Nama : Abu Hanifah

NIM : 09021381520049

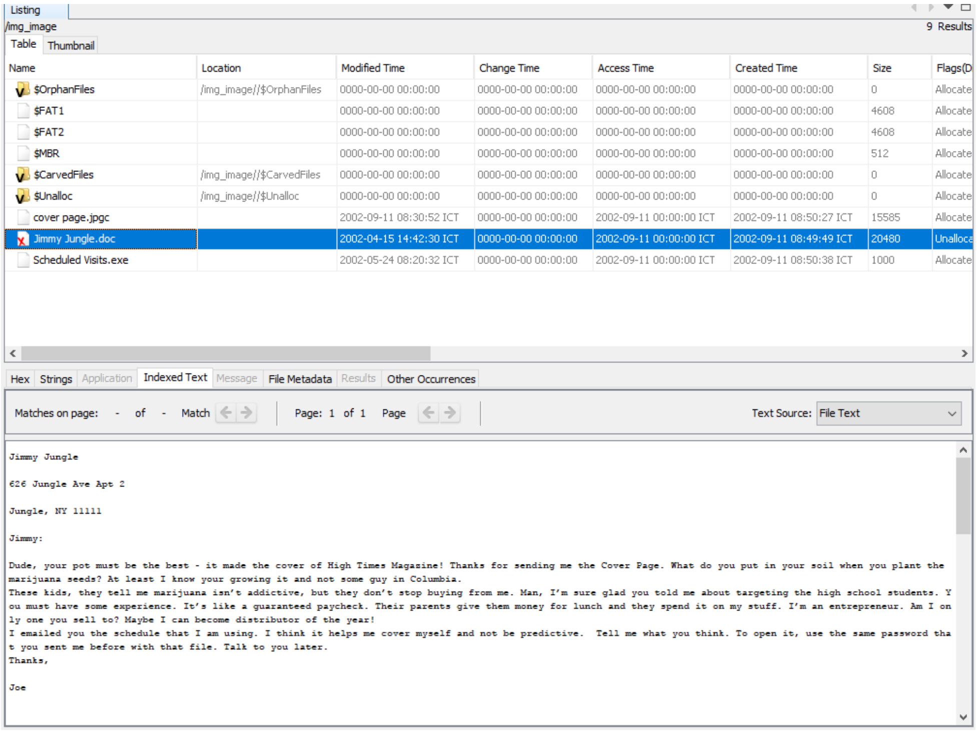
UAS KOMPUTER FORENSIK

1. a. Image file download url : http://old.honeynet.org/scans/scan24/image.zip

   Answer: Already downloaded

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

   Answer: The supplier is Jimmy Jungle. He lives at 626 Jungle Ave, Jungle, NY 11111



/img_image 9 Results

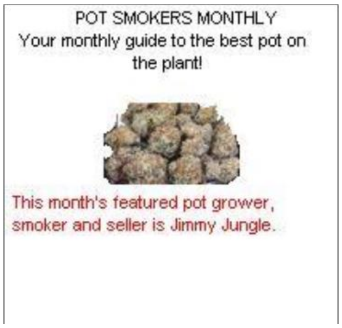
Name	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(D
$OrphanFiles	/img_image//$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocate
$FAT1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4608	Allocate
$FAT2		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4608	Allocate
$MBR		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	512	Allocate
$CarvedFiles	/img_image//$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	Allocate
$Unalloc	/img_image//$Unalloc	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	Allocate
cover page.jpgc		2002-09-11 08:30:52 ICT	0000-00-00 00:00:00	2002-09-11 00:00:00 ICT	2002-09-11 08:50:27 ICT	15585	Allocate
Jimmy Jungle.doc		2002-04-15 14:42:30 ICT	0000-00-00 00:00:00	2002-09-11 00:00:00 ICT	2002-09-11 08:49:49 ICT	20480	Unalloca
Scheduled Visits.exe		2002-05-24 08:20:32 ICT	0000-00-00 00:00:00	2002-09-11 00:00:00 ICT	2002-09-11 08:50:38 ICT	1000	Allocate

Matches on page: - of - Match Page: 1 of 1 Page Text Source: File Text

```
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. Y
ou 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 on
ly 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 tha
t you sent me before with that file. Talk to you later.
Thanks,

Joe
```

