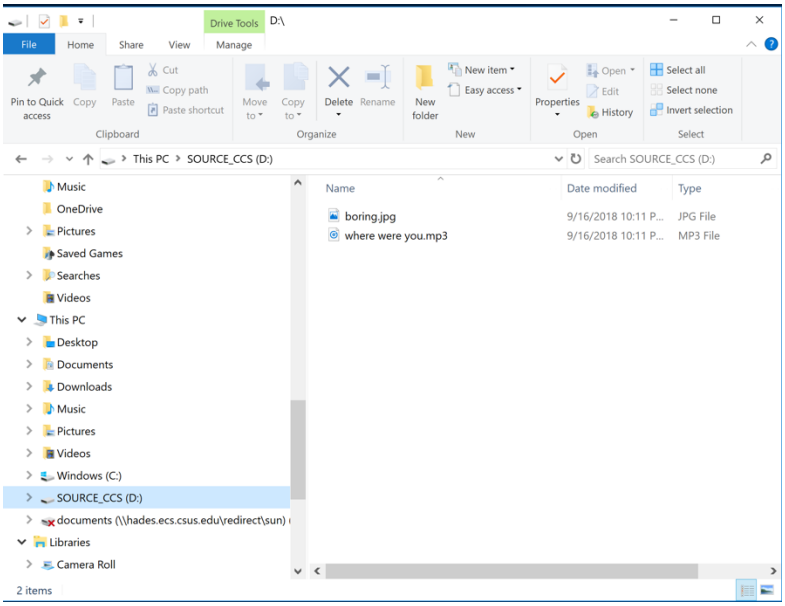
Worcester Polytechnic Institute
Department of Computer Science

Module 4: Analysis of File Headers 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

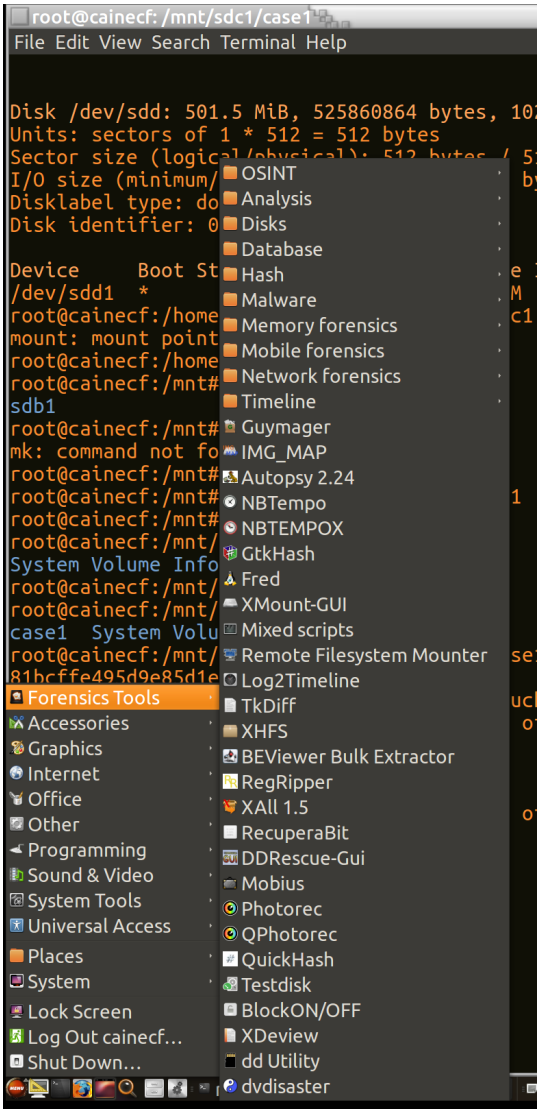
Task 0. Download the image of suspect's drive.

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).

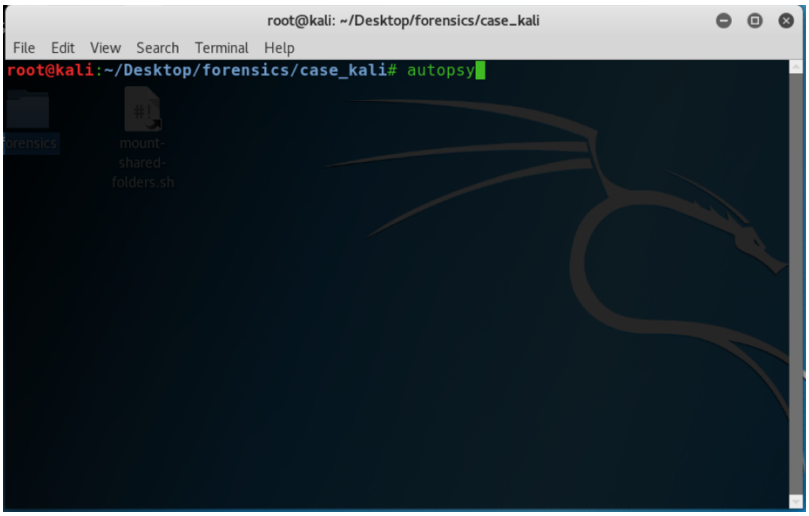
https://drive.google.com/open?id=1xP8ufHByg_zE_8zYzvAn9d0c9UWrunEr

Task 1. Create a new case.

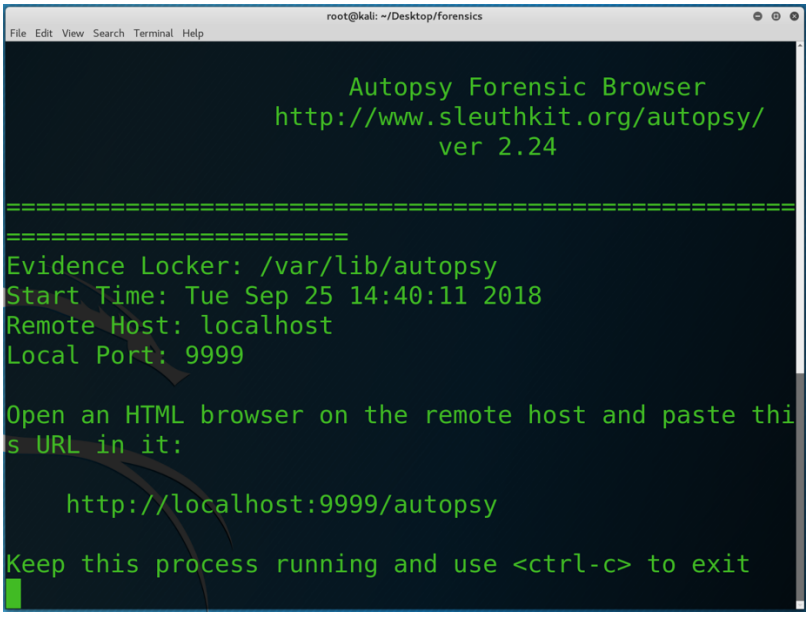
2. Open vmware and log onto the virtual machine.
3. Open autopsy. Click on Main->Forensics Tools->Analysis->Autopsy.



