CSU, College of Engineering and Computer Science
Department of Computer Science
CSC 153 – Computer Forensics Principles and Practice

Catherine Nguyen
CSC 153
10/25/2020

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 on 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
- Part 0: Download the image of the suspect's drive.
- Part 1: Create a new case.
- Part 2: Locate deleted/hidden files
- Part 3: Complete the report and answer questions.

Part 0: Download the image of the suspect's drive

Start off by downloading the suspect's drive onto the virtual machine we will be using to conduct the autopsy. The file name is ***image_zero.dd***.

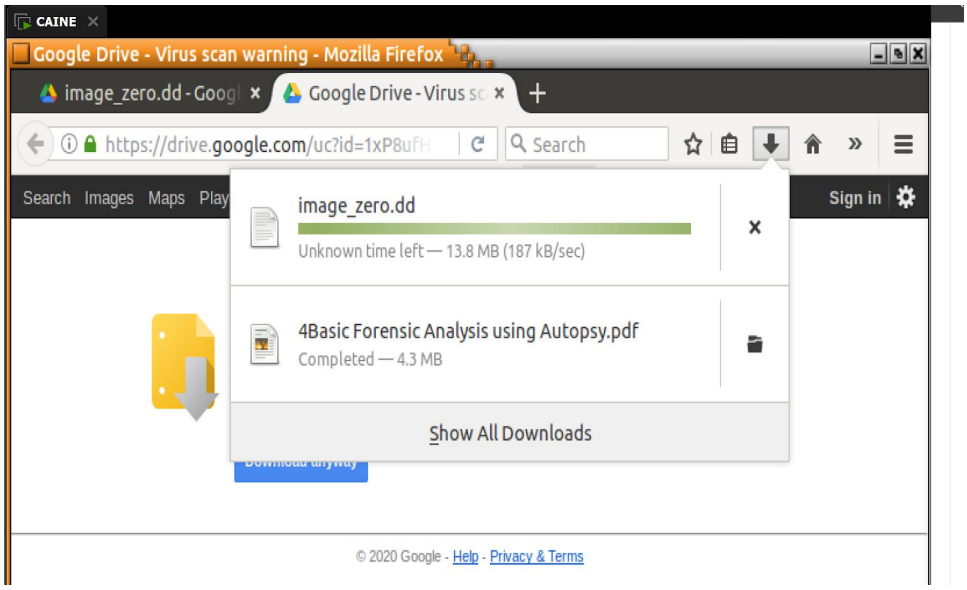


Fig 1: Downloading the suspect's drive

Part 1: Create a new case

Go on your VMware and open up autopsy to create a new case.

