James Gouveia

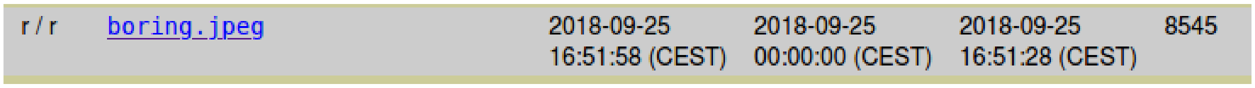
Professor Sun

CSC 153

University of California Sacramento

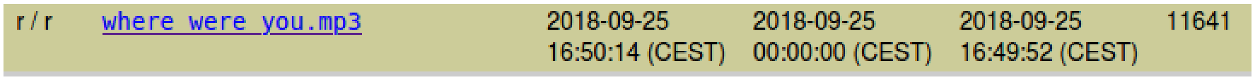
Activity 4

1. There are a total of 2 files on the USB Drive that were not deleted.
   boring.jpeg



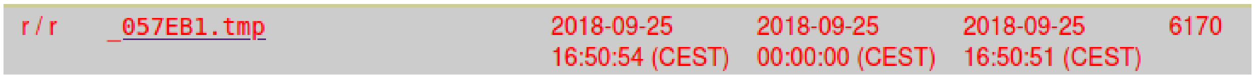
r / r	boring.jpeg	2018-09-25 16:51:58 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:51:28 (CEST)	8545

where were you.mp3 2018-09-25 16:50:14



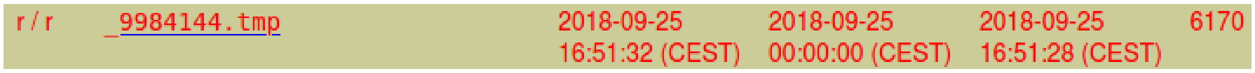
r / r	where were you.mp3	2018-09-25 16:50:14 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:49:52 (CEST)	11641

2. There are total of 22 deleted files
   _057EB1.tmp



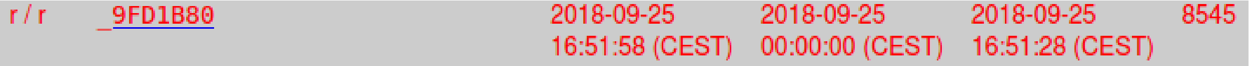
r / r	_057EB1.tmp	2018-09-25 16:50:54 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:50:51 (CEST)	6170

_9984144.tmp



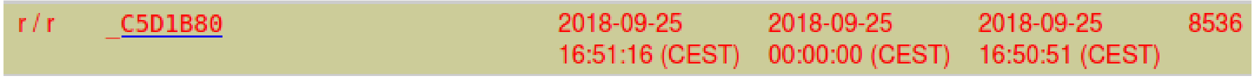
r / r	_9984144.tmp	2018-09-25 16:51:32 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:51:28 (CEST)	6170

_9FD1B80



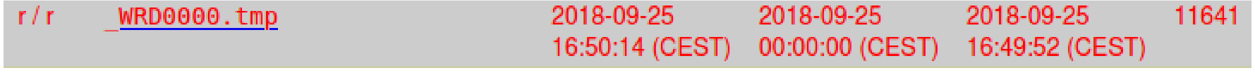
r / r	_9FD1B80	2018-09-25 16:51:58 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:51:28 (CEST)	8545

_C5D1B80



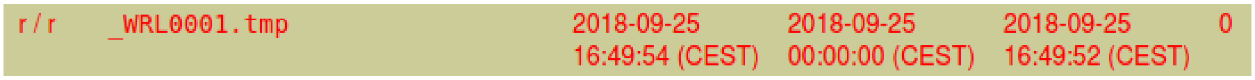
r / r	_C5D1B80	2018-09-25 16:51:16 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:50:51 (CEST)	8536

_ WRD0000.tmp



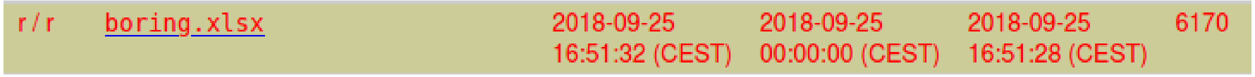
r / r	_WRD0000.tmp	2018-09-25 16:50:14 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:49:52 (CEST)	11641