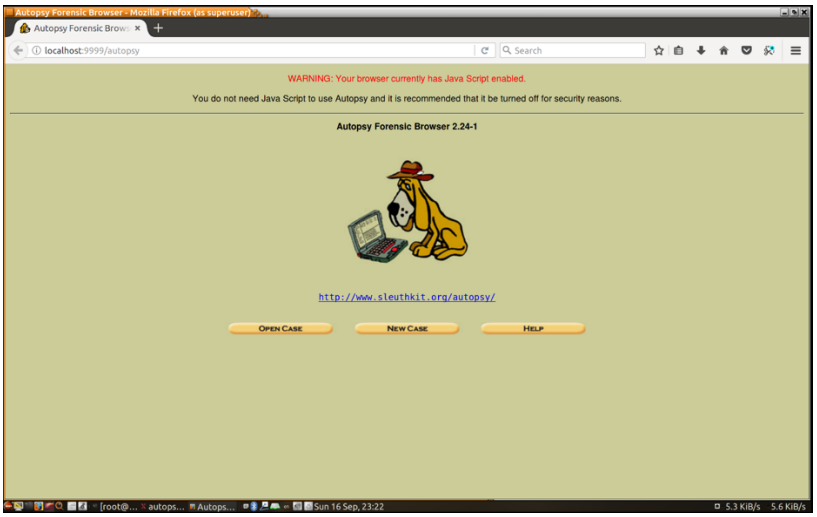
If you work in Kali Linux, you can simply type “autopsy” in command line.



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.

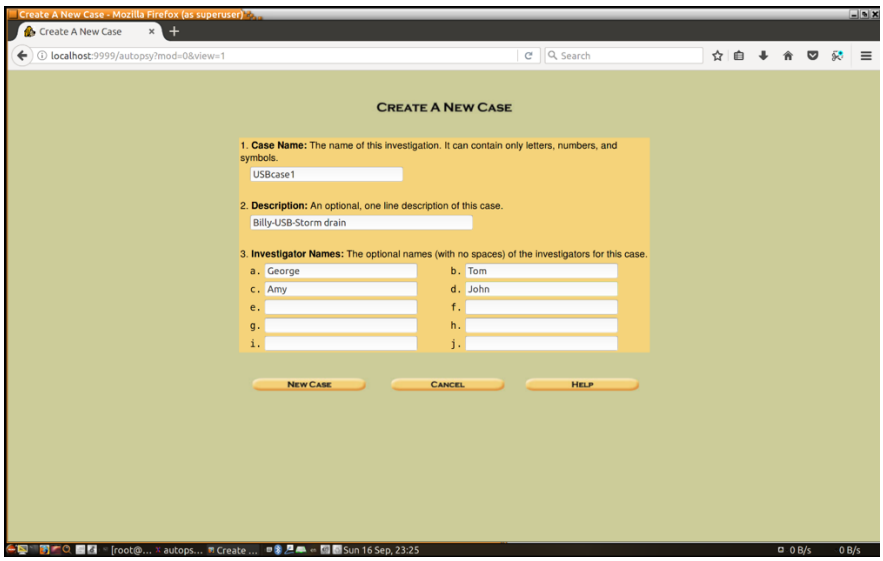


4. Click on the “New Case” button.

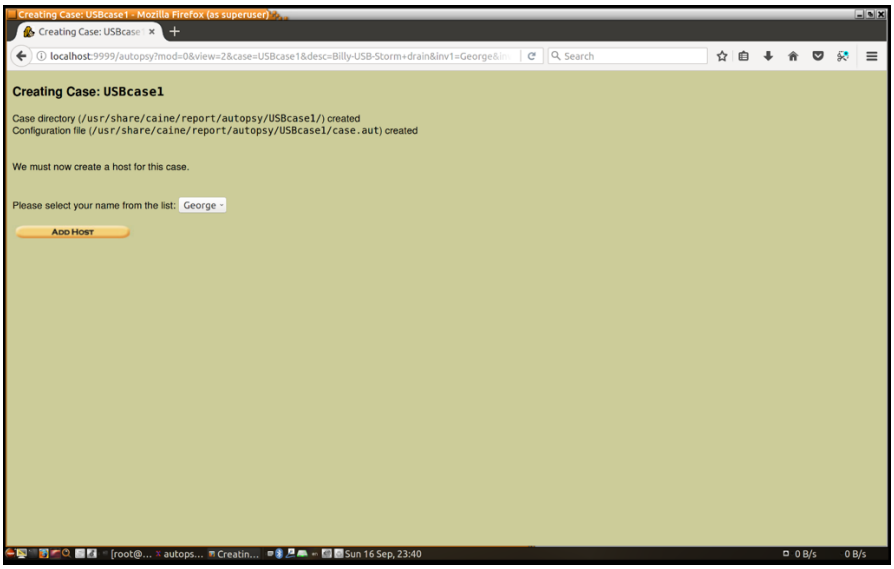


5. Fill in the fields as follows:
   - **a.** "Case Name" – Type: **USBcase1**
   - **b.** "Description" - Add a short sentence describing the case. Reread the scenario at the beginning of this document for help with your short description.
   - **c.** "Investigator Names" - Type in your name and the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

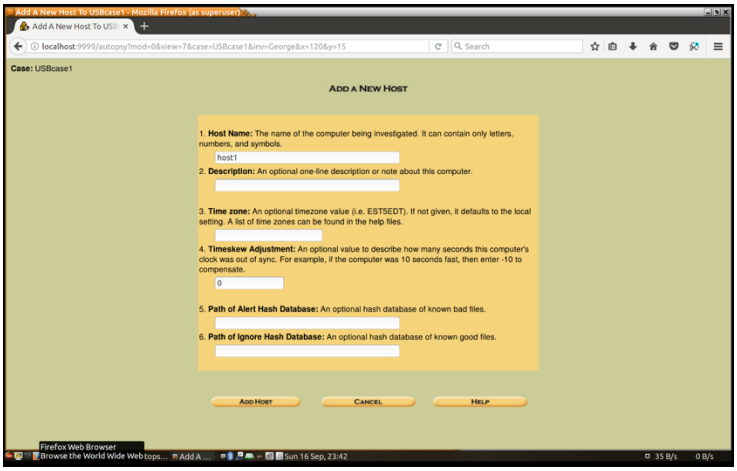
   Click the "New Case" button.



