CSC153: Activity 4 - Basic Forensic Analysis using Autopsy

Ryan Kozak

SACRAMENTO
STATE

2019-10-04

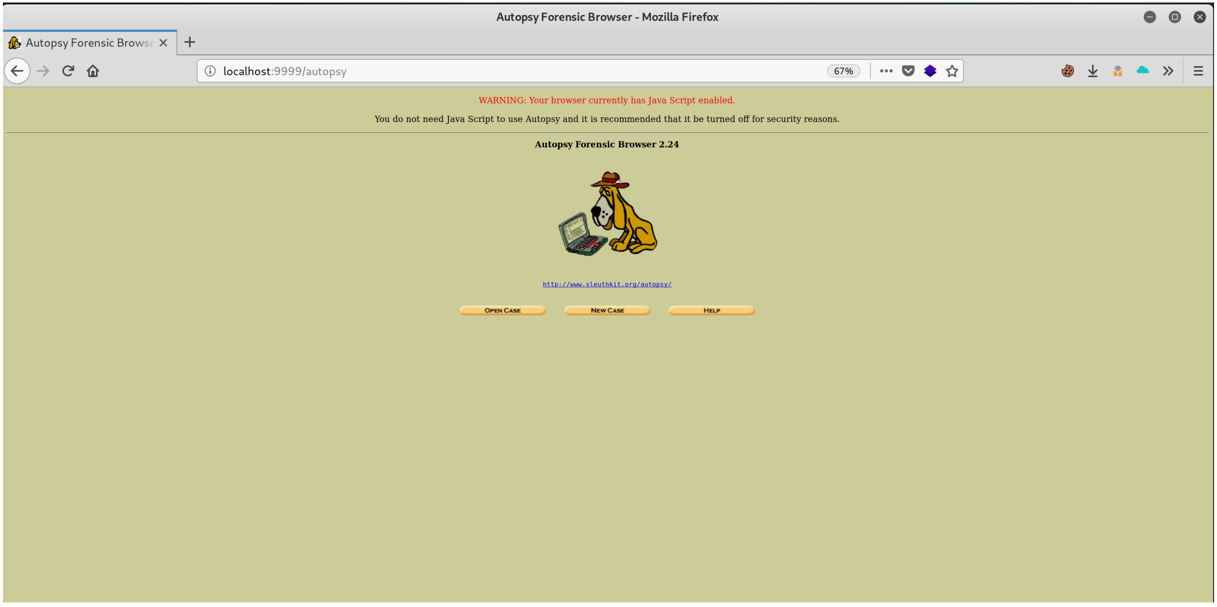
Scenario

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.

Tasks 0 through 2

Below are the steps taken to create a case and investigate the suspect's drive using Autopsy.

Download the image of suspect's drive, open Autopsy.



WARNING: Your browser currently has Java Script enabled.

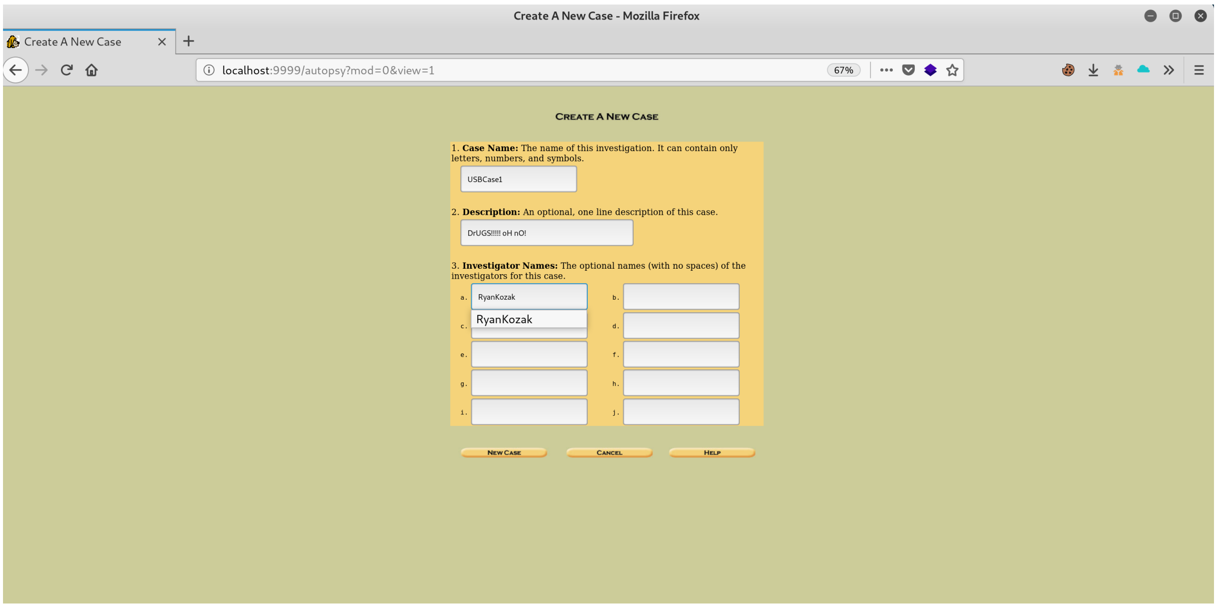
You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

Autopsy Forensic Browser 2.24

http://www.sleuthkit.org/autopsy/

Figure 1: Open Autopsy browser.

Create a new case to begin our investigation.



