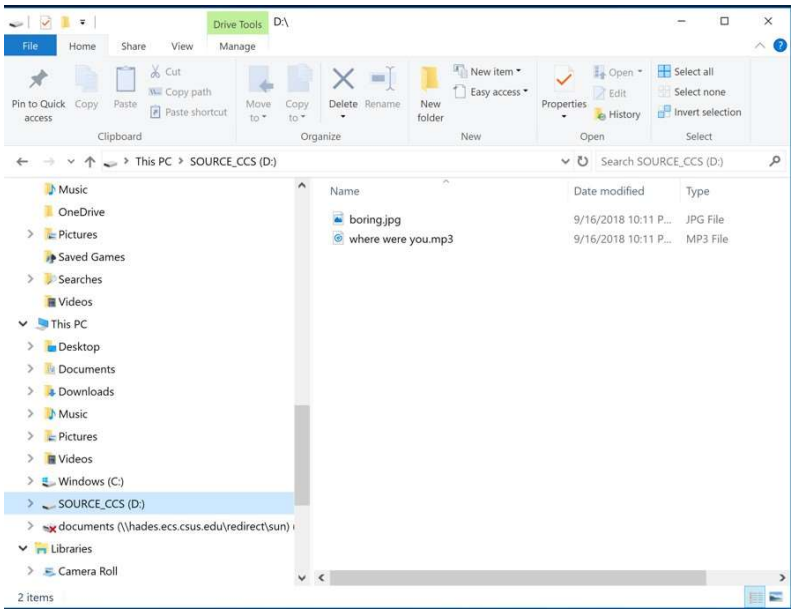
Worcester Polytechnic Institute
Department of Computer Science

Activity 4: Basic Forensic Analysis using Autopsy

Scenario

Last week University police arrested a student, Billy Badguy, for selling cocaine. During the pursuit the student threw a USB drive into a storm drain. The Office of the Physical Plant (OPP) was contacted and they were able to recover the USB drive. The Police department has asked you to perform a forensic analysis on this USB drive. You have created an image and left it on your desktop.

When you open the USB with your own machine, you'll see that only two files are shown in the USB: boring.jpg and where were you.mp3. Your task is to reveal more information by analyzing the image.



Objectives

- Create a case in Autopsy.
- Analyze data in an evidence image
- Locate deleted/hidden files
- Create a case report with any evidence you find.

Tasks

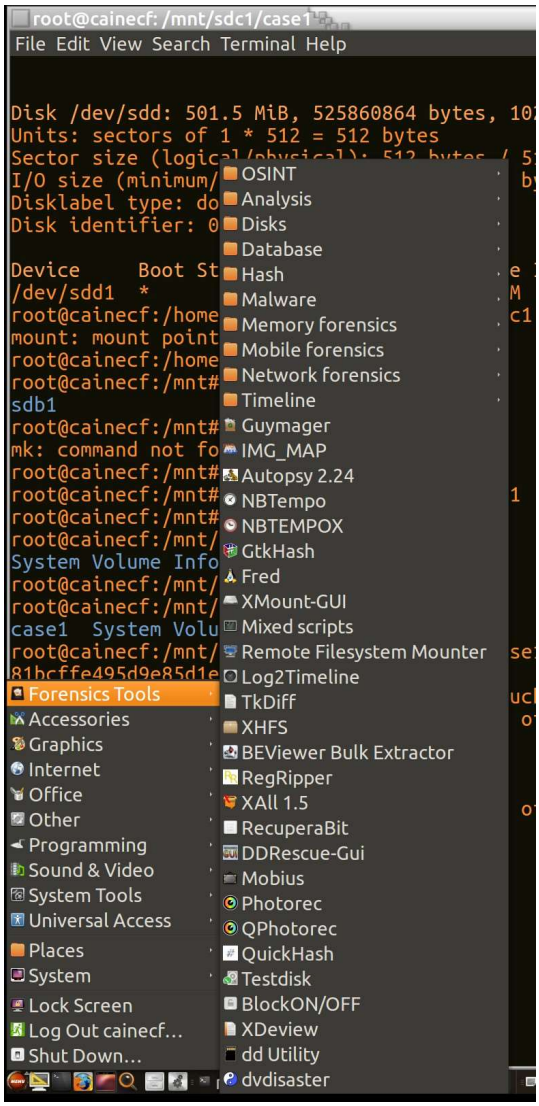
Task 0. Download the image of suspect's drive.

1. On the virtual machine where you'll conduct the investigation, download image of the suspect's USB drive from the link below (The file name is image_zero.dd).