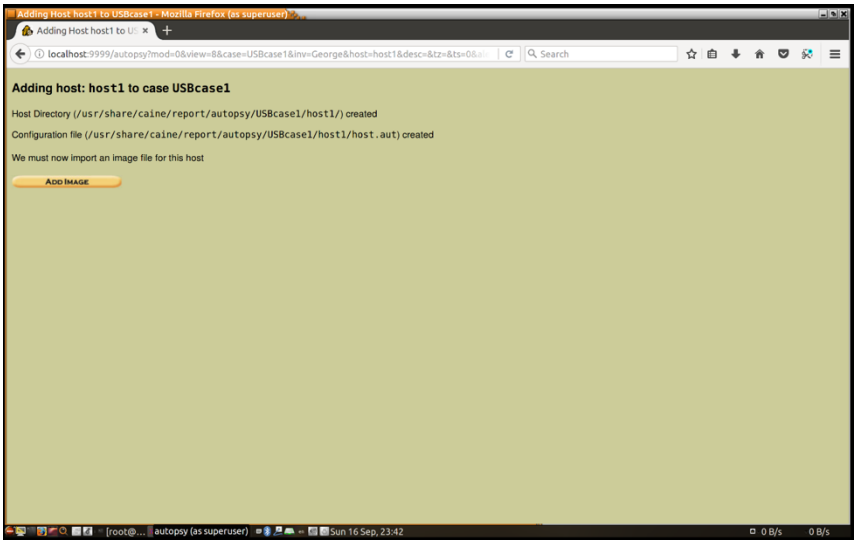
6. Leave the default and click the "Add Host" button at the bottom.



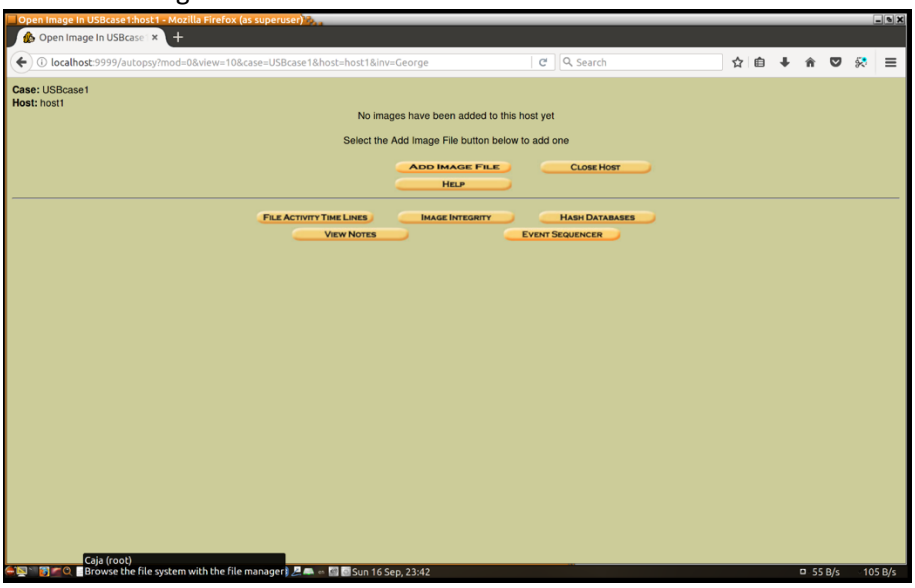
7. Click another “Add Host” button.



8. Click “Add Image.”

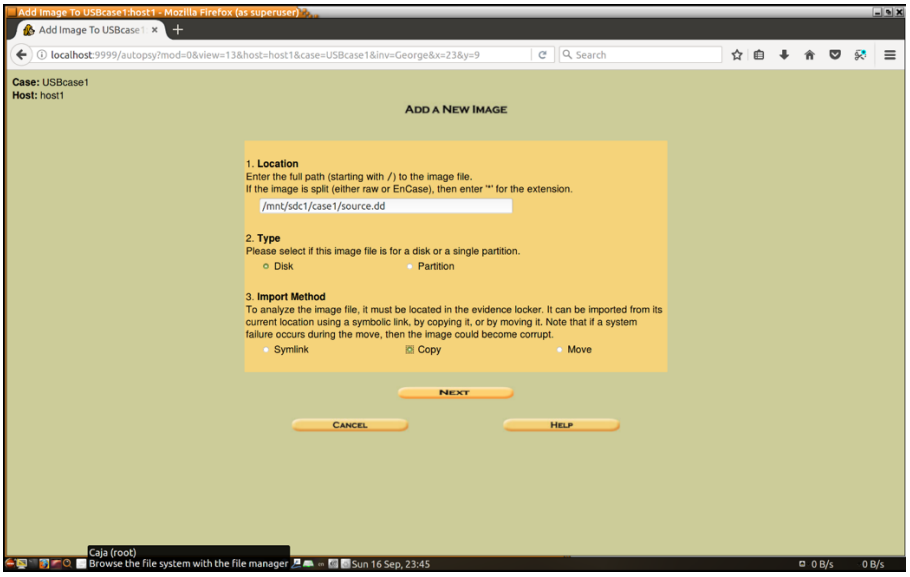


9. Click “Add Image File.”

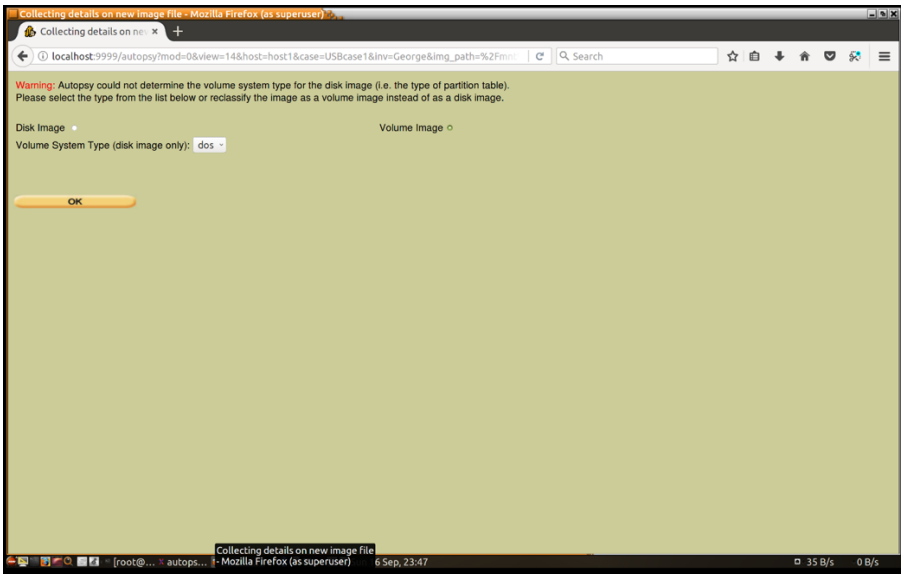


10. Fill in the fields in the “Add a New Image” screen.”
    a. “Location” Type /mnt/sdc1/case1/source.dd (***Please note: here you need to locate the source drive and provide the correct directory information***)
    b. “Import Method” select copy.