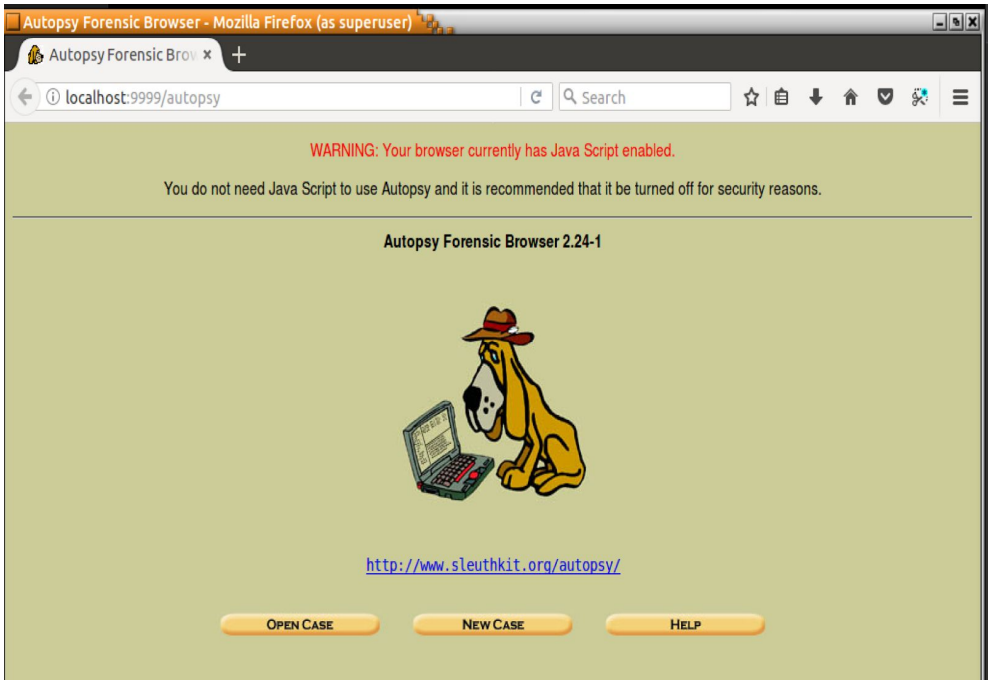


Fig 2: Autopsy is opened

Click a new case and enter information about the case.

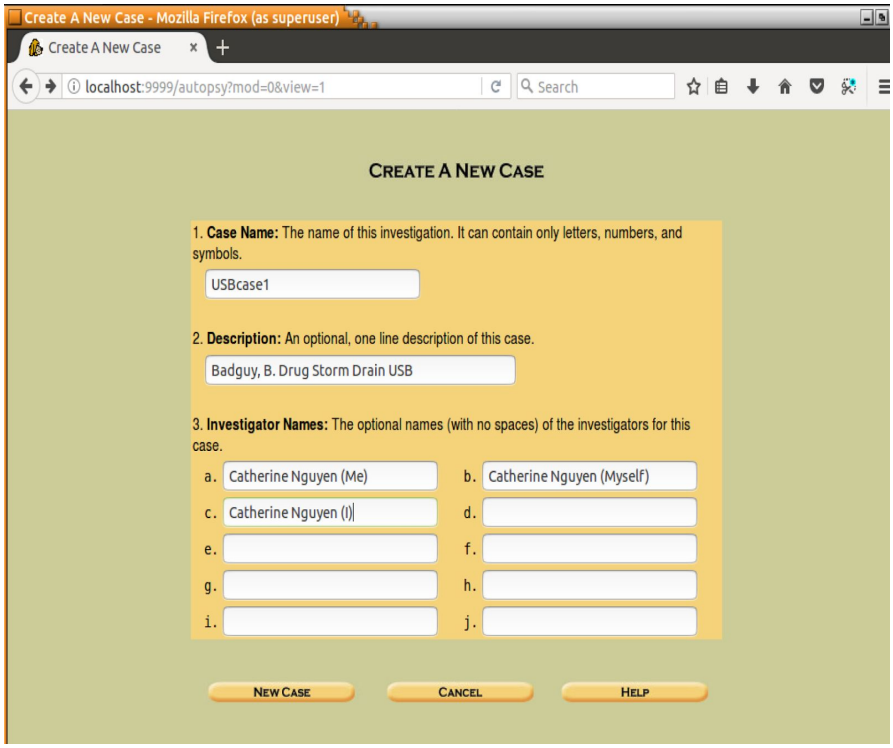


Fig 3: New case page filled in with the information

Add the image into the case using the correct directory.

