Digital Forensic Investigation Report

Case Title: Joe Jacobs Suspected Drug Distribution Case

Prepared by: Danyil Tymchuk (B00167321)

Forensic Laboratory: TU-Dublin Lab-A11

Date of Report: 27/11/2025

Image MD5: AC3F7B85816165957CD4867E62CF452B

OLLSCOIL TEICNEOLAÍOCHTA
BHAILE ÁTHA CLIATH
TECHNOLOGICAL
UNIVERSITY DUBLIN

Table of Contents

1. Introduction

This report documents the forensic examination of a disk image seized during the investigation of Joe Jacobs, suspected of drug distribution to multiple schools. The objective is to identify evidence of dealings with other students, determine the supplier, and uncover any additional relevant information.

This investigation adheres to ISO/NIST digital forensic standards and follows strict chain-of-custody protocols.

2. Scope of Investigation

- Analyse the recovered disk image
- Validate integrity through MD5 hashing
- Extract and examine all files
- Recover hidden or deleted data
- Identify communications, documents, and images related to illicit activity
- Answer investigative questions provided by law enforcement

3. Chain of Custody

Date/Time	Person	Action	Evidence ID	Hash (MD5)
27/11/2025 17:00 – 19:00	Danyil Tymchuk	Perform initial analysis with Autopsy forensics analysis tool	001	ac3f7b85816 165957cd48 67e62cf452b
27/11/2025 21:00 – 23:00	Danyil Tymchuk	Perform second analysis. Using Forensic Toolkit-FTK tool	001	ac3f7b85816 165957cd48 67e62cf452b

4. Forensic Environment

4.1. Hardware Used

Forensics Laboratory: TU-Dublin Lab-A11

Workstation: Lab PC, that are not connected to the internet

4.2. Software Used

Tool	Version	License	Purpose
Autopsy	4.22.1	Open-source	File analysis
FTK Imager	4.7.3.81	Free Licence	Forensic duplicate & File analysis
Forensic Toolkit-FTK	1.62.1	Free Licence	File analysis
Microsoft EXCEL	online	Student's account	Examine decrypted 'Scheduled Visits.xls'

5. Evidence Acquisition

1. Original image hash validated
2. Forensic duplicate created using FTK Imager
3. Duplicate hash verified
4. Analysis performed only on the duplicate copy
5. All steps logged and timestamped

6. Forensic Analysis & Findings

6.1. Autopsy Analysis (Tool 1)

6.1.1. Initial Analysis

The initial examination of the disk image was conducted using Autopsy, an open-source digital forensics platform.

6.1.2. File System Overview

The acquired disk image, named "**weed-image**", uses the FAT file system with a 512-byte sector size. Autopsy identifies the media type as "*Flash Drive*" ("*Description: Flash Drive*"), and metadata indicates the total storage size is **1,474,560 bytes** (1.44 MB), consistent with a small removable storage device.

6.1.3. Files Analysis

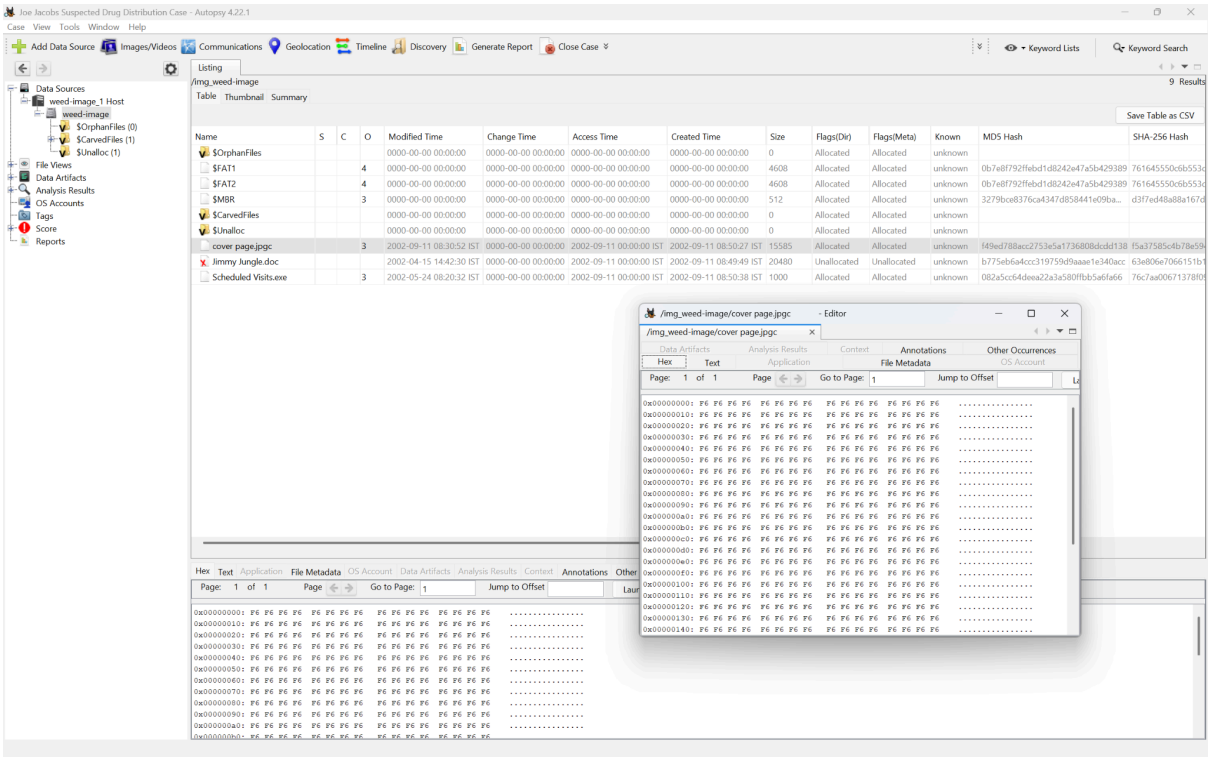
Three files was found using Autopsy tool:

- 'cover page.jpgc'
- 'Jimmy Jungle.doc'
- 'Scheduled Visits.exe'

Additionally, Autopsy identified one file in $Unalloc (Unalloc_4_16896_1474560) and one in $CarvedFiles (f0000000_Jimmy_Jungle.doc). These files look the same as 'Jimmy Jungle.doc' file.
Hash verification confirmed that both recovered files are identical copies of Jimmy Jungle.doc.

6.1.4. Files Examination

‘cover page.jpgc’



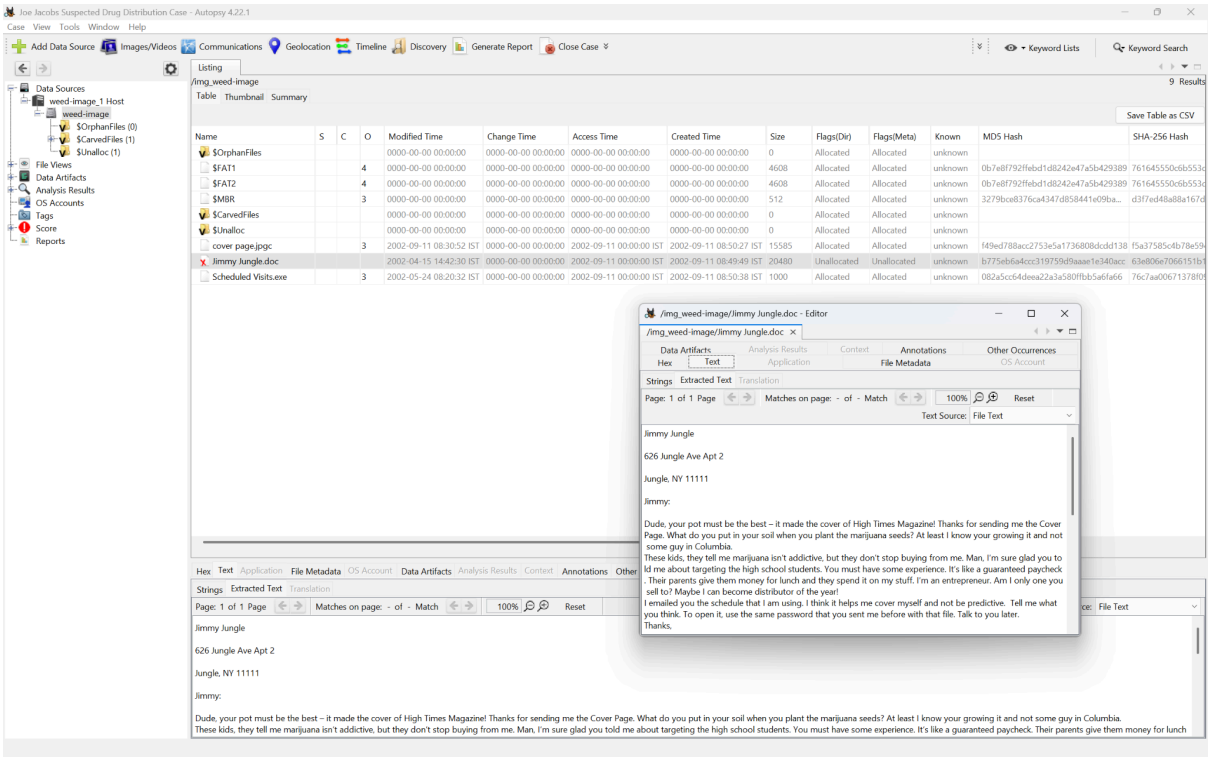
The file contents appear overwritten with **0xF6** bytes, rendering it unreadable. This suggests intentional obfuscation or corruption of the file.

Metadata observations:

- **MIME Type:** application/octet-stream (unknown format)
- **Size:** 15,585 bytes

Discovery Timestamp: 27/11/2025 18:00

‘Jimmy Jungle.doc’



This document contains key investigative information, including the address of **Jimmy Jungle**, the suspected supplier:

“*626 Jungle Ave Apt 2, Jungle, NY 11111*”

The letter strongly implies a supplier–dealer relationship. Notably, Joe references receiving a “*Cover Page*” likely corresponding to the corrupted “cover page.jpgc” file.

Full contents of the letter are:

“*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.