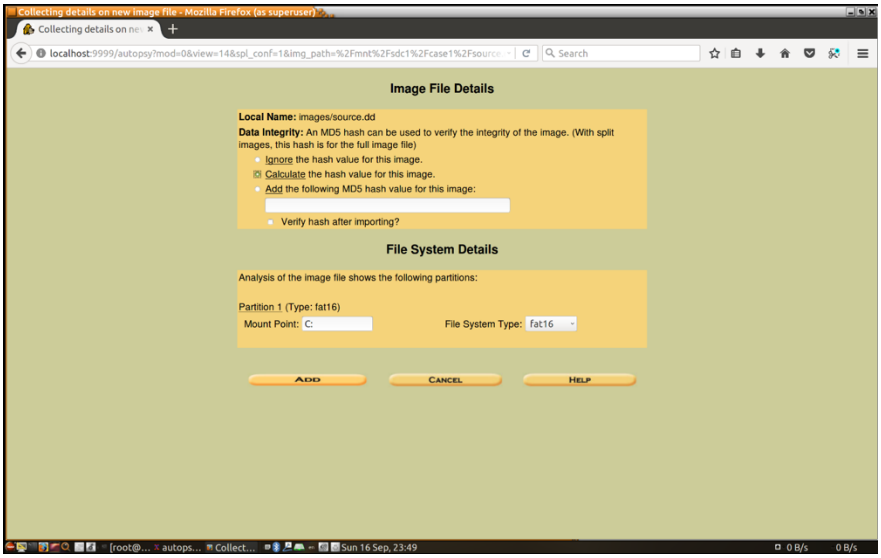
    Click “Next.”



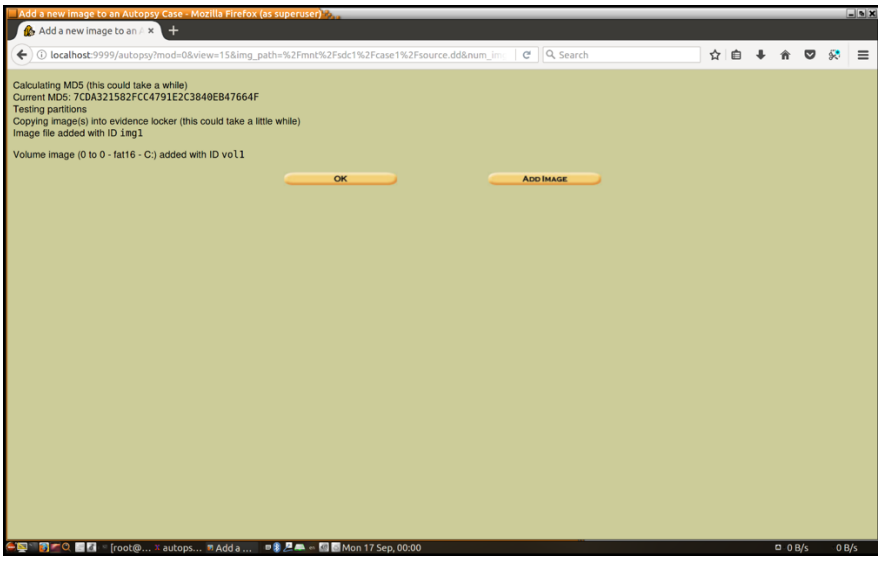
11. Select “Volume Image” on the right, ensure the “dos” is selected in the drop down of “Volume System Type”. Click “OK.”



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

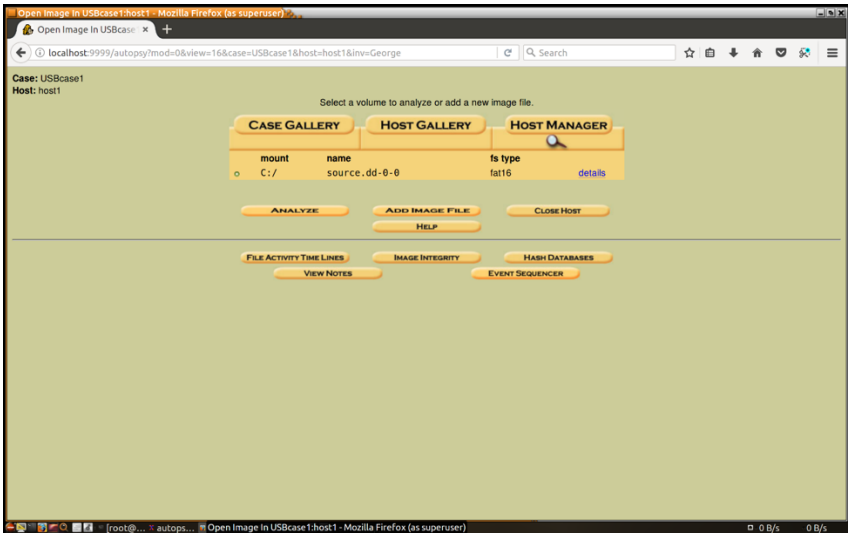


13. Once the calculations are done, click the “OK” button.

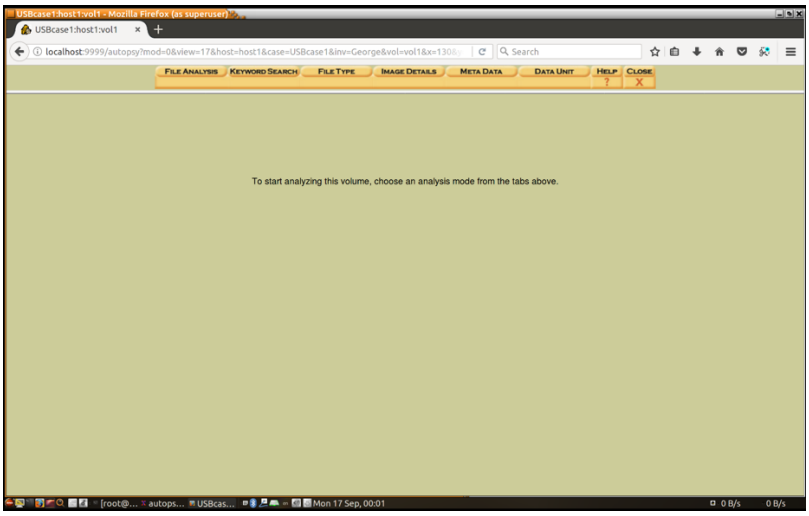


Task 2. Locate deleted/hidden files

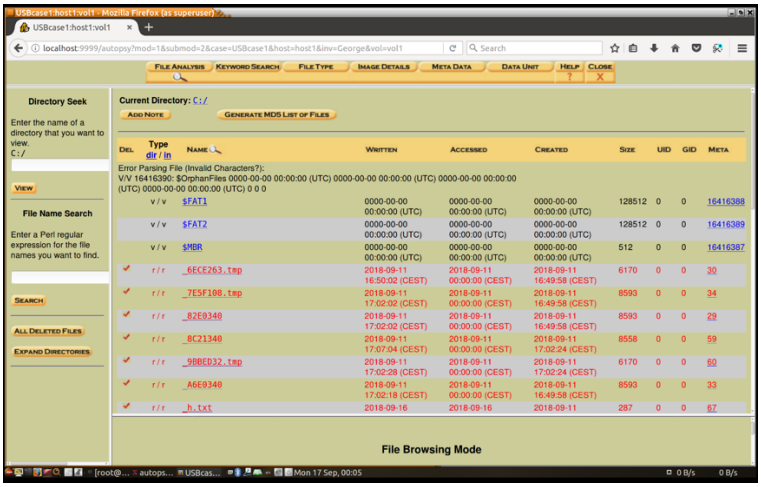
14. Click the “Analyze” button.



