Nama : Farhan Sepryan Ramadhan

NIM : 09021381520076

Laporan Hasil Analisa

1. Analisa Forensik Image File

The scenario is: 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.

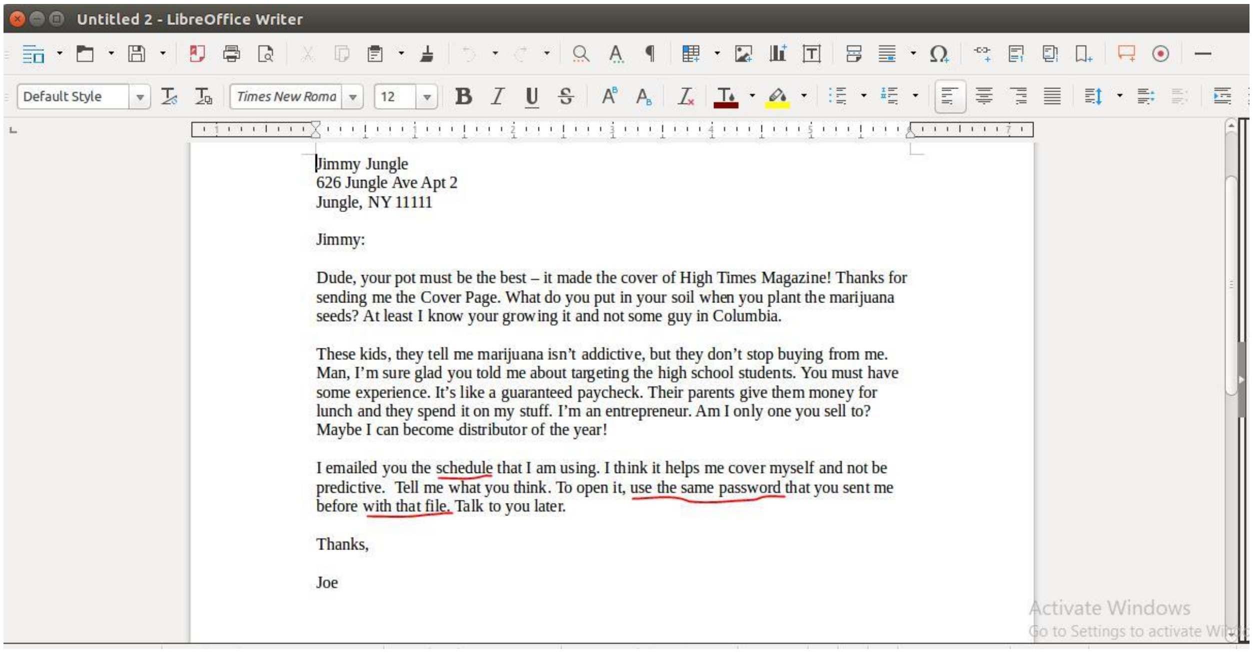
The police have imaged the suspect's floppy disk and have provided you with a copy. They would like you to examine the floppy disk and provide answers to the following questions. The police would like you to pay special attention to any information that might prove that Joe Jacobs was in fact selling 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 by October 25, 2002. 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 onthe floppy disk. Good Luck!

Any names, locations, and situations presented are completely made up. Any resemblance to any name, locations and/or situation is purely coincidence.

1) image file download url : http://old.honeynet.org/scans/scan24/image.zip
2) Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?

Pemasok Ganja Joe Jacob adalah Jimmy Jungle yang tingggal di 626 Jungle Ave Apt 2 Jungle, NY 11111, seperti yang tercantum pada file Jimmy Jungle.doc yang berhasil di recovery dari floopy disk tersangka.



Untitled 2 - LibreOffice Writer
Default Style
Times New Roma
12
Activate Windows
Go to Settings to activate Wi

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!