Create A New Case - Mozilla Firefox
Create A New Case
localhost:9999/autopsy?mod=0&view=1
67%
New Case
Cancel
Help

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

USBCase1

2. **Description:** An optional, one line description of this case.

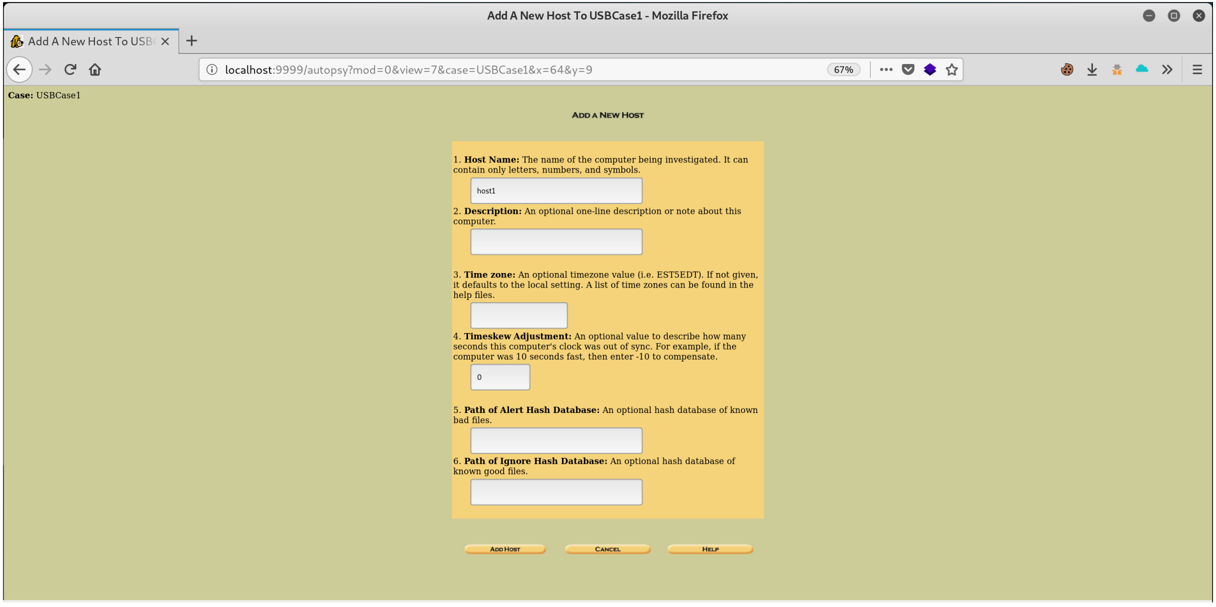
DrUGS!!!!! oH nO!

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. RyanKozak
b.
c.
d.
e.
f.
g.
h.
i.
j.

Figure 2: Create a new case.

Add a new host.



Add A New Host To USBCase1 - Mozilla Firefox
Add A New Host To USB
localhost:9999/autopsy?mod=0&view=7&case=USBCase1&x=64&y=9
67%
Add Host
Cancel
Help

Case: USBCase1

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

host1

2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

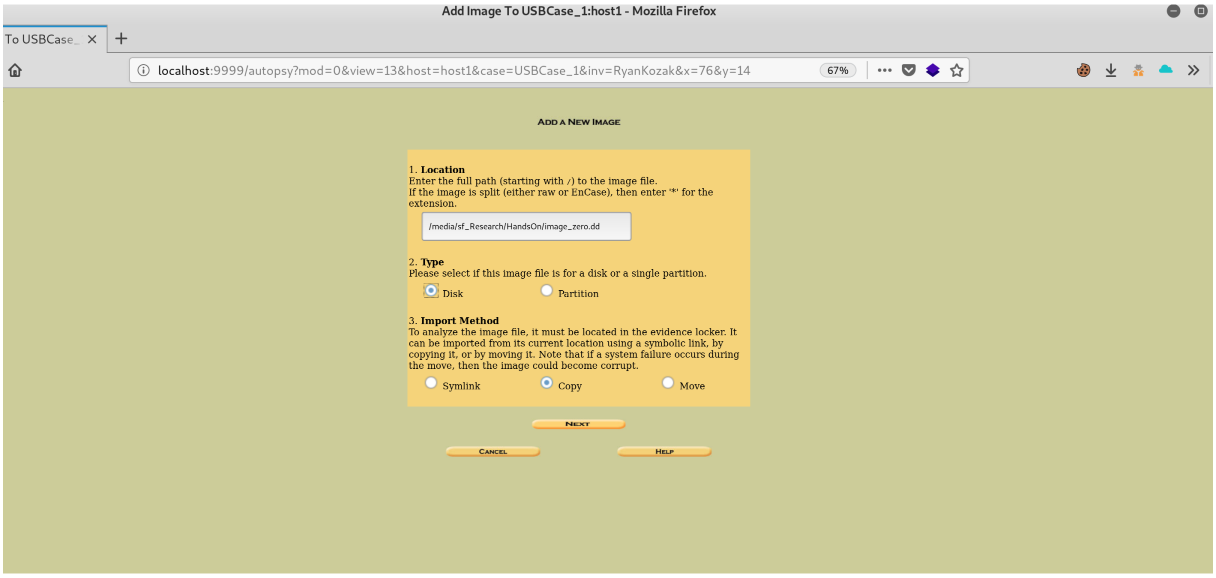
0

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

Figure 3: Add host.

Adding an image of the suspect's drive.