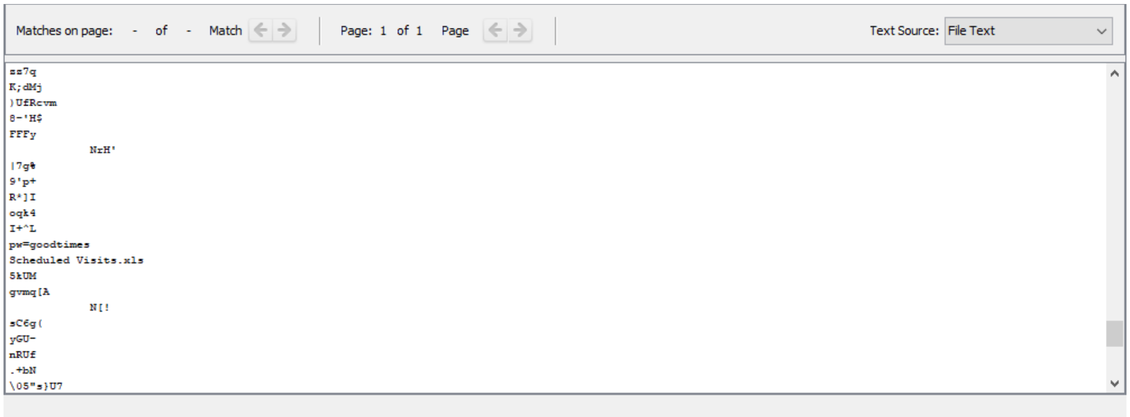
c. What crucial data is available within the coverpage.jpg file and why is this data crucial?

Answer: There is a password for opening a compressed file. That data is crucial because it can be used for extracting Scheduled Visits.xls in which is protected using password.



POT SMOKERS MONTHLY
Your monthly guide to the best pot on the plant!

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

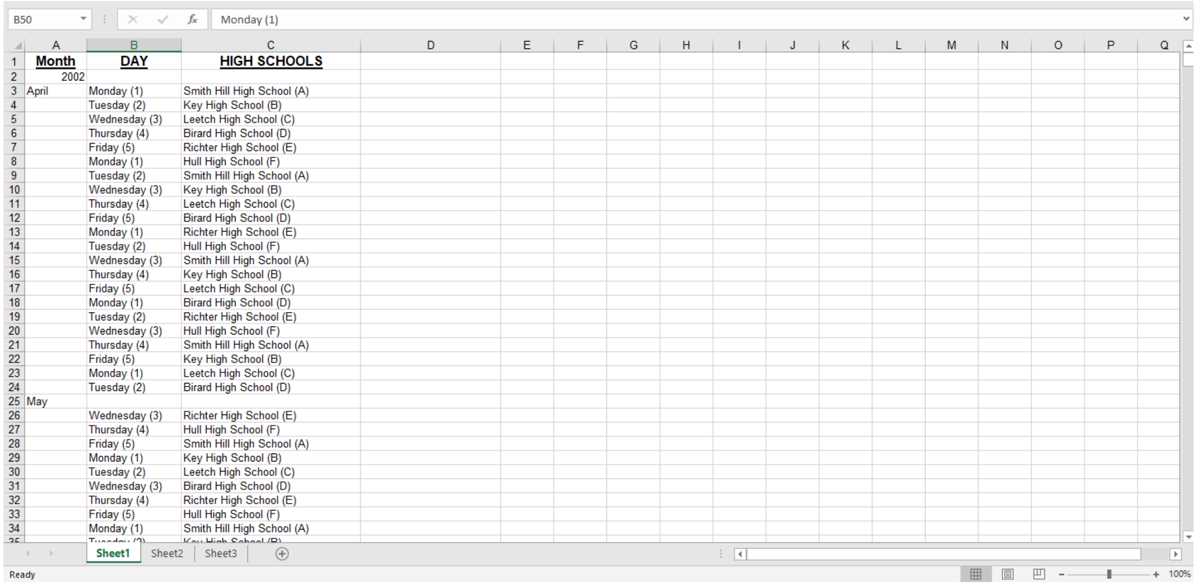


```
ss7q
K;dMj
)UfRcvm
8-'H$
FFFy
            NrH'
|7g%
9'p+
R*]I
oqk4
I+^L
pw=goodtimes
Scheduled Visits.xls
5kUM
gvmq[A
            N[!
sC6g(
yGU-
nRUf
.+bN
\05"s}U7
```

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

Answer: Key Highschool, Leetch Highschool, Birard Highschol, Richter Highschool, Hull

Highschool



	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)