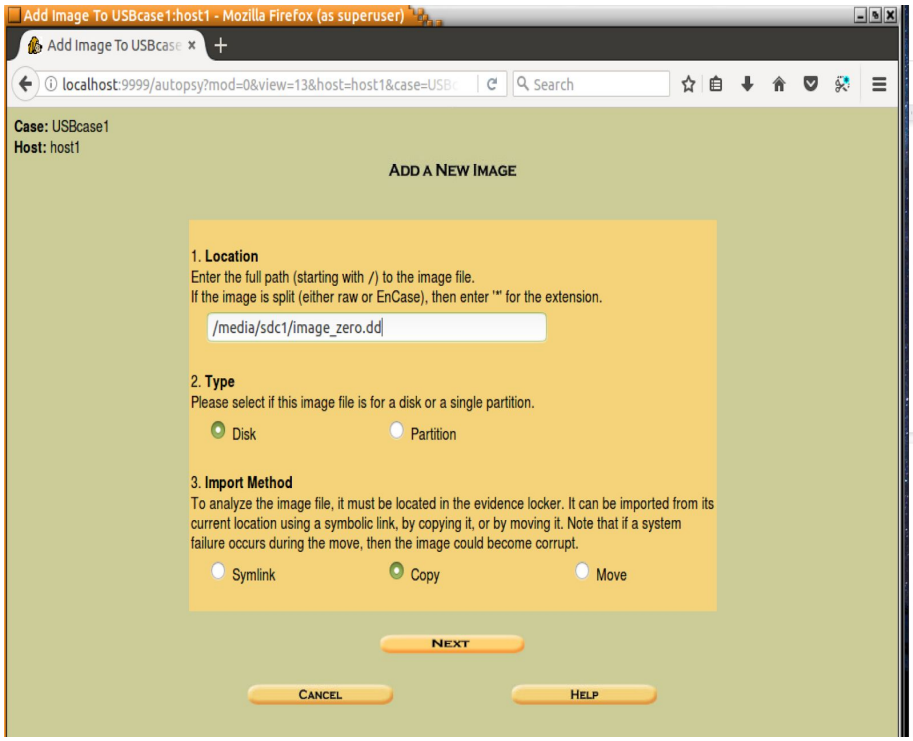


Fig 4: Entered the Directory and configured the import method to copy.

Edit the details of the image file. So we need to calculate the hash value for the image and verify the hash after it's been imported. Also, changed the file system type to fat16. **Error. Fat32 is the one.**