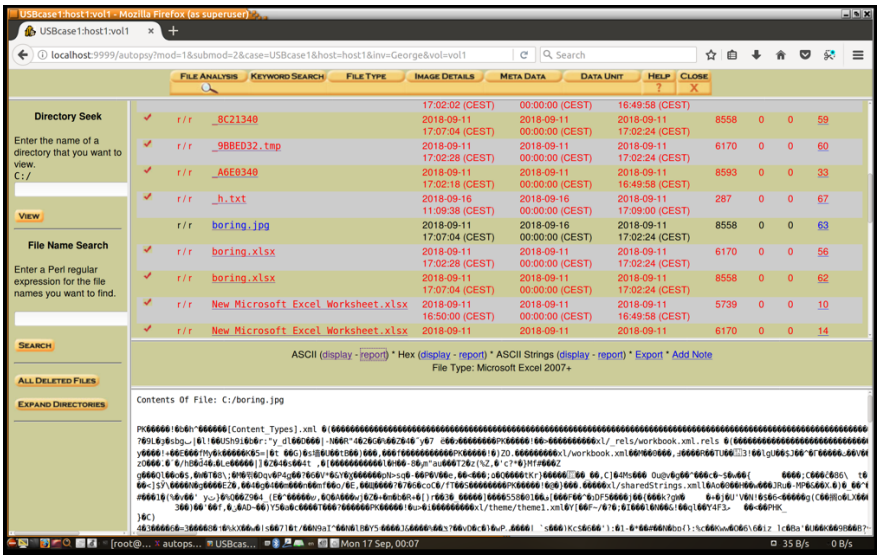
15. Select “File Analysis”.

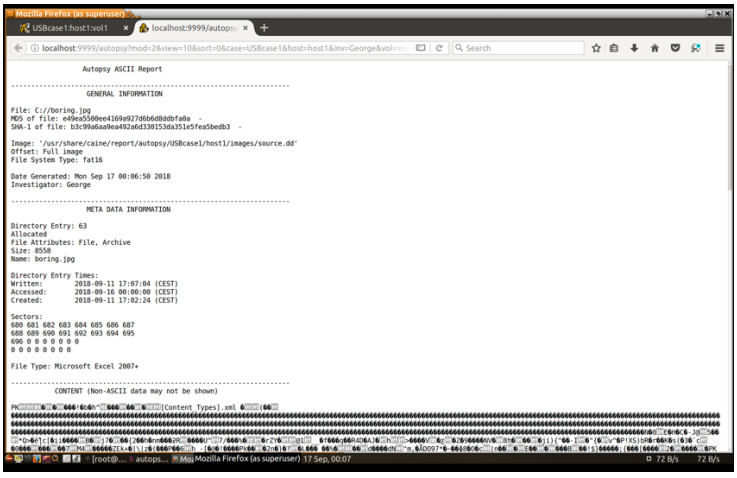


16. The files labeled in red are the deleted files. They also are the ones with a checkmark under the DEL to the left of the filename.
    a. Click on the files and examine them in the window below.

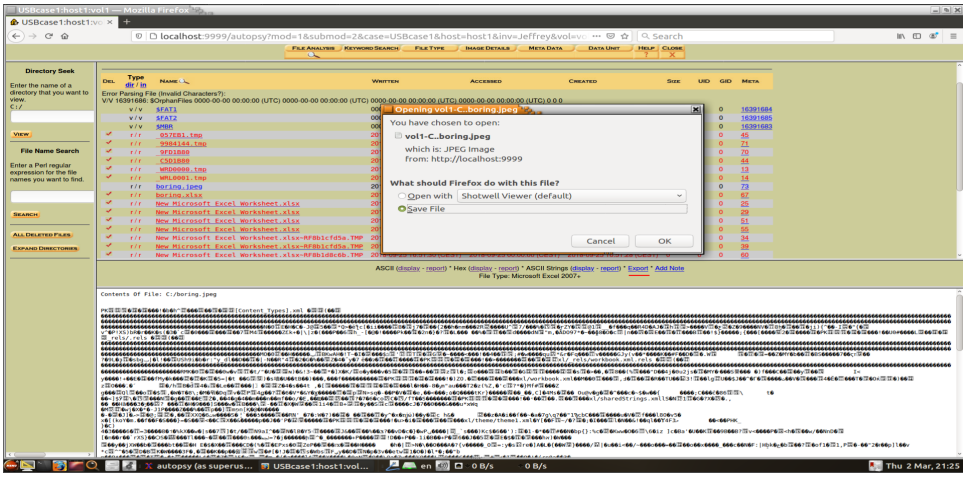


    b. If data appears, click report next to ASCII to view a report of the data. (Clicking on “display” does not give you the report. You must click on the word “report”.) “X” out of this tab.



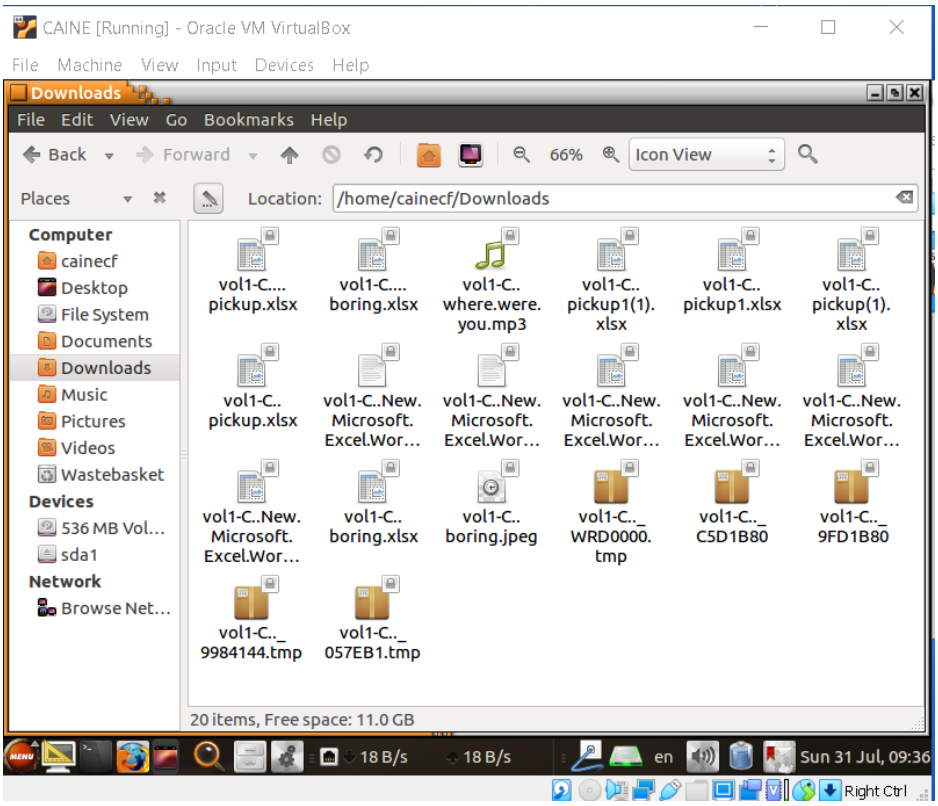


c. Then click “Export” to export the file from the image to the Downloads folder.

