or “test.docx”) file in the USB drive? How do you know? *Please provide a screenshot to prove your answer.*
8. Did you have any surprise in Task 5? Did you see any other files other than “test.doc” or “test.docx”? *Please provide a screenshot to prove your answer.*
9. In Task 8, did you see any other files other than “test.doc” or “test.docx”? *Please provide a screenshot to prove your answer.*
10. To summarize the questions above, what are the difference between disk formatting in Windows and the zero-out operation?

## Write a Forensic Report

You should have the following parts:

A forensic report is ***a step by step list of everything you have done and what the results were***. You don't need to actually list all of the failed attempts or crowd it with non-relevant facts. Keep it accurate, relevant and simple.

***You should also address the questions in Task 9.***

**Finally, you need to submit the report to Canvas in PDF format.**