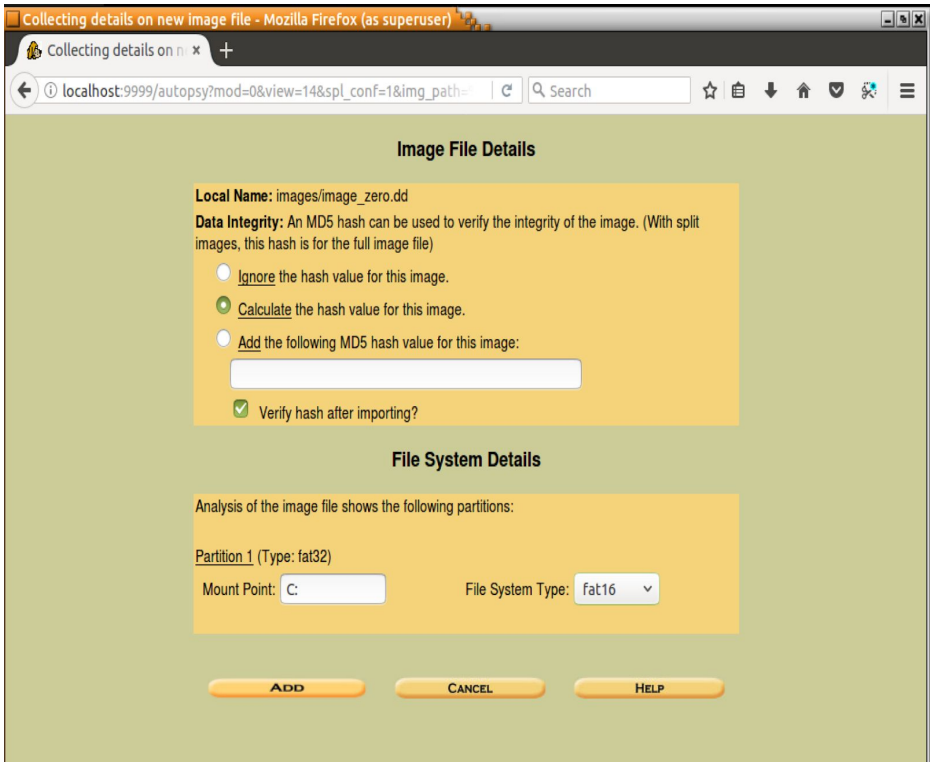


Fig 5: Image File Details

Part 2: Locate Deleted/Hidden Files

The image was successfully added. Now it is time to analyze the drive

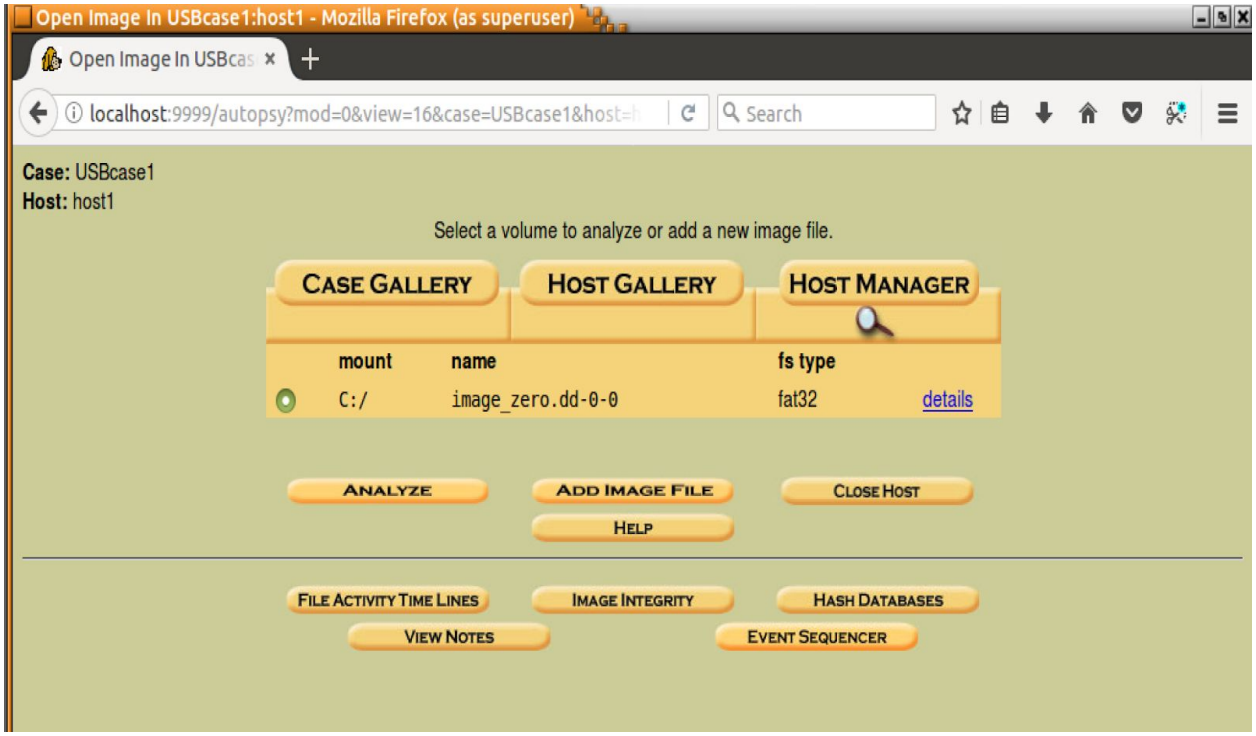


Fig 6: Page showing the added image ready for closer examination.

