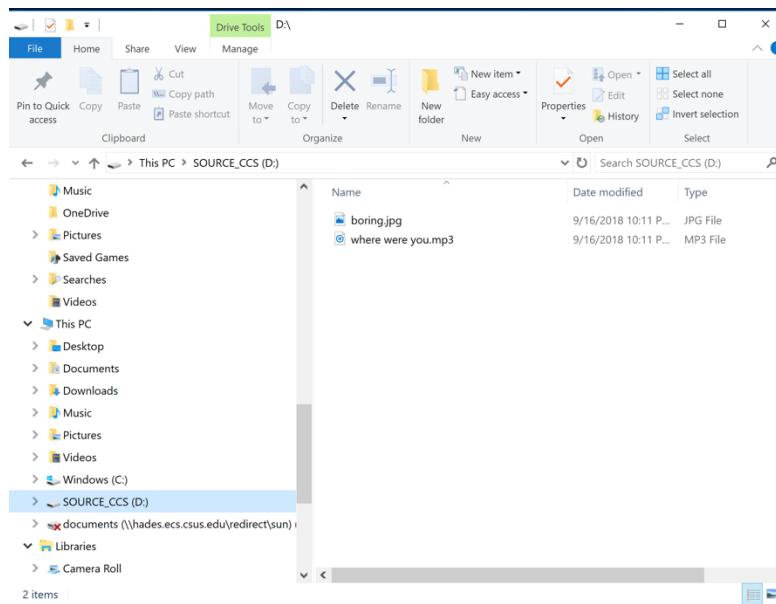


Module 4: Analysis of File Headers using Autopsy

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

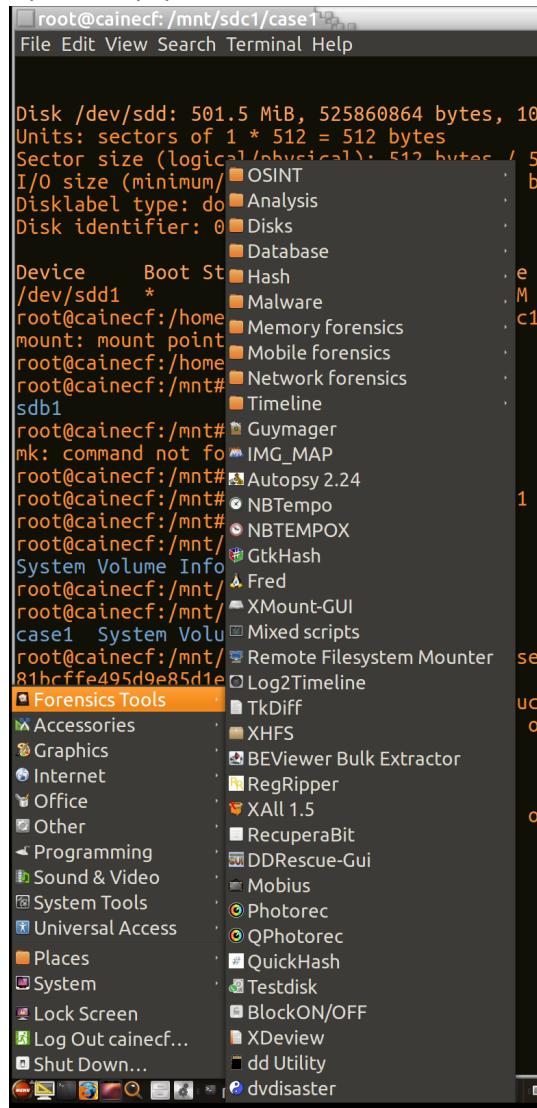
Task 0. Download the image of suspect's drive.

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).

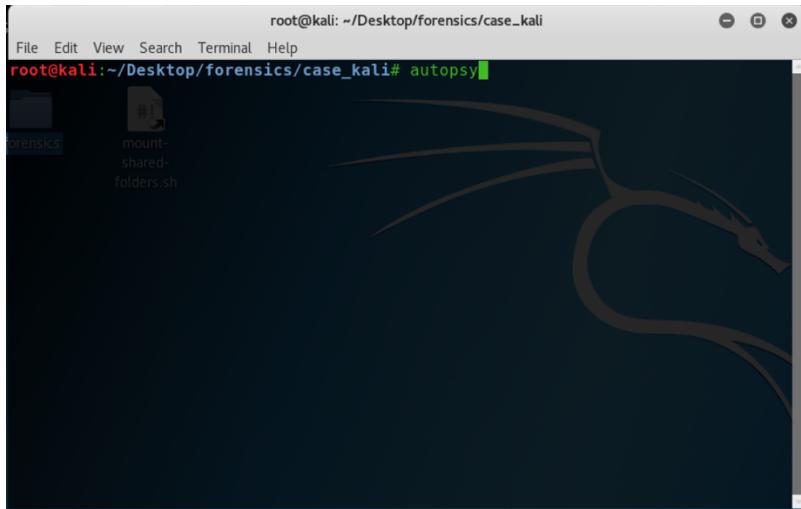
https://drive.google.com/open?id=1xP8ufHByg_zE_8zYzvAn9d0c9UWrunEr

Task 1. Create a new case.

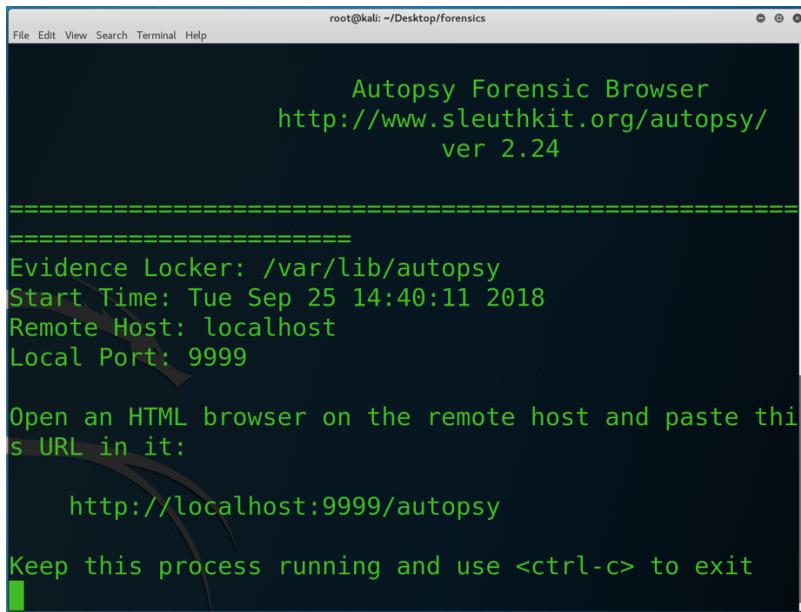
2. Open vmware and log onto the virtual machine.
3. Open autopsy. Click on Main->Forensics Tools->Analysis->Autopsy.