_WRL0001.tmp



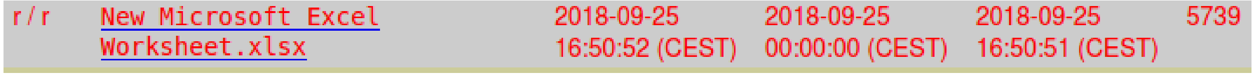
r / r	_WRL0001.tmp	2018-09-25 16:49:54 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:49:52 (CEST)	0

boring.xlsx



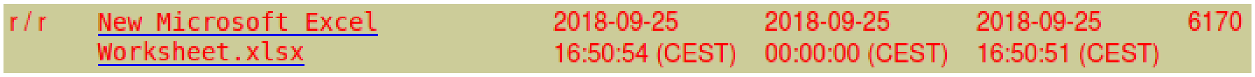
r/r	boring.xlsx	2018-09-25 16:51:32 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:51:28 (CEST)	6170

New Microsoft Excel Worksheet.xlsx



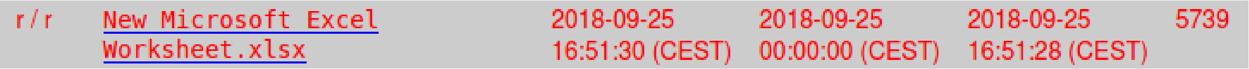
r/r	New Microsoft Excel Worksheet.xlsx	2018-09-25 16:50:52 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:50:51 (CEST)	5739

New Microsoft Excel Worksheet.xlsx



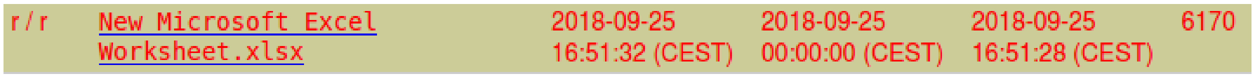
r/r	New Microsoft Excel Worksheet.xlsx	2018-09-25 16:50:54 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:50:51 (CEST)	6170

New Microsoft Excel Worksheet.xlsx



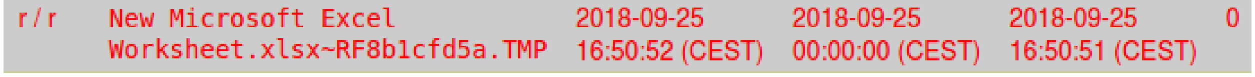
r/r	New Microsoft Excel Worksheet.xlsx	2018-09-25 16:51:30 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:51:28 (CEST)	5739

New Microsoft Excel Worksheet.xlsx



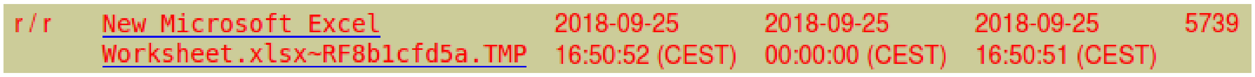
r/r	New Microsoft Excel Worksheet.xlsx	2018-09-25 16:51:32 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:51:28 (CEST)	6170

New Microsoft Excel Worksheet.xlsx~RF8b1cfd5a.TMP



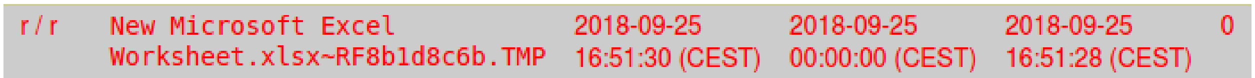
r/r	New Microsoft Excel Worksheet.xlsx~RF8b1cfd5a.TMP	2018-09-25 16:50:52 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:50:51 (CEST)	0

New Microsoft Excel Worksheet.xlsx~RF8b1cfd5a.TMP



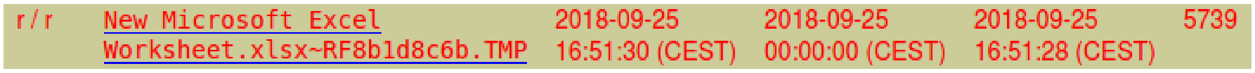
r/r	New Microsoft Excel Worksheet.xlsx~RF8b1cfd5a.TMP	2018-09-25 16:50:52 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:50:51 (CEST)	5739