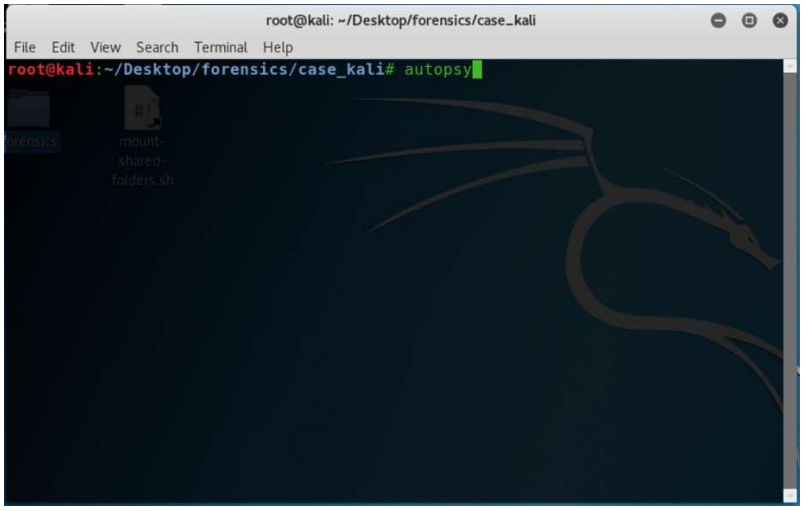
   https://drive.google.com/open?id=1xP8ufHByg_zE_8zYzvAn9d0c9UWrunEr

Task 1. Create a new case.

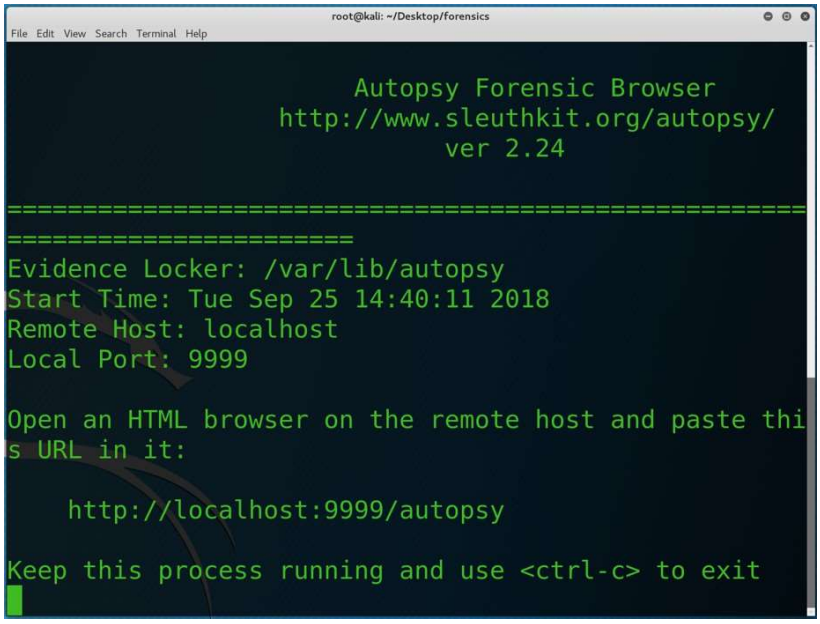
2. Open vmware and log onto the virtual machine.
3. Open autopsy. Click on Main->Forensics Tools->Analysis->Autopsy.



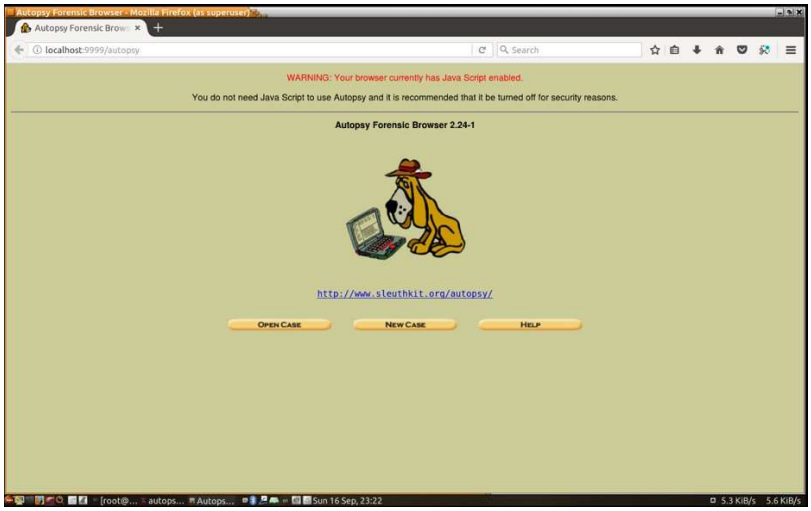
If you work in Kali Linux, you can simply type "autopsy" in command line.



Then it will show the instruction of starting autopsy in the web browser. Open a web browser and type http://localhost:9999/autopsy in the address bar.

