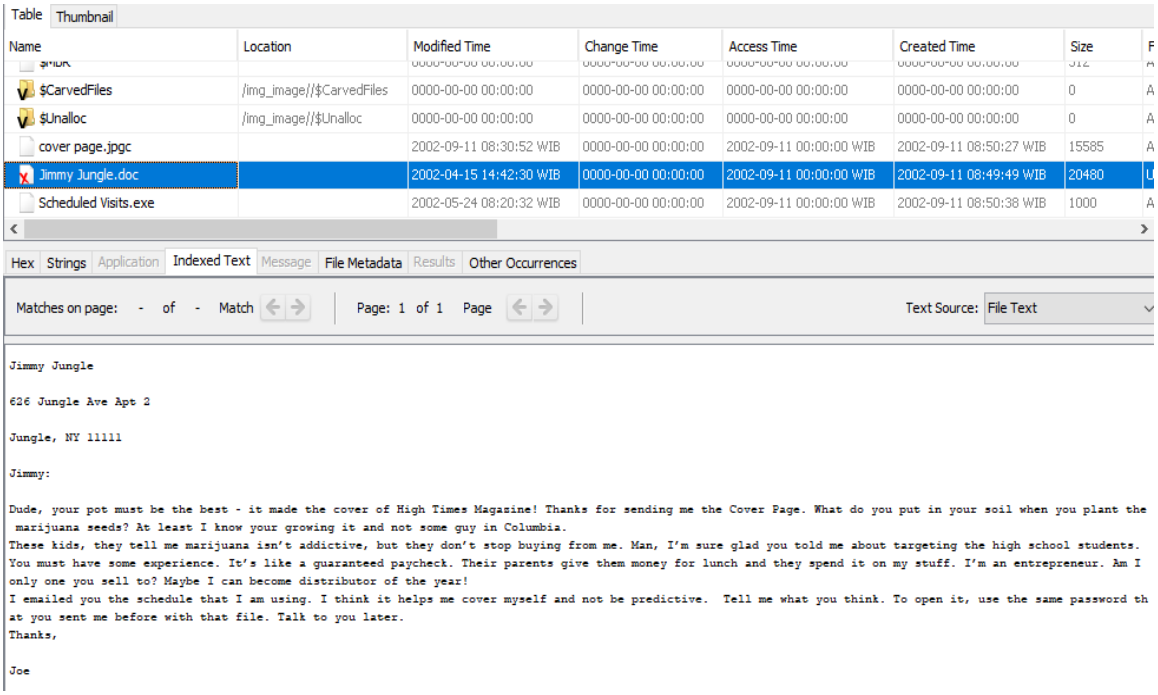
Nama : Redha Bayu Anggara
NIM : 09021381419067

1. Analisa Forensik Image File

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

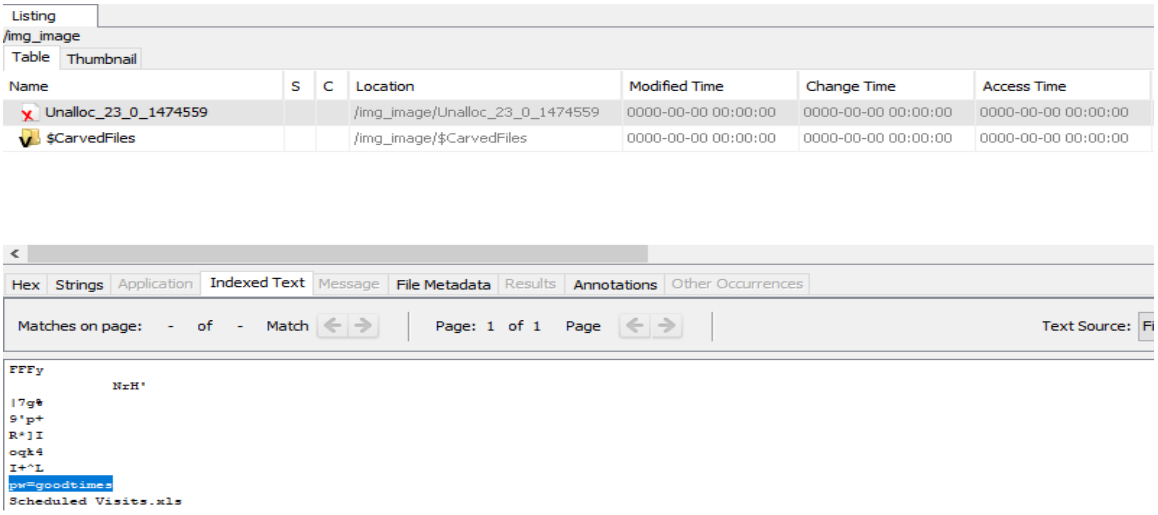
Answer :