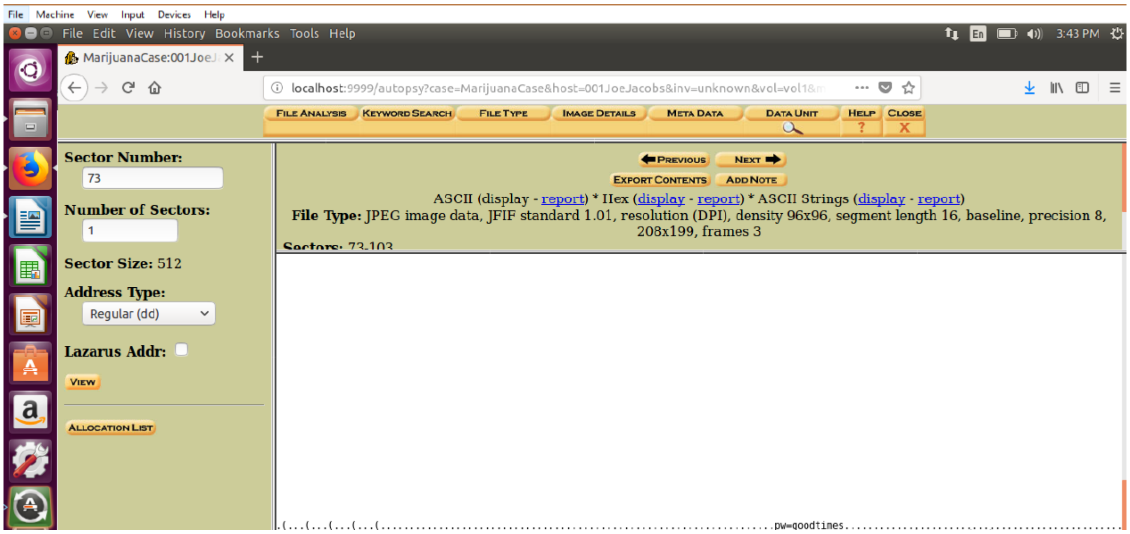
I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive. Tell me what you think. To open it, use the same password that you sent me before with that file. Talk to you later.

Thanks,

Joe

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

Terdapat password untuk membuka file zip yang berisi schedule Joe Jacobs dalam mengedarkan marijuana. Password tersebut berhasil ditemukan saat dilakukan Data Unit Analysis pada file coverpage.jpg menggunakan autopsy. Password diselipkan dalam konten pada file yang bersangkutan.


File Machine View Input Devices Help
File Edit View History Bookmarks Tools Help
3:43 PM
MarijuanaCase:001JoeJ
localhost:9999/autopsy?case=MarijuanaCase&host=001JoeJacobs&inv=unknown&vol=vol1&
File Analysis
Keyword Search
File Type
Image Details
Meta Data
Data Unit
Help
Close
Previous
Next
Export Contents
Add Note
View
Allocation List

Sector Number: 73

Number of Sectors: 1

Sector Size: 512

Address Type: Regular (dd)