New Microsoft Excel Worksheet.xlsx~RF8b1cfd5a.TMP~RF8b1d8c6b.TMP



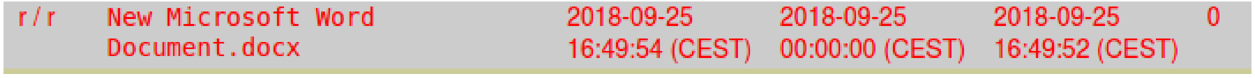
r/r	New Microsoft Excel Worksheet.xlsx~RF8b1d8c6b.TMP	2018-09-25 16:51:30 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:51:28 (CEST)	0

New Microsoft Excel Worksheet.xlsx~RF8b1cfd5a.TMP~RF8b1d8c6b.TMP



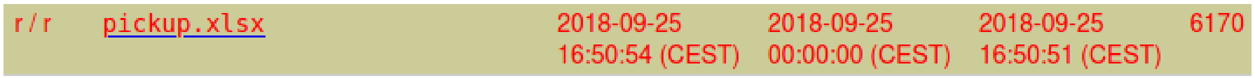
r/r	New Microsoft Excel Worksheet.xlsx~RF8b1d8c6b.TMP	2018-09-25 16:51:30 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:51:28 (CEST)	5739

New Microsoft Word Document.docx



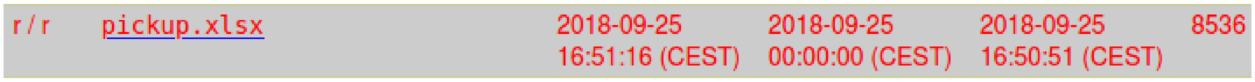
r/r	New Microsoft Word Document.docx	2018-09-25 16:49:54 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:49:52 (CEST)	0

pickup.xlsx 2018-09-25 16:50:54



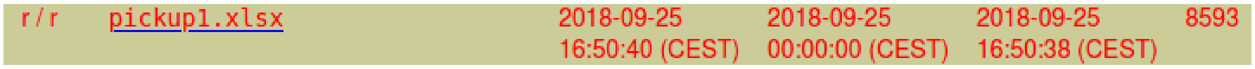
r/r	pickup.xlsx	2018-09-25 16:50:54 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:50:51 (CEST)	6170

pickup.xlsx 2018-09-25 16:51:16



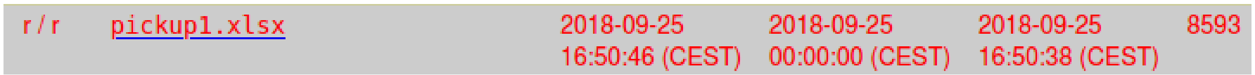
r/r	pickup.xlsx	2018-09-25 16:51:16 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:50:51 (CEST)	8536

pickup1.xlsx 2018-09-25 16:50:40



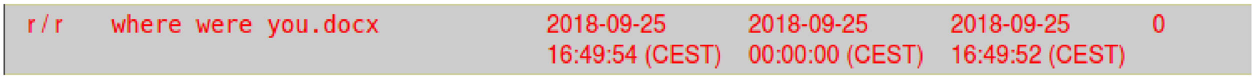
r/r	pickup1.xlsx	2018-09-25 16:50:40 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:50:38 (CEST)	8593

pickup1.xlsx 2018-09-25 16:50:46



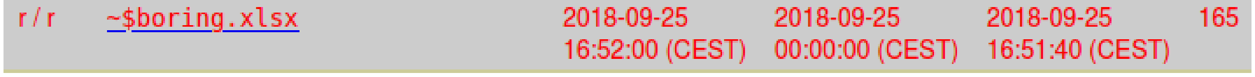
r/r	pickup1.xlsx	2018-09-25 16:50:46 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:50:38 (CEST)	8593

where were you.docx 2018-09-25 16:49:54



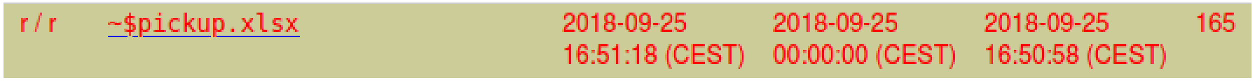
r/r	where were you.docx	2018-09-25 16:49:54 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:49:52 (CEST)	0