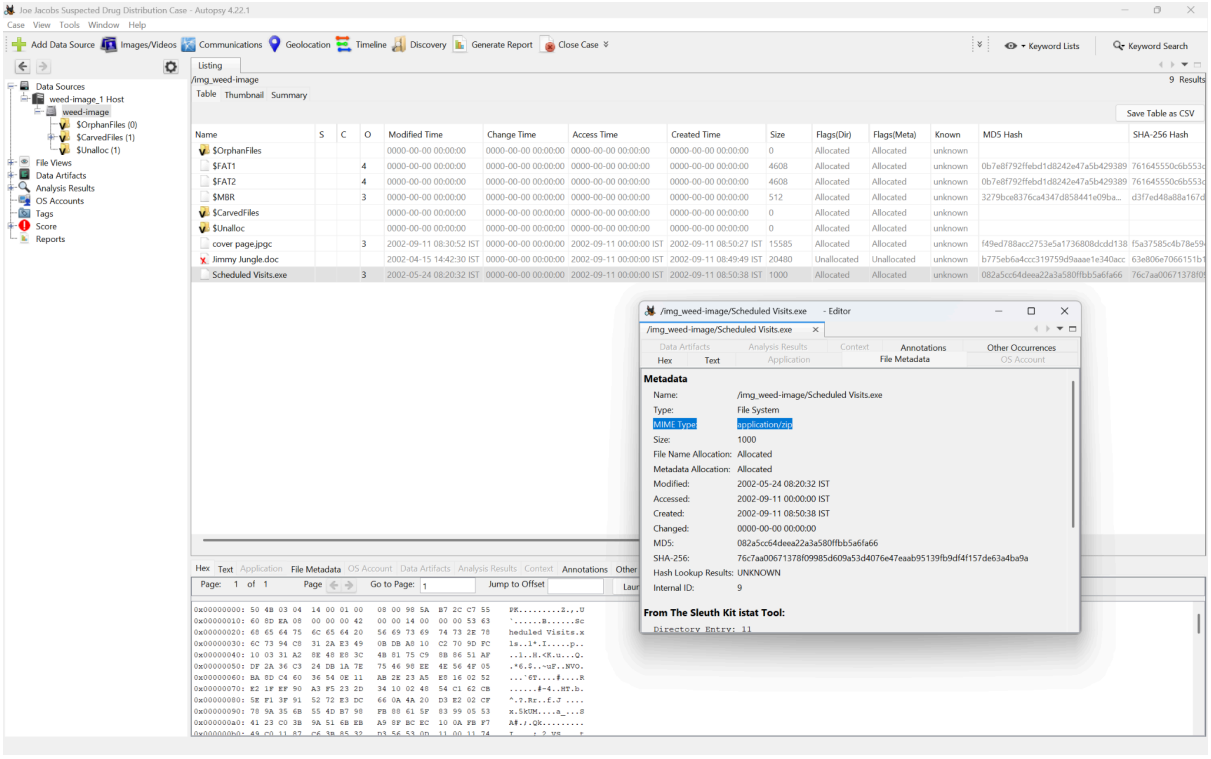
Thanks,

Joe "

This file provides clear evidence of drug distribution, targeting minors, and communication with a known supplier.

Discovery Timestamp: 27/11/2025 18:10

'Scheduled Visits.exe'



This file is a password-protected ZIP archive disguised with an .exe extension.

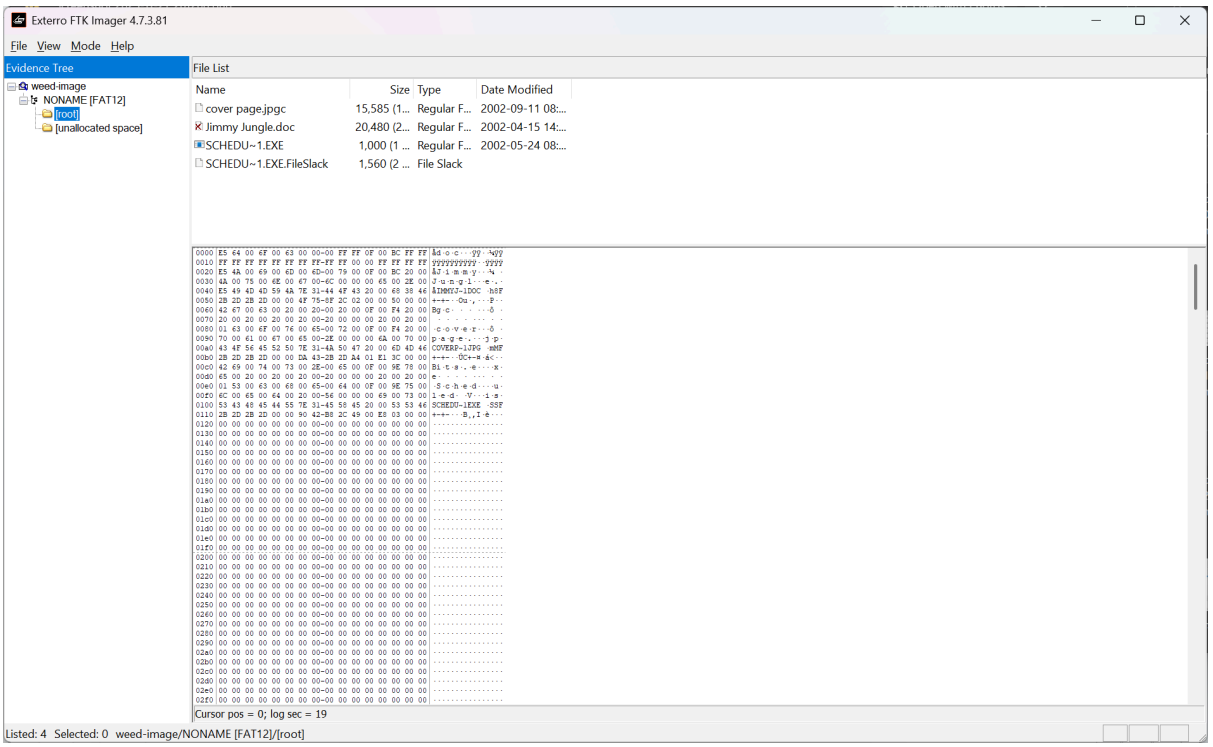
It could not be opened initially due to encryption. Come back to this evidence when the key is received.