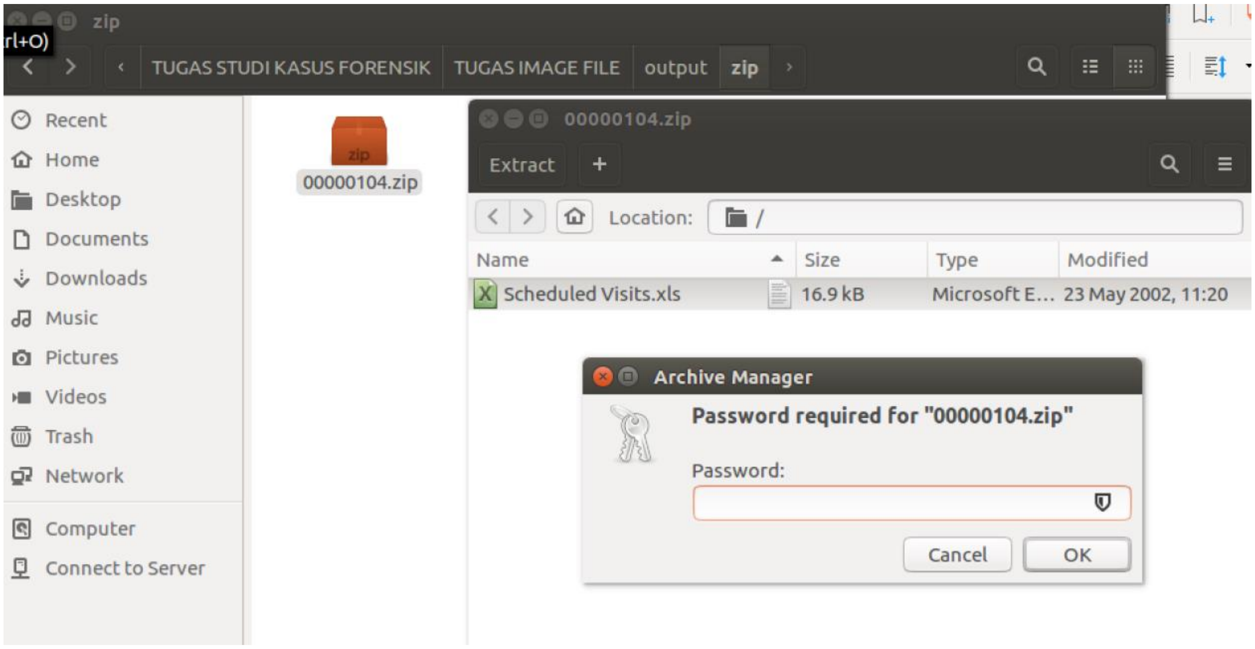
Lazarus Addr: □

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)

File Type: JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 208x199, frames 3

Sectors: 73-103

```
.(...(...(...(...(.....................................................pw=goodtimes.......................................
```



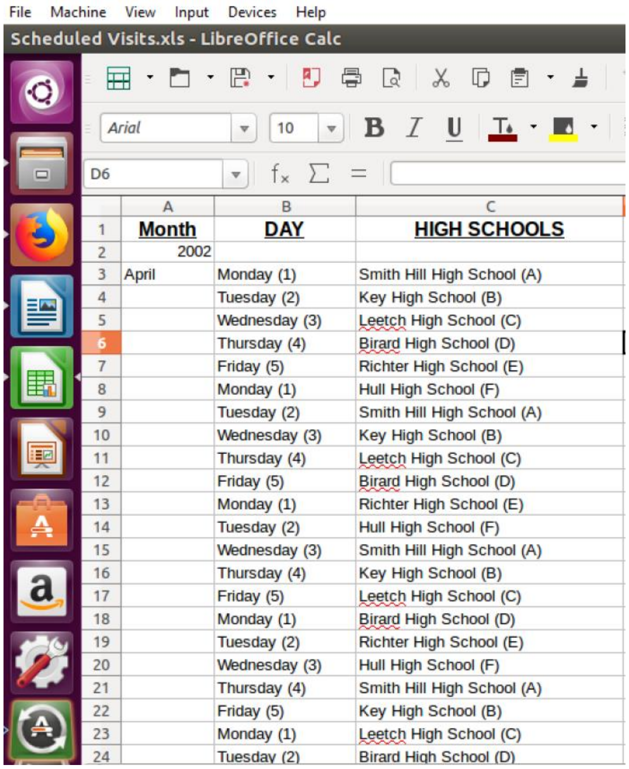
Name	Size	Type	Modified
Scheduled Visits.xls	16.9 kB	Microsoft E…	23 May 2002, 11:20

Password required for "00000104.zip"

Password:

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

Berdasarkan dari file excel yang telah didapatkan didalam zip yang dikunci menggunakan password, Joe Jacobs mengedarkan Marijuana ke 6 sekolah yang berbeda.