Click on “Analyze” and then on “File Analysis”. The opens up a view for us to examine all the files on the drive. With this open, we can answer the questions in part 3. Red = deleted

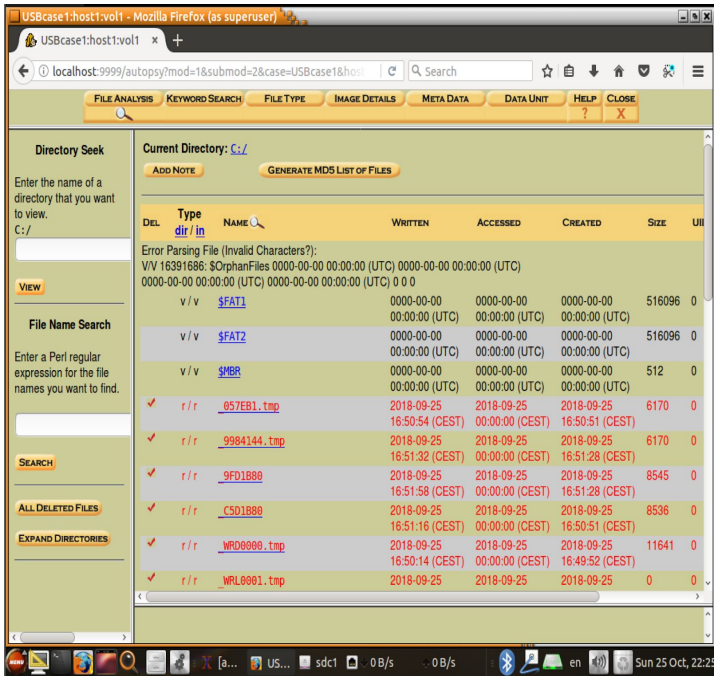


Fig 7: Files visible for autopsy examination.

Part 3: Complete the report and answer the questions.

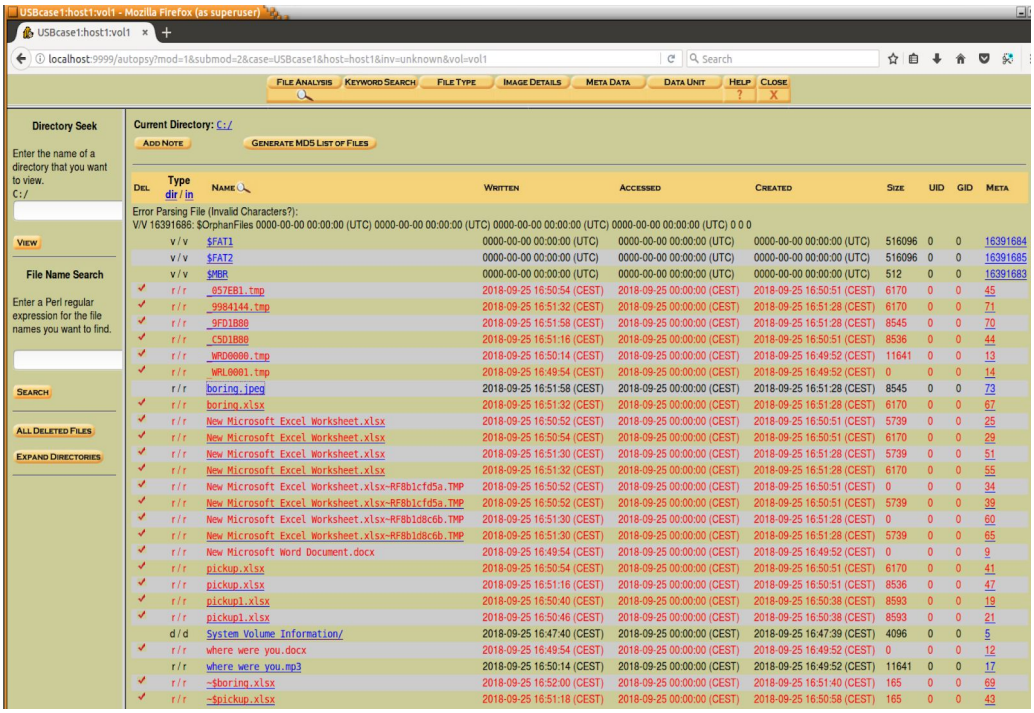
1. **How many files are there on the USB drive? What are they?** *(Take a screenshot for the files.)*
   a. There are only 2 files left on the USB Drive that have not been deleted.
   b. The names are ***boring.jpeg*** and ***where were you.mp3.***
   c. 

