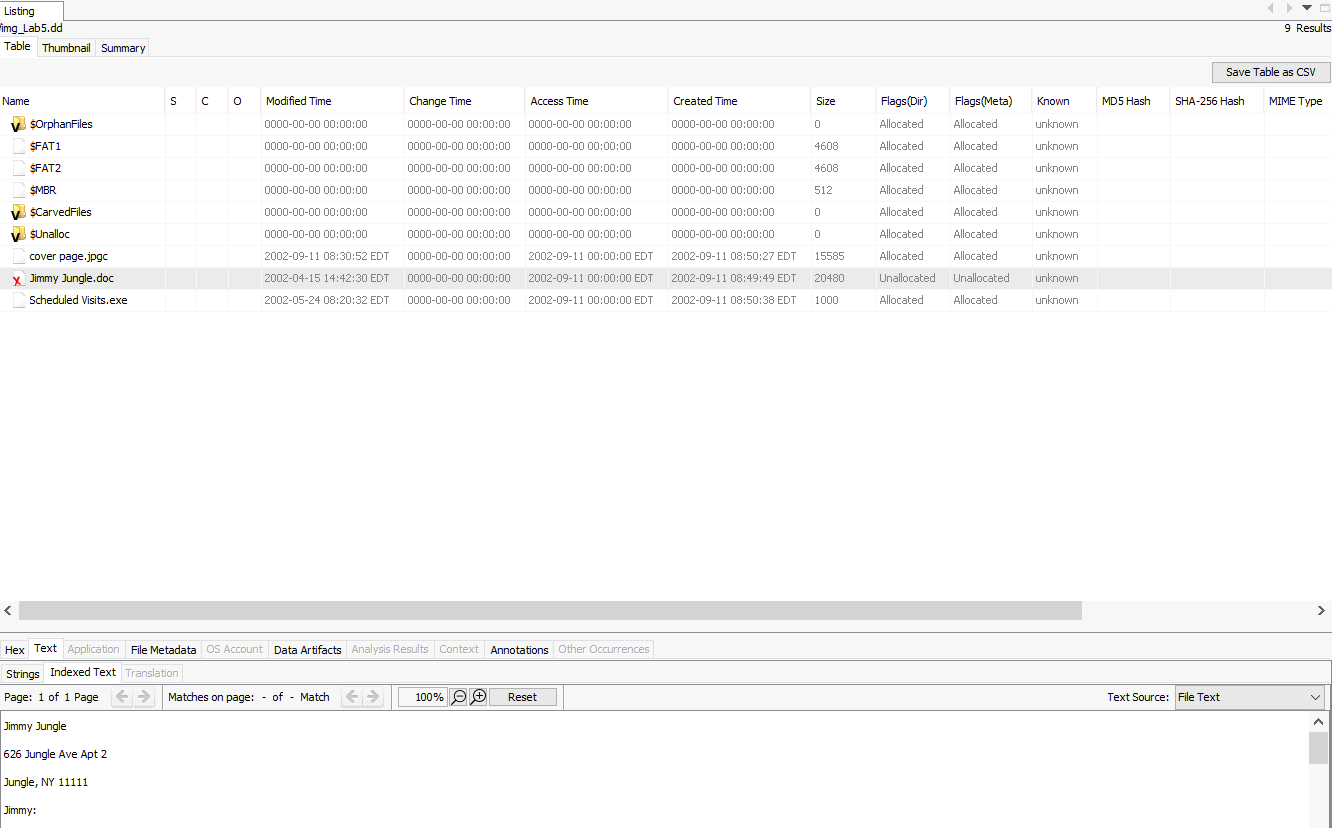
|  |  |
| --- | --- |
| Course | Computer Forensics |
| Lab | Lab 05 |
| Name of the Student | Maisha Khatoon |
| Student ID | 100899259 |

# **LAB: 05**

**Case Study**

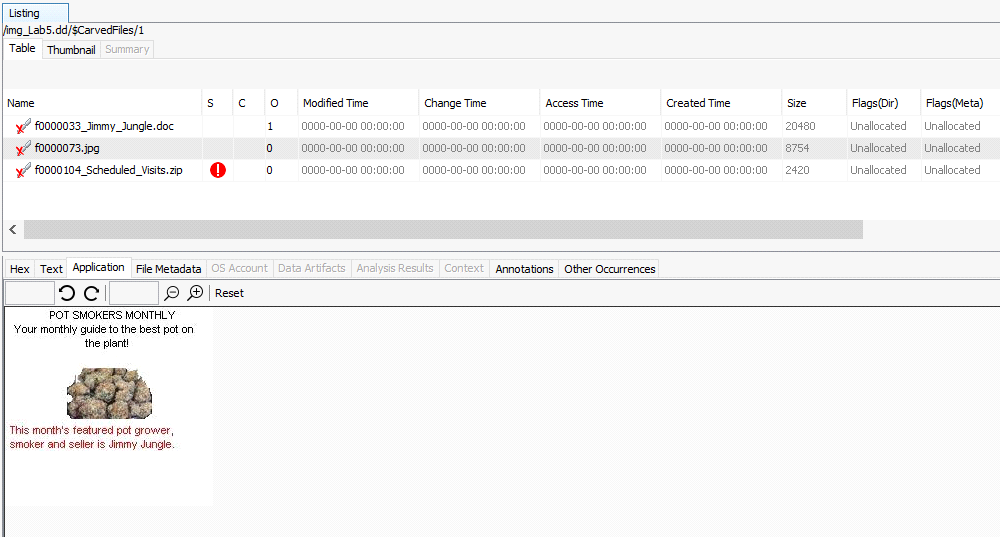
Based on the following case study, you must compile a FULL forensics report with screenshots (visible background) and explanations that answer the following questions.