~$boring.xlsx 2018-09-25 16:52:00



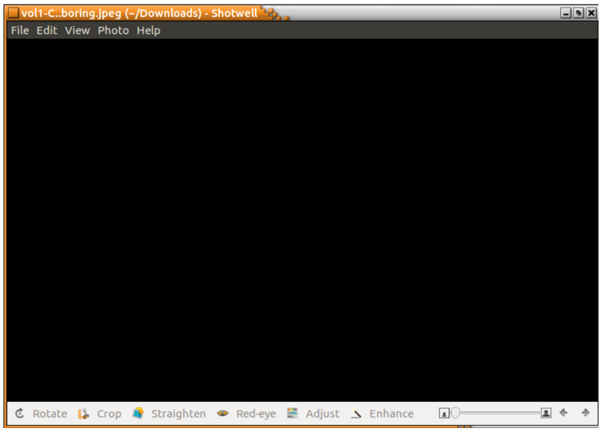
r/r	~$boring.xlsx	2018-09-25 16:52:00 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:51:40 (CEST)	165

~$pickup.xlsx

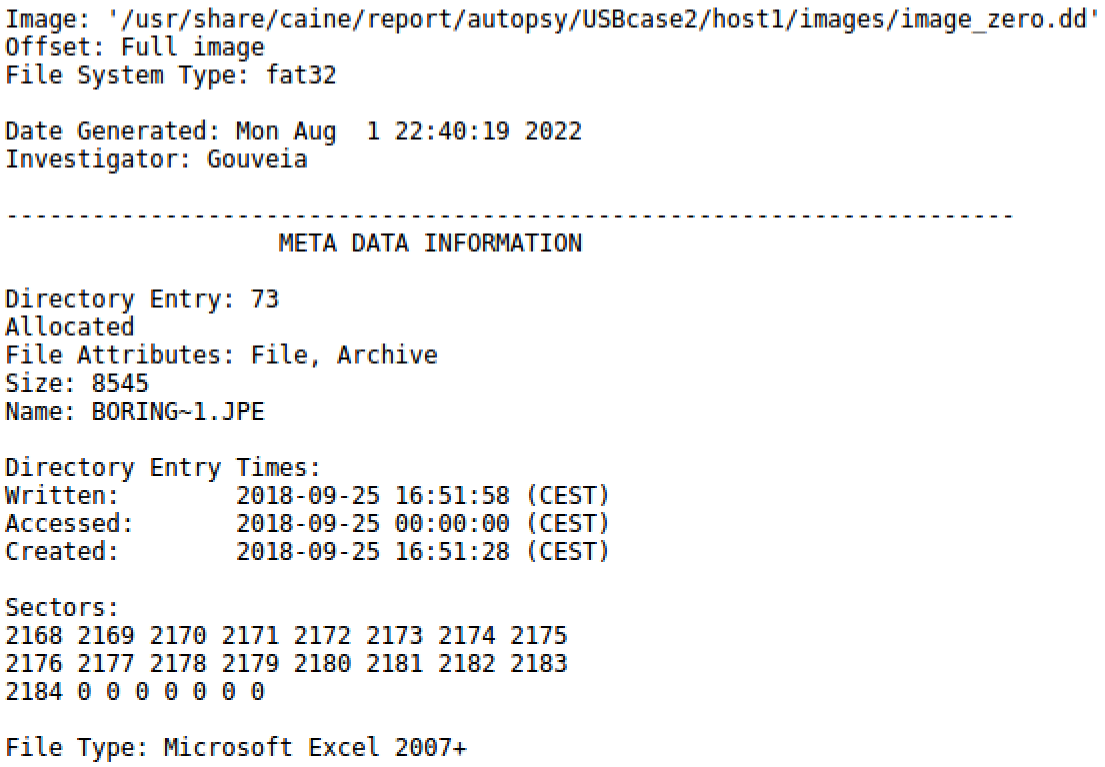


r/r	~$pickup.xlsx	2018-09-25 16:51:18 (CEST)	2018-09-25 00:00:00 (CEST)	2018-09-25 16:50:58 (CEST)	165