   Fig 8: All the files on the drive. 2 are not deleted.

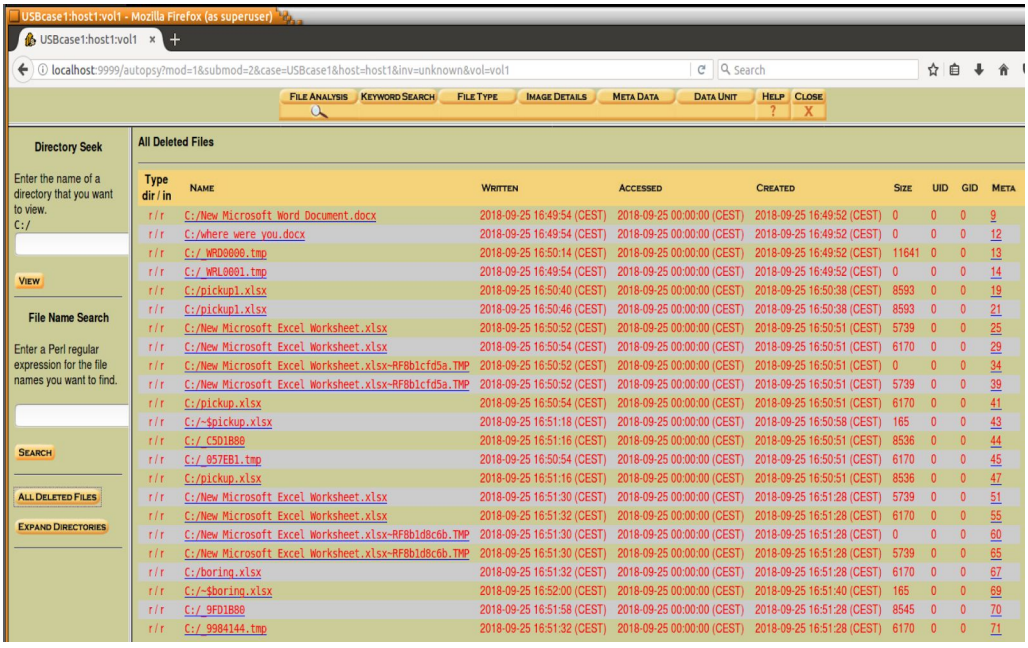
2. **Which file/files are deleted?** *(Take a screenshot of the deleted files.)*
   a. Quite a few. All the red ones have been deleted. Most seem to be renames files.
   b. 

   Fig 9: All 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)*
    a. You can not open the boring.jpg file with an image viewer
    b. The reason being that it is not a jpg file. In fact, the file type is Microsoft Excel 2007+ this is shown in figure 10. below because the magic number 504B stands for an office document specifically an excel sheet.
    c. To eventually view the file we have to change the extension of the file into a .xlxs file then it will allow us to see its contents using an application to view .xlxs files. Figure 11. Below shows us the contents of the file.
    d.