According to the information that recovered from file **Jimmy Jungle.doc**. It is revealed that the Supplier came up with the name **Jimmy Jungle**, who live at **626 Jungle Ave Apt 2 Jungle, NY 11111.**

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

Answer :



Within the **coverpage.jpg** file, It is revealed that the suspect has slipped in a password "**pw=goodtimes**" that will be useful to open the locked **f00000104.zip** file.

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

Answer :

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

P.S : [The Content were modified for simplicity purposes]

From the **Scheduled visits.xls** which is extracted from the **f00000104.zip** file, It is revealed that aside Smith Hill High School, there are other **5 Highschools** that Jacobs visits frequently, they are : [1]Key High School, [2] Leetch High School, [3] Birard High School, [4] Ritcher High School and [5] Hull High School. They are also came up with dates.

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

Answer :

Cover Page.jpg :

The suspect simply change the file extension from .jpg to .jpgc., thus the file is considered as unknown extension by computer and cannot be opened.

Jimmy Jungle.doc :

The suspect have deleted this file.

Scheduled Visits.exe :

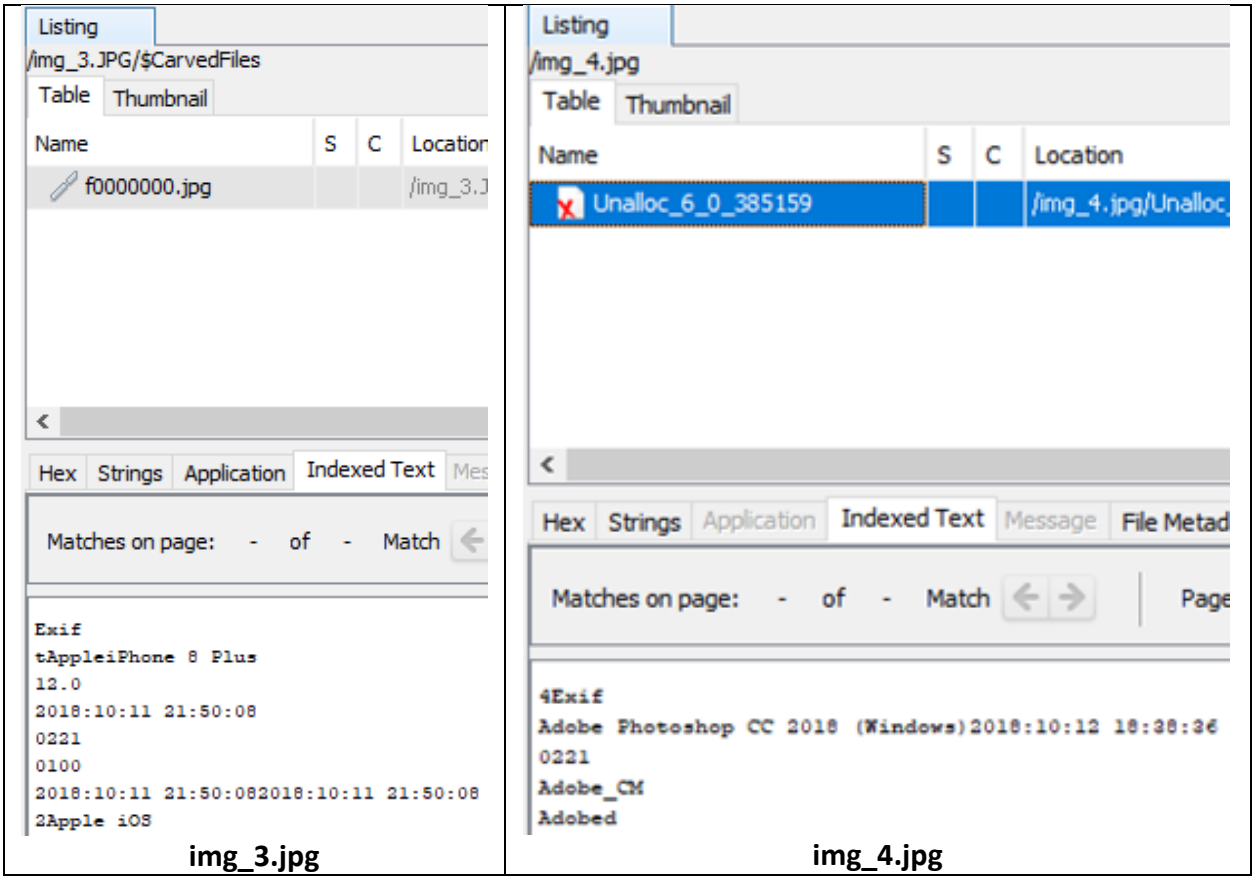
The suspect simply change the file extension from .zip to .exe, he also set up a password to protect this file, in case someone changed the extension type back to .rar/.zip.