3. I was unable to open boring.jpg, the attempt to open the file shows a black background.

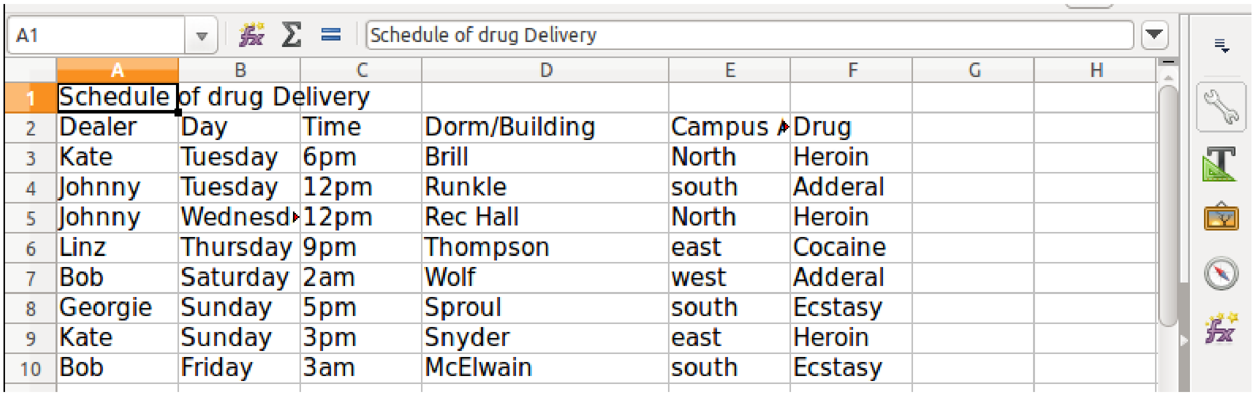

vol1-C..boring.jpeg (~/Downloads) - Shotwell
File Edit View Photo Help
Rotate
Crop
Straighten
Red-eye
Adjust
Enhance

I then checked the autopsy report to see what the meta data says about the file.



```
Image: '/usr/share/caine/report/autopsy/USBcase2/host1/images/image_zero.dd'
Offset: Full image
File System Type: fat32

Date Generated: Mon Aug  1 22:40:19 2022
Investigator: Gouveia

----------------------------------------------------------------------
                   META DATA INFORMATION

Directory Entry: 73
Allocated
File Attributes: File, Archive
Size: 8545
Name: BORING~1.JPE

Directory Entry Times:
Written:        2018-09-25 16:51:58 (CEST)
Accessed:       2018-09-25 00:00:00 (CEST)
Created:        2018-09-25 16:51:28 (CEST)

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: Microsoft Excel 2007+
```