Add Image To USBCase_1:host1 - Mozilla Firefox
To USBCase_
localhost:9999/autopsy?mod=0&view=13&host=host1&case=USBCase_1&inv=RyanKozak&x=76&y=14
67%
ADD A NEW IMAGE
NEXT
CANCEL
HELP

1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

/media/sf_Research/HandsOn/image_zero.dd

2. **Type**
Please select if this image file is for a disk or a single partition.

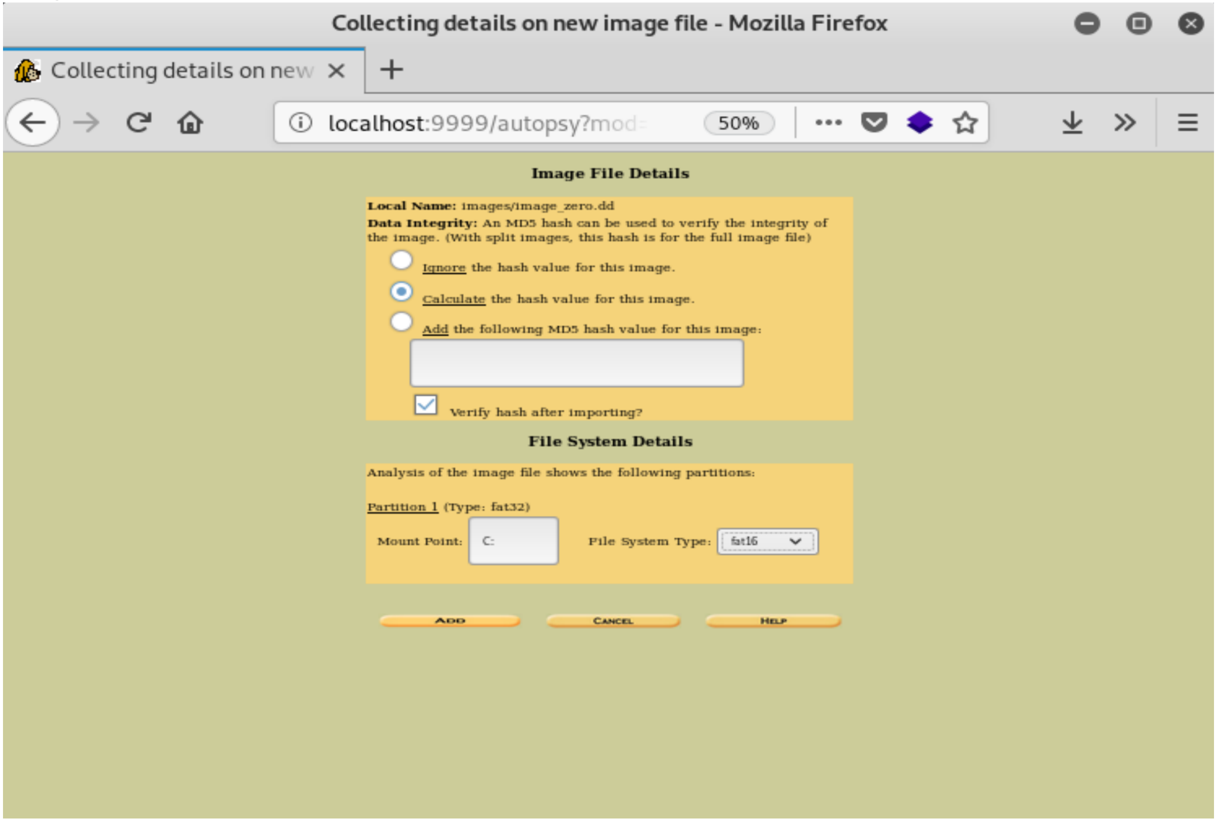
● Disk ○ Partition

3. **Import Method**
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

○ Symlink ● Copy ○ Move

Figure 4: Adding an image.

Image details and hash calculation.


Collecting details on new image file - Mozilla Firefox
Collecting details on new
localhost:9999/autopsy?mod=
50%
Image File Details
File System Details
ADD
CANCEL
HELP

Local Name: images/image_zero.dd
Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

○ Ignore the hash value for this image.
● Calculate the hash value for this image.
○ Add the following MD5 hash value for this image:

☑ Verify hash after importing?

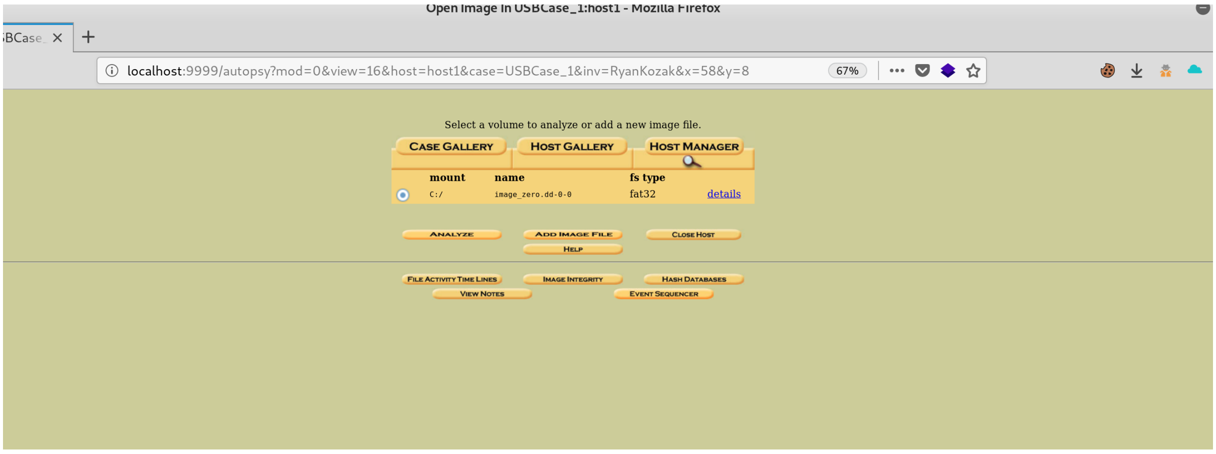
Analysis of the image file shows the following partitions:

Partition 1 (Type: fat32)

Mount Point: C: File System Type: fat16

Figure 5: Image details.