Discovery Timestamp: 27/11/2025 18:20

6.2. FTK Imager (Tool 2)

A supplementary examination was conducted using FTK Imager.

6.2.1. Files Analysis



Although FTK Imager is primarily intended for imaging and preview rather than full analysis, it confirmed the presence of the same three files, with no additional findings.

Discovery Timestamp: 27/11/2025 18:50

6.3. Forensic Toolkit-FTK (Tool 3)

6.3.1. Second Analysis

A more in-depth analysis was conducted using AccessData Forensic Toolkit (FTK).

6.3.2. File System Verification

AccessData's Forensics Toolkit confirms that the disk uses the FAT12 file system.

6.3.3. Files Analysis

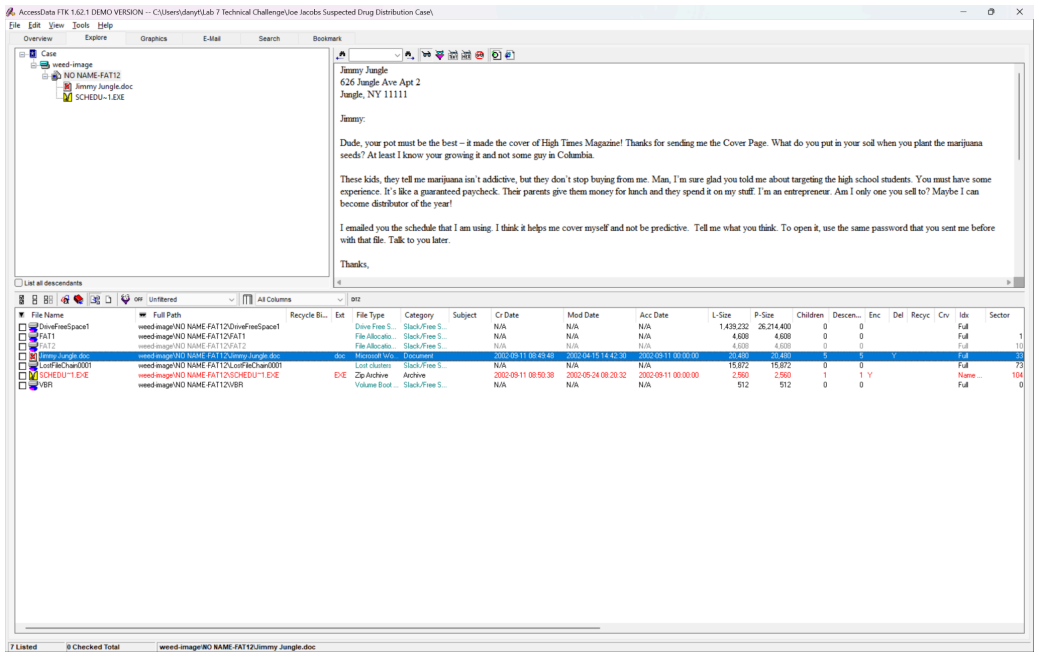
FTK revealed additional relevant evidence not shown in Autopsy

New file:

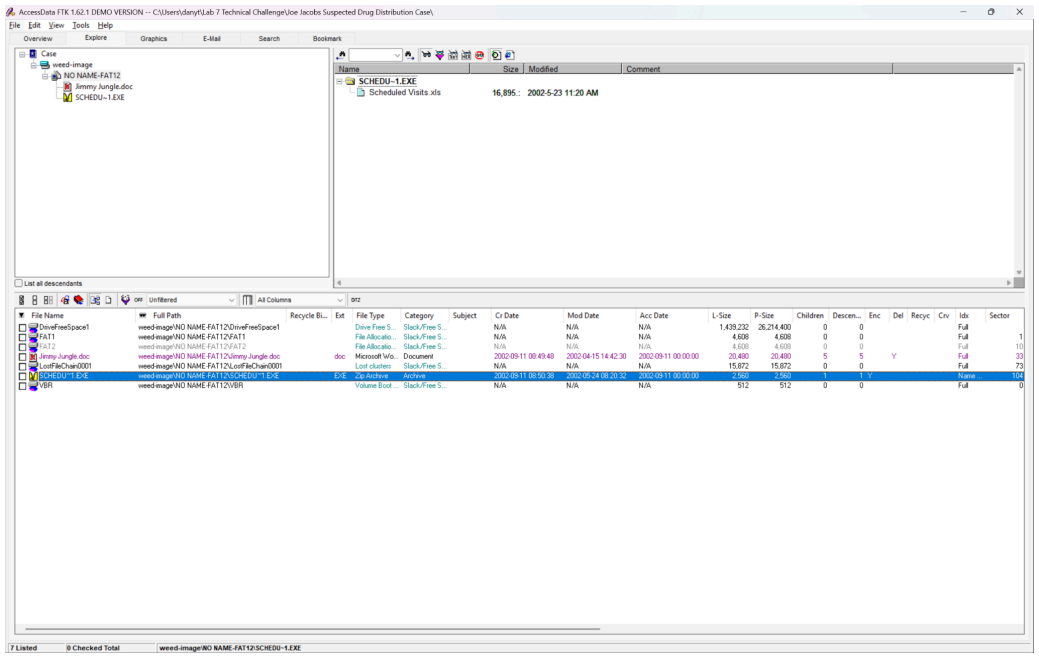
- '**LostFileChain0001**' (Slack Space file)