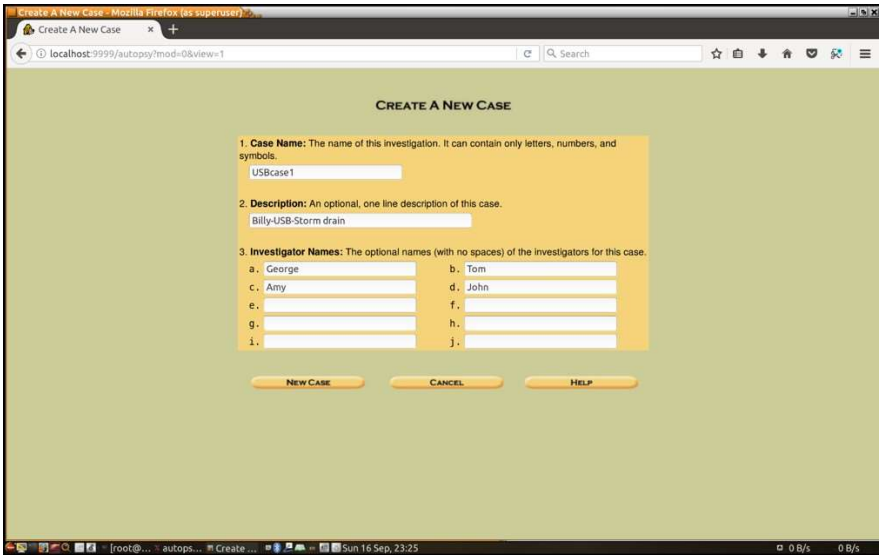


4. Click on the “New Case” button.

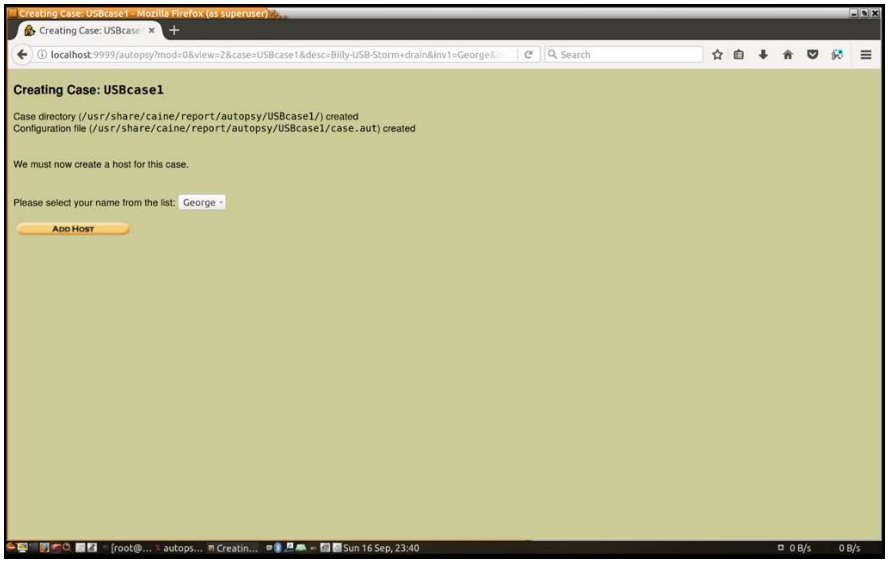


5. Fill in the fields as follows:
   - **a.** "Case Name" – Type: **USBcase1**
   - **b.** "Description" - Add a short sentence describing the case. Reread the scenario at the beginning of this document for help with your short description.
   - **c.** "Investigator Names" - Type in your name and the names of the members of your team.

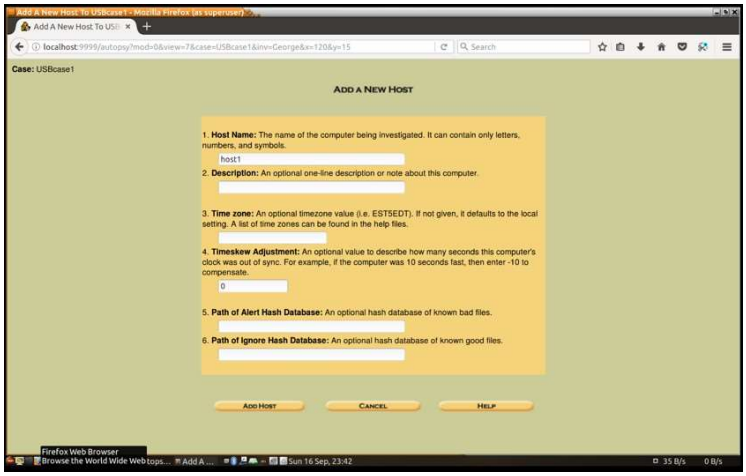
   Click the "New Case" button.