After adding the image we then are ready to analyze the drive.



Open Image In USBCase_1:host1 - Mozilla Firefox
BCase ×
+
localhost:9999/autopsy?mod=0&view=16&host=host1&case=USBCase_1&inv=RyanKozak&x=58&y=8
67%

Select a volume to analyze or add a new image file.

	mount	name	fs type	
●	C:/	image_zero.dd-0-0	fat32	details

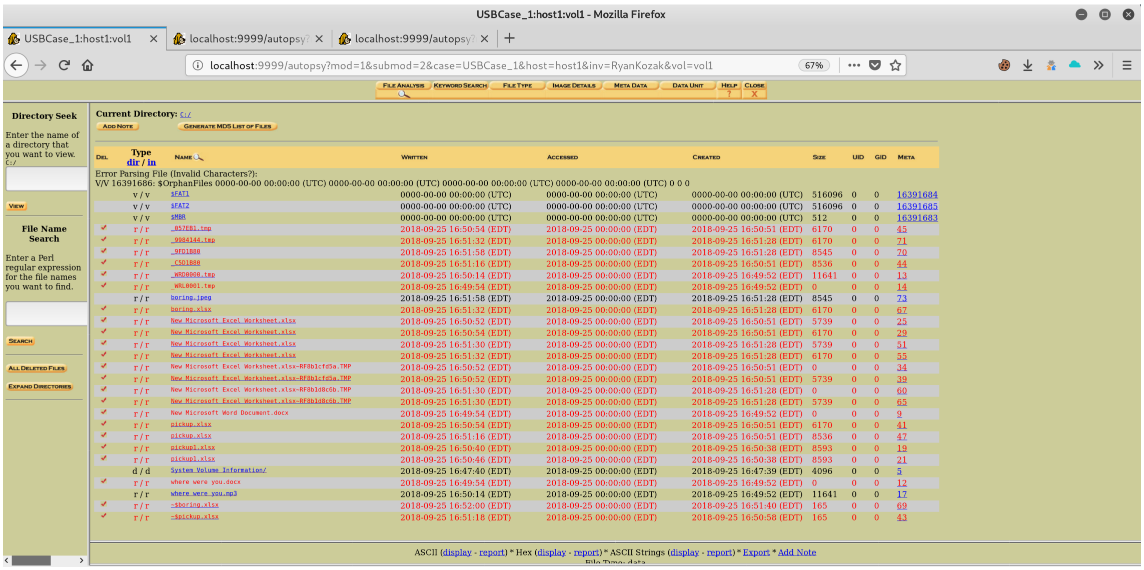
Figure 6: Image ready for analysis.

The rest of the screen shots of the analysis can be found in the questions answered below. This makes more sense to me than repeating screen shots and making this even longer than it has to be

Task 3

1. How many files are there on the USB drive? What are they?

   - There are two files that have not been deleted, `boring.jpg` and `where_were_you.mp3` (ignoring the system files such as the boot record.). See figure 7 below.



USBCase_1:host1:vol1 - Mozilla Firefox
USBCase_1:host1:vol1 ×
localhost:9999/autopsy? ×
localhost:9999/autopsy? ×
+
localhost:9999/autopsy?mod=1&submod=2&case=USBCase_1&host=host1&inv=RyanKozak&vol=vol1
67%
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
?
CLOSE
X

Directory Seek

Enter the name of a directory that you want to view.

C:/

File Name Search

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

SEARCH
ALL DELETED FILES
EXPAND DIRECTORIES

Current Directory: C:/

ADD NOTE
GENERATE MD5 LIST OF FILES

Error Parsing File (Invalid Characters?):
V/V 16391686: $OrphanFiles 0000-00-00 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