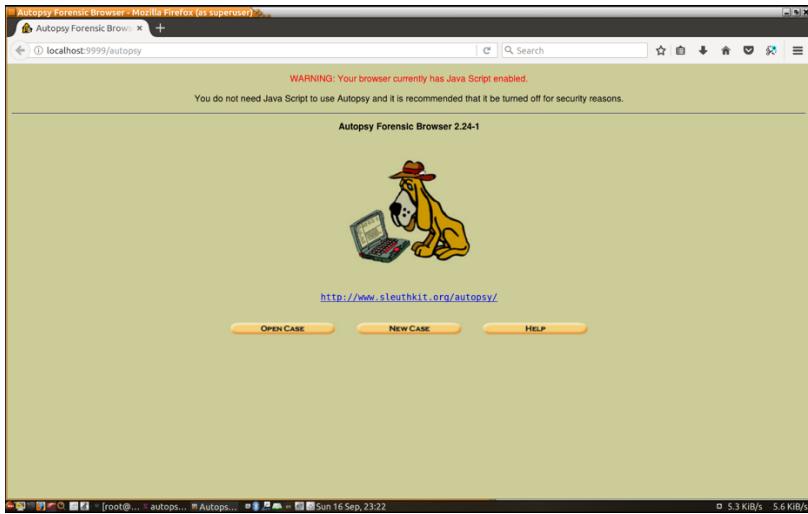
If you work in Kali Linux, you can simply type “autopsy” in command line.



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.



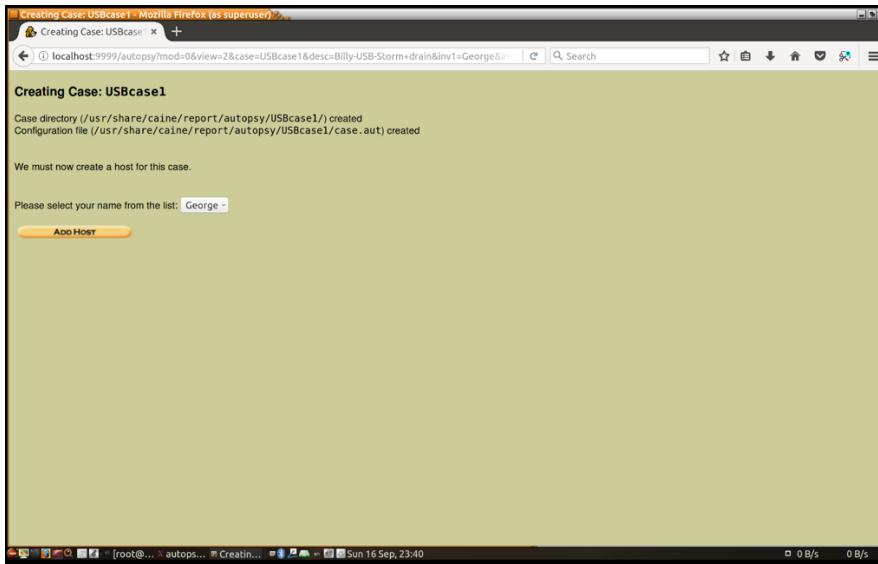
4. Click on the “New Case” button.



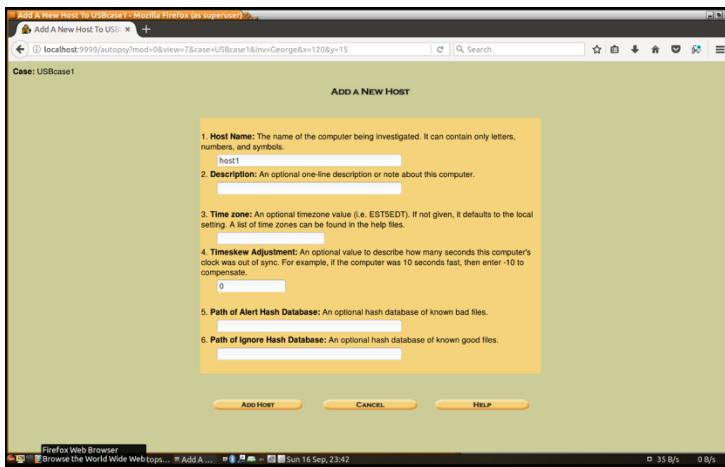
5. Fill in the fields as follows:
 - a. "Case Name" – Type: **USBcase1**
 - b. "Description" - Add a short sentence describing the case. Reread the scenario at the beginning of this document for help with your short description.
 - c. "Investigator Names" - Type in your name and the names of the members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

Click the "New Case" button.

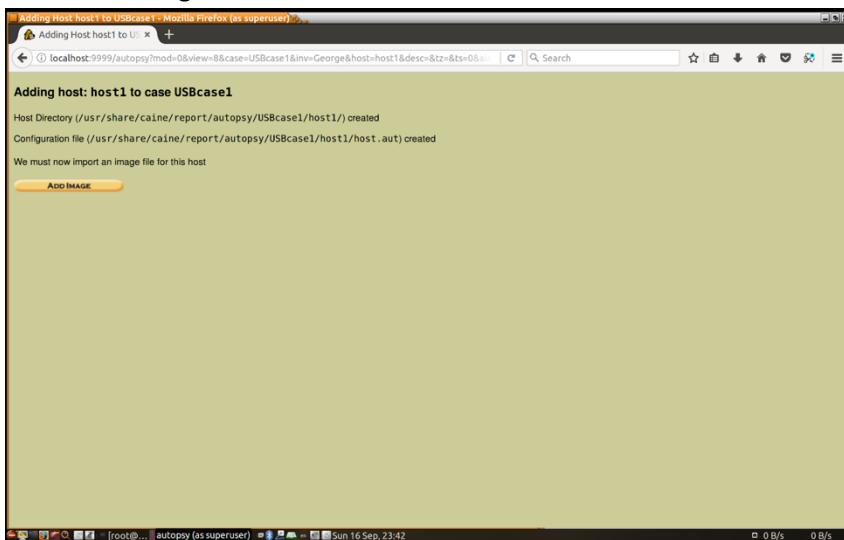
6. Leave the default and click the "Add Host" button at the bottom.