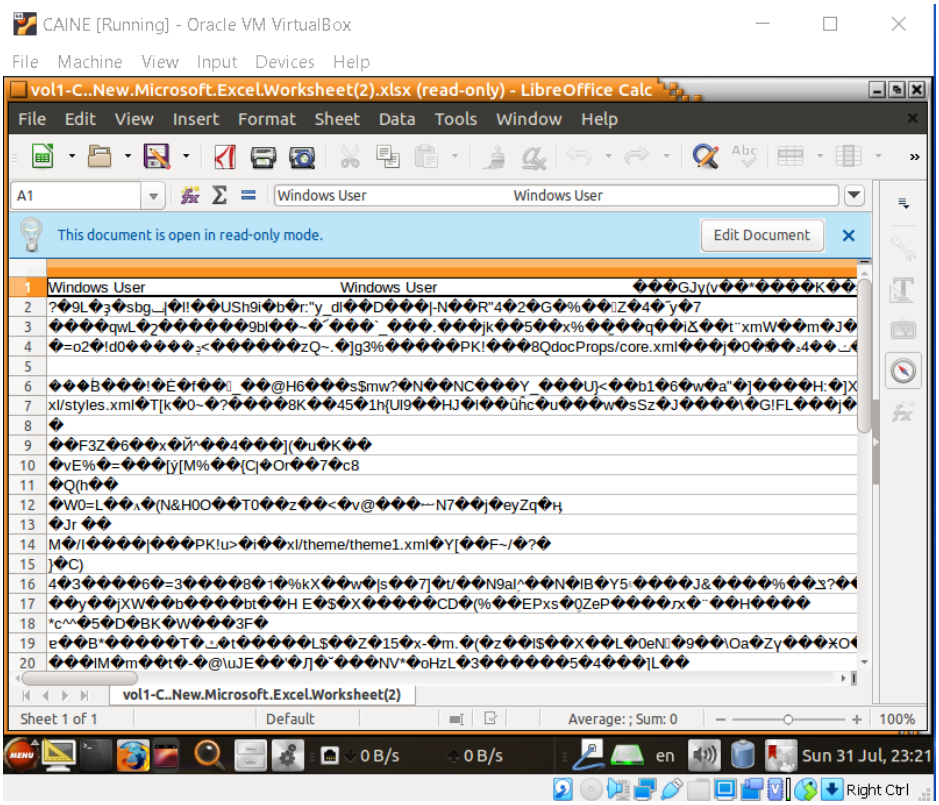


d. Once the files are saved outside the image open them and examine the data.

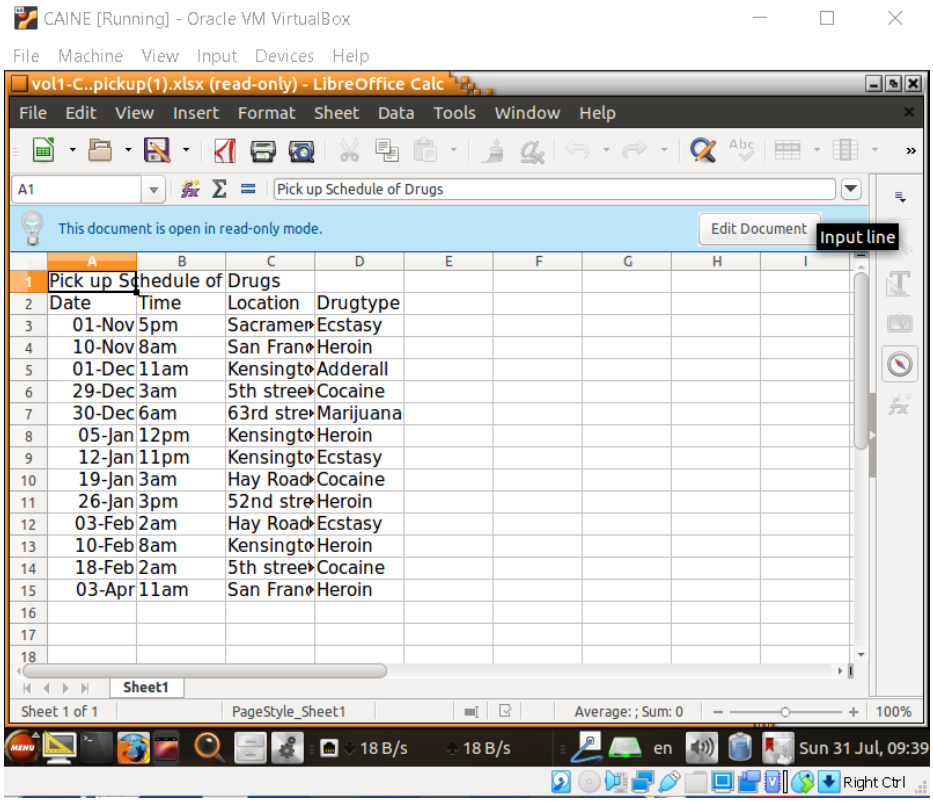
e. Let’s look at the content of our downloaded files.



There are 20 files that we were able to download from Autopsy.