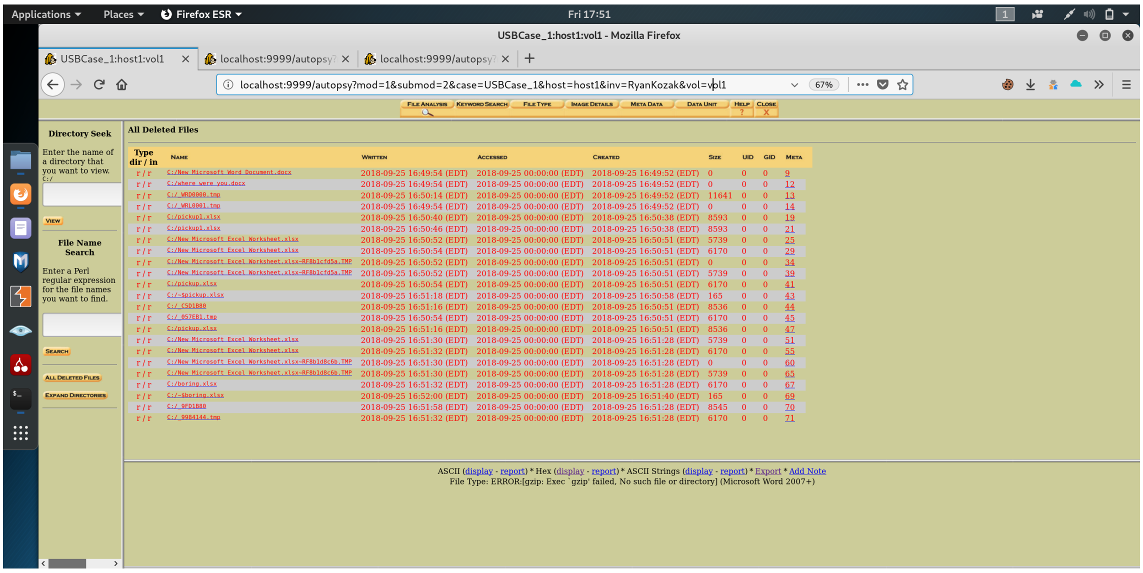
DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	v / v	$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	516096	0	0	16391684
	v / v	$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	516096	0	0	16391685
	v / v	$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	16391683
✓	r / r	_057EB1.tmp	2018-09-25 16:50:54 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:51 (EDT)	6170	0	0	45
✓	r / r	_9984144.tmp	2018-09-25 16:51:32 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:28 (EDT)	6170	0	0	71
✓	r / r	_9FD1B80	2018-09-25 16:51:58 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:28 (EDT)	8545	0	0	70
✓	r / r	_C5D1B80	2018-09-25 16:51:16 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:51 (EDT)	8536	0	0	44
✓	r / r	_WRD0000.tmp	2018-09-25 16:50:14 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:49:52 (EDT)	11641	0	0	13
✓	r / r	_WRL0001.tmp	2018-09-25 16:49:54 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:49:52 (EDT)	0	0	0	14
	r / r	boring.jpeg	2018-09-25 16:51:58 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:28 (EDT)	8545	0	0	73
✓	r / r	boring.xlsx	2018-09-25 16:51:32 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:28 (EDT)	6170	0	0	67
✓	r / r	New Microsoft Excel Worksheet.xlsx	2018-09-25 16:50:52 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:51 (EDT)	5739	0	0	25
✓	r / r	New Microsoft Excel Worksheet.xlsx	2018-09-25 16:50:54 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:51 (EDT)	6170	0	0	29
✓	r / r	New Microsoft Excel Worksheet.xlsx	2018-09-25 16:51:30 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:28 (EDT)	5739	0	0	51
✓	r / r	New Microsoft Excel Worksheet.xlsx	2018-09-25 16:51:32 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:28 (EDT)	6170	0	0	55
✓	r / r	New Microsoft Excel Worksheet.xlsx~RF8b1cfd5a.TMP	2018-09-25 16:50:52 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:51 (EDT)	0	0	0	34
✓	r / r	New Microsoft Excel Worksheet.xlsx~RF8b1cfd5a.TMP	2018-09-25 16:50:52 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:51 (EDT)	5739	0	0	39
✓	r / r	New Microsoft Excel Worksheet.xlsx~RF8b1d8c6b.TMP	2018-09-25 16:51:30 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:28 (EDT)	0	0	0	60
✓	r / r	New Microsoft Excel Worksheet.xlsx~RF8b1d8c6b.TMP	2018-09-25 16:51:30 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:28 (EDT)	5739	0	0	65
✓	r / r	New Microsoft Word Document.docx	2018-09-25 16:49:54 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:49:52 (EDT)	0	0	0	9
✓	r / r	pickup.xlsx	2018-09-25 16:50:54 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:51 (EDT)	6170	0	0	41
✓	r / r	pickup.xlsx	2018-09-25 16:51:16 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:51 (EDT)	8536	0	0	47
✓	r / r	pickup1.xlsx	2018-09-25 16:50:40 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:38 (EDT)	8593	0	0	19
✓	r / r	pickup1.xlsx	2018-09-25 16:50:46 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:38 (EDT)	8593	0	0	21
	d / d	System Volume Information/	2018-09-25 16:47:40 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:47:39 (EDT)	4096	0	0	5
✓	r / r	where were you.docx	2018-09-25 16:49:54 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:49:52 (EDT)	0	0	0	12
	r / r	where were you.mp3	2018-09-25 16:50:14 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:49:52 (EDT)	11641	0	0	17
✓	r / r	~$boring.xlsx	2018-09-25 16:52:00 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:40 (EDT)	165	0	0	69
✓	r / r	~$pickup.xlsx	2018-09-25 16:51:18 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:58 (EDT)	165	0	0	43

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note
File Type: data

Figure 7: Files on USB drive.

2. Which file/files are deleted?

- It appears as if there are around 23 deleted files. Some of these files are renamed versions of one another, probably temp files from the OS, see figure 8.



