

# Computer And Network Forensics CA

## Technical Challenge

**Abel Melinte**  
**B00137882**

***Technological University, Blanchardstown***  
***Dublin 15.***

**[Word Limit for Assignment: No word limit**

**Actual Word Count: 1956]**

**Bachelor of Science in Computing**  
**Computer and Network Forensics**  
**01/12/22**

## Table of Contents

Executive Summary.....	2
Introduction .....	3
Tools Used.....	3
Chain of Custody .....	4
Step by Step .....	5
Questions .....	11
Questions Part 2.....	12
Conclusion.....	13

## Executive Summary

In this report I have been given a recovered disk, my aim was to search the disk and try find as many possible messages as possible or any strong hidden messages that could complete the entire investigation.

TU-Dublin Michael Hegarty

Yesterday, someone was detained on suspicion of peddling drugs to college students. Joe Jacobs approached a local police officer in the Smith Hill High School parking lot while pretending to be a student. Jacobs asked the undercover officer if he wanted to purchase any marijuana. Jacobs took some out of his pocket and showed it to the officer before the undercover cop could respond. Jacobs stated to the policeman "Look at this stuff, only Colombians could grow it better! My supplier grows it himself in addition to selling it directly to me." Around 2:30 pm, when school typically ends for the day, Jacobs was frequently seen hanging around at several nearby schools. Since Jacobs' arrival at their school, administrators from many high schools have reported an upsurge in student drug use and have called the police. Police are attempting to ascertain whether Joe Jacobs has been distributing drugs to pupils at schools other than Smith Hill. Students won't volunteer to assist the cops in any way. The authorities are trying to track down Joe Jacob's marijuana supplier and producer considering Joe's remark about the Colombians. In addition to denying selling drugs at any other schools besides Smith Hill, Jacobs won't provide the police the identity of his drug producer or supplier. Jacobs also declines to confirm the claim he made to the undercover cop just before being apprehended. The cops were able to find a minor quantity of marijuana after obtaining a search warrant and examining the suspect's home. A single disk was also taken by the authorities, although the home was devoid of any computers or other media. The police have imaged the suspect's disk and have given you a copy; if you have shared any of your responses, you will automatically receive a grade of 0. They want you to look over the disk and respond to their inquiries. You should pay close attention to any information that could support the police's claim that Joe Jacobs was indeed peddling drugs other high schools besides Smith Hill. They also want you to attempt and identify Joe Jacob's supplier, if you can. Bail for Jacob was set at €10,000.00. Because they are concerned that he might leave town, they want to lock him up as quickly as they can. The police have requested that you complete all the results to achieve this. Please present the police with a solid case that details your

precise conclusions in relation to the questions. Keeping in mind that this case will ultimately be heard in court and that the conclusions must hold up to scrutiny

Keywords: Autopsy, MD5, Investigation, Report, Software, Disk, Encryption, Decryption.

## Introduction

In this report I have been given a recovered disk that includes an image on it and my only option is to use some tools to be able to take a better look at that image file and see if there is any hidden messages or valuable information on it. The two tools I will mainly focused on and will be used as it has been said that they are the most advanced tools out of the others will be Autopsy and some extra tools that will mentioned throughout this report.

## Tools Used

Here are the tools which have been used throughout this investigation

**FTK Imager**

**Product Version – 3.4.0.5**

**Autopsy**

**Product Version – 4.19.3**

**WinMD5**

**Product Version – 1.0.1.0**

## Chain of Custody

**Case Number: 1**

### Equipment

Item: 0001	Description: SSD 240 GB
Manufacturer: Kingston	Model: SA400S37/240G
Serial Number: C91F92CJ77YP8NW6T5VG86E	

### Details about the image

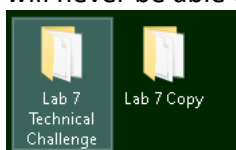
Created by: Joe Jacobs Date: 8/11/21	Image Name: weed-image
Driver: SSD	MD5 Hash: AC3F7B85816165957CD4867E62CF452B

### Chain of Custody

Sequence: 0001	Date: 30/11/22 Time: 8:38 PM
Source: Joe Jacobs	Destination: TUD Technological University Dublin A11
Reason: Selling drugs at a high school to students	Disk has been stored safely in a secured HDD and hasn't been touched or used ever since