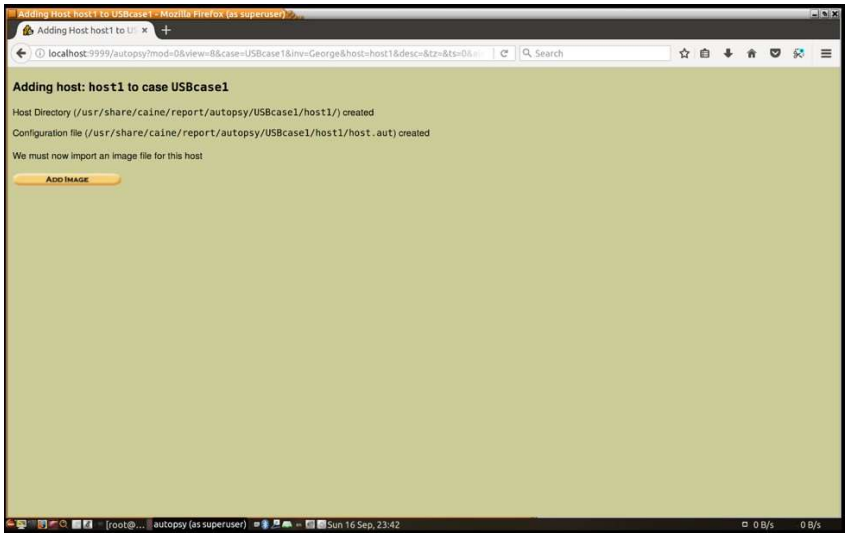
6. Leave the default and click the "Add Host" button at the bottom.



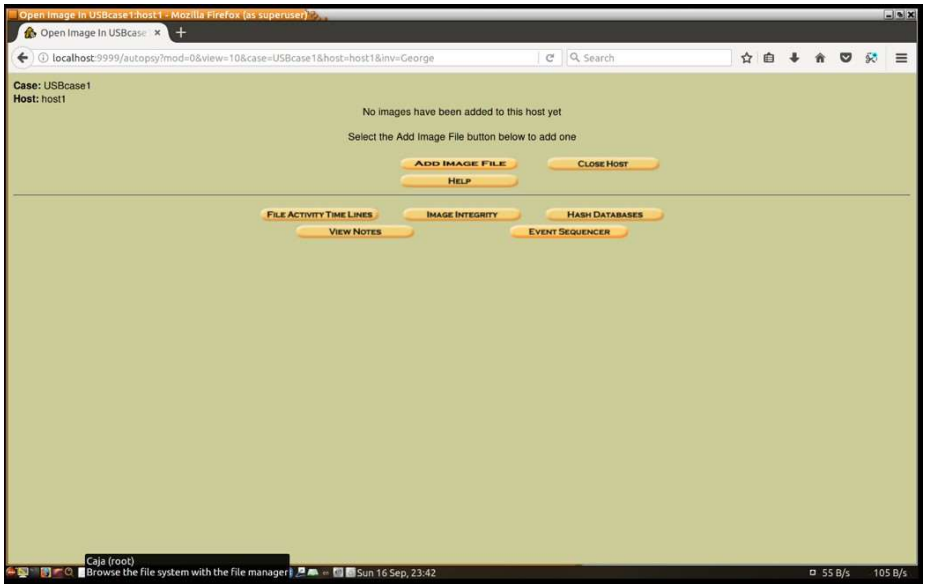
7. Click another “Add Host” button.