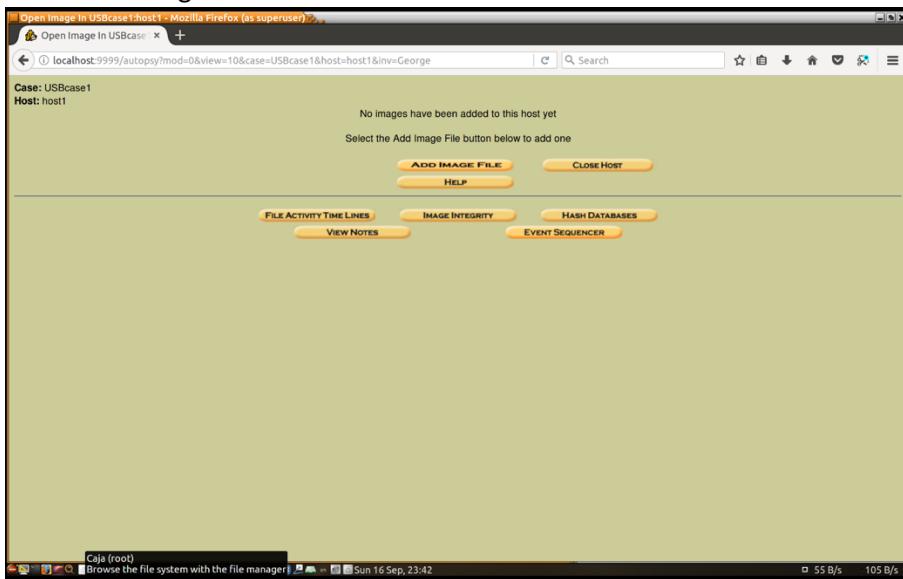
7. Click another “Add Host” button.



- #### 8. Click “Add Image.”



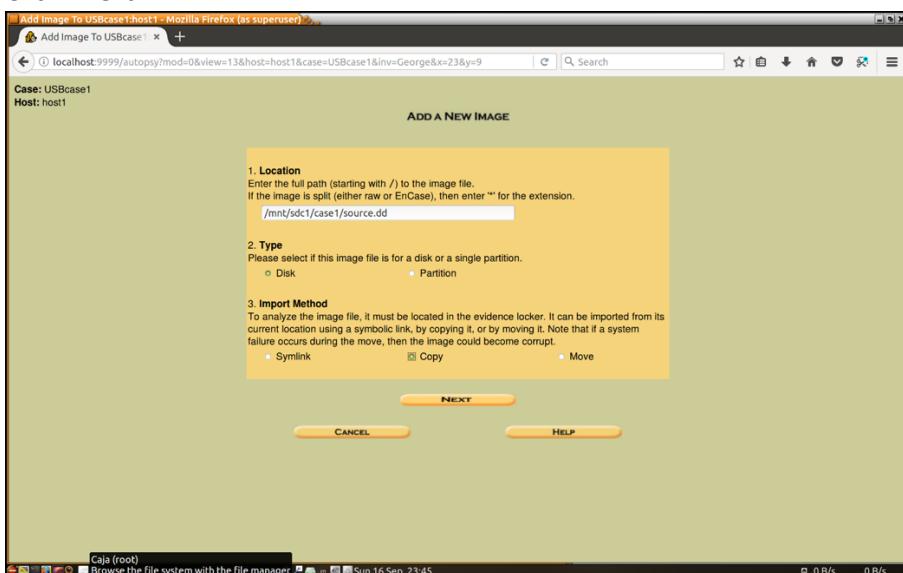
9. Click “Add Image File.”



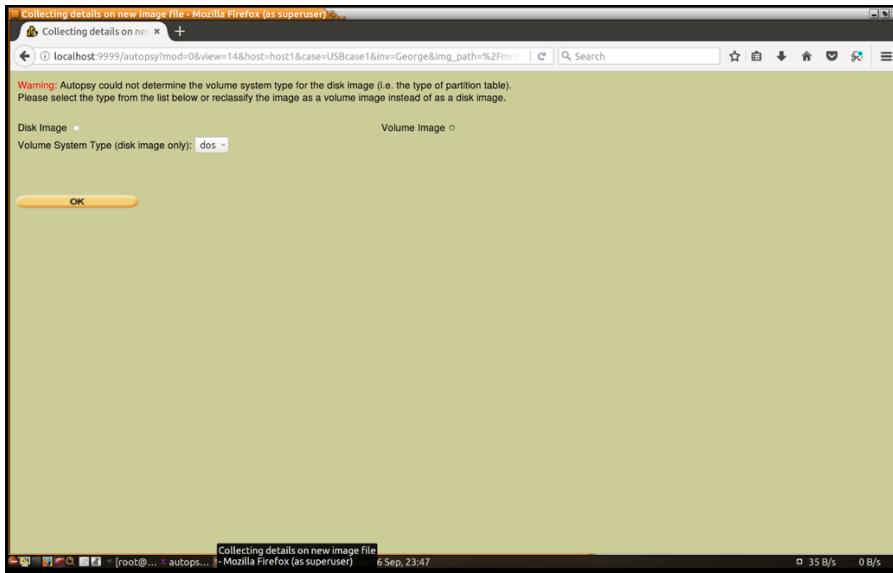
10. Fill in the fields in the “Add a New Image” screen.”

- “Location” Type /mnt/sdc1/case1/source.dd (***Please note: here you need to locate the source drive and provide the correct directory information***)
- “Import Method” select copy.

