Universidad Carlos III de Madrid

Reporte de caso 0

Juan Diego Llano Miraval

Fecha: 16/05/2024

procedure

As a first step we checked the integrity of the file by getting the MD5:

```
zud@z:~/Downloads$ md5sum case1.zip
5662fbc923fe2484f03f4a477f1a0d03  case1.zip
```

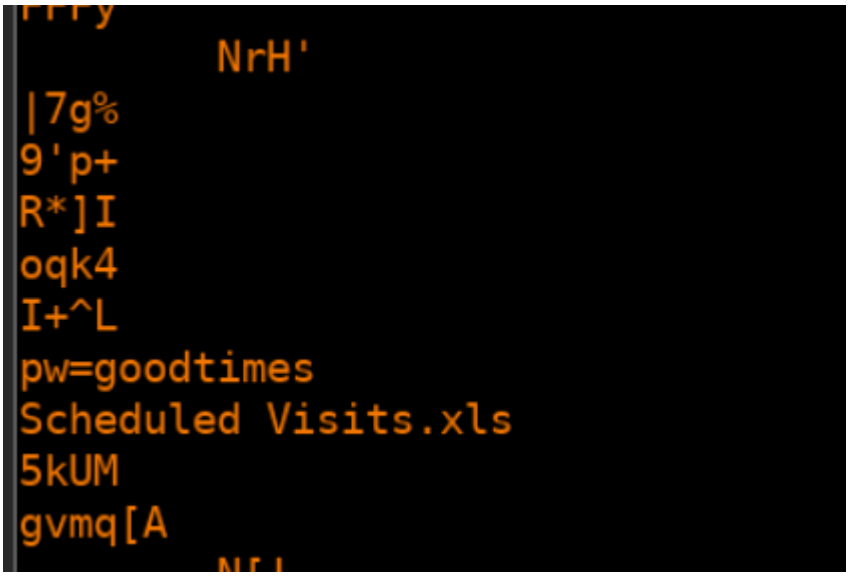
I ran strings into the image of the floppy disk and i was able to extract a message from the dealer to the provider:

```
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
```

```
zud@z:~/Downloads$ strings image
MSDOS5.0
NO NAME    FAT12   3
|8N$}$
|&f;
r9&8-t
at2Nt
NTLDR
Remove disks or other media.
Disk error
Press any key to restart
IMMYJ~1DOC
h8F+-+-
COVERP~1JPG
mMF+-+-
SCHEDU~1EXE
SSF+-+-
bjbj
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 kno
w 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 s
pend 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
```

we also were able to extract the password of the mentioned schedule:



from here we run binwalk to extract the files:

```
zud@z:~/Downloads$ binwalk -e image

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
37376         0x9200          JPEG image data, JFIF standard 1.01
53248         0xD000          Zip archive data, encrypted at least v2.0 to extra
ct, compressed size: 2282, uncompressed size: 16896, name: Scheduled Visits.xls
55646         0xD95E          End of Zip archive, footer length: 22
```

we were able to unzip the zip file with the password found on the step before. To the extracted file we checked the type of file it is and changed the name to be properly opend:

```
zud@z:~/Downloads/_image.extracted$ file 'Scheduled Visits.xls (2)'
Scheduled Visits.xls (2): Composite Document File V2 Document, Little Endian, Os
: Windows, Version 5.1, Code page: 1252, Author: CSTC, Last Saved By: CSTC, Name
 of Creating Application: Microsoft Excel, Create Time/Date: Thu May 23 16:04:12
 2002, Last Saved Time/Date: Thu May 23 16:20:47 2002, Security: 0
zud@z:~/Downloads/_image.extracted$ cp 'Scheduled Visits.xls (2)' file.xls
```

when we opened the file we got:

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)
	Monday (1)	Hull High School (F)
	Tuesday (2)	Smith Hill High School (A)

Questions:

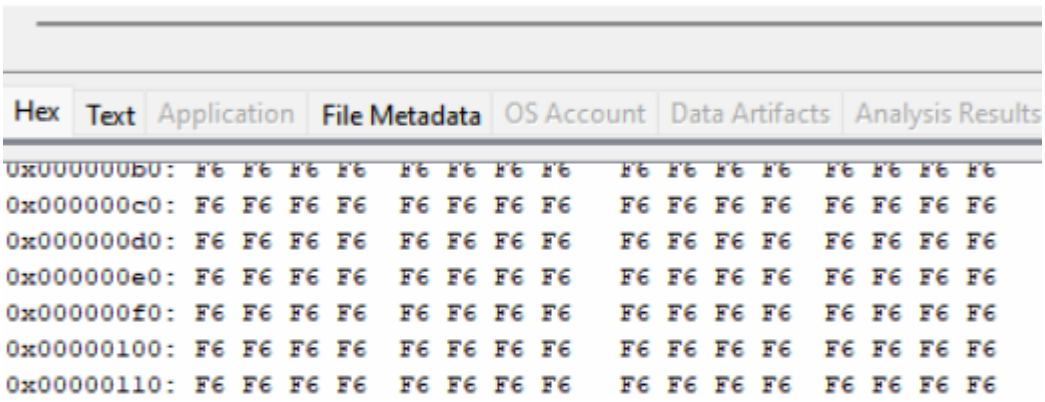
1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?

R. 626 Jungle Ave Apt 2

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

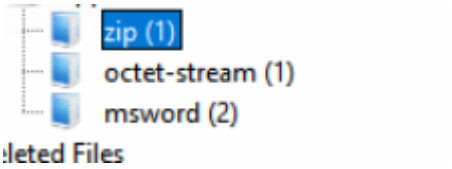
R. On the analysis I did, there was no jpg file on the binwalk extraction, in autopsy I saw it but there was no information:


cover page.jpgc
0
2002-09-11 08:30:52 CEST
0000-00-


Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
0x000000b0: F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6
0x000000c0: F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6
0x000000d0: F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6
0x000000e0: F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6
0x000000f0: F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6
0x00000100: F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6
0x00000110: F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6

```
0x00000120: F6 F6 F6 F6  F6 F6 F6 F6   F6 F6 F6 F6  F6 F6 F6 F6
0x00000130: F6 F6 F6 F6  F6 F6 F6 F6   F6 F6 F6 F6  F6 F6 F6 F6
0x00000140: F6 F6 F6 F6  F6 F6 F6 F6   F6 F6 F6 F6  F6 F6 F6 F6
0x00000150: F6 F6 F6 F6  F6 F6 F6 F6   F6 F6 F6 F6  F6 F6 F6 F6
0x00000160: F6 F6 F6 F6  F6 F6 F6 F6   F6 F6 F6 F6  F6 F6 F6 F6
0x00000170: F6 F6 F6 F6  F6 F6 F6 F6   F6 F6 F6 F6  F6 F6 F6 F6
0x00000180: F6 F6 F6 F6  F6 F6 F6 F6   F6 F6 F6 F6  F6 F6 F6 F6
0x00000190: F6 F6 F6 F6  F6 F6 F6 F6   F6 F6 F6 F6  F6 F6 F6 F6
0x000001a0: F6 F6 F6 F6  F6 F6 F6 F6   F6 F6 F6 F6  F6 F6 F6 F6
0x000001b0: F6 F6 F6 F6  F6 F6 F6 F6   F6 F6 F6 F6  F6 F6 F6 F6
0x000001c0: F6 F6 F6 F6  F6 F6 F6 F6   F6 F6 F6 F6  F6 F6 F6 F6
0x000001d0: F6 F6 F6 F6  F6 F6 F6 F6   F6 F6 F6 F6  F6 F6 F6 F6
0x000001e0: F6 F6 F6 F6  F6 F6 F6 F6   F6 F6 F6 F6  F6 F6 F6 F6
0x000001f0: F6 F6 F6 F6  F6 F6 F6 F6   F6 F6 F6 F6  F6 F6 F6 F6
```

autopsy detected the zip and 2 document files:



when I added the image as unallocated Space image, i can see the image, but no crucial information inside.

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

R. They are in the schedule extracted: Key High School, Leetch High School, Birard High School, Richter High School and Hull High School.

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

R. for the document, he delete it, the zip file, the extension was changed to .exe and it had a password. for the jpg file, the extension was also changed to jpgc.

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

R. the process is explained before in the document, first we analyzed the content of the image with autopsy, first allocating the image as disk and later as unallocated space image, and the strings in it. We were able to find the documents, the zip and the existence of the schedule because of that. In the Unallocated part of the memory was the password, that we could also retrieve with strings. Then I used binwalk to extract the zipfile in it, and extract the xls file, I checked that it was an excel file, and adjust the extension before opening it.