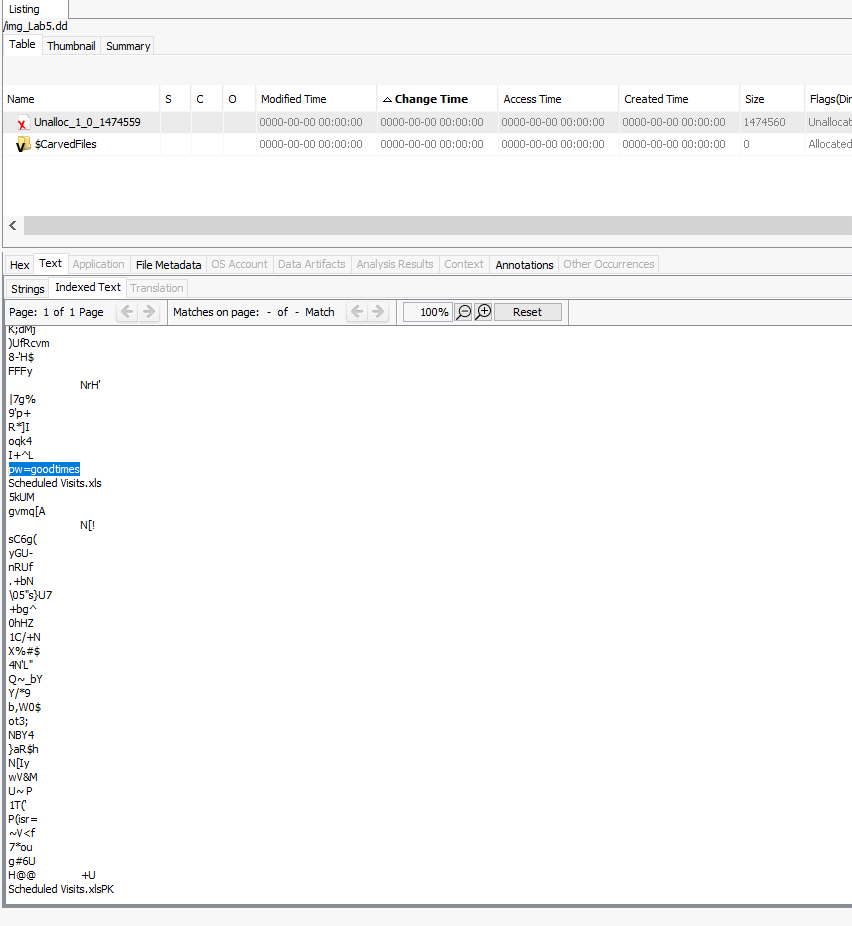
1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?



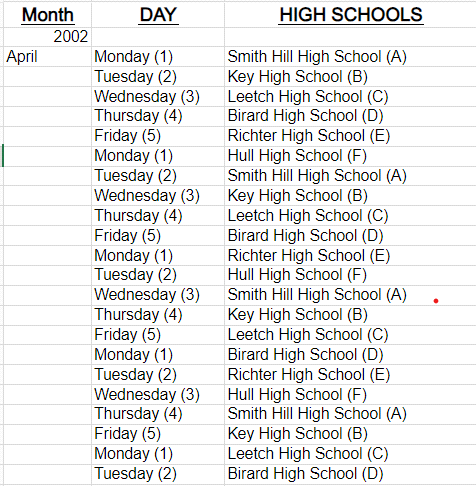
Data extracted from the file "Jimmy Jungle.doc" suggests the following. Jimmy Jungle, of 626 Jungle Avenue, Flat 2, Jungle, New York 11111, is revealed to be the Supplier's creation.

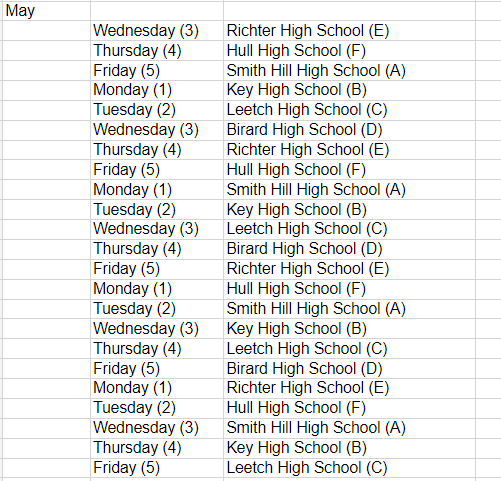
1. What crucial data is available within the coverpage.jpg file and why is this data crucial?