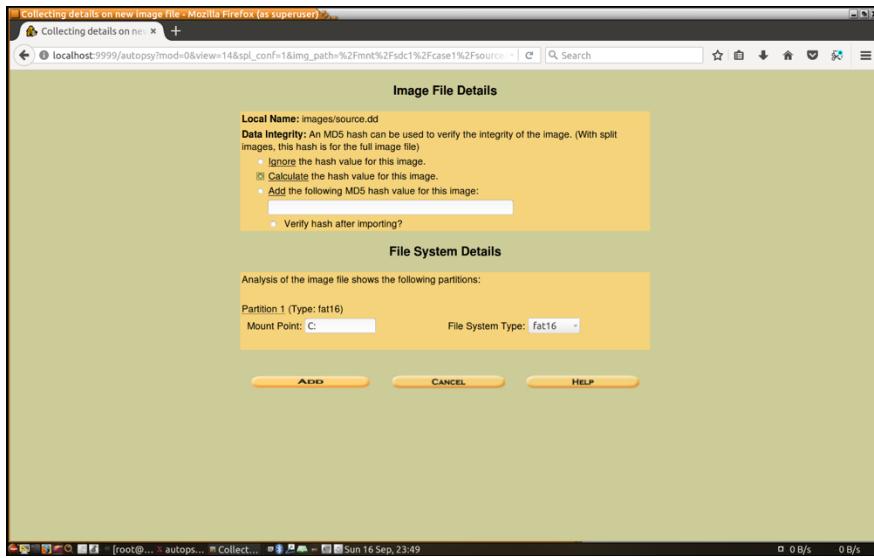
Click “Next.”



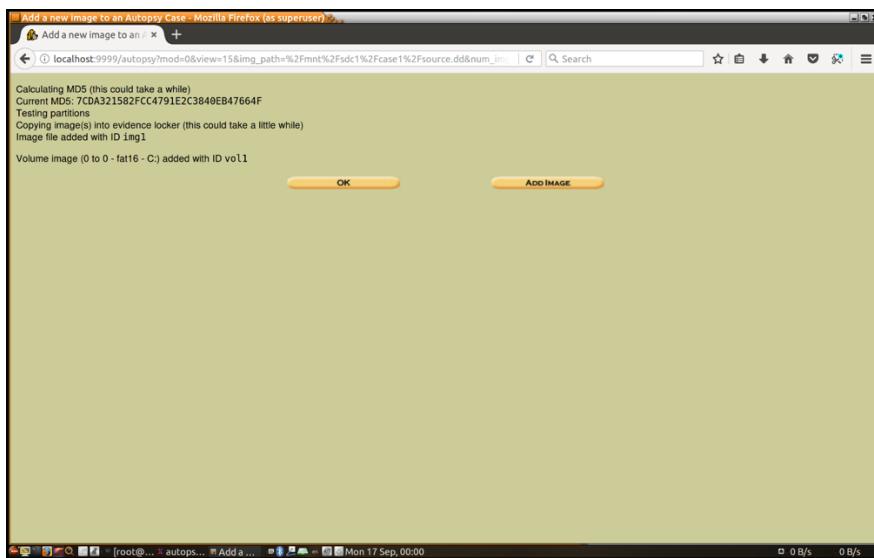
11. Select “Volume Image” on the right, ensure the “dos” is selected in the drop down of “Volume System Type”. Click “OK.”