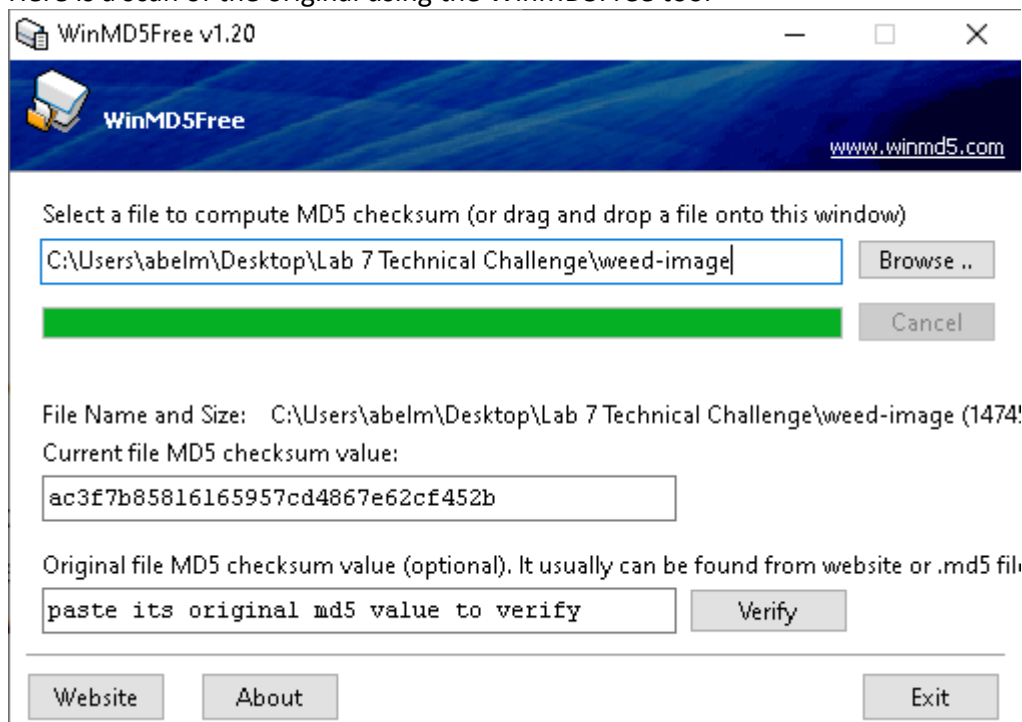
## Step by Step

Before beginning this investigation, the first step I done was that I had to duplicate the recovered disk so we can always work on the duplication instead of working on the main disk as that would ruin the entire investigation and if in any form you cause an issue you will never be able to revert back to the start the way it was before.