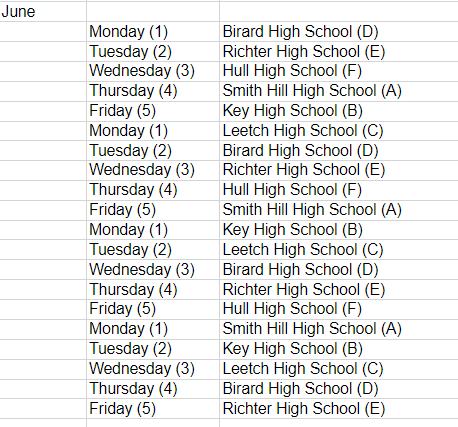




1. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?







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

Cover Page.jpg: By changing the file's extension from .jpg to .jpgc, the suspect rendered the file inaccessible and prevented access by making it appear to the computer to have an unidentified extension. The fact that the file was rendered unavailable makes the suspect in this situation a suspect.

Jimmy Jungle Document This file was allegedly deleted by the suspect.

Visits Scheduled.exe: Simply changing the file extension from.zip to.exe is all the suspect changed. In case the file's extension was changed back to .rar or.zip, he additionally password-protected it.

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

Answer: Further examination reveals three files: Jimmy Jungle.doc [deleted], Scheduled Visits.exe, and cover page.jpgc. Aside from the response to the first question, I have searched the files for indications but have come up empty-handed. As a result, I've added the image files to Autopsy once more, but this time I've put them in the Unallocated Space picture file. Like previously, I was able to locate three files, but this time I could see what was inside of them. I already knew the answer to question 1, so I didn't need to go inside the f0000033.doc file, which is truly the Jimmy Jungle.doc. I attempted to find the answer to question 2 in the file f0000073.jpg, which I believe to be the Coverpage.jpg, but I was unable. The hidden hint ("pw=goodtimes") was then located in the coverpage.jpg extension using Autopsy, which I used to search through the whole picture file. For question number three [Other high schools], I use the last file, f0000104.zip, which I assume is the Scheduled visits file. To access the archive, I had to transfer it to my computer's desktop because.zip files are opaque to Autopsy. Once I exported the zipped file, it asked for a password, so I typed in the one I had previously obtained (good times). I was able to decrypt the archive and view the Scheduled Visits.xls file's contents after it had been encrypted. It appears that the paperwork listed the dates, locations, and times that marijuana was sold.

**Conclusion**

It has been found that Joe Jacobs is indeed accountable for the charge that he supplied narcotics to high school children after carefully evaluating all the available evidence. These pieces of evidence also provided the answers to all the questions the police had that he had sidestepped or denied. The supplier's address is listed on the letter that was copied from the photo as "626 Jungle Avenue, Apartment 2, Jungle, New York 11111." We recommend that a search warrant be granted, and Jimmy Jungle is detained right away based on the front page and the letter.

**Note: Please include a screenshot of each step. Corp your screenshot to show relevant information only. Uncropped screenshots will result in a 10% deduction from your marks.**

Joe Jacobs, 28, was arrested yesterday on charges of selling illegal drugs to high school students. A local police officer posed as a high school student was approached by Jacobs in the parking lot of Smith Hill High School. Jacobs asked the undercover cop if he would like to buy some marijuana. Before the undercover cop could answer, Jacobs pulled some out of his pocket and showed it to the officer. Jacobs said to the officer "Look at this stuff, Colombians couldn't grow it better! My supplier not only sells it direct to me, he grows it himself."

Jacobs has been seen on numerous occasions hanging out at various local high school parking lots around 2:30pm, the time school usually ends for the day. School officials from multiple high schools have called the police regarding Jacobs' presence at their school and noted an increase in drug use among students, since his arrival.

The police need your help. They want to try and determine if Joe Jacobs has been selling drugs to students at other schools besides Smith Hill. The problem is no students will come forward and help the police. Based on Joe's comment regarding the Colombians, the police are interested in finding Joe Jacob's supplier/producer of marijuana.

Jacobs has denied selling drugs at any other school besides Smith Hill and refuses to provide the police with the name of his drug supplier/producer. Jacobs also refuses to validate the statement that he made to the undercover officer right before his arrest. Upon issuing a search warrant and searching of the suspect's house the police were able to obtain a small amount of marijuana. The police also seized a single floppy disk, but no computer and/or other media was present in the house.

The police have imaged the suspect's floppy disk and have provided you with a copy. They would like you to examine the floppy disk and provide answers to the previous questions. The police would like you to pay special attention to any information that might prove that Joe Jacobs was in fact selling drugs at other high schools besides Smith Hill. They would also like you to try and determine if possible who Joe Jacob's supplier is. Jacob's posted bail set at $10,000.00. Afraid he may skip town; the police would like to get him locked up as soon as possible. To do so, the police have asked that you have the results fully completed and submitted as soon as possible. Please provide the police with a strong case consisting of your specific findings related to the questions, where the findings are located on the disk, processes and techniques used, and any actions that the suspect may have taken to intentionally delete, hide and/or alter data on the floppy disk.