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

  Answer :

  First, I mount the image file to **Autopsy 4.9.1.** for the examination. I've added it to **Disk Image/ VM File category**. Then I've spotted there are **3 files** : **cover page.jpgc, Jimmy Jungle.doc [deleted] and Scheduled Visits.exe**. I've checked the files for clues [Reading through with Indexed Text method] but it was a dead end except for the question number 1 [The supplier's name]. Then I've adding back the image file to Autopsy, but this time I add them to **Unallocated Space Image file** instead. From there, I can begin my analysis as I found **3 files** just like earlier, but this time I can see what is the hidden content behind the files. The **f0000033.doc** is the Jimmy Jungle.doc file so I ignore it as I already had the answer for question number 1. For answering question number 2 [Crucial data], I immediately check the **f0000073.jpg** file, which I believe is the **Coverpage.jpg**, but it was an another dead end as I can't find anything that can help me. Then I check the entire image file, it came with name **Unalloc_17_0_1474559** in Autopsy, after I carefully examined the file, I finally discovered a clue, "**pw=goodtimes**" as the clue was actually hidden in **coverpage.jpg** file. Then for question number 3 [Other high schools] I use the last file named **f0000104.zip**, which I believe is the **Scheduled visits** file. But, since Autopsy can't see through the zip files, I had to export the .zip file to my Desktop for further examination. After I exported it, the zip file asking for a password, so I use the password that I acquired earlier [goodtimes] to **unlock the zip file**. Now that the zip have been unlocked, I finally can access the hidden file, **Scheduled Visits.xls** and see what is inside it. Turns out, it appears that the file was containing **the dates and the locations** of the marijuana sales.

2. Analisa Forensik Gambar / Foto



img_3.jpg **img_4.jpg**

[both images were processed with Autopsy 4.9.1]

From the comparasion above, we clearly can see that **img_4.jpg was fake** as the image was edited with Adobe Photoshop CC 2018 (Windows) at 2018:10:12 18:28:36,

While img_3.jpg was taken with Apple iPhone 8 Plues camera at 2018:10:11 21:50:08 [real].