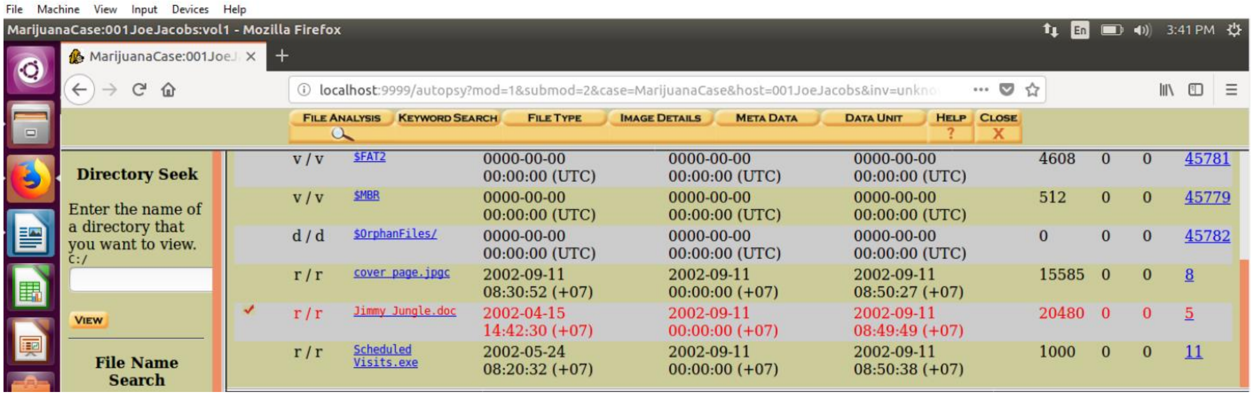


Scheduled Visits.xls - LibreOffice Calc

D6

	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)

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



MarijuanaCase:001JoeJacobs:vol1 - Mozilla Firefox

localhost:9999/autopsy?mod=1&submod=2&case=MarijuanaCase&host=001JoeJacobs&inv=unkno

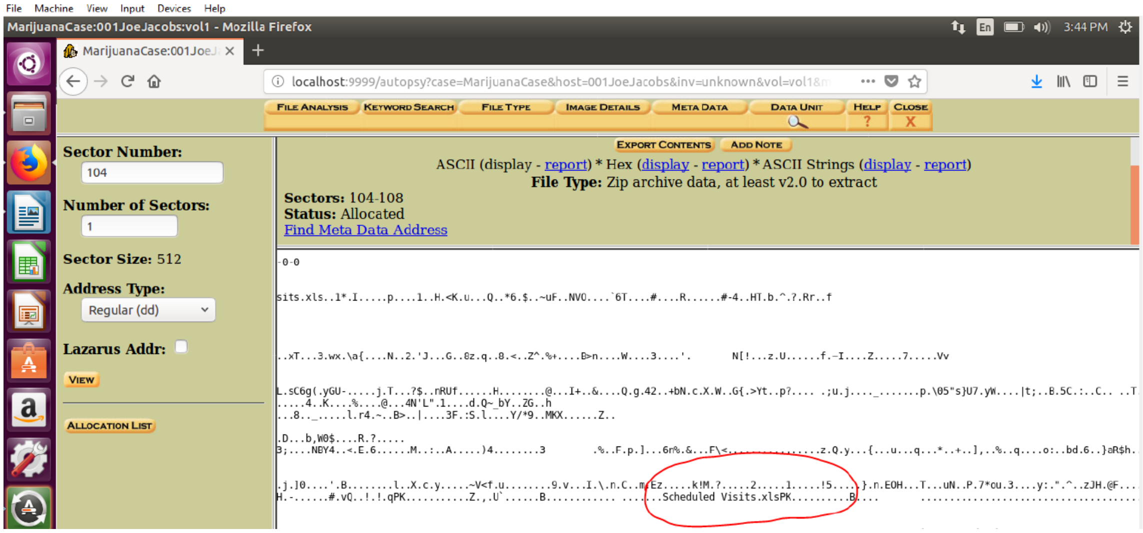
Directory Seek

Enter the name of a directory that you want to view.
C:/

File Name Search

	v / v	$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45781
	v / v	$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	45779
	d / d	$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	45782
	r / r	cover page.jpgc	2002-09-11 08:30:52 (+07)	2002-09-11 00:00:00 (+07)	2002-09-11 08:50:27 (+07)	15585	0	0	8
✓	r / r	Jimmy Jungle.doc	2002-04-15 14:42:30 (+07)	2002-09-11 00:00:00 (+07)	2002-09-11 08:49:49 (+07)	20480	0	0	5
	r / r	Scheduled Visits.exe	2002-05-24 08:20:32 (+07)	2002-09-11 00:00:00 (+07)	2002-09-11 08:50:38 (+07)	1000	0	0	11

Terdapat 3 file penting didalam floopy disk Joe Jacobs. Ekstensi dari file “cover page.jpgc” diubah, membuat file tidak teregister sebagai file gambar. File Jimmy Jungle di hapus. Ekstensi File “Scheduled Visits.exe” diubah menjadi exe, dengan menggunakan Data Unit Analysis, dapat diketahui bahwa file yang bersangkutan merupakan file xls.