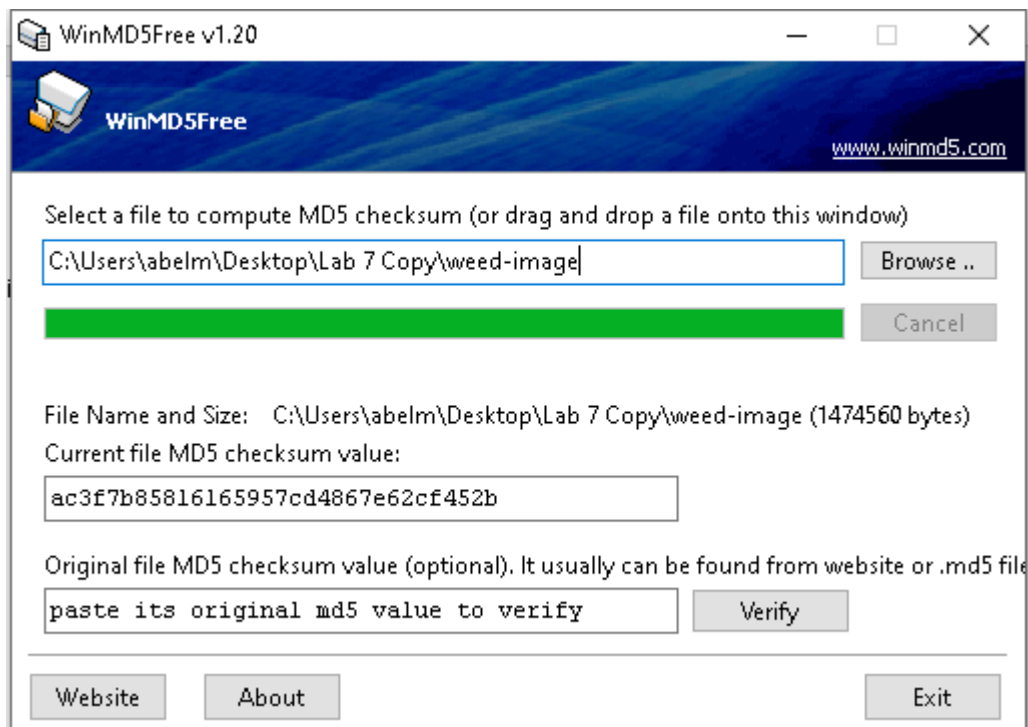


In the instruction page I have been given the Image MD5 which is:

Here is a scan of the original using the WinMD5Free tool



Here is a scan of the copy just to make sure it's the same MD5 value



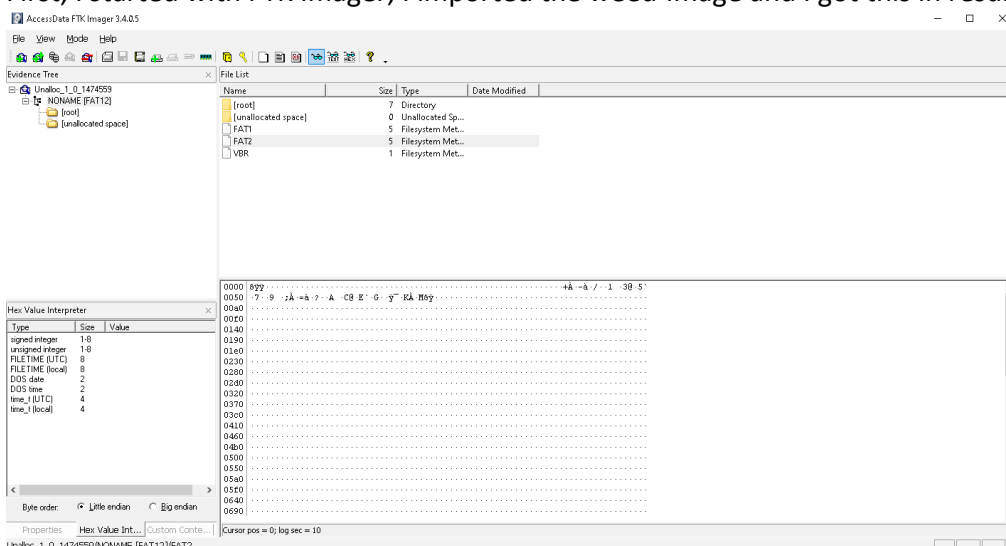
In result they both have the same Image MD5 so that means it's identical to the original which leads me to make a start of the investigation on the duplicated disk.

Here is the duplicated folder of the original, these are the files which were inside.





Name	Date modified	Type	Size
Lab 7 Instructions.pdf	08/11/2021 3:03 pm	Brave HTML Docu...	724 KB
weed-image	08/11/2021 2:59 pm	File	1,440 KB

It contains an image file which needs to be investigated and searched for hidden information.

First, I started with FTK Imager, I imported the weed-image and I got this in result



I opened the root folder which contained 3 files.

	cover page.jpggc	16	Regular File	11/09/2002 08:...
	Jimmy Jungle.doc	20	Regular File	15/04/2002 14:...
	SCHEDU~1.EXE	1	Regular File	24/05/2002 08:...
	SCHEDU~1.EXE.FileSla...	2	File Slack	

I extracted all the files to my desktop as I tried to access them, the only file that I was able to open and view was "Jimmy Jungle.doc", here is what the document said. Joe used Microsoft Word 10.0 in order to write out this email.

```
2710 | .STC . . . . . Normal .u . . . . . 0000t1 .u . . . . . 9 .TC . . . . . Microsoft Word 10.0 .@ . . .
2760 | .i° . . . . . @ . . . . . 0 .PwAA .@ . . . . . _EAA . . . . .
```

Jimmy Jungle  
626 Jungle Ave Apt 2  
Jungle, NY 11111

Jimmy:

Dude, your pot must be the best – it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you put in your soil when you plant the marijuana seeds? At least I know your growing it and not some guy in Columbia.