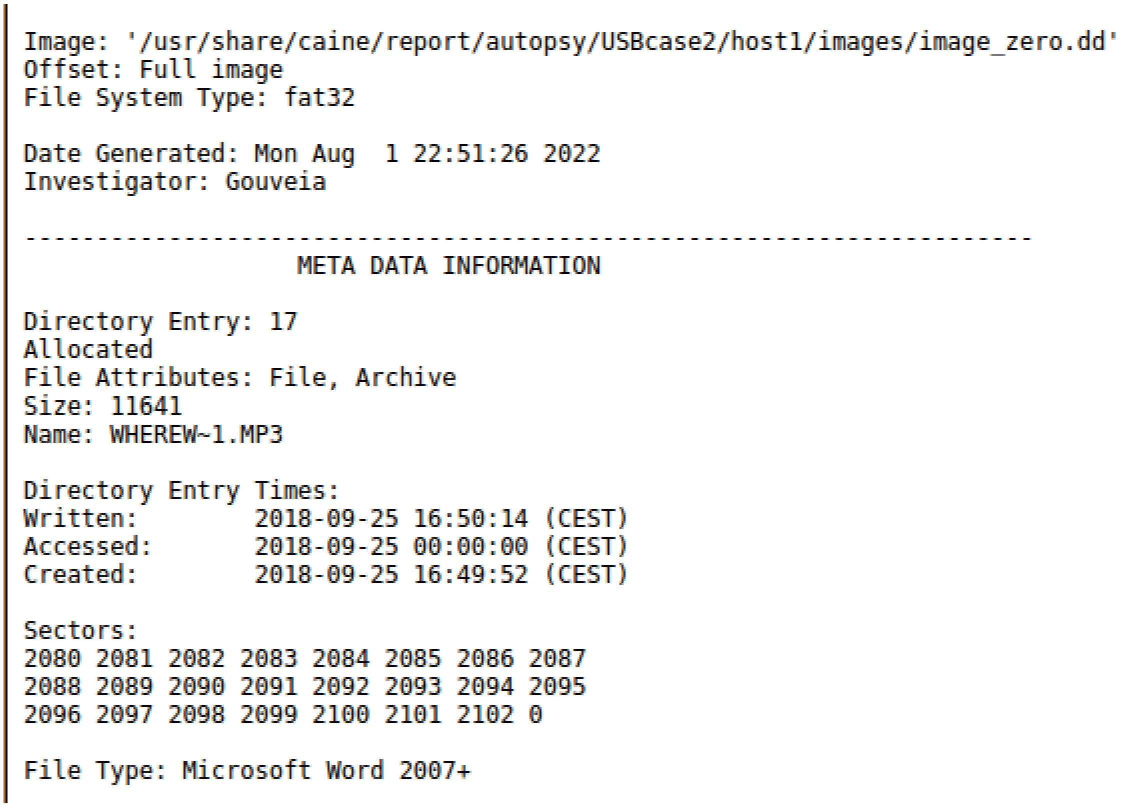
The report says the file is an Excel file. I chanced the extension to .xls and was able to open the file.



A1 | Schedule of drug Delivery

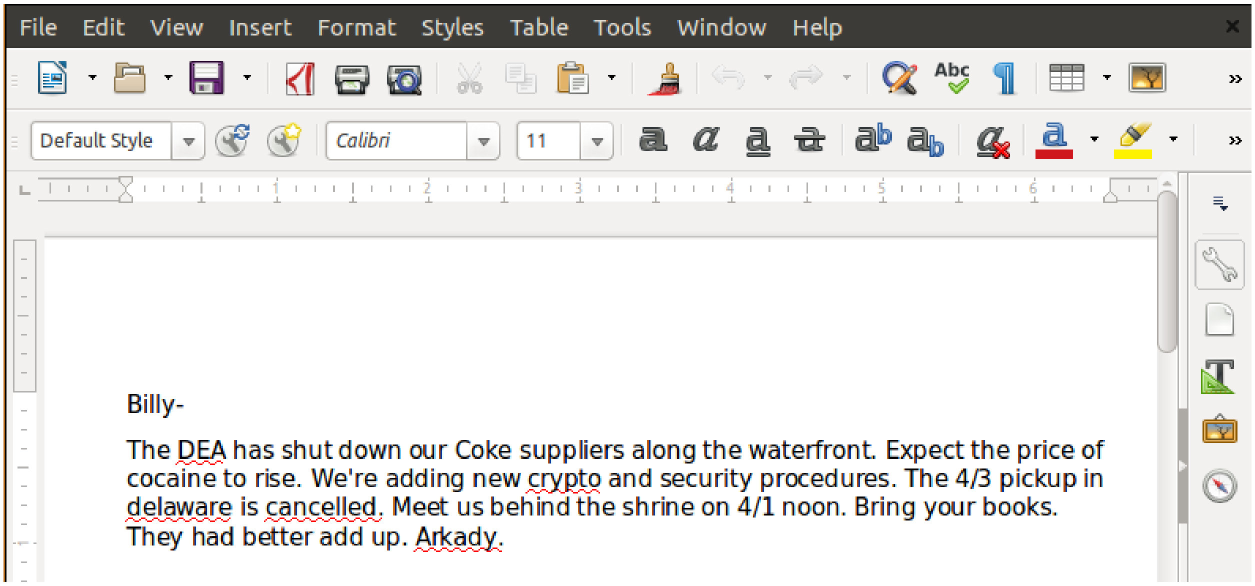
	A	B	C	D	E	F	G	H
1	Schedule of drug Delivery							
2	Dealer	Day	Time	Dorm/Building	Campus	Drug		
3	Kate	Tuesday	6pm	Brill	North	Heroin		
4	Johnny	Tuesday	12pm	Runkle	south	Adderal		
5	Johnny	Wednesd	12pm	Rec Hall	North	Heroin		
6	Linz	Thursday	9pm	Thompson	east	Cocaine		
7	Bob	Saturday	2am	Wolf	west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