8. Click “Add Image.”

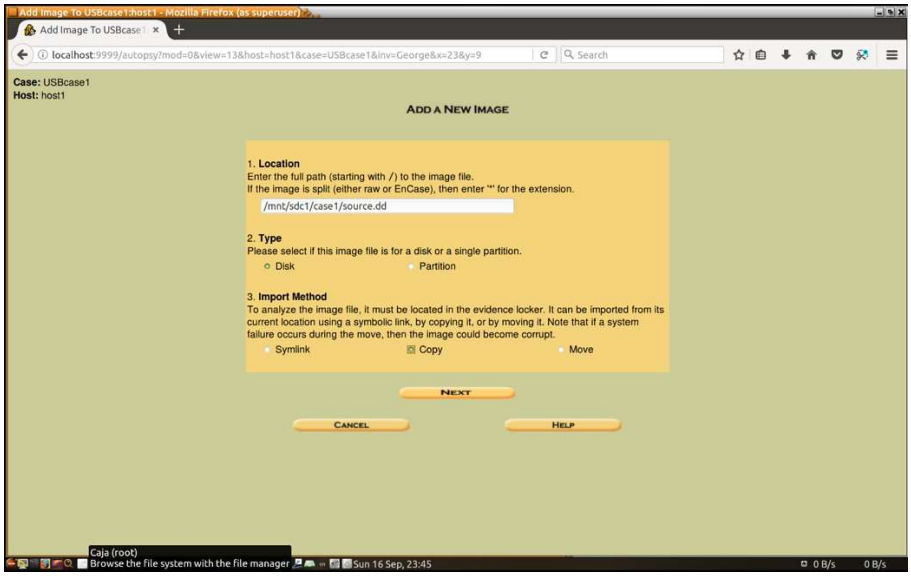


9. Click “Add Image File.”

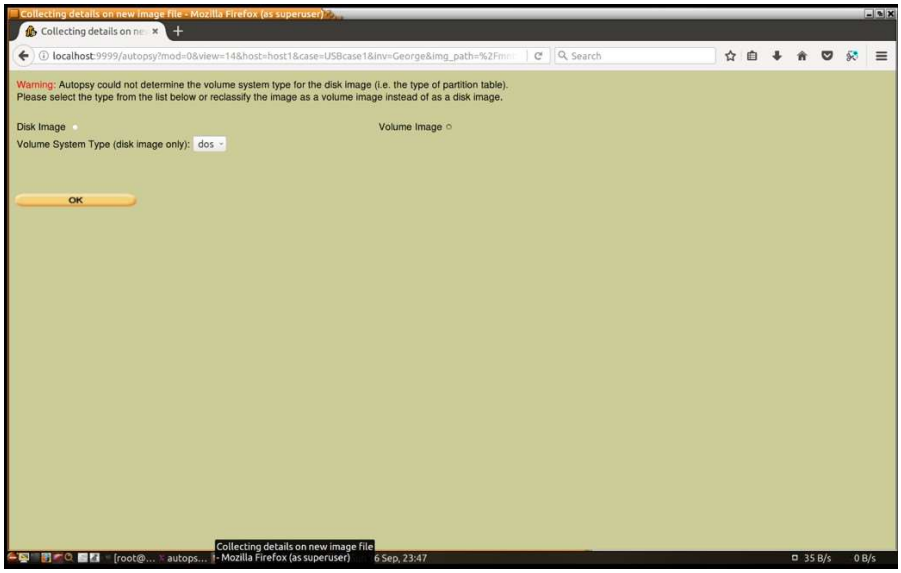


10. Fill in the fields in the “Add a New Image” screen.”
    a. “Location” Type /mnt/sdc1/case1/source.dd (***Please note: here you need to locate the source drive and provide the correct directory information***)
    b. “Import Method” select copy.

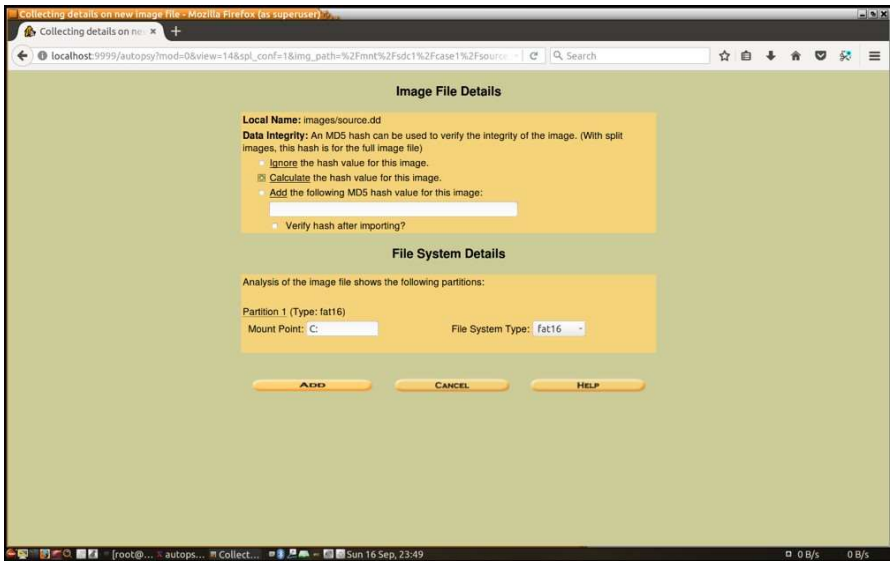
    Click “Next.”



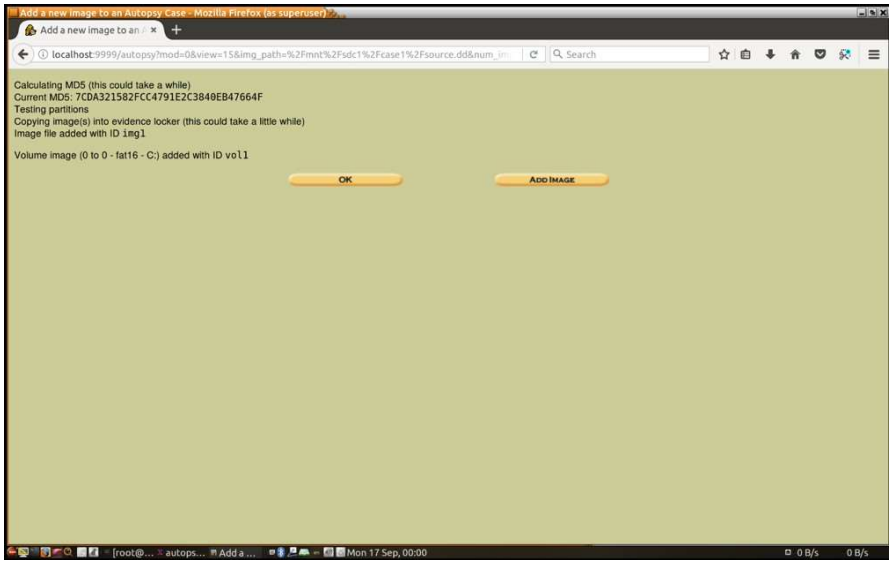
11. Select “Volume Image” on the right, ensure the “dos” is selected in the drop down of “Volume System Type”. Click “OK.”