These kids, they tell me marijuana isn't addictive, but they don't stop buying from me. Man, I'm sure glad you told me about targeting the high school students. You must have some experience. It's like a guaranteed paycheck. Their parents give them money for lunch and they spend it on my stuff. I'm an entrepreneur. Am I only one you sell to? Maybe I can become distributor of the year!

I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive. Tell me what you think. To open it, use the same password that you sent me before with that file. Talk to you later.

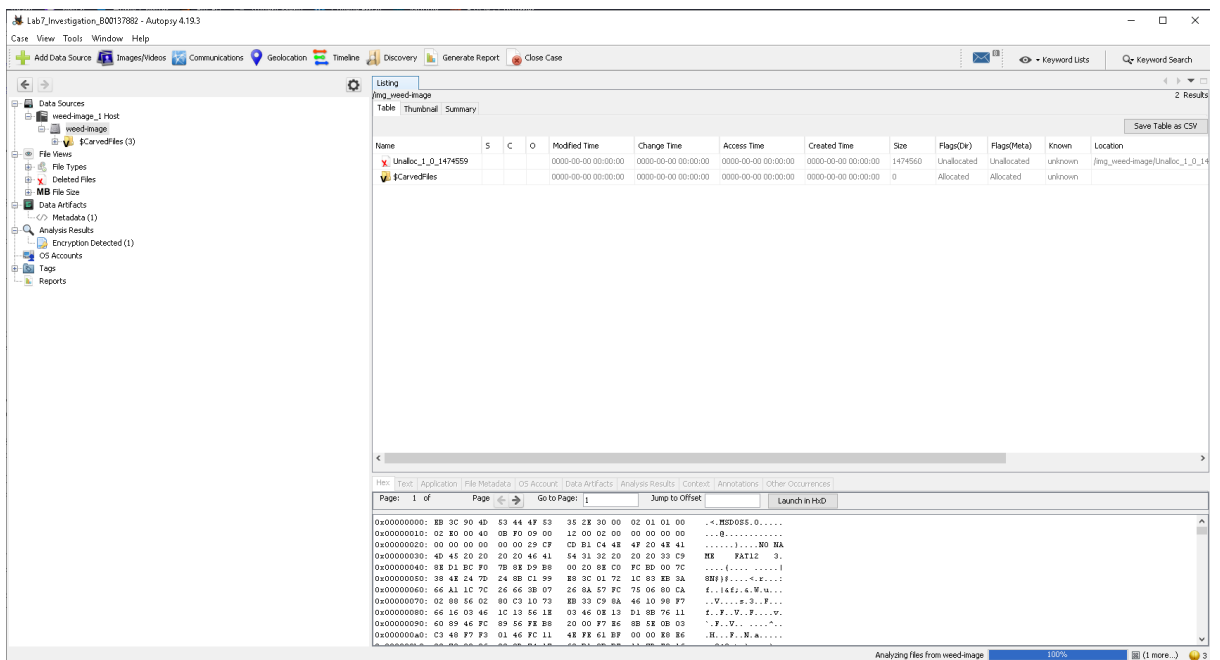
Thanks,

Joe

For the remaining files, I wasn't able to view as they had incorrect extensions such as .jpgc and a broken .exe. I tried changing the jpgc to jpg but it was still unsupported. I had nothing to do on FTK Imager as they were the only files on it which contained one evidence, the proof of address of the dealer and that's about it, but I knew there was much more evidence to be solved just not on FTK Imager.