All Deleted Files

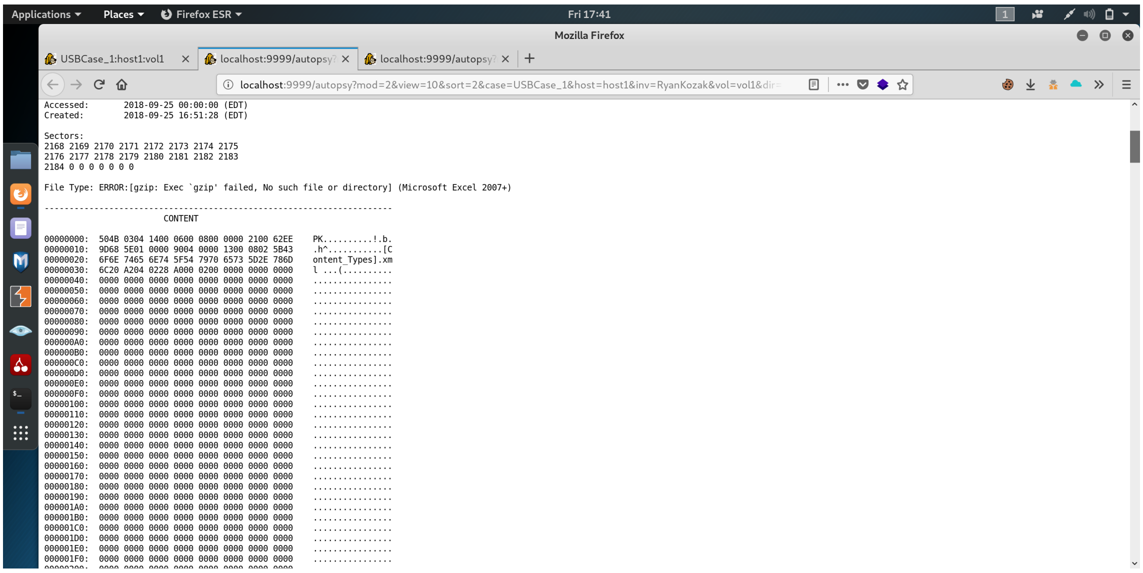
Type dir / in	Name	Written	Accessed	Created	Size	UID	GID	Meta
r / r	C:/New Microsoft Word Document.docx	2018-09-25 16:49:54 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:49:52 (EDT)	0	0	0	9
r / r	C:/where were you.docx	2018-09-25 16:49:54 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:49:52 (EDT)	0	0	0	12
r / r	C:/_WRD0000.tmp	2018-09-25 16:50:14 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:49:52 (EDT)	11641	0	0	13
r / r	C:/_WRL0001.tmp	2018-09-25 16:49:54 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:49:52 (EDT)	0	0	0	14
r / r	C:/pickup1.xlsx	2018-09-25 16:50:40 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:38 (EDT)	8593	0	0	19
r / r	C:/pickup1.xlsx	2018-09-25 16:50:46 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:38 (EDT)	8593	0	0	21
r / r	C:/New Microsoft Excel Worksheet.xlsx	2018-09-25 16:50:52 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:51 (EDT)	5739	0	0	25
r / r	C:/New Microsoft Excel Worksheet.xlsx	2018-09-25 16:50:54 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:51 (EDT)	6170	0	0	29
r / r	C:/New Microsoft Excel Worksheet.xlsx~RF8b1cfd5a.TMP	2018-09-25 16:50:52 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:51 (EDT)	0	0	0	34
r / r	C:/New Microsoft Excel Worksheet.xlsx~RF8b1cfd5a.TMP	2018-09-25 16:50:52 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:51 (EDT)	5739	0	0	39
r / r	C:/pickup.xlsx	2018-09-25 16:50:54 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:51 (EDT)	6170	0	0	41
r / r	C:/~$pickup.xlsx	2018-09-25 16:51:18 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:58 (EDT)	165	0	0	43
r / r	C:/_C5D1B80	2018-09-25 16:51:16 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:51 (EDT)	8536	0	0	44
r / r	C:/_057EB1.tmp	2018-09-25 16:50:54 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:51 (EDT)	6170	0	0	45
r / r	C:/pickup.xlsx	2018-09-25 16:51:16 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:50:51 (EDT)	8536	0	0	47
r / r	C:/New Microsoft Excel Worksheet.xlsx	2018-09-25 16:51:30 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:28 (EDT)	5739	0	0	51
r / r	C:/New Microsoft Excel Worksheet.xlsx	2018-09-25 16:51:32 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:28 (EDT)	6170	0	0	55
r / r	C:/New Microsoft Excel Worksheet.xlsx~RF8b1d8c6b.TMP	2018-09-25 16:51:30 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:28 (EDT)	0	0	0	60
r / r	C:/New Microsoft Excel Worksheet.xlsx~RF8b1d8c6b.TMP	2018-09-25 16:51:30 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:28 (EDT)	5739	0	0	65
r / r	C:/boring.xlsx	2018-09-25 16:51:32 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:28 (EDT)	6170	0	0	67
r / r	C:/~$boring.xlsx	2018-09-25 16:52:00 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:40 (EDT)	165	0	0	69
r / r	C:/_9FD1B80	2018-09-25 16:51:58 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:28 (EDT)	8545	0	0	70
r / r	C:/_9984144.tmp	2018-09-25 16:51:32 (EDT)	2018-09-25 00:00:00 (EDT)	2018-09-25 16:51:28 (EDT)	6170	0	0	71

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note
File Type: ERROR:[gzip: Exec `gzip' failed, No such file or directory] (Microsoft Word 2007+)

Figure 8: Deleted files.