4. I was able to find a secret message in the where were you.mp3 file. When I looked at the autopsy report I noticed is not an mp3 file but is a word document.



```
Image: '/usr/share/caine/report/autopsy/USBcase2/host1/images/image_zero.dd'
Offset: Full image
File System Type: fat32

Date Generated: Mon Aug  1 22:51:26 2022
Investigator: Gouveia

----------------------------------------------------------------------
                  META DATA INFORMATION

Directory Entry: 17
Allocated
File Attributes: File, Archive
Size: 11641
Name: WHEREW~1.MP3

Directory Entry Times:
Written:        2018-09-25 16:50:14 (CEST)
Accessed:       2018-09-25 00:00:00 (CEST)
Created:        2018-09-25 16:49:52 (CEST)

Sectors:
2080 2081 2082 2083 2084 2085 2086 2087
2088 2089 2090 2091 2092 2093 2094 2095
2096 2097 2098 2099 2100 2101 2102 0

File Type: Microsoft Word 2007+
```

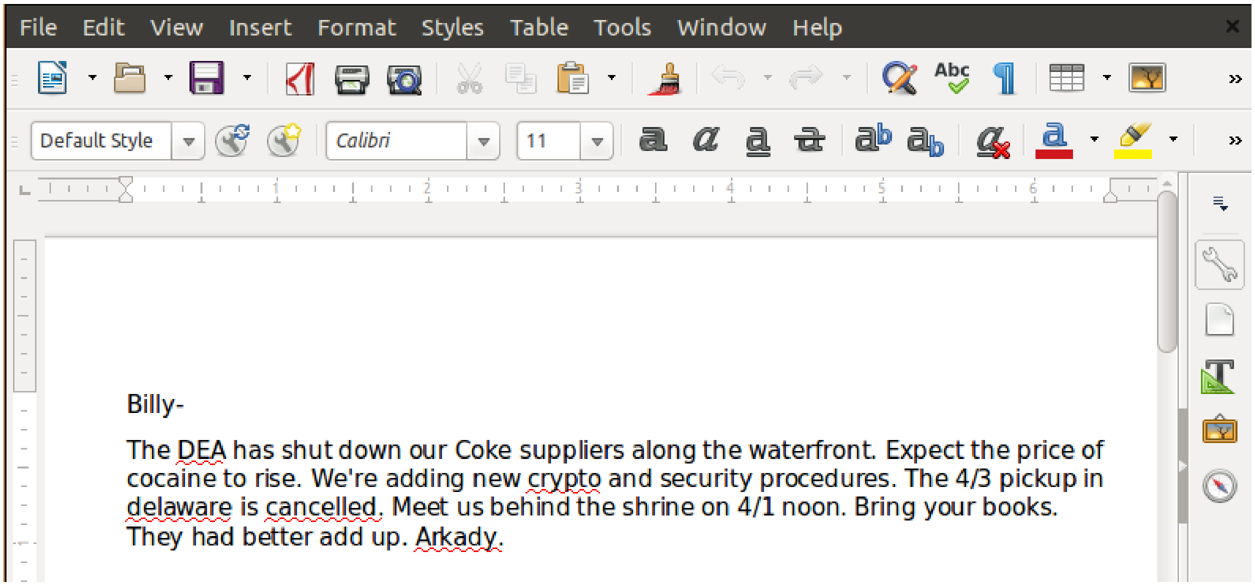
I change the file extension to .doc and found the following.



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.