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

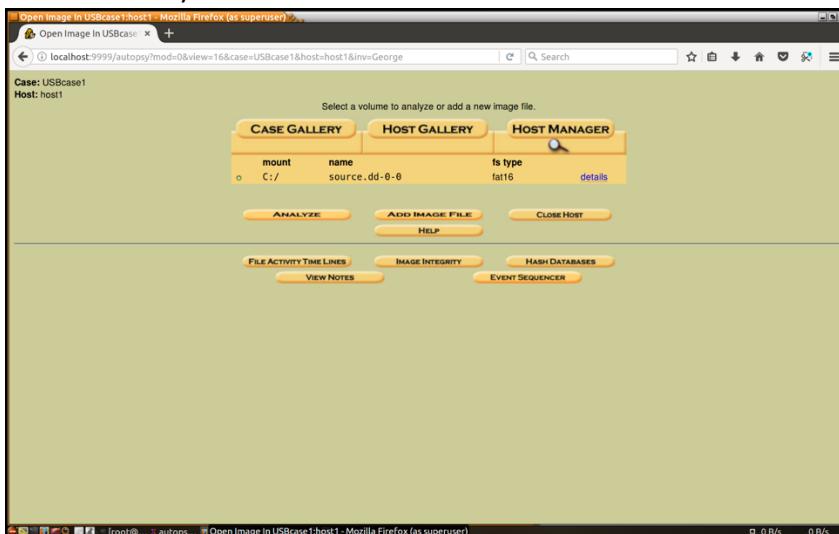


13. Once the calculations are done, click the “OK” button.

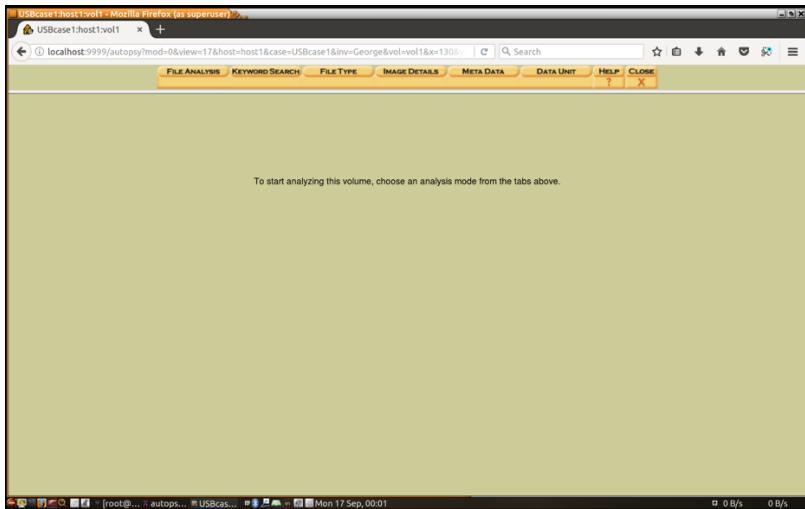


Task 2. Locate deleted/hidden files

14. Click the “Analyze” button.



15. Select “File Analysis”.

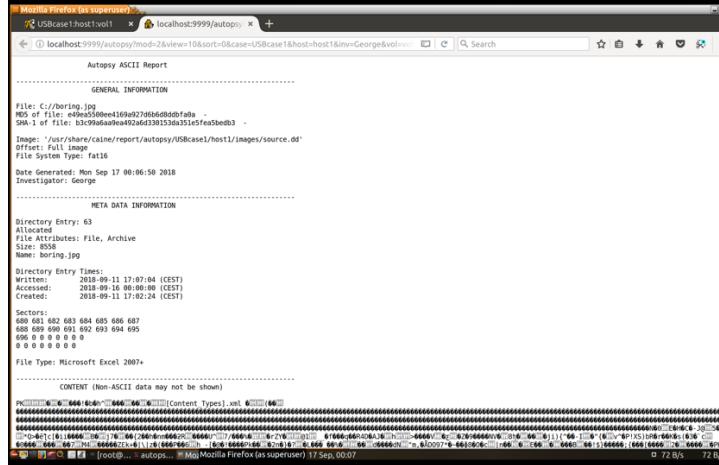
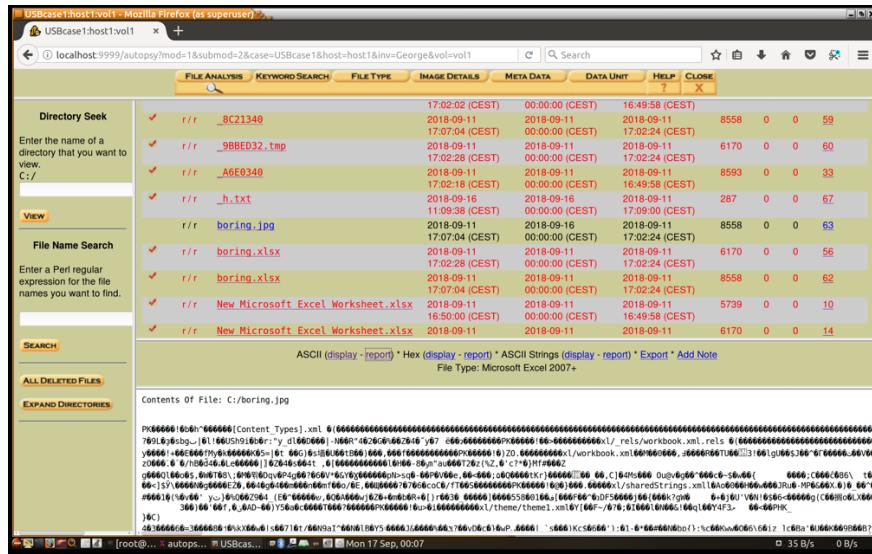


16. The files labeled in red are the deleted files. They also are the ones with a checkmark under the DEL to the left of the filename.

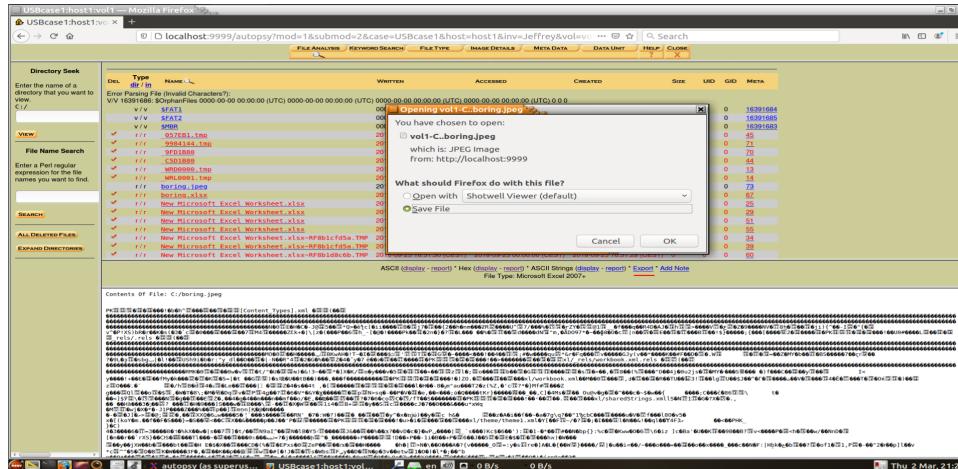
- a. Click on the files and examine them in the window below.

Current Directory: C:/									
DEL	Type	Name	Written	Accessed	Created	Size	UID	GID	META
Error for file name (invalid characters):									
VV15416329 - \$OrphanFile 0000-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC), 0000-00-00 00:00:00 (UTC) 0 0 0									
v/v	SFAT1		0000-00-00	0000-00-00	0000-00-00	128512	0	0	16416388
v/v	SFAT2		0000-00-00	0000-00-00	0000-00-00	128512	0	0	16416389
v/v	\$MBR		0000-00-00	0000-00-00	0000-00-00	512	0	0	16416387
✓	r/r	6ECE263.tmp	2018-09-11	2018-09-11	2018-09-11	6170	0	0	30
✓	r/r	7E5F108.tmp	2018-09-11	2018-09-11	2018-09-11	8593	0	0	34
✓	r/r	82E9340	2018-09-11	2018-09-11	2018-09-11	8593	0	0	28
✓	r/r	8C21340	2018-09-11	2018-09-11	2018-09-11	8558	0	0	59
✓	r/r	98BED032.tmp	2018-09-11	2018-09-11	2018-09-11	6170	0	0	60
✓	r/r	A6E9340	2018-09-11	2018-09-11	2018-09-11	8593	0	0	33
✓	r/r	h.txt	2018-09-16	2018-09-16	2018-09-11	287	0	0	67

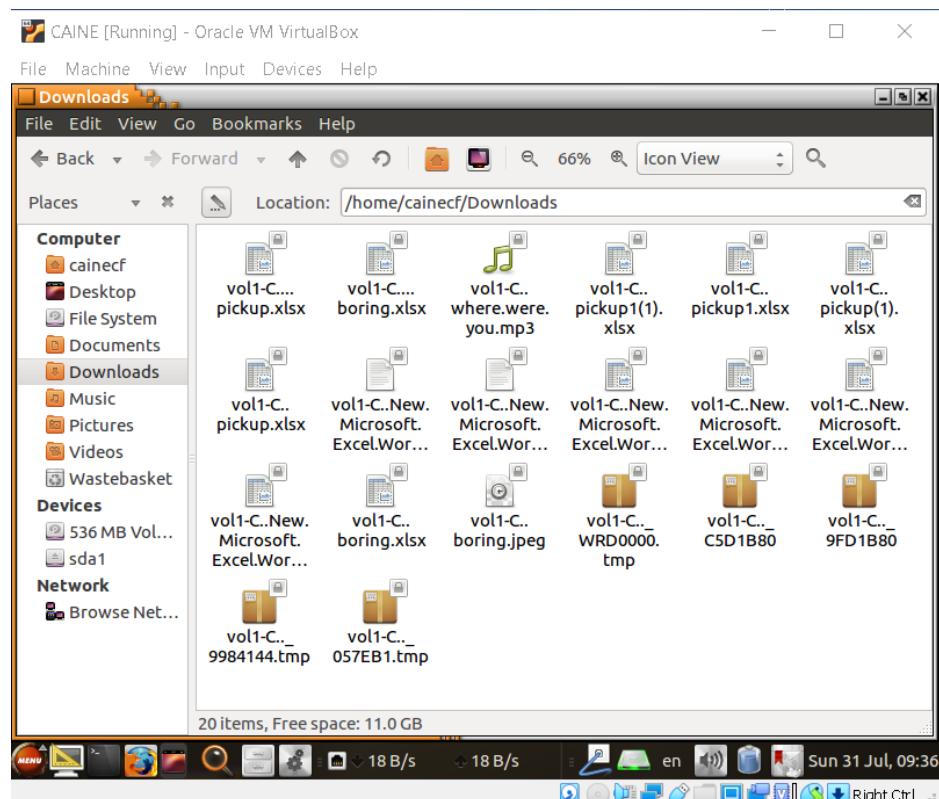
- b. If data appears, click report next to ASCII to view a report of the data. (Clicking on "display" does not give you the report. You must click on the word "report".) "X" out of this tab.