File Machine View Input Devices Help
MarijuanaCase:001JoeJacobs:vol1 - Mozilla Firefox
3:44 PM
MarijuanaCase:001JoeJ
localhost:9999/autopsy?case=MarijuanaCase&host=001JoeJacobs&inv=unknown&vol=vol1&m
File Analysis
Keyword Search
File Type
Image Details
Meta Data
Data Unit
Help
Close
Export Contents
Add Note
View
Allocation List

Sector Number: 104

Number of Sectors: 1

Sector Size: 512

Address Type: Regular (dd)

Lazarus Addr: □

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)

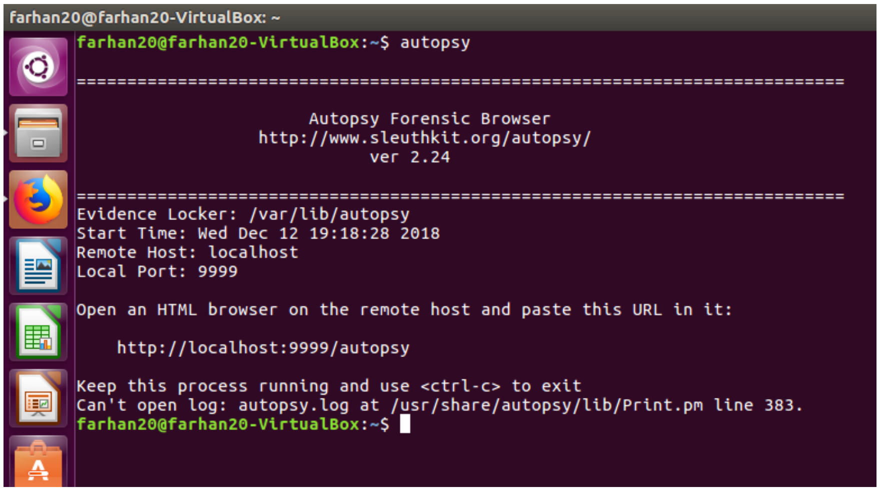
File Type: Zip archive data, at least v2.0 to extract

Sectors: 104-108
Status: Allocated
Find Meta Data Address

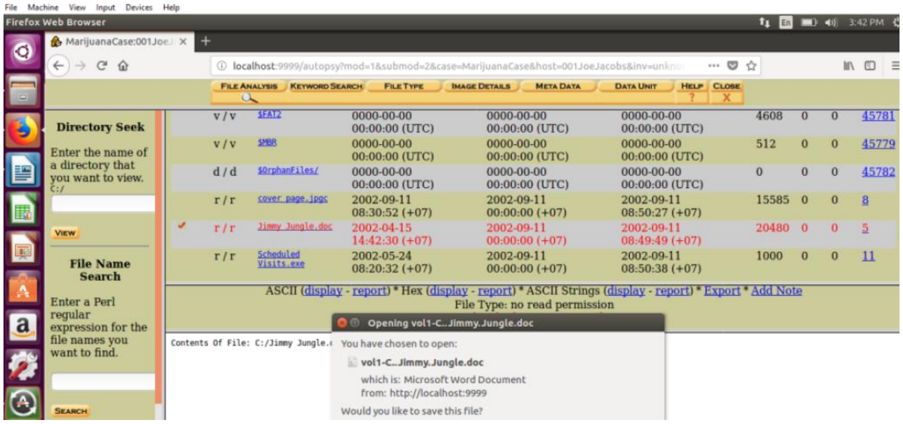
```
-0-0

sits.xls..1*.I.....p....1..H.<K.u...Q..*6.$..~uF..NVO....`6T....#....R......#-4..HT.b.^.?.Rr..f


..xT...3.wx.\a{....N..2.'J...G..8z.q..8.<..Z^.%+....B>n....W....3....'.       N[!...z.U......f.-I....Z.....7.....Vv

L.sC6g(.yGU-.....j.T...?$..nRUf......H........@...I+..&....Q.g.42..+bN.c.X.W..G{.>Yt..p?.... .;u.j...._.......p.\05"s}U7.yW....|t;..B.5C.:..C.. ..T
.....4..K....%....@...4N'L".1....d.Q~_bY..ZG..h
...8.._.....l.r4.~..B>..|....3F.:S.l....Y/*9..MKX......Z..

.D...b,W0$....R.?.....
3;....NBY4..<.E.6......M..:..A.....)4........3       .%..F.p.]...6n%.&...F\<...............z.Q.y...{...u...q...*..+..],..%..q....o:..bd.6..}aR$h.

.j.]0....'.B........l..X.c.y.....~V<f.u........9.v...I.\.n.C..m.Ez.....k!M.?.....2.....1.....!5.....}.n.EOH...T...uN..P.7*ou.3....y:.".^..zJH.@F...
H.-......#.vQ..!.!.qPK..........Z.,.U`......B............ .......Scheduled Visits.xlsPK..........B....       ....................................
```