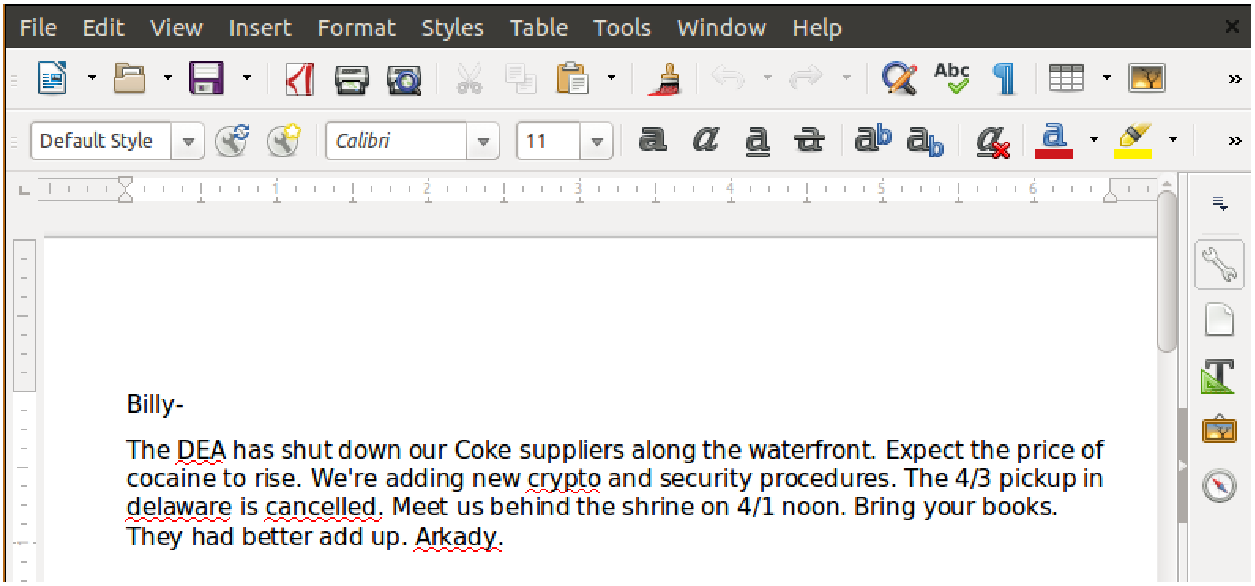
5. Based on the evidence found in the file where were you.mp3, it appears Arkady is Billy's supplier.



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.

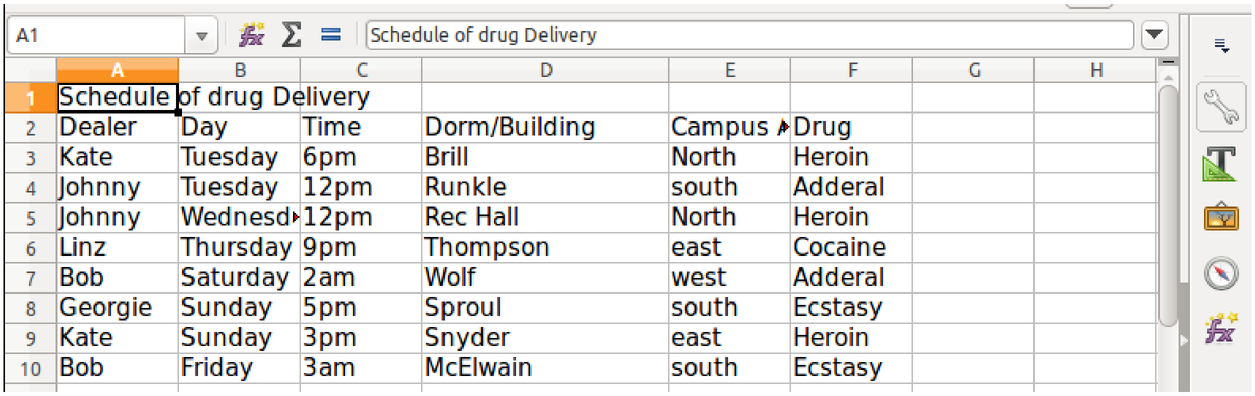
6. Based on the evidence found in the file where were you.mp3, it appears the next meeting is on 4/1 and will occur behind the "shrine".



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.

7. Based on the contents found in the file boring.jpg, the following people are involved on campus: Kate, Johnny, Linz, Bob, Georgie



A1 Schedule of drug Delivery

	A	B	C	D	E	F	G	H
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		