Already known files:

- '*Jimmy Jungle.doc*' – Letter from Joe to Jimmy Jungle

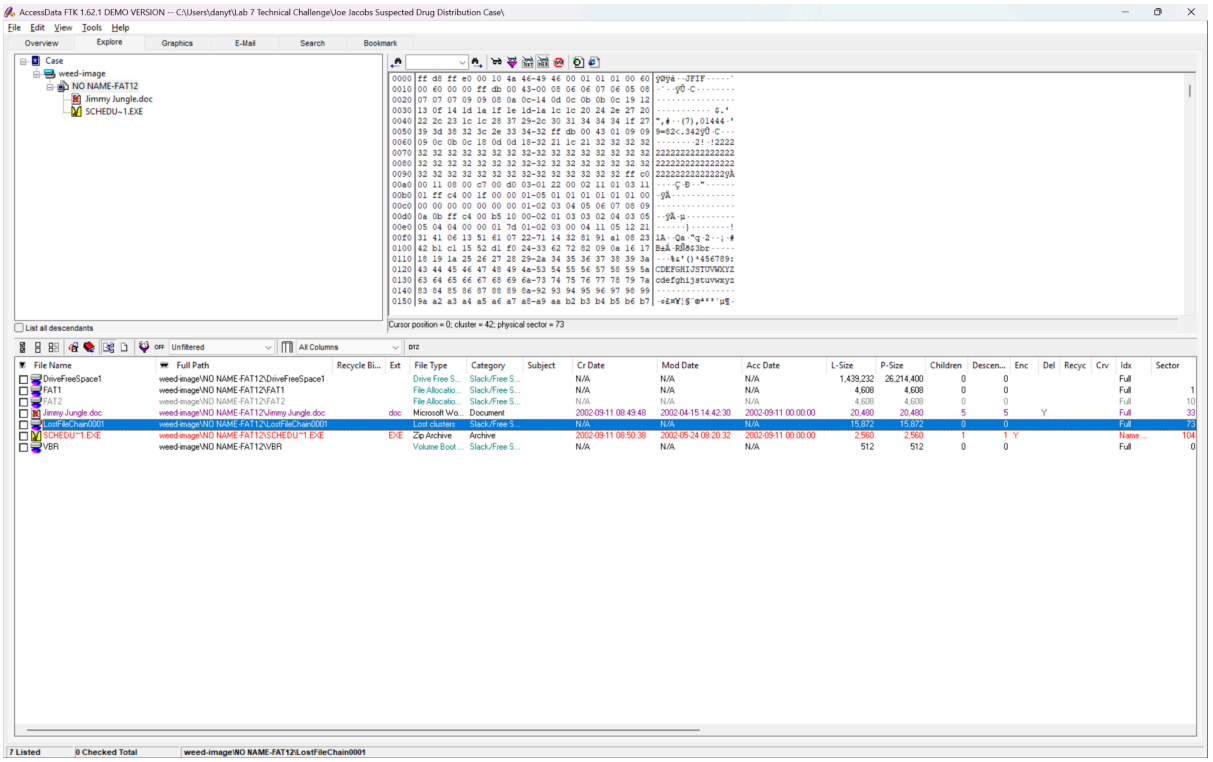


- '*SCHEDU~1.EXE*' → 'Scheduled Visits.xls' – Encrypted Archive (zip)



6.3.4. File Examination

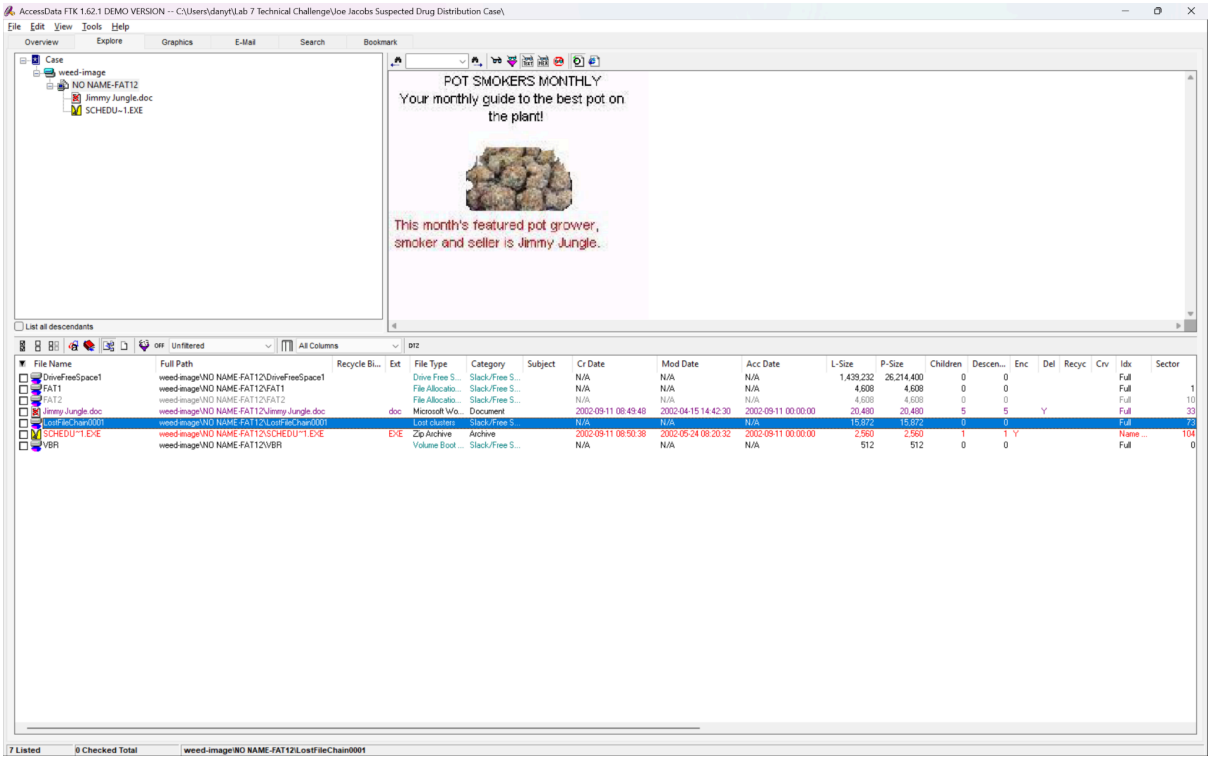
‘LostFileChain0001’