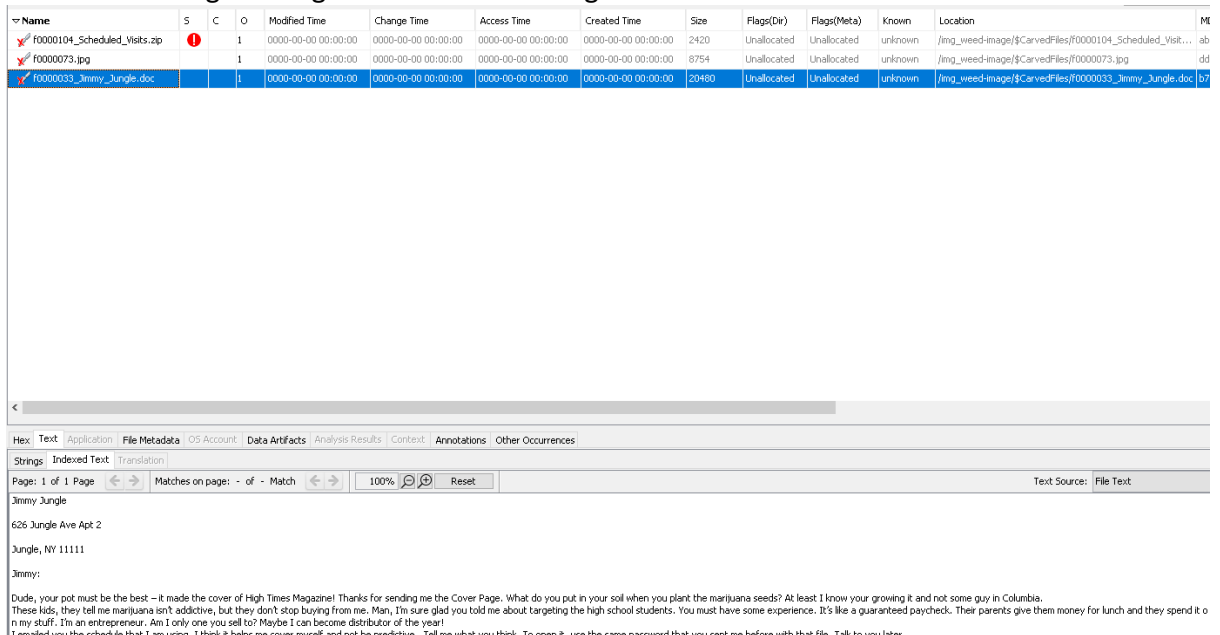
My second plan was to use Autopsy and see what I can discover.

Here is an image after I created a case and imported the image file to Autopsy.



I began to look deep into the file and see if I can come across anything suspicious that might be extremely helpful.

I instantly found this doc file by the name of “f0000033\_Jimmy\_Jungle.doc” I viewed it in Autopsy and noticed that it’s an email that Joe has sent to his drug dealer(Jimmy) and told him about selling his drugs to students from high school.



After searching “Unalloc\_1\_0\_1474559” I came across something which was extremely useful I saw “pw” which rang a bell that it might be the password to the zip file when I tried extracting it



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MDS Hash	SHA-256 Hash
Unalloc_1_0_1474559				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1474560	Unallocated	Unallocated	unknown	img_wweed-image/Unalloc_1_0_1474559		
\$CarvedFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown			

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Indexed Text

Translation

Page: 1 of 1 Page

Matches on page: - of - Match

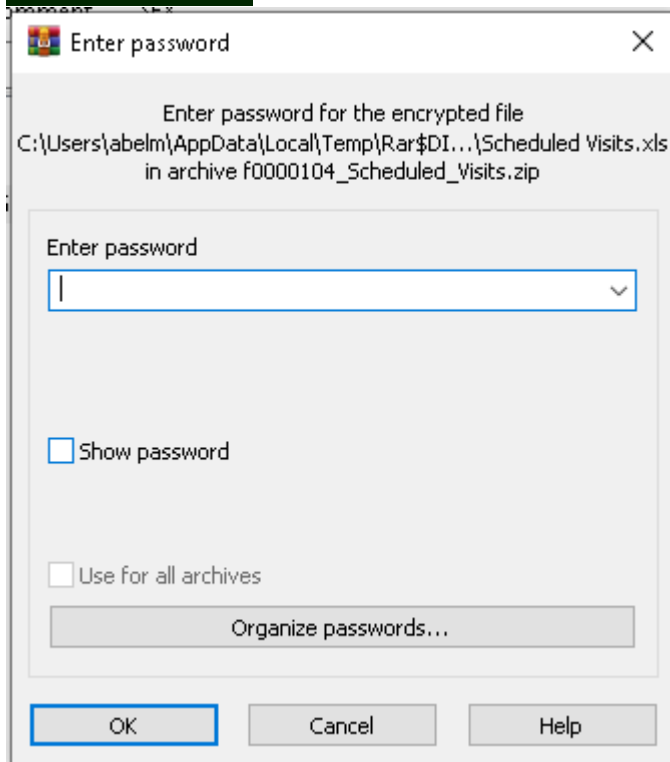
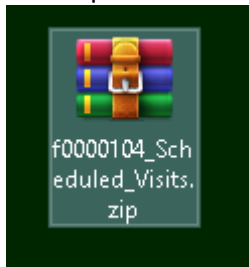
100%