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

   1. **Autopsy** digunakan untuk melakukan Data Unit Analysis, dan pe recover an file yang dihapus. Dengan ini ditemukan ekstensi asli dari file yang telah diubah, dan password yang disembunyikan seperti pada gambar di soal no 3.



```
farhan20@farhan20-VirtualBox:~$ autopsy

============================================================================

                       Autopsy Forensic Browser
                    http://www.sleuthkit.org/autopsy/
                               ver 2.24

============================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Wed Dec 12 19:18:28 2018
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
Can't open log: autopsy.log at /usr/share/autopsy/lib/Print.pm line 383.
farhan20@farhan20-VirtualBox:~$ 
```


File Machine View Input Devices Help
Firefox Web Browser
3:42 PM
MarijuanaCase:001Joe
localhost:9999/autopsy?mod=1&submod=2&case=MarijuanaCase&host=001JoeJacobs&inv=unkn
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
Directory Seek
Enter the name of a directory that you want to view.
C:/
VIEW
File Name Search
Enter a Perl regular expression for the file names you want to find.
SEARCH

	v / v	$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45781
	v / v	$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	45779
	d / d	$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	45782
	r / r	cover page.jpgc	2002-09-11 08:30:52 (+07)	2002-09-11 00:00:00 (+07)	2002-09-11 08:50:27 (+07)	15585	0	0	8
✓	r / r	Jimmy Jungle.doc	2002-04-15 14:42:30 (+07)	2002-09-11 00:00:00 (+07)	2002-09-11 08:49:49 (+07)	20480	0	0	5
	r / r	Scheduled Visits.exe	2002-05-24 08:20:32 (+07)	2002-09-11 00:00:00 (+07)	2002-09-11 08:50:38 (+07)	1000	0	0	11

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note

File Type: no read permission

Contents Of File: C:/Jimmy Jungle.d

Opening vol1-C..Jimmy.Jungle.doc

You have chosen to open:

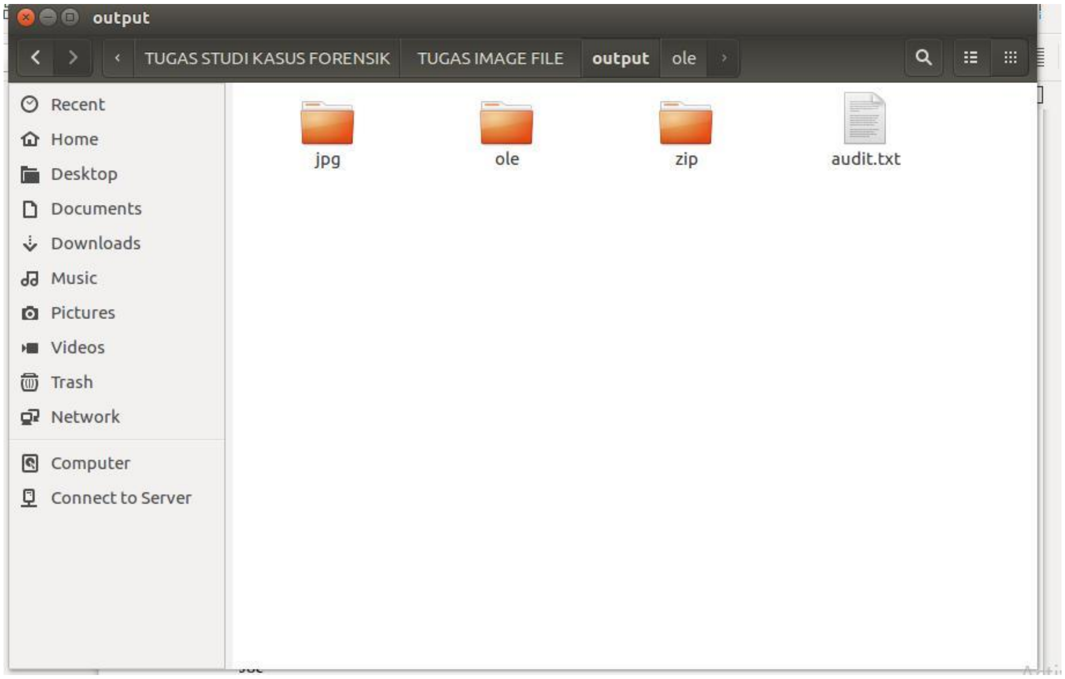
vol1-C..Jimmy.Jungle.doc

which is: Microsoft Word Document

from: http://localhost:9999

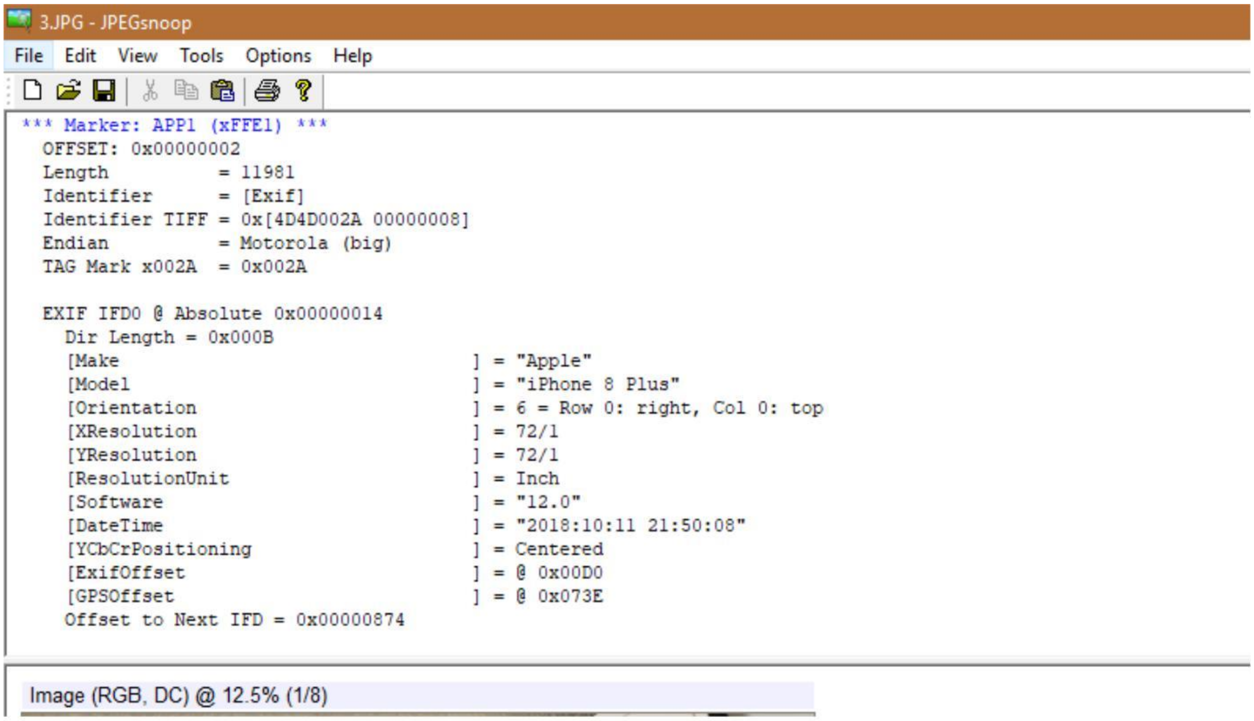
Would you like to save this file?

2. **Foremost**, file image dapat langsung direcover dan diperbaiki. Gambar berikut merupakan hasil dari foremost.