This file seems to be the SlaskSpace for ‘cover page.jpgc’ file. It also has ‘**JFIF**’ in the EXIF, which means that it was an image.

This slack-space artifact contains remnants of the original cover page image, and FTK was able to reconstruct it.

Trying to view this file as an image:



The recovered image displays the following text:

"POT SMOKERS MONTHLY

Your monthly guide to the pot on the plant!

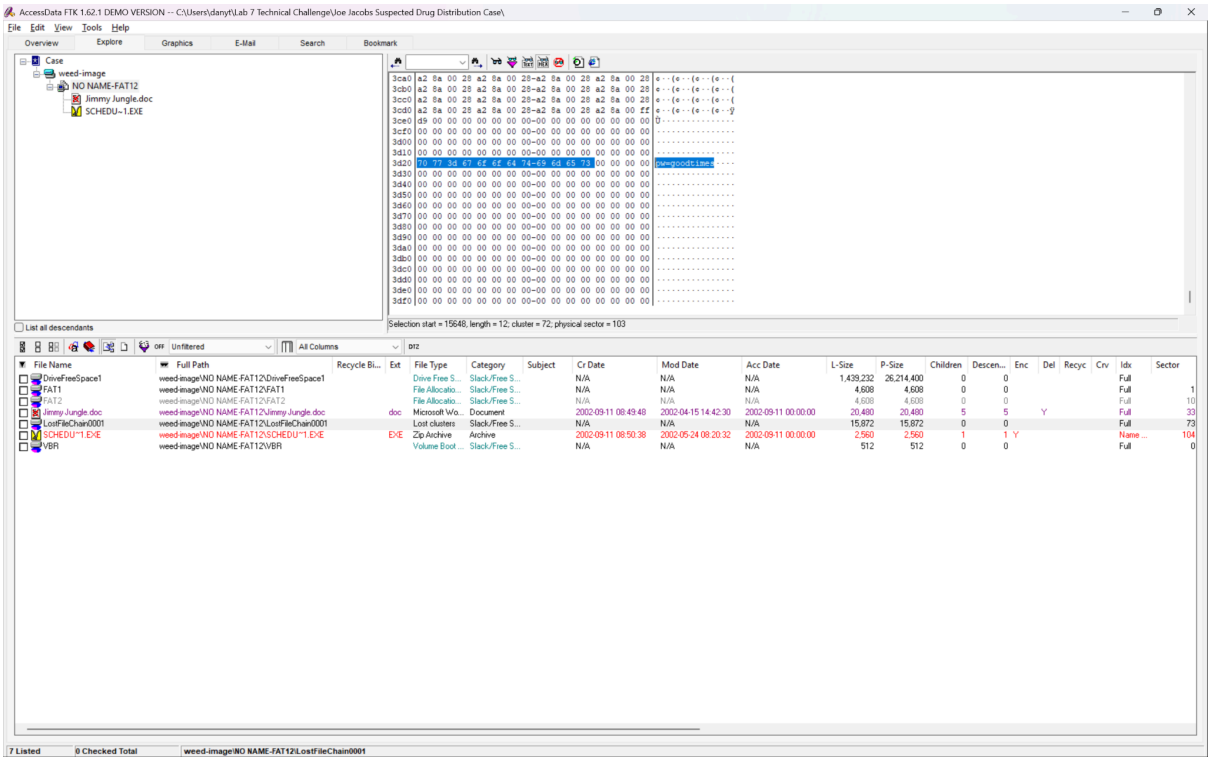
The month's featured pot grower, smoker and seller is Jimmy Jungle."

This image confirms that:

- The corrupted file 'cover page.jpgc' originally contained this magazine-style image.
- Jimmy Jungle is referenced as a prominent marijuana grower and seller.

From this we can say with high probability that this is the same file as the 'cover page.jpgc' file.

Password Discovery



Hex inspection of the slack space file revealed the following embedded text:

> '**pw=goodtimes**'

This string is the encryption password for Scheduled Visits.exe.