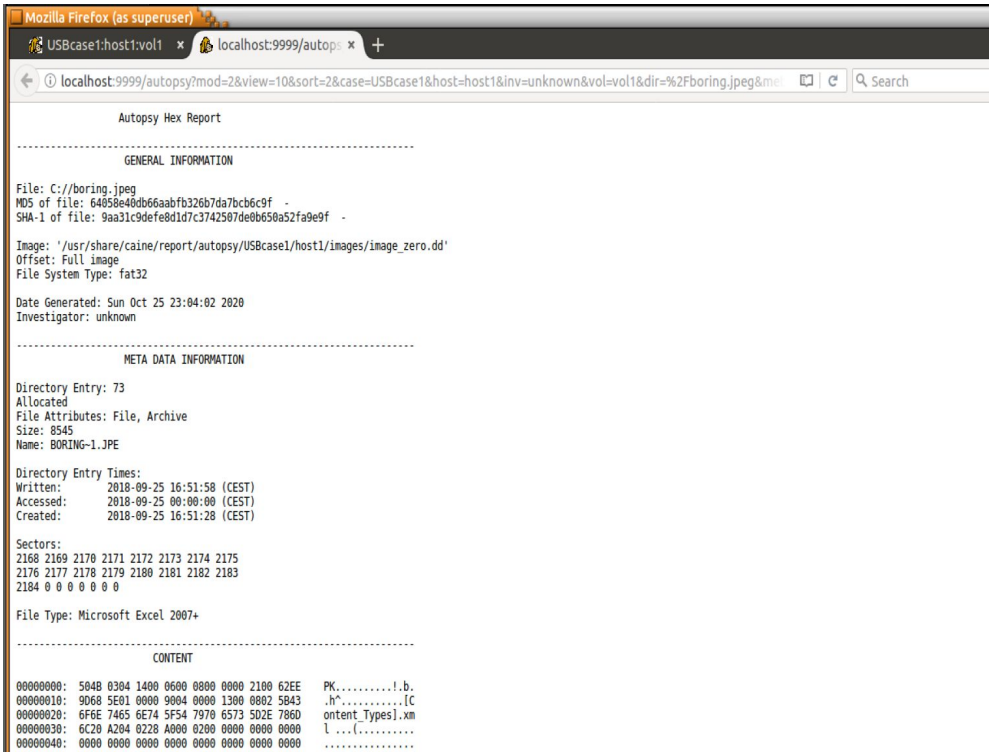
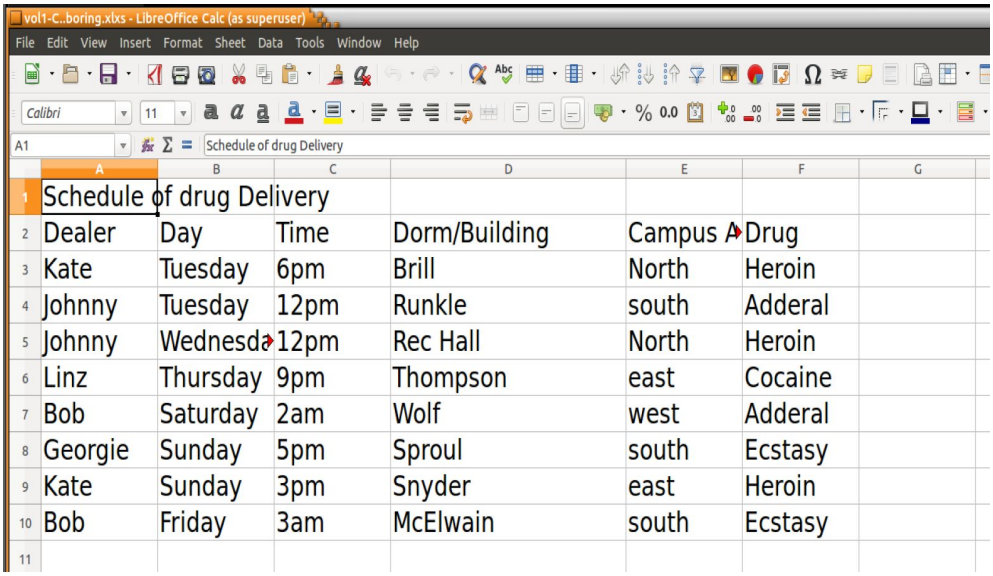


Fig 10: Magic number 504B stands for .xlxs file

e.



	A	B	C	D	E	F	G
1	Schedule of drug Delivery						
2	Dealer	Day	Time	Dorm/Building	Campus A	Drug	
3	Kate	Tuesday	6pm	Brill	North	Heroin	
4	Johnny	Tuesday	12pm	Runkle	south	Adderal	
5	Johnny	Wednesda	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	
11							

Fig 11: Sheet of all the scheduled meetings for drug delivery.