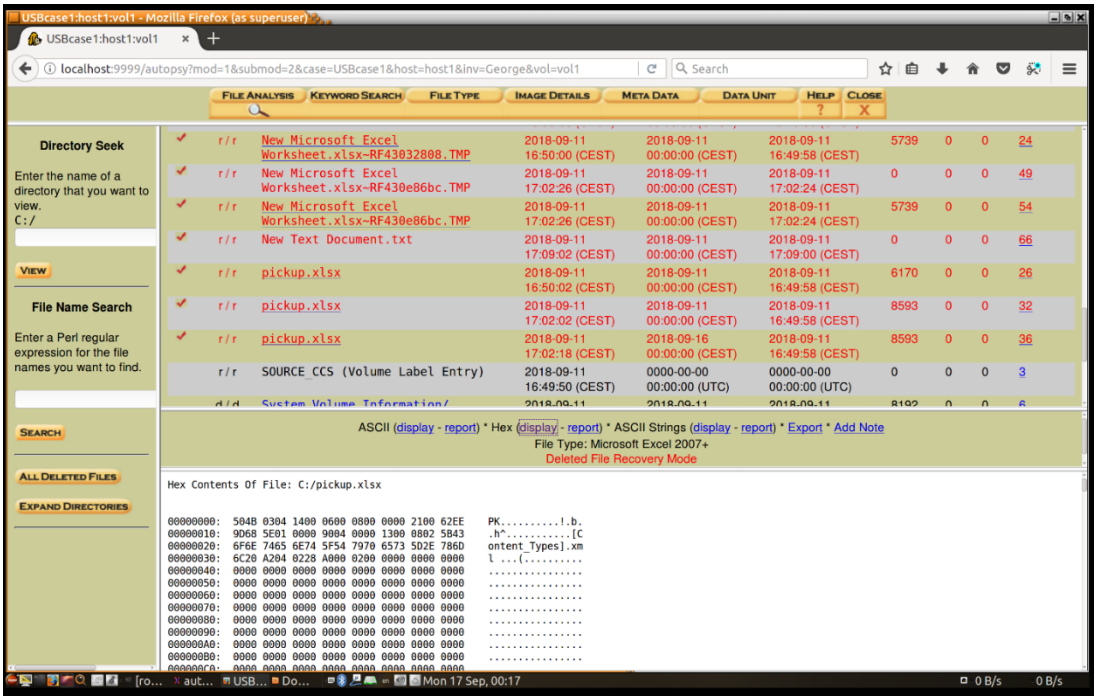


Most of them are either blank or corrupted.

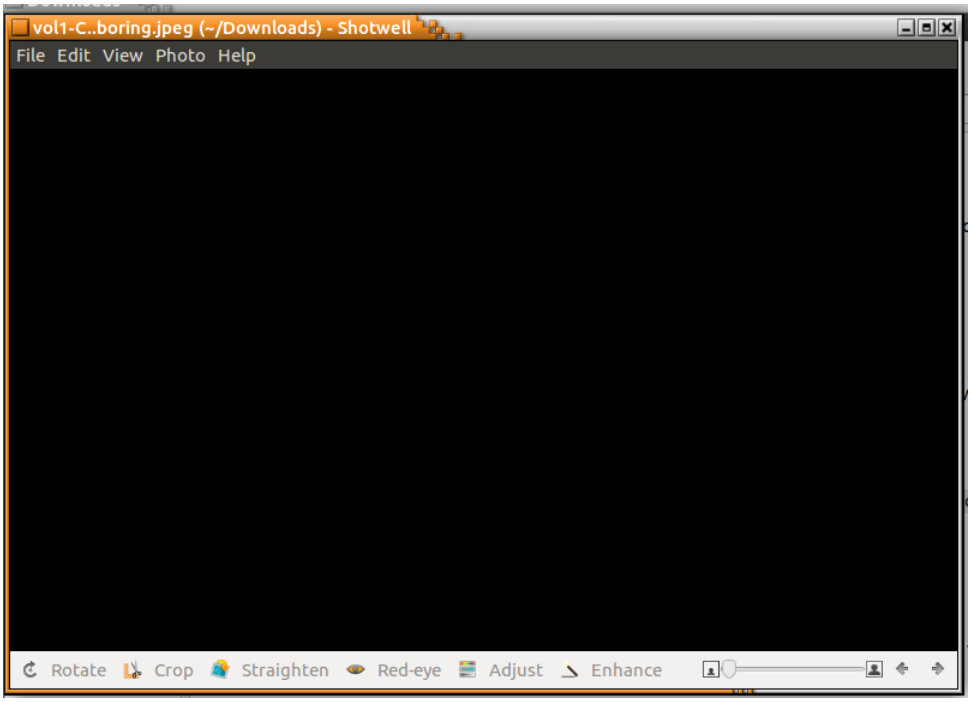


It looks like vol1-C..pickup(1).xlsx still has data on it.

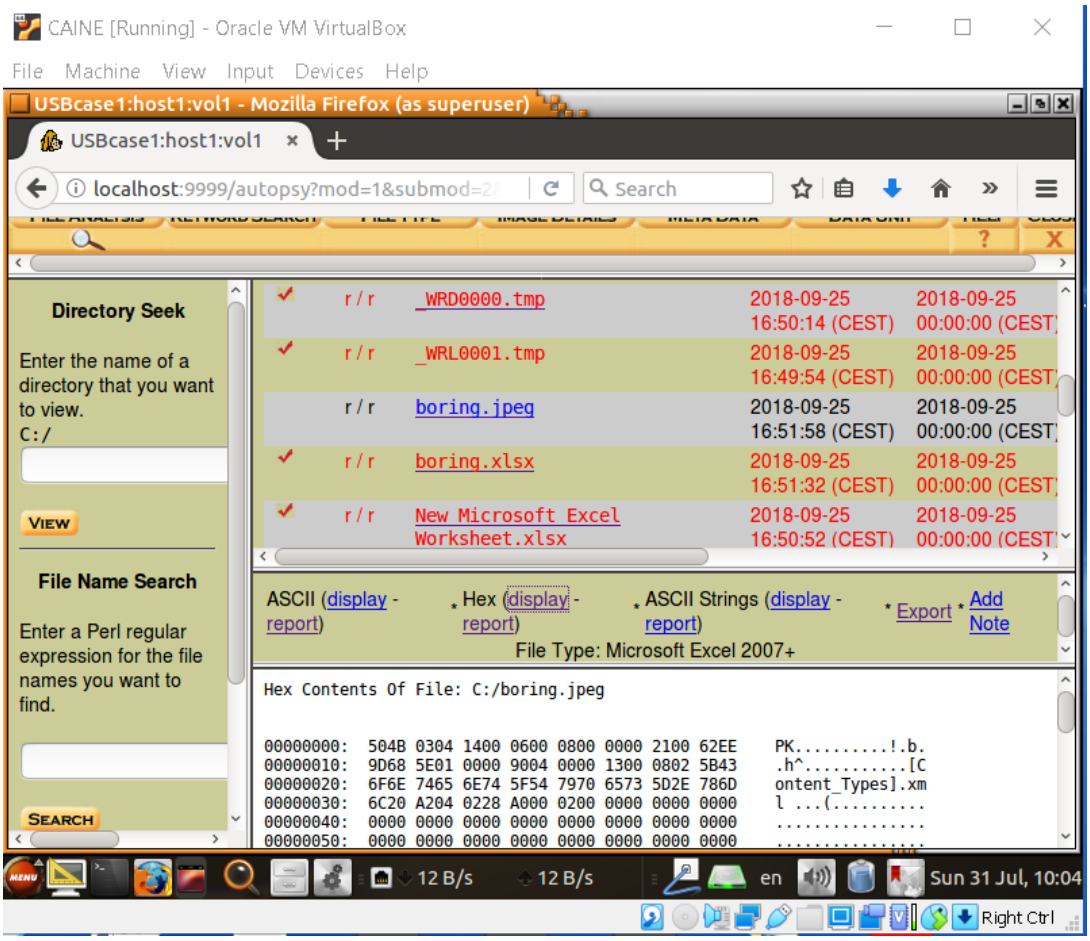
17. Click on the “display” in the Hex tab to display the file in hex.