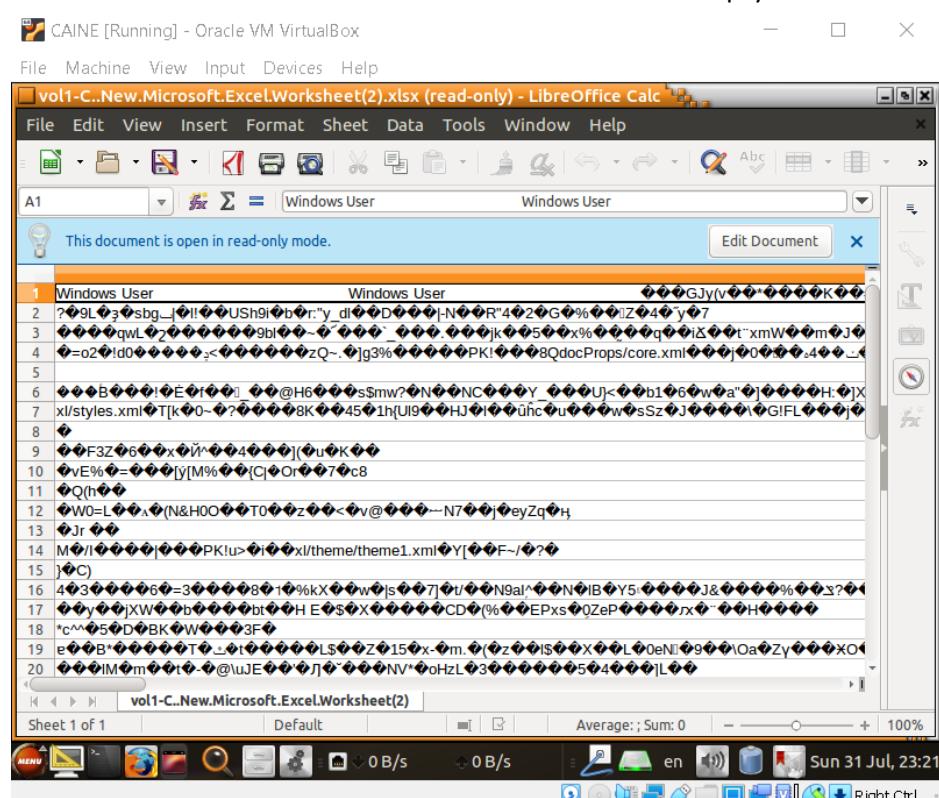
- c. Then click “Export” to export the file from the image to the Downloads folder.



- 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

CAINE [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

vol1-C..pickup(1).xlsx (read-only) - LibreOffice Calc

A1 Pick up Schedule of Drugs

This document is open in read-only mode.

Edit Document Input line

A	B	C	D	E	F	G	H	I
1	Pick up Schedule of Drugs							
2	Date	Time	Location	Drugtype				
3	01-Nov	5pm	Sacramen	Ecstasy				
4	10-Nov	8am	San Fran	Heroin				
5	01-Dec	11am	Kensingto	Adderall				
6	29-Dec	3am	5th stree	Cocaine				
7	30-Dec	6am	63rd stree	Marijuana				
8	05-Jan	12pm	Kensingto	Heroin				
9	12-Jan	11pm	Kensingto	Ecstasy				
10	19-Jan	3am	Hay Road	Cocaine				
11	26-Jan	3pm	52nd stree	Heroin				
12	03-Feb	2am	Hay Road	Ecstasy				
13	10-Feb	8am	Kensingto	Heroin				
14	18-Feb	2am	5th stree	Cocaine				
15	03-Apr	11am	San Fran	Heroin				
16								
17								
18								

Sheet1 | PageStyle_Sheet1 | Average: Sum: 0 | 100% | Sun 31 Jul, 09:39 | Right Ctrl

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.

USBcase1:host1:vol1 - Mozilla Firefox (as superuser)

localhost:9999/autopsy?mod=1&submod=2&case=USBcase1&host=host1&inv=George&vol=vol1

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE

Directory Seek
Enter the name of a directory that you want to view.
C:/

VIEW

File Name Search
Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES EXPAND DIRECTORIES