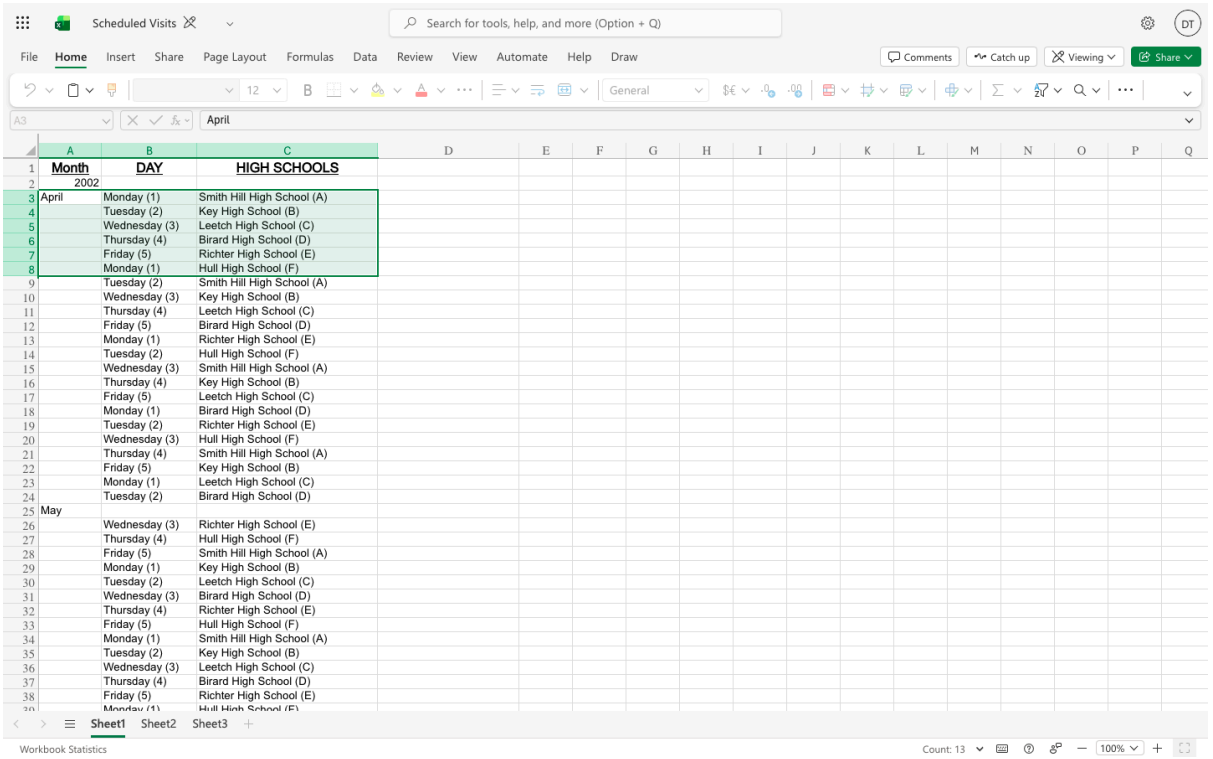
Discovery Timestamp: 27/11/2025 21:30

6.4. Decryption and Analysis of 'Scheduled Visits.xls'

6.4.1. Decryption Procedure

1. Export the file 'SCHEDU~1[13].EXE' / 'Scheduled Visits.exe'
2. Change its extension from '.exe' → '.zip' (because this is zip archive)
3. Enter the recovered password: '**goodtimes**'
4. Extract and open 'Scheduled Visits.xls' in Microsoft Excel

6.4.2. Findings



Month	DAY	HIGH SCHOOLS
2002		
April	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leetch High School (C)
	Thursday (4)	Birard High School (D)
	Friday (5)	Richter High School (E)
	Monday (1)	Hull High School (F)
	Tuesday (2)	Smith Hill High School (A)
	Wednesday (3)	Key High School (B)
	Thursday (4)	Leetch High School (C)
	Friday (5)	Birard High School (D)
	Monday (1)	Richter High School (E)
	Tuesday (2)	Hull High School (F)
	Wednesday (3)	Smith Hill High School (A)
	Thursday (4)	Key High School (B)
	Friday (5)	Leetch High School (C)
	Monday (1)	Birard High School (D)
	Tuesday (2)	Richter High School (E)
	Wednesday (3)	Hull High School (F)
	Thursday (4)	Smith Hill High School (A)
	Friday (5)	Key High School (B)
	Monday (1)	Leetch High School (C)
	Tuesday (2)	Birard High School (D)
May		
	Wednesday (3)	Richter High School (E)
	Thursday (4)	Hull High School (F)
	Friday (5)	Smith Hill High School (A)
	Monday (1)	Key High School (B)
	Tuesday (2)	Leetch High School (C)
	Wednesday (3)	Birard High School (D)
	Thursday (4)	Richter High School (E)
	Friday (5)	Hull High School (F)
	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leetch High School (C)
	Thursday (4)	Birard High School (D)
	Friday (5)	Richter High School (E)

The spreadsheet contains a schedule listing high schools and corresponding dates, indicating locations Joe Jacobs intended to visit for drug distribution.

This file identifies six high schools Joe Jacobs was targeting.

Excerpt from spreadsheet:

Month	DAY	HIGH SCHOOLS
2002		
April	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leetch High School (C)
	Thursday (4)	Birard High School (D)
	Friday (5)	Richter High School (E)
	Monday (1)	Hull High School (F)

Discovery Timestamp: 27/11/2025 22:00

7. Conclusion

The forensic examination of the recovered disk image successfully identified multiple pieces of evidence indicating coordinated drug distribution activity involving the suspect, Joe Jacobs, and an associated supplier. Through the use of industry-standard forensic tools and adherence to proper handling procedures, the investigation recovered and validated critical files—including an encrypted visit schedule, correspondence discussing drug cultivation and sales, and an image linking the supplier to marijuana production.