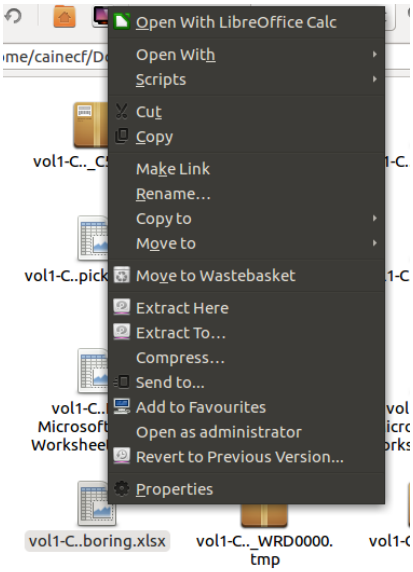
18. Follow the same procedure for the files listed in blue. These are files that exist openly on the drive. If the file does not work when you open it, examine the "magic number" as seen in the magic number chart (see Appendix) to ensure that the file is labeled correctly. The Magic Number is the first 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.



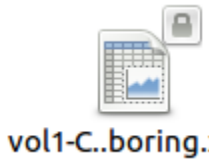
19. The 2 files that were not deleted from the USB drive were boring.jpeg and where.were.you.mp3. You should notice that they do not work when you open them. (Above is a screenshot of boring.jpeg)



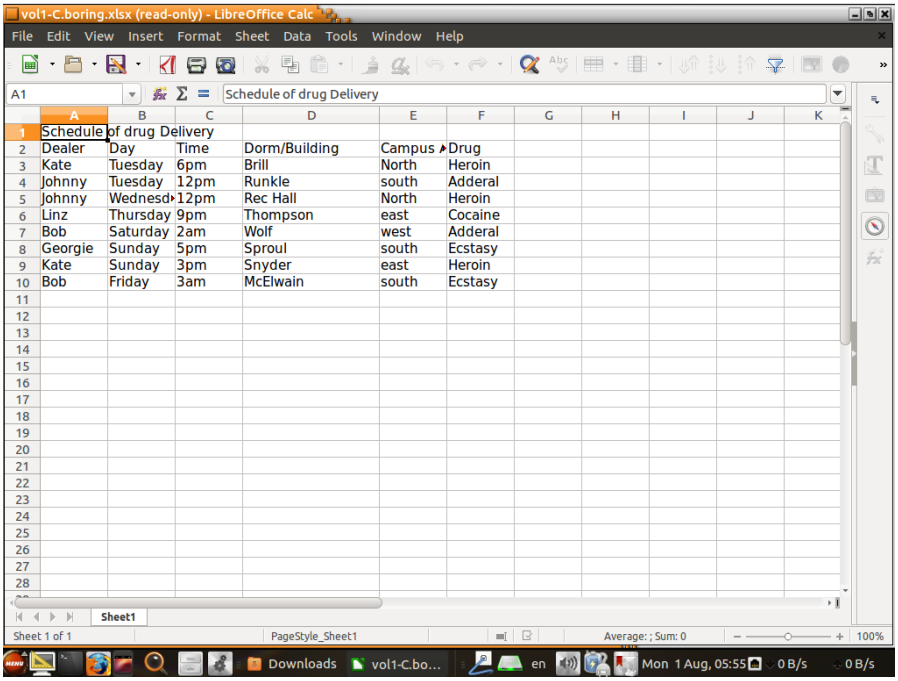
20. When we look at their hex values in Autopsy, their headers start with 504B 0304. According to the chart at the end of this document, this should be the header for Office 2007 documents. (Above is a screenshot of boring.jpeg's hex values.)



In the folder with the downloaded files, right click “vol1-C..boring.jpeg” and click “Rename…” to change the .jpeg extension to .xlsx. You might need to change the name if you have another file with the same name.



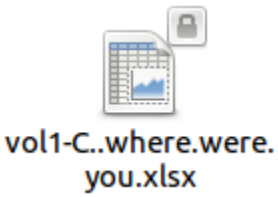
If you changed the extension correctly, the icon should have changed.



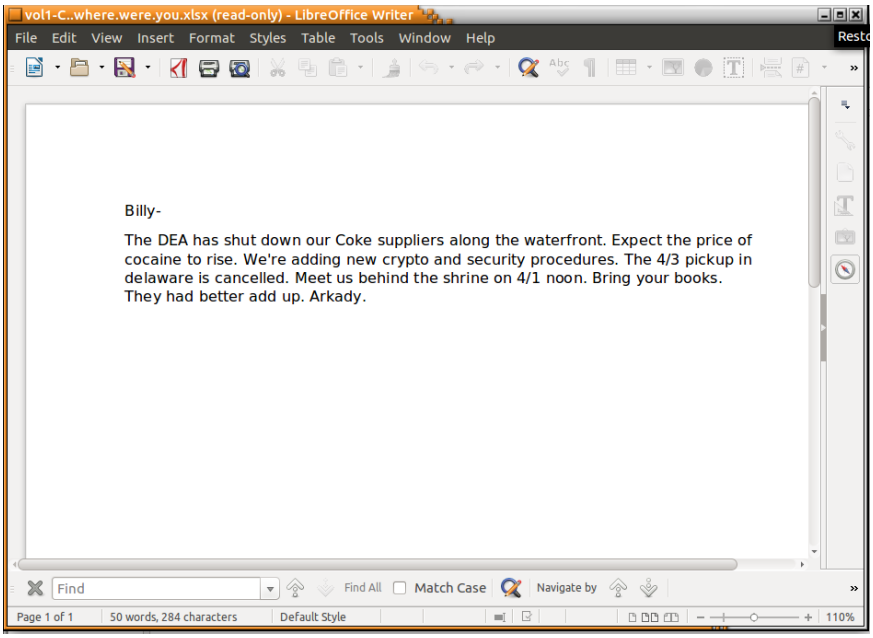
	A	B	C	D	E	F
1	Schedule of drug Delivery					
2	Dealer	Day	Time	Dorm/Building	Campus	Drug
3	Kate	Tuesday	6pm	Brill	North	Heroin
4	Johnny	Tuesday	12pm	Runkle	south	Adderal
5	Johnny	Wednesd	12pm	Rec Hall	North	Heroin
6	Linz	Thursday	9pm	Thompson	east	Cocaine
7	Bob	Saturday	2am	Wolf	west	Adderal
8	Georgie	Sunday	5pm	Sproul	south	Ecstasy
9	Kate	Sunday	3pm	Snyder	east	Heroin
10	Bob	Friday	3am	McElwain	south	Ecstasy

Now, open the renamed file and open it. You should see that it was hiding a secret schedule of drug deliveries.

At the beginning of step 20, we also noticed that where.were.you.mp3 was also an Office 2007 document, so we need to change the extension for that file as well.



Once again, right click “vol1-C..where.were.you.mp3” and change the extension to .xlsx.



Now, when we open this file we can see a secret message to Billy about his next Coke delivery.

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