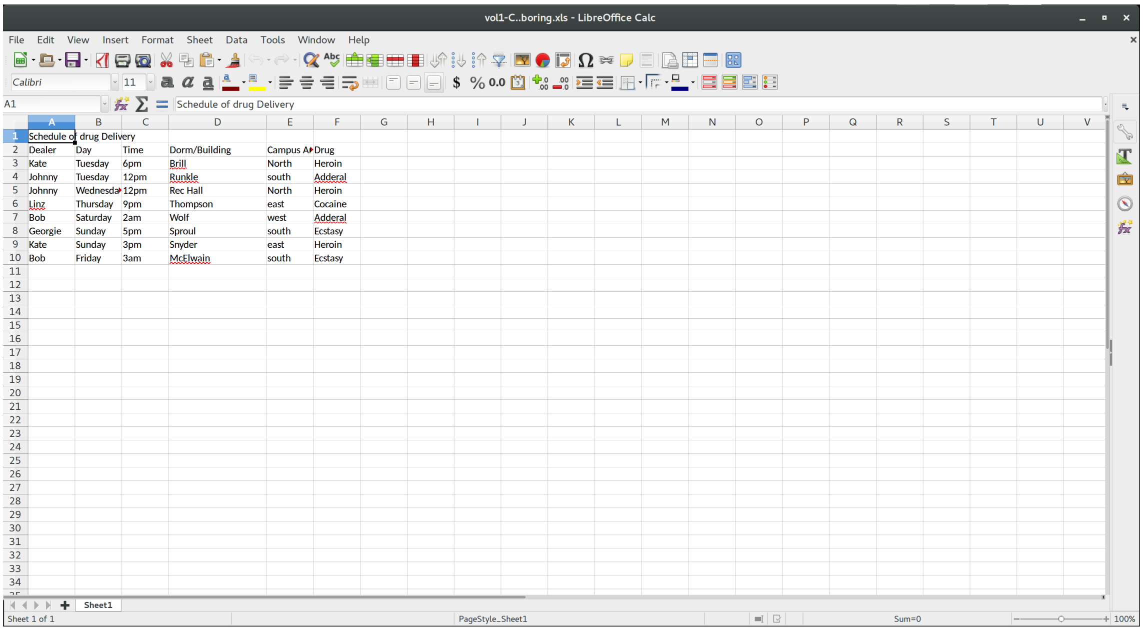
3. Can you open the `boring.jpg` file with an image viewer? Why? How did you open it eventually?

    - You cannot open `boring.jpg` with an image viewer because it is not an actual `.jpg` file. The file is a Microsoft Excel file. This can be determined a few ways. The way we were told to determine it was to look at the hex code to determine the magic number, which is `504b`. Autopsy also tells you in plain English that this is a Microsoft Excel 2007+ file. Both indications are visible in figure 9. The file can be opened simply by changing the file extension to `.xls` (see figure 10).



```
Accessed:       2018-09-25 00:00:00 (EDT)
Created:        2018-09-25 16:51:28 (EDT)

Sectors:
2168 2169 2170 2171 2172 2173 2174 2175
2176 2177 2178 2179 2180 2181 2182 2183
2184 0 0 0 0 0 0 0

File Type: ERROR:[gzip: Exec `gzip' failed, No such file or directory] (Microsoft Excel 2007+)

----------------------------------------------------------------------
                        CONTENT

00000000:  504B 0304 1400 0600 0800 0000 2100 62EE    PK.........!.b.
00000010:  9D68 5E01 0000 9004 0000 1300 0802 5B43    .h^..........[C
00000020:  6F6E 7465 6E74 5F54 7970 6573 5D2E 786D    ontent_Types].xm
00000030:  6C20 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    ................
00000100:  0000 0000 0000 0000 0000 0000 0000 0000    ................
00000110:  0000 0000 0000 0000 0000 0000 0000 0000    ................
00000120:  0000 0000 0000 0000 0000 0000 0000 0000    ................
00000130:  0000 0000 0000 0000 0000 0000 0000 0000    ................
00000140:  0000 0000 0000 0000 0000 0000 0000 0000    ................
00000150:  0000 0000 0000 0000 0000 0000 0000 0000    ................
00000160:  0000 0000 0000 0000 0000 0000 0000 0000    ................
00000170:  0000 0000 0000 0000 0000 0000 0000 0000    ................
00000180:  0000 0000 0000 0000 0000 0000 0000 0000    ................
00000190:  0000 0000 0000 0000 0000 0000 0000 0000    ................
000001A0:  0000 0000 0000 0000 0000 0000 0000 0000    ................
000001B0:  0000 0000 0000 0000 0000 0000 0000 0000    ................
000001C0:  0000 0000 0000 0000 0000 0000 0000 0000    ................
000001D0:  0000 0000 0000 0000 0000 0000 0000 0000    ................
000001E0:  0000 0000 0000 0000 0000 0000 0000 0000    ................
000001F0:  0000 0000 0000 0000 0000 0000 0000 0000    ................
```

Figure 9: Hexadecimal content of `boring.jpg`.



vol1-C..boring.xls - LibreOffice Calc
File Edit View Insert Format Sheet Data Tools Window Help
Calibri
11
A1
Sheet1
Sheet 1 of 1
PageStyle_Sheet1
Sum=0
100%