12. Select “Calculate” under the topic, “Data Integrity” and check “Verify hash after importing”. Click the “Add” button.

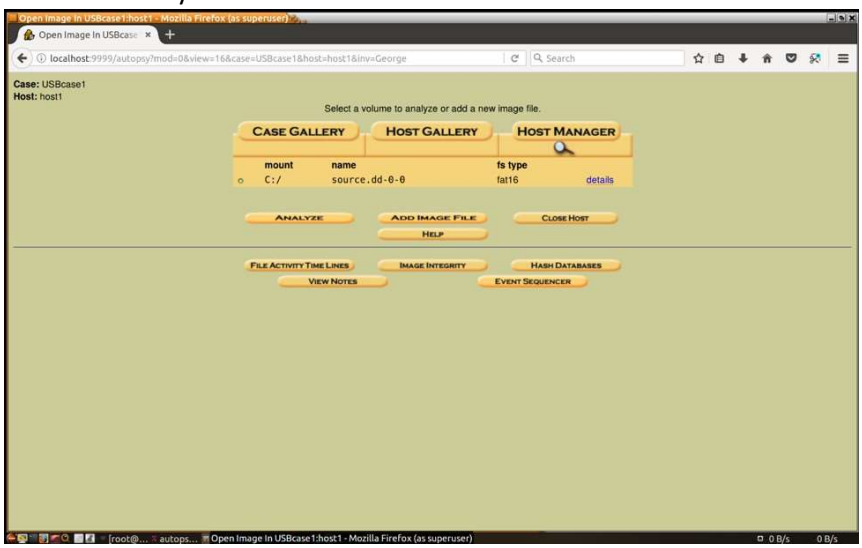


13. Once the calculations are done, click the “OK” button.

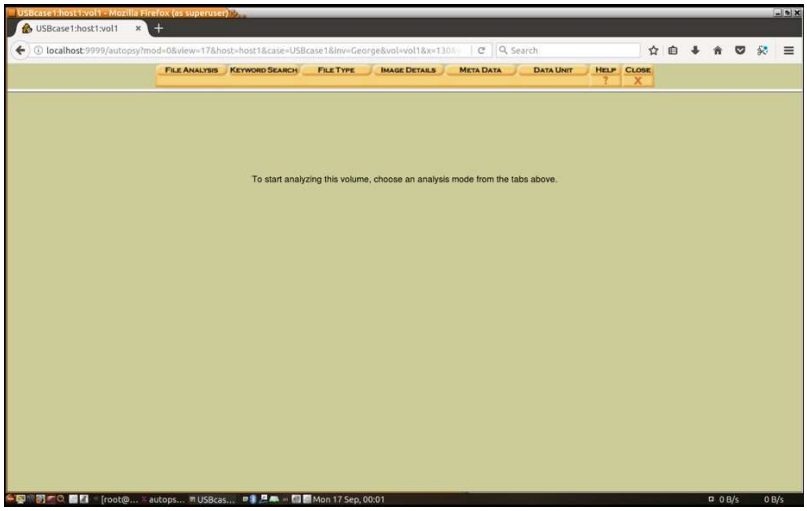


Task 2. Locate deleted/hidden files

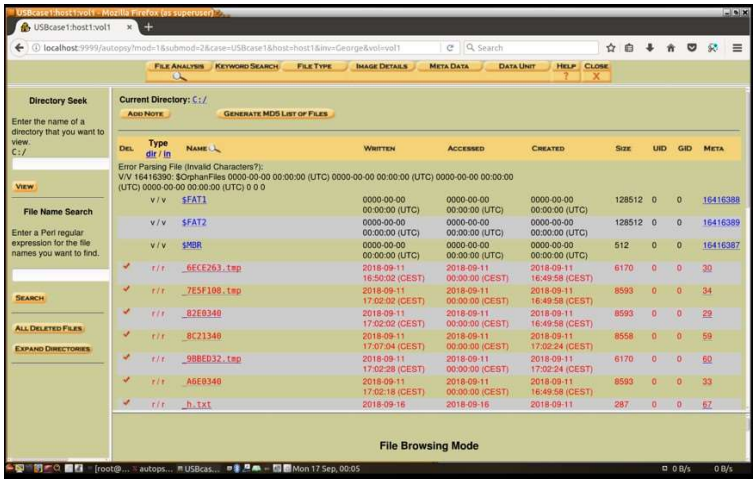
14. Click the “Analyze” button.