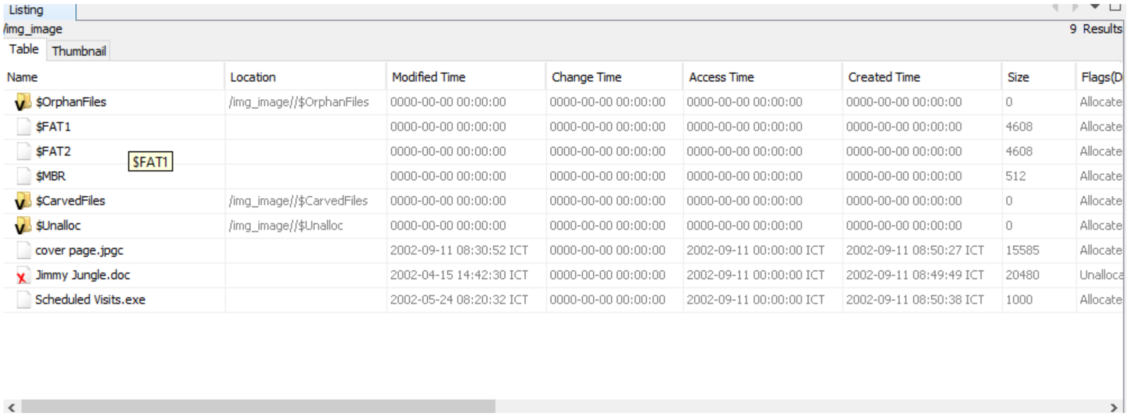
e. For each file, what processes were taken by the suspect to mask them from others?

Answer:

1. The suspect altered coverpage.jpg to jpgp and slipped a password for compressed file.

2. The suspect sent a message to Jimmy Jungle then he deleted it.

3. The suspect compressed Scheduled visits.xls with a password and altered it from xls to exe.



Name	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(D
$OrphanFiles	/img_image//$OrphanFiles	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	Allocate
$FAT1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4608	Allocate
$FAT2		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4608	Allocate
$MBR		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	512	Allocate
$CarvedFiles	/img_image//$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	Allocate
$Unalloc	/img_image//$Unalloc	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	Allocate
cover page.jpgc		2002-09-11 08:30:52 ICT	0000-00-00 00:00:00	2002-09-11 00:00:00 ICT	2002-09-11 08:50:27 ICT	15585	Allocate
Jimmy Jungle.doc		2002-04-15 14:42:30 ICT	0000-00-00 00:00:00	2002-09-11 00:00:00 ICT	2002-09-11 08:49:49 ICT	20480	Unalloca
Scheduled Visits.exe		2002-05-24 08:20:32 ICT	0000-00-00 00:00:00	2002-09-11 00:00:00 ICT	2002-09-11 08:50:38 ICT	1000	Allocate

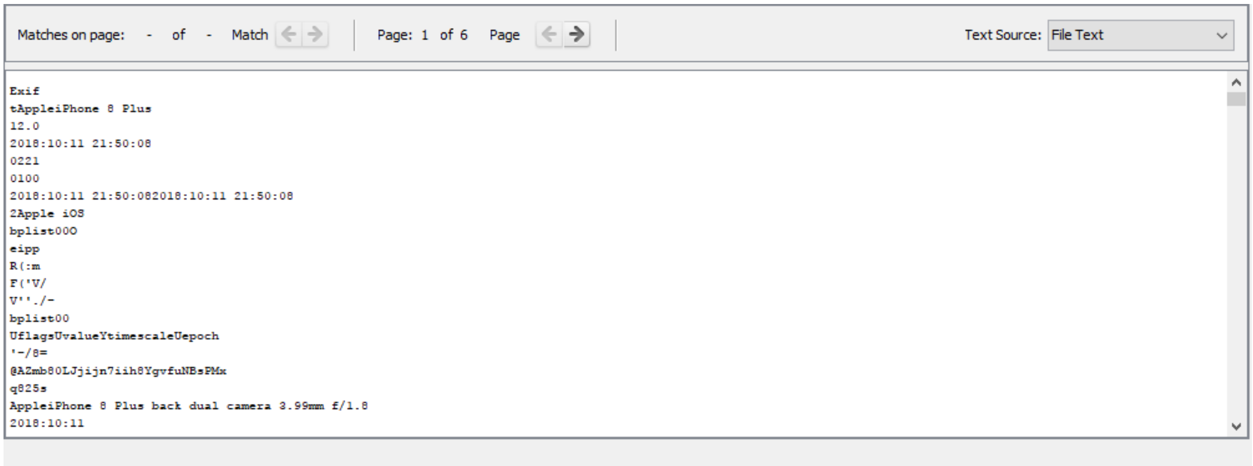
f. What processes did you (the investigator) use to successfully examine the entire contents of each file?