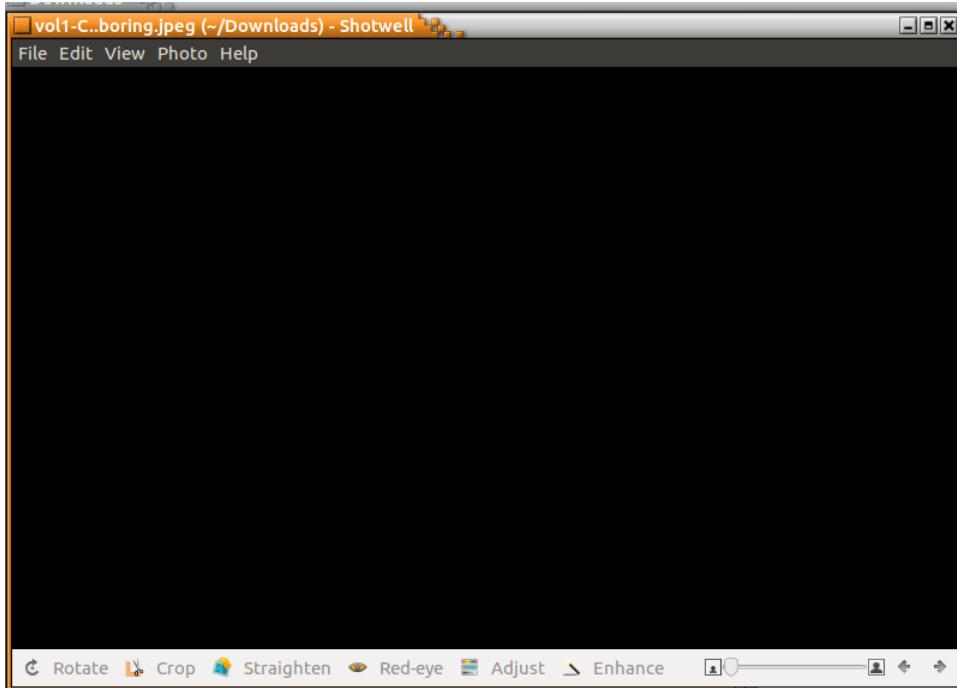
✓	r/r	New Microsoft Excel Worksheet.xlsx-RF430e86bc.TMP	2018-09-11 16:50:00 (CEST)	00:00:00 (CEST)	16:49:58 (CEST)	5739	0	0	24
✓	r/r	New Microsoft Excel Worksheet.xlsx-RF430e86bc.TMP	2018-09-11 17:02:26 (CEST)	00:00:00 (CEST)	17:02:24 (CEST)	0	0	0	49
✓	r/r	New Microsoft Excel Worksheet.xlsx-RF430e86bc.TMP	2018-09-11 17:02:26 (CEST)	00:00:00 (CEST)	17:02:24 (CEST)	5739	0	0	54
✓	r/r	New Text Document.txt	2018-09-11 17:09:02 (CEST)	00:00:00 (CEST)	17:09:00 (CEST)	0	0	0	66
✓	r/r	pickup.xlsx	2018-09-11 16:50:02 (CEST)	00:00:00 (CEST)	16:49:58 (CEST)	6170	0	0	26
✓	r/r	pickup.xlsx	2018-09-11 17:02:02 (CEST)	00:00:00 (CEST)	16:49:58 (CEST)	8593	0	0	32
✓	r/r	pickup.xlsx	2018-09-11 17:02:18 (CEST)	00:00:00 (CEST)	16:49:58 (CEST)	8593	0	0	36
	r/r	SOURCE_CCS (Volume Label Entry)	2018-09-11 16:49:50 (CEST)	00:00:00-00:00	00:00:00-00:00	0	0	0	3
	d/d	System Volume Information/	2018-09-11	2018-09-11	2018-09-11	8192	0	0	6

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note
File Type: Microsoft Excel 2007+ Deleted File Recovery Mode

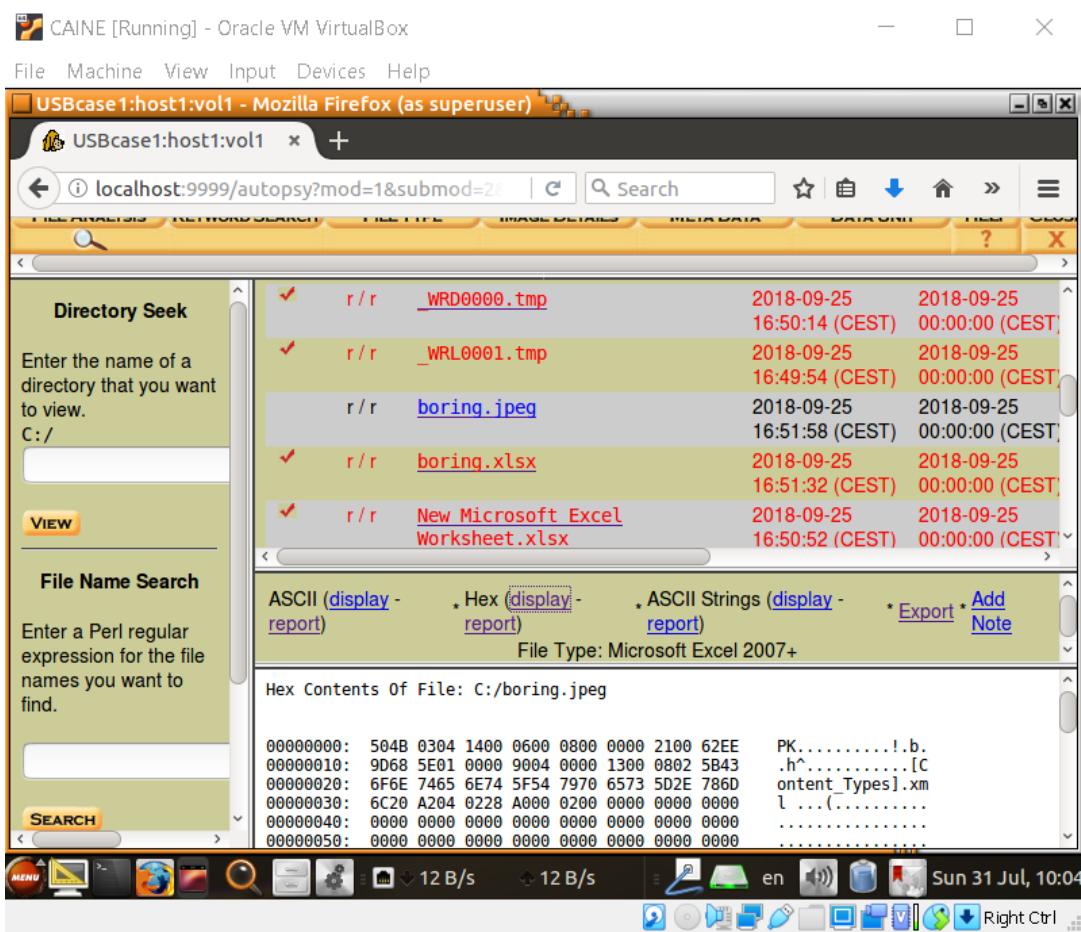
Hex Contents Of File: C:/pickup.xlsx

```
00000000: 5B48 0304 1408 0600 0800 0000 2100 62EE PK.....l.b.
00000010: 0008 5E01 0000 0004 0000 1300 0002 5843 .h.....[C
00000020: 6F6E 7465 6E74 5F54 7979 6573 5D2E 7860 ontent_Types.xml
00000030: 6C28 A204 0228 A000 0200 0000 0000 0000 l...{.....
00000040: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000050: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000060: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000070: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000080: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000090: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000A0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000B0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000C0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000D0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000E0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000F0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000G0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000H0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000I0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000J0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000K0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000L0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000M0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000N0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000O0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000P0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000Q0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000R0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000S0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000T0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000U0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000V0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000W0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000X0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000Y0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000Z0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000a0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000b0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000c0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000d0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000e0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000f0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000g0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000h0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000i0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000j0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000k0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000l0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000m0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000n0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000o0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000p0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000q0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000r0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000s0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000t0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000u0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000v0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000w0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000x0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000y0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000z0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000a1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000b1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000c1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000d1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000e1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000f1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000g1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000h1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000i1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000j1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000k1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000l1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000m1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000n1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000o1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000p1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000q1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000r1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000s1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000t1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000u1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000v1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000w1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000x1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000y1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000z1: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000a2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000b2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000c2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000d2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000e2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000f2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000g2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000h2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000i2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000j2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000k2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000l2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000m2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000n2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000o2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000p2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000q2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000r2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000s2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000t2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000u2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000v2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000w2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000x2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000y2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000z2: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000a3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000b3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000c3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000d3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000e3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000f3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000g3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000h3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000i3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000j3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000k3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000l3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000m3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000n3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000o3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000p3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000q3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000r3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000s3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000t3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000u3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000v3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000w3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000x3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000y3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000z3: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000a4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000b4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000c4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000d4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000e4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000f4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000g4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000h4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000i4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000j4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000k4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000l4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000m4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000n4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000o4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000p4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000q4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000r4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000s4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000t4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000u4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000v4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000w4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000x4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000y4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000z4: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000a5: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000b5: 0
```