The analysis demonstrated clear attempts at concealment, such as encryption, deleted data, and hidden information within slack space, further reinforcing the integrity and relevance of the recovered evidence. All findings were extracted, verified, and documented following accepted forensic methodologies, ensuring their admissibility in court and maintaining the chain of custody throughout the investigation.

Overall, the evidence collectively presents a consistent narrative of intentional, organized, and ongoing illegal activity. This report provides a comprehensive, methodologically sound account of the suspect's digital activity and supports further legal action based on the recovered data.

8. Appendices

Appendix A — Hash Verification

9. Question Responses

9.1. Question Responses (Section A)

A.1 Where was the analysis of evidence conducted?

TU-Dublin Lab-A11

A.2 When did the analysis commence?

27/11/2025

A.3 What evidence supports this timeline?

Chain of Custody

A.4 Who, if anyone, aided during the process?

No one

A.5 How can the authenticity of your evidence be verified?

Hash checksums are the same at before and after investigation

A.6 What forensic tools were utilized for evidence analysis?

Software Used: Autopsy, FTK Imager, Forensic Toolkit-FTK

a. Are these tools admissible in court?

   Yes

b. How can their admissibility be determined?

   Compliance With Accepted Forensic Standards: NIST, ISO/IEC

A.7 Outline the procedures involved in uploading the evidence for analysis.

1. **Verified the Image Hash**
2. **Created a Forensic Duplicate**
3. **Prepared a Controlled Forensic Environment**
4. **Imported the Image into Analysis Tools**

A.8 How many files are presented in the complete image?

3 files:

- **'Jimmy Jungle.doc'**
- **'SCHEDU~1.EXE' → 'Scheduled Visits.exe'**
- **'cover page.jpgc' and SlackSpace for this file is: 'LostFileChain0001'**

A.9 What specific file system is currently in use?

FAT12

9.2. Question Responses (Section B)

B.1 Who is the supplier of marijuana for Joe Jacobs, and what address is associated with the supplier? Identify the key individuals involved in this case.

- **The Suspect: 'Joe Jacobs'**
- **Supplier Name: 'Jimmy Jungle'**
- **Supplier Address: '626 Jungle Ave Apt 2 Jungle, NY 11111'**

B.2 Within the coverpage.jpg file, what critical data is contained, and why is this data considered pivotal to the investigation?

The 'coverpage.jpg' file contains none useful data, but from Joe's letter we can say that this is 'the cover of High Times Magazine' that Jimmy had sended to Joe. But there are also was the SlackSpace file, that seems to be related to this file, and this SlackSpace contains the password to decrypts the archive ('Scheduled Visits.exe')

B.3 Besides Smith Hill, which, if any, other high schools did Joe Jacobs frequently visit?

- **Smith Hill High School**
- **Key High School**
- **Leetch High School**
- **Birard High School**
- **Richter High School**
- **Hull High School**

B.4 In each file, what methods did the suspect employ to conceal them from prying eyes?

- **'Jimmy Jungle.doc' – Delete this file**
- **'SCHEDU~1.EXE' → 'Scheduled Visits.exe' – Encrypt this file**
- **'cover page.jpgc' and SlackSpace (I assume) for this file is: 'LostFileChain0001' – Tried secure deletion (worked, but left the SlackSpace); Hiding password inside the file (or SlackSpace) – Steganography**

B.5 What investigative techniques were employed to comprehensively examine the entire contents of each file?

- **'Jimmy Jungle.doc' – Recover the file and standard document preview and text extraction**
- **'SCHEDU~1.EXE' → 'Scheduled Visits.exe'**
  - **File type mismatch analysis (EXE identified as encrypted ZIP)**
  - **Decryption using recovered password ("goodtimes")**

    - **File extraction and conversion to XLS**
    - **Spreadsheet examination in Microsoft Excel**
- **‘cover page.jpgc’**
    - **File metadata analysis**
    - **Hex-level examination of file contents**
- **‘LostFileChain0001’**
    - **Slack space recovery and file carving**
    - **EXIF and JFIF signature identification**
    - **Hex-level inspection**
    - **Image rendering to confirm readability**

B.6 Which Microsoft program was utilized in the creation of the Cover Page file, and what evidence supports this claim?

There is no direct forensic evidence identifying which specific Microsoft program created the Cover Page file.

The recovered version (‘LostFileChain0001’) is a JFIF JPEG image with no application-specific metadata. While the design resembles something that could be produced in programs like Microsoft Word or other layout software, no program indicators, metadata tags, or file structure markers were present to confirm the exact application used. An EXIF viewer tool did not help reveal this answer.

B.7 Are there any additional findings or information that could be instrumental in ensuring a conviction?

Several additional findings strengthen the case:

- **the decrypted ‘Scheduled Visits.xls’ file clearly shows a planned schedule of high school visits, demonstrating intent to distribute drugs to minors;**
- **the ‘Jimmy Jungle.doc’ letter confirms communication with the supplier and discusses drug cultivation and sales;**
- **and the recovered slack-space image (‘LostFileChain0001’) identifying “Jimmy Jungle” as a grower directly links the supplier to the operation.**