

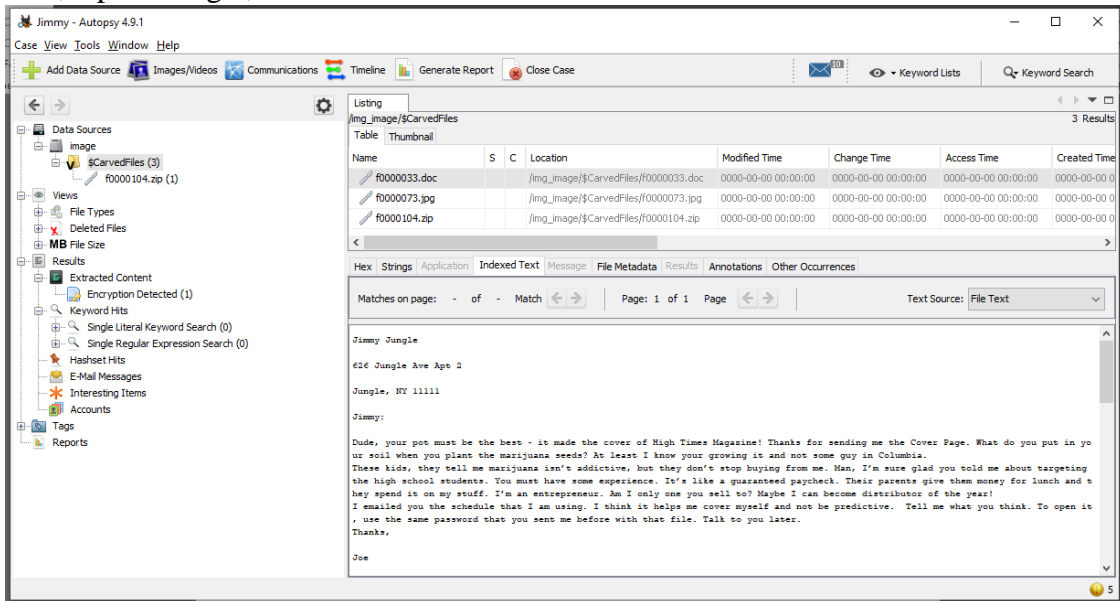
Nama : Ali Zaenal Abidin

NIM : 09021281520072

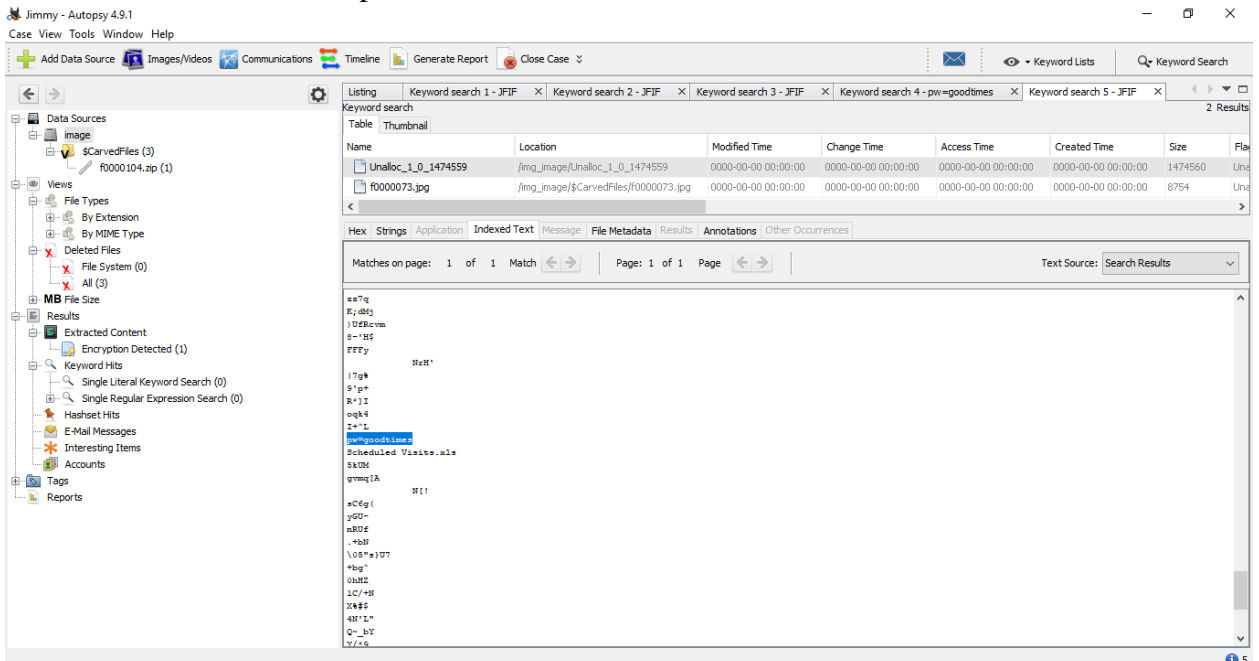
KOMPUTER FORENSIK

1.

- b. Berdasarkan f0000033.doc didapatkan hasil: Supplier : Jimmy Jungle; Alamat : 626 Jungle Ave, Apt 2. Jungle, NY 11111



- c. Crucial data adalah bagian "pw=goodtimes" karena menunjukkan password untuk membuka file f00000104.zip.