Reset

Text Source: File Text

9p+  
R\*JI  
oq4  
I+<N  
pr=goodtimes  
Scheduled Visits.xls  
SIUM  
gvm2A  
N!

After discovering where the “Scheduled\_Visits.zip” was, I exported it directly to my desktop so I can work with it much easier.






When trying to unzip the file it asks for the password, the password was “goodtimes”.

	A	B	C
1	Month	DAY	HIGH SCHOOLS
2	2002		
3	April	Monday (1)	Smith Hill High School (A)
4		Tuesday (2)	Key High School (B)
5		Wednesday (3)	Leetch High School (C)
6		Thursday (4)	Birard High School (D)
7		Friday (5)	Richter High School (E)
8		Monday (1)	Hull High School (F)
9		Tuesday (2)	Smith Hill High School (A)
10		Wednesday (3)	Key High School (B)
11		Thursday (4)	Leetch High School (C)
12		Friday (5)	Birard High School (D)
13		Monday (1)	Richter High School (E)
14		Tuesday (2)	Hull High School (F)
15		Wednesday (3)	Smith Hill High School (A)
16		Thursday (4)	Key High School (B)
17		Friday (5)	Leetch High School (C)
18		Monday (1)	Birard High School (D)
19		Tuesday (2)	Richter High School (E)
20		Wednesday (3)	Hull High School (F)
21		Thursday (4)	Smith Hill High School (A)
22		Friday (5)	Key High School (B)
23		Monday (1)	Leetch High School (C)
24		Tuesday (2)	Birard High School (D)
25	May		
26		Wednesday (3)	Richter High School (E)
27		Thursday (4)	Hull High School (F)
28		Friday (5)	Smith Hill High School (A)
29		Monday (1)	Key High School (B)
30		Tuesday (2)	Leetch High School (C)
31		Wednesday (3)	Birard High School (D)
32		Thursday (4)	Richter High School (E)
33		Friday (5)	Hull High School (F)
34		Monday (1)	Smith Hill High School (A)
35		Tuesday (2)	Key High School (B)
36		Wednesday (3)	Leetch High School (C)
37		Thursday (4)	Birard High School (D)
38		Friday (5)	Richter High School (E)
39		Monday (1)	Hull High School (F)
40		Tuesday (2)	Smith Hill High School (A)
41		Wednesday (3)	Key High School (B)
42		Thursday (4)	Leetch High School (C)
43		Friday (5)	Birard High School (D)
44		Monday (1)	Richter High School (E)
45		Tuesday (2)	Hull High School (F)
46		Wednesday (3)	Smith Hill High School (A)
47		Thursday (4)	Key High School (B)
48		Friday (5)	Leetch High School (C)
49	June		
50		Monday (1)	Birard High School (D)
51		Tuesday (2)	Richter High School (E)
52		Wednesday (3)	Hull High School (F)
53		Thursday (4)	Smith Hill High School (A)
54		Friday (5)	Key High School (B)
55		Monday (1)	Leetch High School (C)
56		Tuesday (2)	Birard High School (D)
57		Wednesday (3)	Richter High School (E)
58		Thursday (4)	Hull High School (F)
59		Friday (5)	Smith Hill High School (A)
60		Monday (1)	Key High School (B)
61		Tuesday (2)	Leetch High School (C)
62		Wednesday (3)	Birard High School (D)
63		Thursday (4)	Richter High School (E)
64		Friday (5)	Hull High School (F)

After opening the .xls file I came across the scheduled visits that the drug dealer has made for himself.

