Nama : Dian Ayu Budiarti

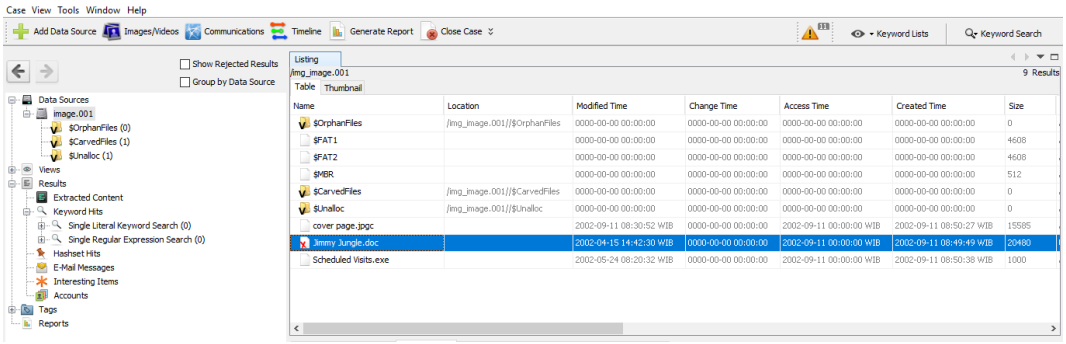
NIM : 09021181520010

Mata Kuliah : Komputer Forensik

Program Study : Teknik Informatika Reguler ‘15

UAS KOMPUTER FORENSIK

1. Dilakukan pencarian file yang telah dihapus oleh jacob dengan menggunakan aplikasi autopsy dan ditemukan file “jimmyjungle.doc” yang telah dihapus.



Isi file “jimmyjungle.doc” yang dihapus :

Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111

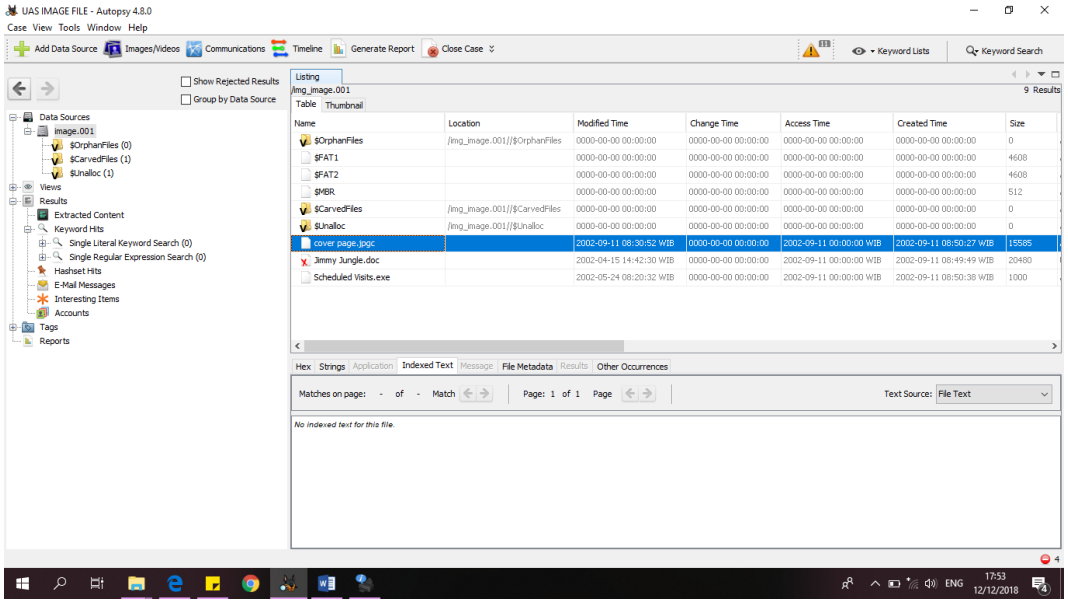
Jimmy:

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?