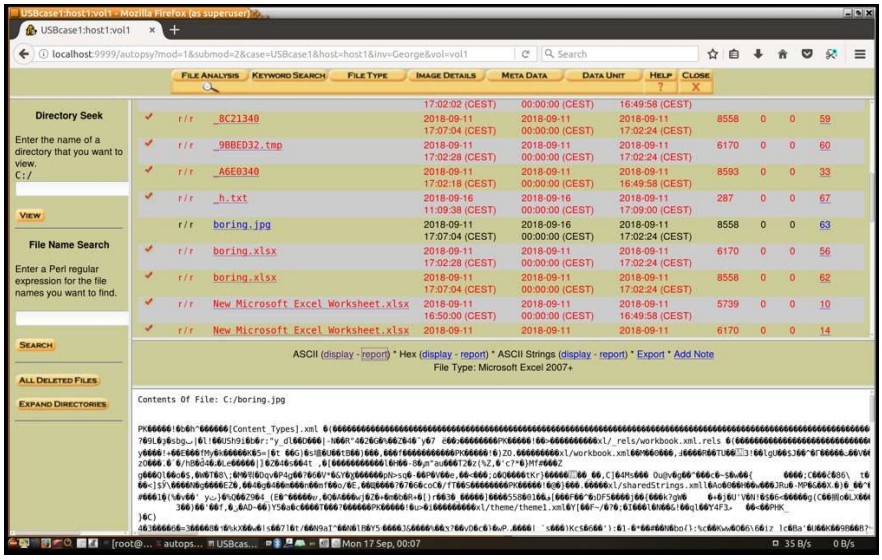
15. Select “File Analysis”.

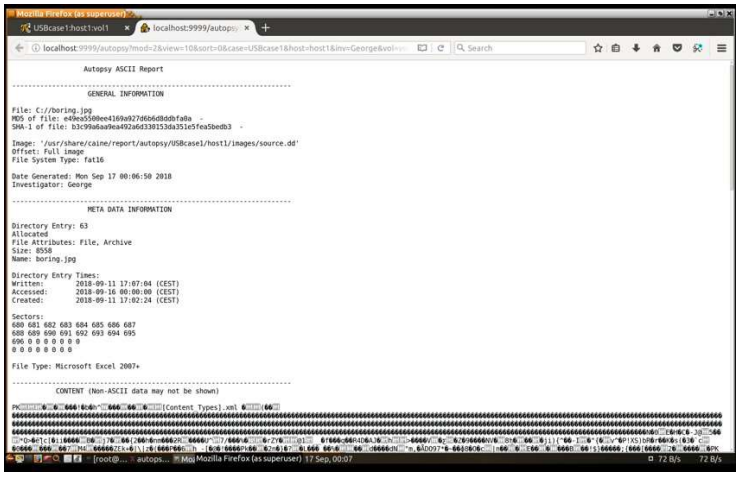


16. The files labeled in red are the deleted files. They also are the ones with a checkmark under the DEL to the left of the filename.
    a. Click on the files and examine them in the window below.

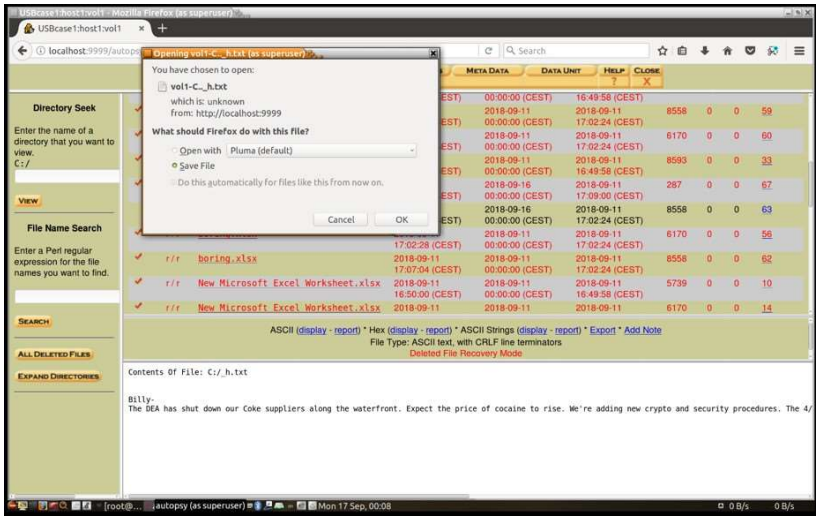


    b. If data appears, click report next to ASCII and get a screenshot of the report to use in your report later. (Clicking on “display” does not give you the report. You must click on the word “report”.) “X” out of this tab.