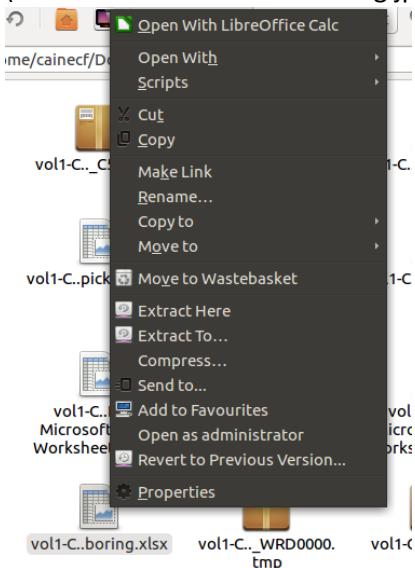
18. Follow the same procedure for the files listed in blue. These are files that exist openly on the drive. If the file does not work when you open it, examine the “magic number” as seen in the magic number chart (see Appendix) to ensure that the file is labeled correctly. The Magic Number is the first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



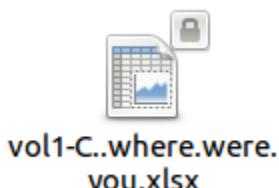
If you changed the extension correctly, the icon should have changed.

A screenshot of the LibreOffice Calc application window. The title bar says "vol1-C.boring.xlsx (read-only) - LibreOffice Calc". The main area shows a table titled "Schedule of drug Delivery". The columns are labeled A through K. The data includes rows for dealers like Dealer, Kate, Johnny, Linz, Bob, George, and others, detailing their day, time, dorm/building, campus location, and drug type. The table has 10 rows of data from 2 to 11, followed by empty rows 12 through 28.

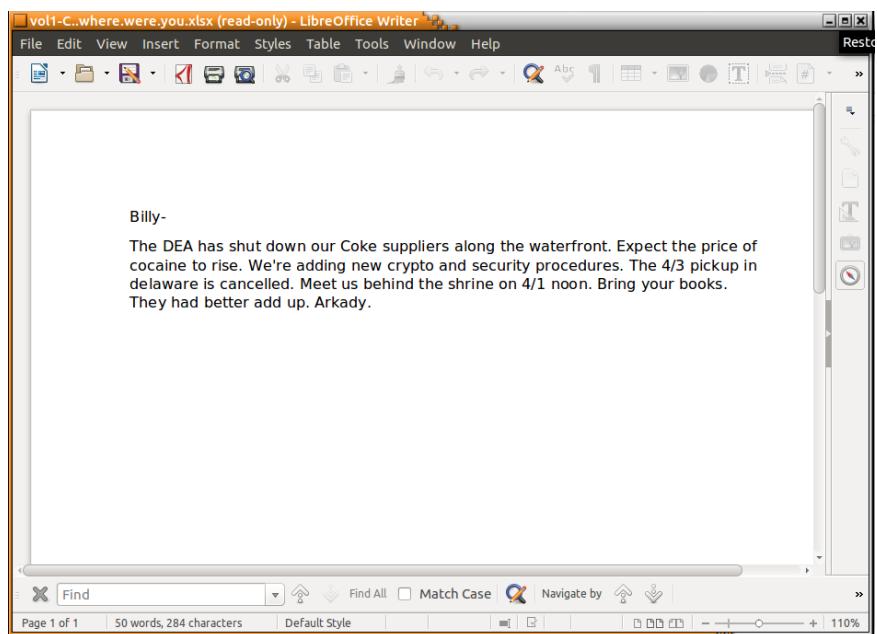
A	B	C	D	E	F	G	H	I	J	K
1	Schedule	of drug Delivery								
2	Dealer	Day	Time	Dorm/Building	Campus	Drug				
3	Kate	Tuesday	6pm	Brill	North	Heroin				
4	Johnny	Tuesday	12pm	Runkle	south	Adderal				
5	Johnny	Wednesday	12pm	Rec Hall	North	Heroin				
6	Linz	Thursday	9pm	Thompson	east	Cocaine				
7	Bob	Saturday	2am	Wolf	west	Adderal				
8	George	Sunday	5pm	Sprout	south	Ecstasy				
9	Kate	Sunday	3pm	Snyder	east	Heroin				
10	Bob	Friday	3am	McElwain	south	Ecstasy				
11										
12										
13										
14										
15										
16										
17										
18										
19										
20										
21										
22										
23										
24										
25										
26										
27										
28										

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