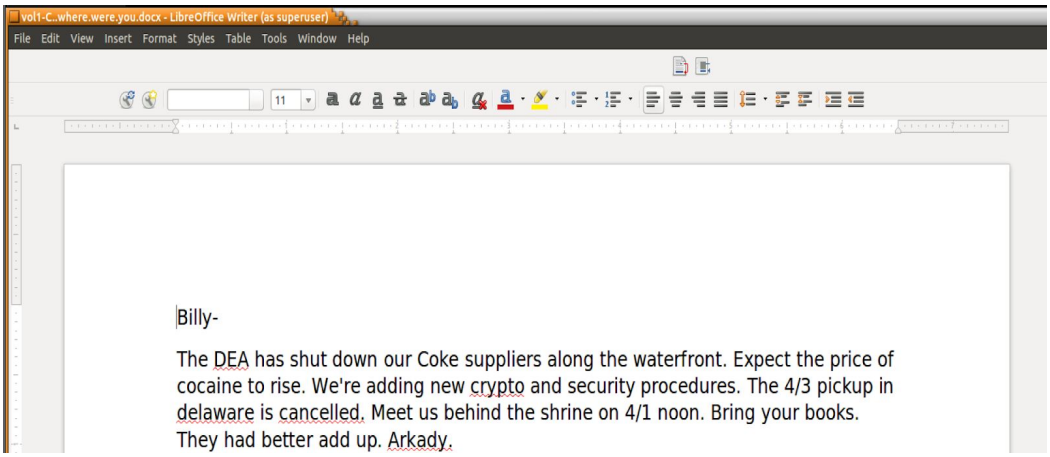
4. **Were there any secret messages? If so, in which file are they located?** *(Take a screenshot of the secret message)*
    a. Yes, there is a secret message. You can examine this message in where were you.mp3 which is actually a Microsoft Word Document. The magic number is 504B.
    b. In order to see the message, we have to follow the same procedure for boring.jpg. We need to export the file and change the file extension as a .docx to view.
    c. 

Fig 12: Message in where were you.mp3

5. **What is the name of Billy's supplier?** *(Take a screenshot to prove the answer)*
    a. Arkady
    b.

Billy-

The DEA has shut down our Coke suppliers along the waterfront. Expect the price of cocaine to rise. We're adding new crypto and security procedures. The 4/3 pickup in delaware is cancelled. Meet us behind the shrine on 4/1 noon. Bring your books. They had better add up. Arkady.

Fig 13: Close up of the letter. Arkady sent it to Billy.

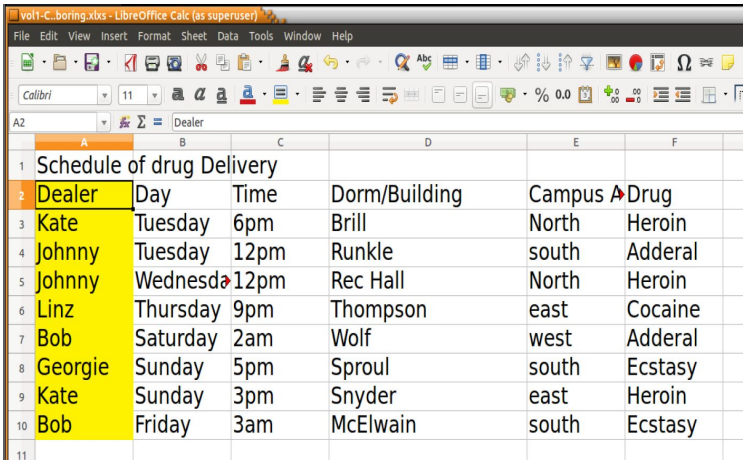
6. **When and where is the next meet?** *(Take a screenshot to prove the answer)*
    a. "Meet us behind the shrine on 4/1 noon." In Figure 13 above shows that that is the meet location and time.
7. **Who else on campus is involved?** *(Take a screenshot to prove the answer)*
    a. Kate, Johnny, Linz, Bob, and Georgie.
    b. 

Fig 14: Highlighted is the names of the other student dealers.