Answer:

First, I use a Windows application called Autopsy. Then I click New Case and put my case information. After that I click “Add Data Source” and choose Disk Image/VM Files. Then I found there are 3 files which are: **cover page.jpgc, Jimmy Jungle.doc (deleted)** and **Scheduled visits.exe**. The only file that can fully extracted and run is Jimmy Jungle.doc and the rest can’t be exctracted and opened. After that I click “Add Data Source” again but instead choosing Disk Image/VM Files, I chose Unallocated Space Image Files. Then I found 3 files which are: **f0000033.doc (Jimmy Jungle.doc)**, **f0000073.jpg (cover page.jpg)**, and **f0000104.zip** that contains **Scheduled visits.xls**. I exctracted **f0000104.zip** but i couldn’t because it required a password to extract it. After looking at **f0000073.jpg’s** hex, i found “pw=goodtimes” which can be used as password for opening that zip file. After that I can extract **Scheduled visits.xls** that contains information about other school Joe Jacob sells marijuana to.

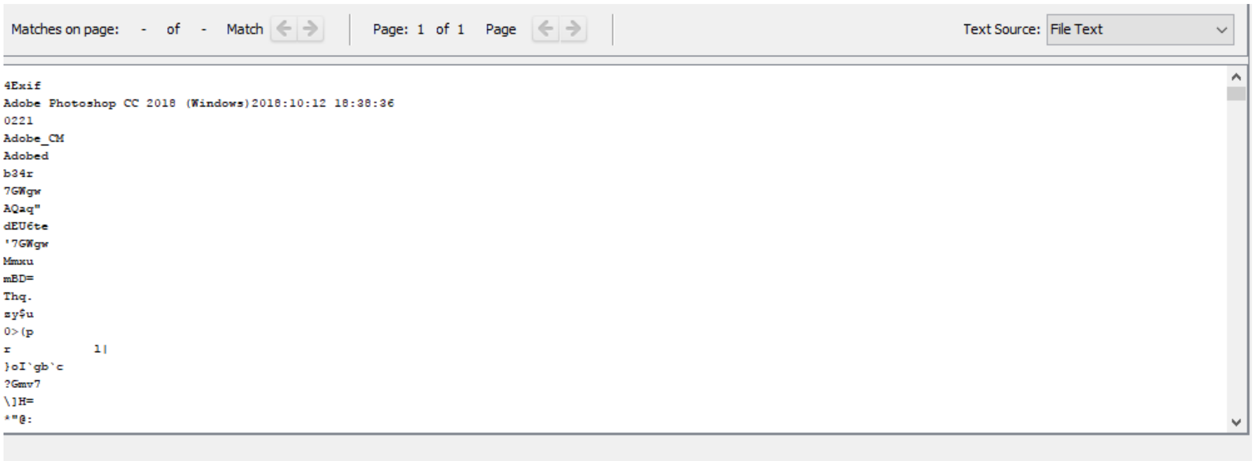
2. Melakukan forensic pada 2 gambar/foto dengan melakukan analisa pada metadata gambar/foto, membandingkan yang mana asli dan yang mana palsu.

3.JPG



```
Exif
tAppleiPhone 8 Plus
12.0
2018:10:11 21:50:08
0221
0100
2018:10:11 21:50:082018:10:11 21:50:08
2Apple iOS
bplist00O
eipp
R(:m
F('V/
V''./-
bplist00
UflagsUvalueYtimescaleUepoch
'-/8=
@AZmb80LJjijn7iih8YgvfuNBsPMx
q825s
AppleiPhone 8 Plus back dual camera 3.99mm f/1.8
2018:10:11
```

4.jpg



```
4Exif
Adobe Photoshop CC 2018 (Windows)2018:10:12 18:38:36
0221
Adobe_CM
Adobed
b34r
7GWgw
AQaq"
dEU6te
'7GWgw
Mmxu
mBD=
Thq.
zy$u
0>(p
r          1|
}oI`gb`c
?Gmv7
\]H=
*"@:
```

Pada 3.JPG di tab Indexed text, terdapat sumber foto yang berasal dari Iphone 8 Plus

Sedangkan pada 4.jpg di tab Indexed text terdapat sumber foto yang berasal dari Adobe Photoshop CC 2018

Jadi, kesimpulannya adalah foto 3.JPG adalah foto asli dan foto 4.jpg adalah foto palsu