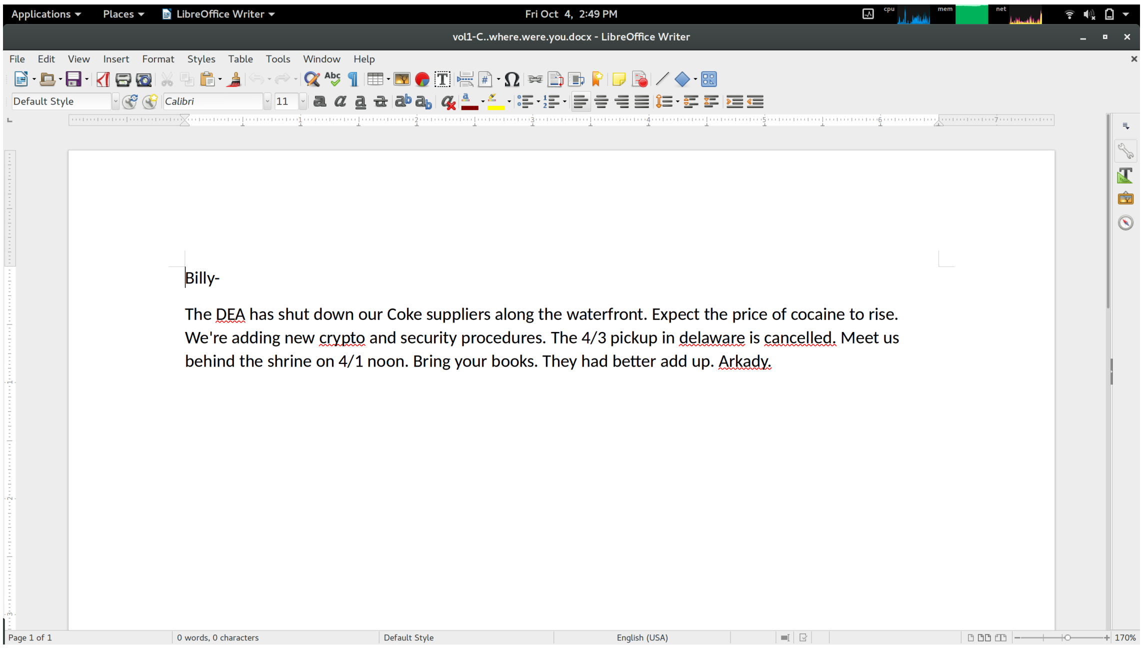
Schedule of drug Delivery

	A	B	C	D	E	F
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

Figure 10: Opened Excel file containing bad guys.

4. Were there any secret messages? If so, in which file are they located?

    - There was a secret message (...secret) in the `where_were_you.mp3` file found on the drive. It was actually a Microsoft `.doc` file (see figure 11).



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.

Figure 11: Where were you message.

5. What is the name of Billy's supplier?

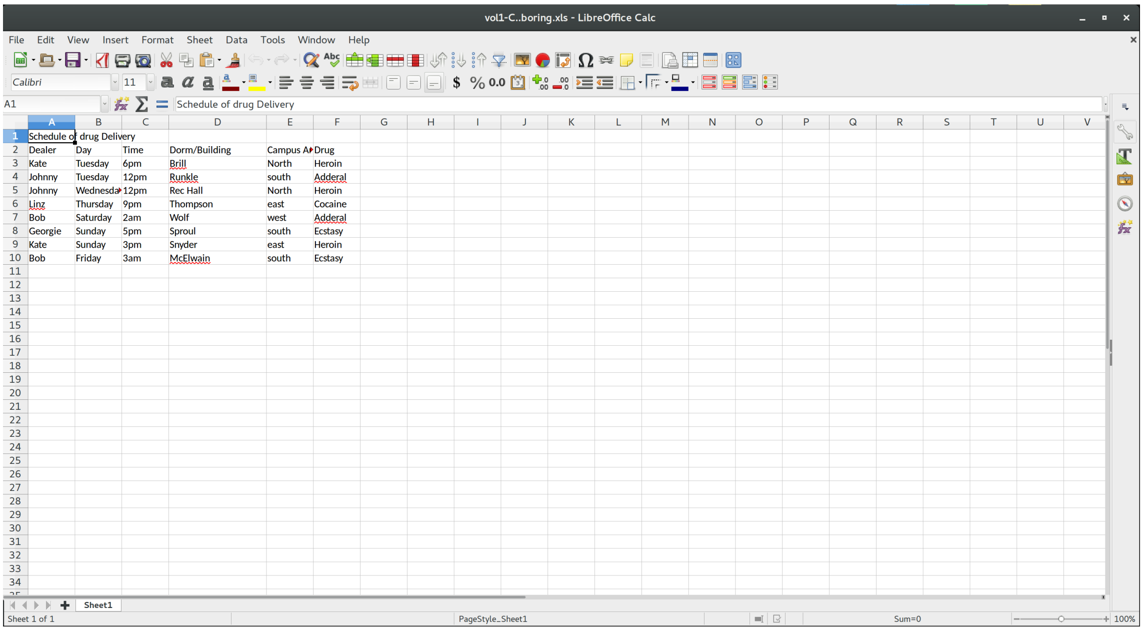
   - I'm not the police, but judging by the message found in figure 11 above it's **Arkady**.

6. When and where is the next meet?

   - See figure 11 again, because it appears they're meeting "behind the shrine" on 4/1 at noon.

7. Who else on campus is involved? (Take a screenshot to prove the answer)

   - We can determine the first names of the other individuals involved to be Kate, Johnny, Linz, and Bob. All the names listen in the `boring.jpg` Microsoft Excel sheet. See figure 12, a repeat of figure 10.



vol1-C..boring.xls - LibreOffice Calc
File Edit View Insert Format Sheet Data Tools Window Help
Calibri
11
A1
Sheet1
Sheet 1 of 1
PageStyle_Sheet1
Sum=0
100%

	A	B	C	D	E	F
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

Figure 12: The first names of those involved are in the dealers column.