- d. Key High School, Leetch High School, Birard High School, Ritcher High School, Hull High School

| 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) |

- e. Cover page.jpg, File ini salah menunjuk ke sektor 451 pada disk untuk unit datanya; seharusnya mengarah ke sektor 73. Setiap upaya untuk membuka file akan menghasilkan unit data di sektor 451 yang memiliki semua byte yang disetel ke 'f6'. Jimmy Jungle.doc, File ini telah dihapus. ScheduledVisit.exe, Panjang untuk file ini menyatakan itu hanya 1000 byte; Namun itu sebenarnya 2560 byte. Ekstensi file tidak sesuai dengan jenis file. File itu juga dilindungi kata sandi.
- f. Dengan Menggunakan **Autopsy 4.9.1**, dilakukan 4 Proses : Insert File Image, Read Indexed Text, Use Keyword Search, Extract File. Setelah memasukan file image, terdapat 1 file unallocated dan 1 folder yang berisi 3 file yaitu dokumen f0000033.doc, image f0000073.jpg dan sebuah file zip f0000104.zip. Didalam file dokumen ini investigator melihat Indexed Text yang ada didalam file tersebut, berisi sebuah surat yang memiliki nama dan alamat yang dituju. lihat dari isi surat tersebut menunjukkan bahwa surat tersebut ditujukan kepada suplier. Dari file f0000073.jpg terdapat gambar, tapi tidak menemukan apa apa didalamnya. Investigator kemudian melakukan pencarian kata JFIF pada seluruh file image dan ternyata ada 2 file yang cocok dengan pencarian tersebut yaitu f0000073.jpg dan file unallocated, didalam IndexedText file unallocated terdapat string pw=goodtimes dan ScheduledVisit.xls investigator berasumsi bahwa goodtimes adalah password untuk membuka file ScheduledVisit.xls. Dari file f0000104.zip setelah diekstrak ternyata didalamnya terdapat 1 file excel yaitu ScheduledVisit.xls tapi file ini membutuhkan password, kemudian investigator memasukkan password yang didapat dari

file gambar sebelumnya dan file tersebut bisa dibuka dan isinya adalah tanggal dan tempat yang dikunjungi.

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

Dari kedua file tersebut, setelah investigator melakukan analisis gambar dengan nama **4.jpg** adalah **PALSU**.

Investigator melakukan analisis menggunakan aplikasi **Autopsy 4.9.1** dari nilai Hex dan strings yang terdapat pada gambar 3.jpg terdapat informasi mengenai kapan gambar tersebut diambil, menggunakan apa gambar tersebut diambil

Apple

iPhone 8 Plus

12.0

2018:10:11 21:50:08

0221

0100

2018:10:11 21:50:08

2018:10:11 21:50:08

Apple iOS

Generate Report Close Case

18 Keyword Lists Keyword Search

Listing Data Sources 2 Results

| Name | Type | Size (Bytes) | Sector Size (Bytes) | MD5 Hash | Timezone | Device ID |
|-------|-------|--------------|---------------------|----------|--------------|--------------------------------------|
| 3.JPG | Image | 3419124 | 512 | | Asia/Bangkok | bd8f47b3-9aba-4cd8-9028-851621cd5e4b |
| 4.jpg | Image | 385160 | 512 | | Asia/Bangkok | 4608f949-5376-47fc-a5ff-6e65da38067f |

Hex Strings Application Indexed Text Message File Metadata Results Annotations Other Occurrences

Page: 1 of 209 Page Go to Page: 8 Script: Latin - Basic

```

Exif
Apple
iPhone 8 Plus
12.0
2018:10:11 21:50:08
0221
0100
2018:10:11 21:50:08
2018:10:11 21:50:08
Apple iOS
bplist000
!AEEEE-
«I:AEIII»
+~*IOxµ
-~.Ea'IUXç
»c*II
^!GöwÜ
%AEÄ
!4"O
~*E
.YÖa.!
eipp
R(:mAF('V
EV''./-
Öæçø*-
ÖæYex
wëuIEöáö+u
lNæ+Äeäi
bplist00
flagsUvalueYtimescaleUepoch

```

Sedangkan dari nilai hex dan strings yang terdapat dalam 4.jpg hanya

Adobe Photoshop CC 2018 (Windows)

2018:10:12 18:38:36

0221

Adobe_CM

Adobe

Yang membuktikan bahwa bisa saja gambar tersebut sudah dimanipulasi menggunakan aplikasi Adobe Photoshop

Listing ◀ ▶ ▢

Data Sources 2 Results

Table Thumbnail

| Name | Type | Size (Bytes) | Sector Size (Bytes) | MD5 Hash | Timezone | Device ID |
|-------|-------|--------------|---------------------|----------|--------------|--------------------------------------|
| 3.JPG | Image | 3419124 | 512 | | Asia/Bangkok | bd8f47b3-9aba-4cd8-9028-851621cd5e4b |
| 4.jpg | Image | 385160 | 512 | | Asia/Bangkok | 4608f949-5376-47fc-a5ff-6e65da38067f |

Hex Strings Application Indexed Text Message File Metadata Results Annotations Other Occurrences

Page: 1 of 24 Page ← → Go to Page: Script: Latin - Basic

```

Exif
Adobe Photoshop CC 2018 (Windows)
2018:10:12 18:38:36
0221
Adobe_CM
Adobe
dEIt6
GWgw
AQaq"
EU6te
7GWgw
Mmxu
Thq.
0>(p
}oI'gb`c
7Gmv7
{<=0
2+mM}uC
nPsi~
U|,/
d#}0#C
{2\8
;-_H
-;{1
|=G3c
Q:j>
-z2mx%
Qsju
4SEU
#VE.s
  
```

5