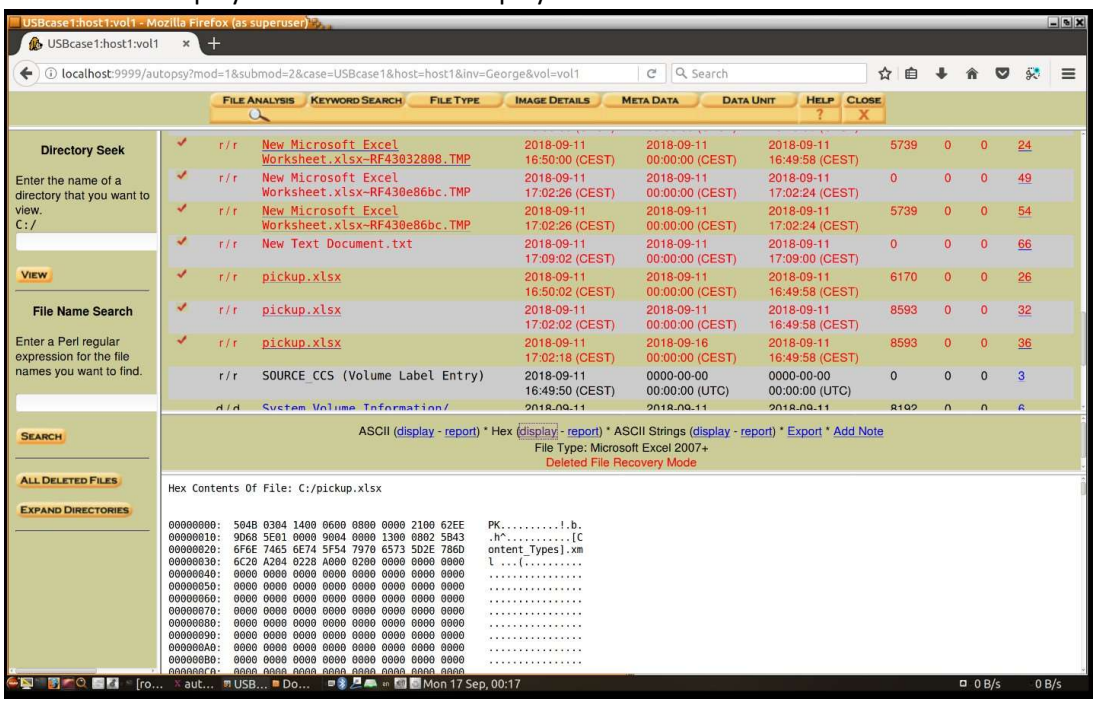
c. Then click “Export” to export the file from the image to the Downloads folder.



d. Once the files are saved outside the image open them and get a screen shot of the data in the file for your report to the police.

e. For the files you've downloaded, are you able to open it? If yes, what's the content? If no, why?

17. Click on the "display" in the Hex tab to display the file in hex.



18. Follow the same procedure for the files listed in blue. These are files that exist openly on the drive. If the file does not work when you open it, examine the "magic number" as seen in the magic number chart (see Appendix) to ensure that the file is labeled correctly. The Magic Number is the first few bytes as seen in hex. A file that has been mislabeled won't open properly but can still hold data uncorrupted. The magic number can be seen in Autopsy if you examine the file in hex. It will be the first few bytes. For a magic number that is not included in the Magic Number Chart, simply google it.

Task 3. Complete the report and answer the questions.

Note: 1) Please provide at least 5 screenshots with proper narratives to document the most important steps of your hands-on activity. 2) Answer questions below and attach screenshots necessary to prove your answers. **Submit your report to Canvas in PDF format.**

1. How many files are there on the USB drive? What are they? (Take a screenshot for the files.)
2. Which file/files are deleted? (Take a screenshot of the deleted files.)
3. Can you open the boring.jpg file with an image viewer? Why? How did you open it eventually? (Take a screenshot of the file content)
4. Were there any secret messages? If so, in which file are they located? (Take a screenshot of the secret message)
5. What is the name of Billy's supplier? (Take a screenshot to prove the answer)

6. When and where is the next meet? (Take a screenshot to prove the answer)
7. Who else on campus is involved? (Take a screenshot to prove the answer)

Appendix: Magic Number Chart

Here are a few magic numbers, These are of image files.

File type	Typical extension	Hex digits xx = variable	Ascii digits . = not an ascii char
Bitmap format	.bmp	42 4d	BM
Office2007 Documents	.xlsx	50 4B 03 04 14 00 06 00	PK
GIF Format	.gif	47 49 46 38	GIF8
MP3	.mp3	49 44 33	ID3
PDF	.PDF	25 50 44 46	%PDF
JPEG File Interchange Format	.jpg	ff d8 ff e0	....
NIFF (Navy TIFF)	.nif	49 49 4e 31	IIN1
PM format	.pm	56 49 45 57	VIEW
PNG format	.png	89 50 4e 47	.PNG
Postscript format	.[e]ps	25 21	%!
Sun Rasterfile	.ras	59 a6 6a 95	Y.j.
Targa format	.tga	xx xx xx	...
TIFF format (Motorola - big endian)	.tif	4d 4d 00 2a	MM.*
TIFF format (Intel - little endian)	.tif	49 49 2a 00	II*.
X11 Bitmap format	.xbm	xx xx	
XCF Gimp file structure	.xcf	67 69 6d 70 20 78 63 66 20 76	gimp xcf
Xfig format	.fig	23 46 49 47	#FIG