After looking for more suspicious things on Autopsy I came across \$CarvedFiles which contained 3 files.

Name
 f0000104_Scheduled_Visits.zip
 f0000073.jpg
 f0000033_Jimmy_Jungle.doc

Here is the MD5/SHA-256 hash values of each file.

F0000104\_Scheduled\_Visits.zip -

F0000073.jpg -

F0000033\_Jimmy\_Jungle.doc -

MD5 Hash	SHA-256 Hash
ab6a87ff7acf36eb2803dfd12ec2036f	24e13de91301efb536419aa26bb41364e54883edc337228...
dd5c7e571e9e4b229141b98bf183469f	e4e0036e92f37ad800d7922d4183178c2c10b98542c80f54...
b775eb6a4ccc319759d9aaae1e340acc	63e806e7066151b1f7e9a01a5c8c391ab7253b37a992fd03...

## Questions

### 1. Where did the analysis of evidence take place?

The analysis took place at Technological University Dublin (TUD) A-11 Room

### When did you start the analysis? What proof have you got?

The analysis began at 8:38 PM on 30/11/22, the proof is in the chain of custody which is completed above.

### Who (if anyone) assisted you with the process?

Nobody has assisted me during this investigation.

### Why should we believe your evidence to be true?

My evidence should be trusted as it's all been documented step by step and it also required high quality software's to investigate the disk.

### What tools did you use to analyse the evidence

The tools that have been used throughout this investigation were Autopsy, FTK Imager and WinMD5

#### a. Are these tools accepted in court? How do you find out?

These tools are accepted in court as I there were some previous cases that used these tools to investigate other equipment.

#### b. Does the company have a website? What information is available there?

FTK Imager - <https://accessdata.com/>

Autopsy - <https://www.autopsy.com/>

WinMD5 - <https://www.winmd5.com/>

### 2. Document the steps you went through to upload evidence

### 3. How many files are listed on the complete image?

On Autopsy there was 4 files that have been discovered on the image  
And on FTK Imager there was 3 files which were working.

### 4. What file system is in use?

The file system which is being used in this disk image is folders.

## Questions Part 2

**1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?**

The person who Joe buys his marijuana seems to be called Jimmy Jungle, I came across his name when I viewed the .docx file that was situated on the disk, his address is also 626 Jungle Ave Apt 2, Jungle, NY 11111

**Who are the main players or people involved with this scenario?**

The main people that were involved in this scenario were Joe Jacobs and Jimmy Jungle, Joe known as the marijuana buyer and Jimmy known as the drug dealer

**2. What crucial data is available within the coverpage.jpg file and why is this data crucial?**

When searching deep into the coverpage.jpg I have not come across any crucial data, the other files have crucial data but coverpage.jpg did not.

**3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?**

There were multiple different high schools that Joe has attended and began to sell the marijuana he bought of Jimmy, here is a list of the high schools.

- Key High School
- Leetch High School
- Birard High School
- Richter High School
- Hull High School

**4. For each file, what processes were taken by the suspect to mask them from others?**

Joe tried hiding himself by changing the extensions from each file such as he changed the "coverpage.jpg" to "coverpage.jpgc" which this prevents anyone to open it as it's unsupported extensions, he also changed the extension on a file that was named "ScheduledVisits.xls" to "SCHEDU-1.exe" .

**5. What processes did you (the investigator) use to successfully examine the entire contents of each file?**

The software that had the ability to view the deep contents of each file with Autopsy, when I was working on FTK Imager the files were unsupported to open or were just created with wrong extensions where with Autopsy all files opened, and I was able to view every

**6. What Microsoft program was used to create the Cover Page file. What is your proof?**

I couldn't find out what program was used to create the Cover Page file.

**7. What other additional information can you find that may help to secure a conviction?**

No additional information was gathered to secure a conviction.

## Conclusion

Overall, this investigation has strongly motivated me to have the patience and be able to surf along different software and tools to find different crucial data that other tools weren't able to find. It also shows that the more work/time/effort you put into it the more results you will get out of it.