Data :
Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 111111

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



Terdapat file Cover page.jpgc , selanjutnya di extract dan diubah ekstensinya menjadi .jpg. Pada file coverpage.jpg, berisi string pw = goodtimes yang tampaknya merupakan kata sandi. Kata sandi diperlukan untuk mendekripsi dan membuka file zip.

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

	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)

Sheet1 Sheet2 Sheet3 +

Leetch High School, Birard High School, Richter High School, Key High School, dan Hull High School

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

Jimmyjungle.doc -> dihapus
Cover page.jpgc - > sebenarnya merupakan file jpg
Scheduled visits.exe -> sebenarnya merupakan file zip yg dipassword yang didalamnya terdapat file xls.

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

Proses yang saya lakukan adalah dengan menganalisa bukti yang ada dengan software autopsy, dari situ didapatkan 3 buah file yaitu :

Jimmyjungle.doc -> dihapus
Cover page.jpgc - > sebenarnya merupakan file jpg
Scheduled visits.exe -> sebenarnya merupakan file zip yg dipassword yang didalamnya terdapat file xls.

Kemudian membuka cover page.jpg dengan menggunakan ihex kemudian ditemukan password : goodtimes yang ternyata merupakan password dari file Scheduledvisits.zip yang berisi daftar tempat Jacob menjual Marijuananya.

Soal Analisis Gambar :

Foto 3.jpg merupakan foto asli yang diambil menggunakan smartphone apple iPhone 8 Plus, pada tanggal 11 Oktober 2018, pada pukul 21:50:08.

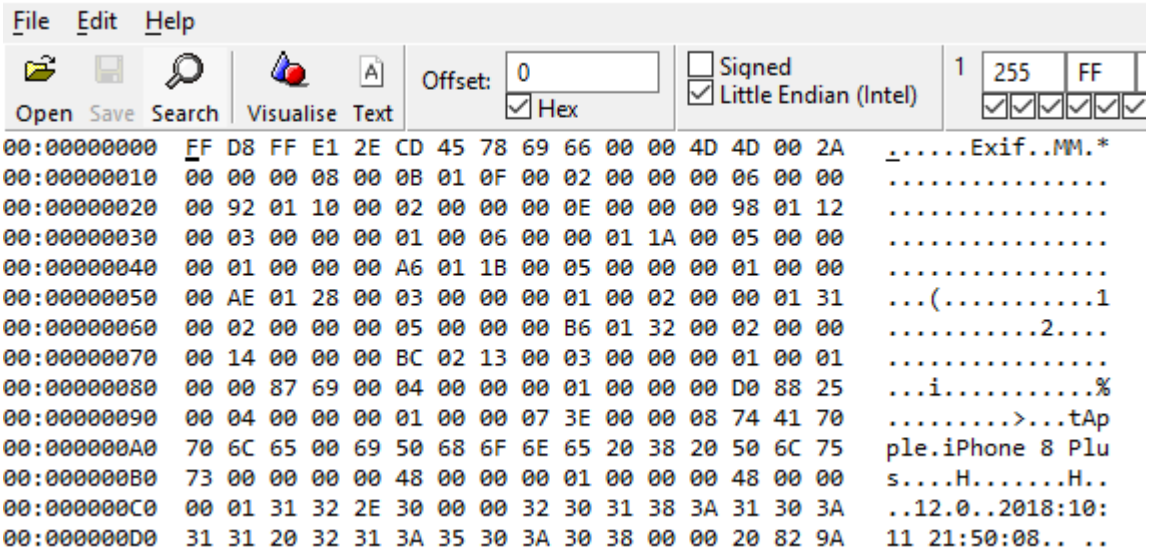


Foto 4.jpg merupakan foto yang telah di edit merupakan Adobe Photoshop CC 2018 pada tanggal 12 Oktober 2018 pada pukul 18:38:36.