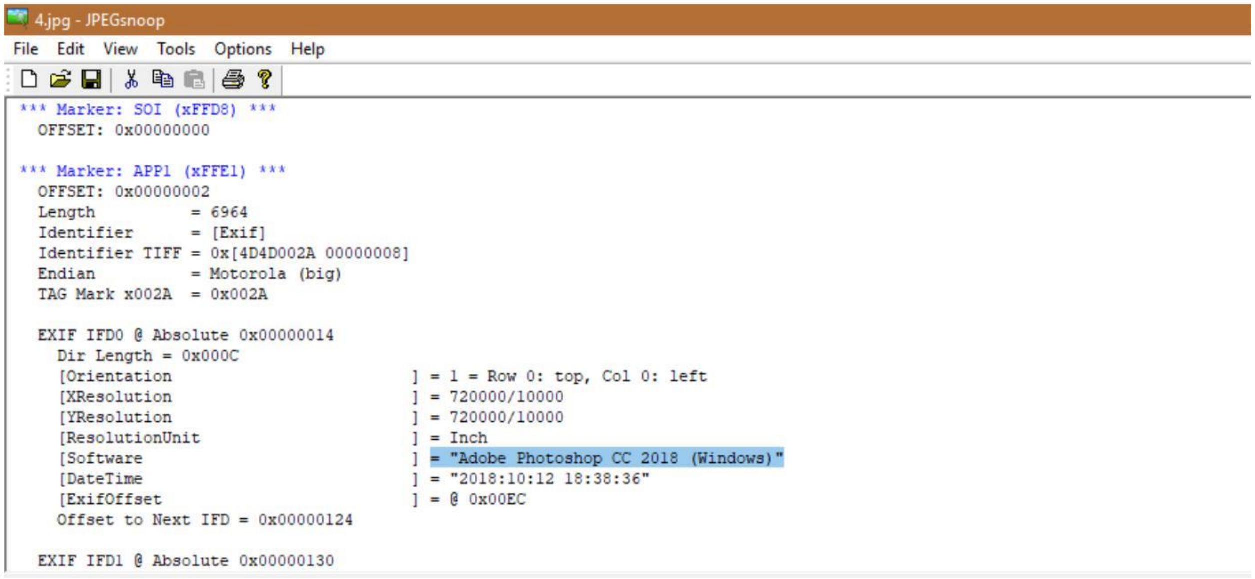
2. Analisa Forensik Gambar / Foto

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



```
*** Marker: APP1 (xFFE1) ***
  OFFSET: 0x00000002
  Length          = 11981
  Identifier      = [Exif]
  Identifier TIFF = 0x[4D4D002A 00000008]
  Endian          = Motorola (big)
  TAG Mark x002A  = 0x002A

  EXIF IFD0 @ Absolute 0x00000014
    Dir Length = 0x000B
    [Make                                    ] = "Apple"
    [Model                                   ] = "iPhone 8 Plus"
    [Orientation                             ] = 6 = Row 0: right, Col 0: top
    [XResolution                             ] = 72/1
    [YResolution                             ] = 72/1
    [ResolutionUnit                          ] = Inch
    [Software                                ] = "12.0"
    [DateTime                                ] = "2018:10:11 21:50:08"
    [YCbCrPositioning                        ] = Centered
    [ExifOffset                              ] = @ 0x00D0
    [GPSOffset                               ] = @ 0x073E
    Offset to Next IFD = 0x00000874
```

Image (RGB, DC) @ 12.5% (1/8)



```
*** Marker: SOI (xFFD8) ***
  OFFSET: 0x00000000

*** Marker: APP1 (xFFE1) ***
  OFFSET: 0x00000002
  Length          = 6964
  Identifier      = [Exif]
  Identifier TIFF = 0x[4D4D002A 00000008]
  Endian          = Motorola (big)
  TAG Mark x002A  = 0x002A

  EXIF IFD0 @ Absolute 0x00000014
    Dir Length = 0x000C
    [Orientation                             ] = 1 = Row 0: top, Col 0: left
    [XResolution                             ] = 720000/10000
    [YResolution                             ] = 720000/10000
    [ResolutionUnit                          ] = Inch
    [Software                                ] = "Adobe Photoshop CC 2018 (Windows)"
    [DateTime                                ] = "2018:10:12 18:38:36"
    [ExifOffset                              ] = @ 0x00EC
    Offset to Next IFD = 0x00000124

  EXIF IFD1 @ Absolute 0x00000130
```

Menggunakan JPEGsnoop, dapat diketahui dari metadata diatas bahwa file “4.jpg” telah diedit menggunakan software Adobe Photoshop CC 2018.