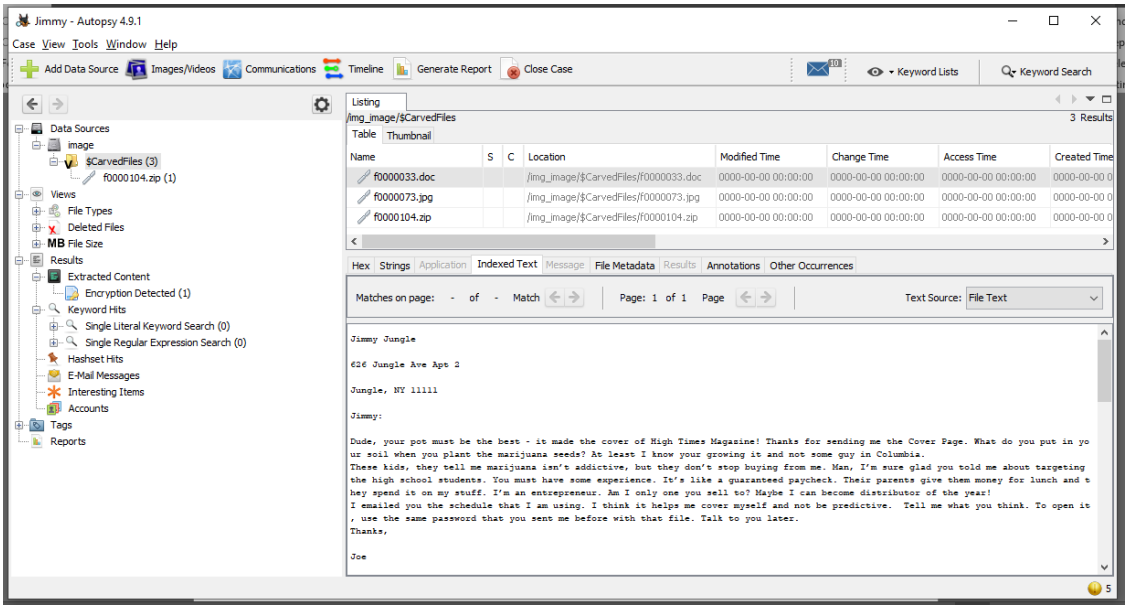
Nama : Rizki Pratama Putra

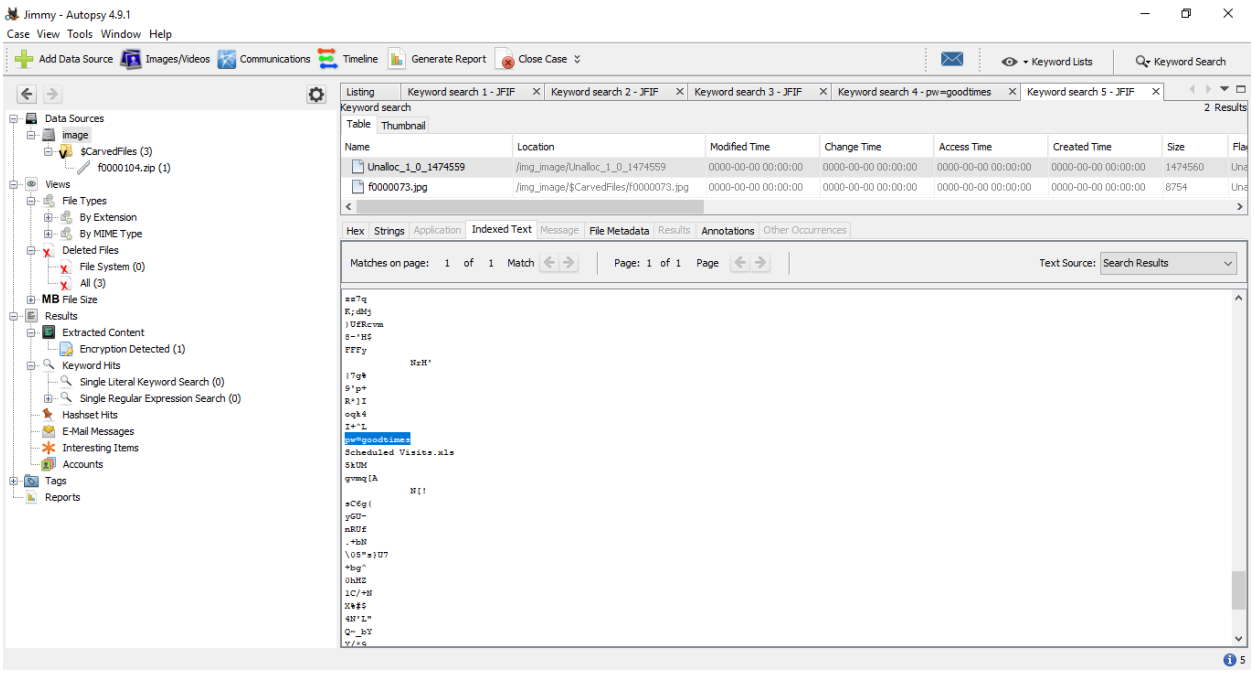
NIM : 09021281520094

KOMPUTER FORENSIK

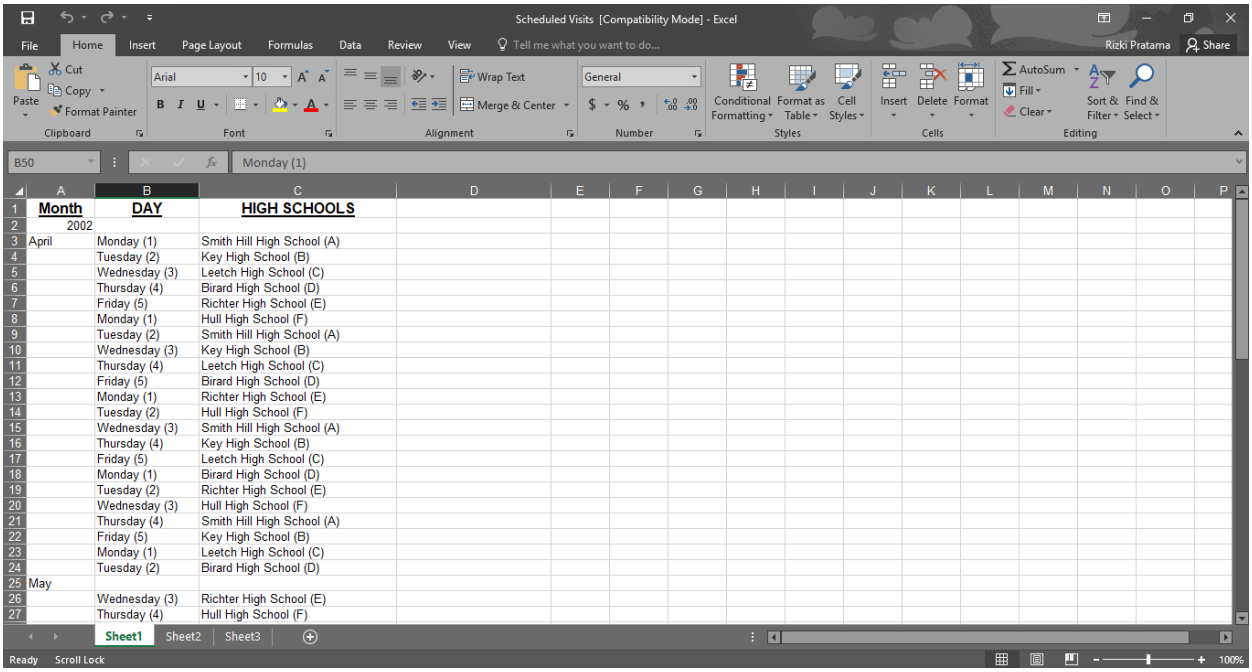
b. Who is Joe Jacob's Supplier of marijuana and what is the address listed for the supplier?
Answer:
Berdasarkan f0000033.doc, supplier dan alamatnya adalah Jimmy Jungle alamat 626 Jungle Ave, Apt 2. Jungle, NY 11111



c. What crucial data is available within the coverpage.jpg file and why is this data crucial?
Answer:
Ditemukan string "pw=goodtimes" yang nantinya akan menjadi password untuk membuka file f00000104.zip



d. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?
Answer:
Dari file f00000104.zip terdapat sebuah file excel yang mencantumkan tanggal kunjungan ke beberapa sekolah berikut :
Key High School, Leetch High School, Birard High School, Richter 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. For each file, what processes were taken by the suspect to mask them from others?
   Answer:
   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. What processes did you (the investigator) use to successfully examine the entire contents of each file?
   Answer :
   Dengan menggunakan **Autopsy 4.9.1**, setelah memasukan file image aplikasi ini secara otomatis mendapatkan 1 file unallocated dan 1 folder yang berisi 3 file yaitu dokumen f0000033.doc, image f0000073.jpg dan sebuah file zip f0000104.zip. pada file dokumen ini investigator melihat Indexed Text yang ada didalam file tersebut yang berisi sebuah surat yang memiliki nama dan alamat yang dituju, dilihat 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.

   p.s : Dengan menggunakan **Autopsy 4.9.1** yang dilakukan oleh investigator secara keseluruhan adalah Insert File Image, Read IndexedText, Use KeywordSearch ,Extract File.

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

Answer:

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 tedapat pada gambar 3.jpg tedapat informasi mengenai kapan gambar tersebut diambil, menggunakan apa gambar tersebut diambil

Apple

iPhone 8 Plus

12.0

2018:10:11 21:50:08

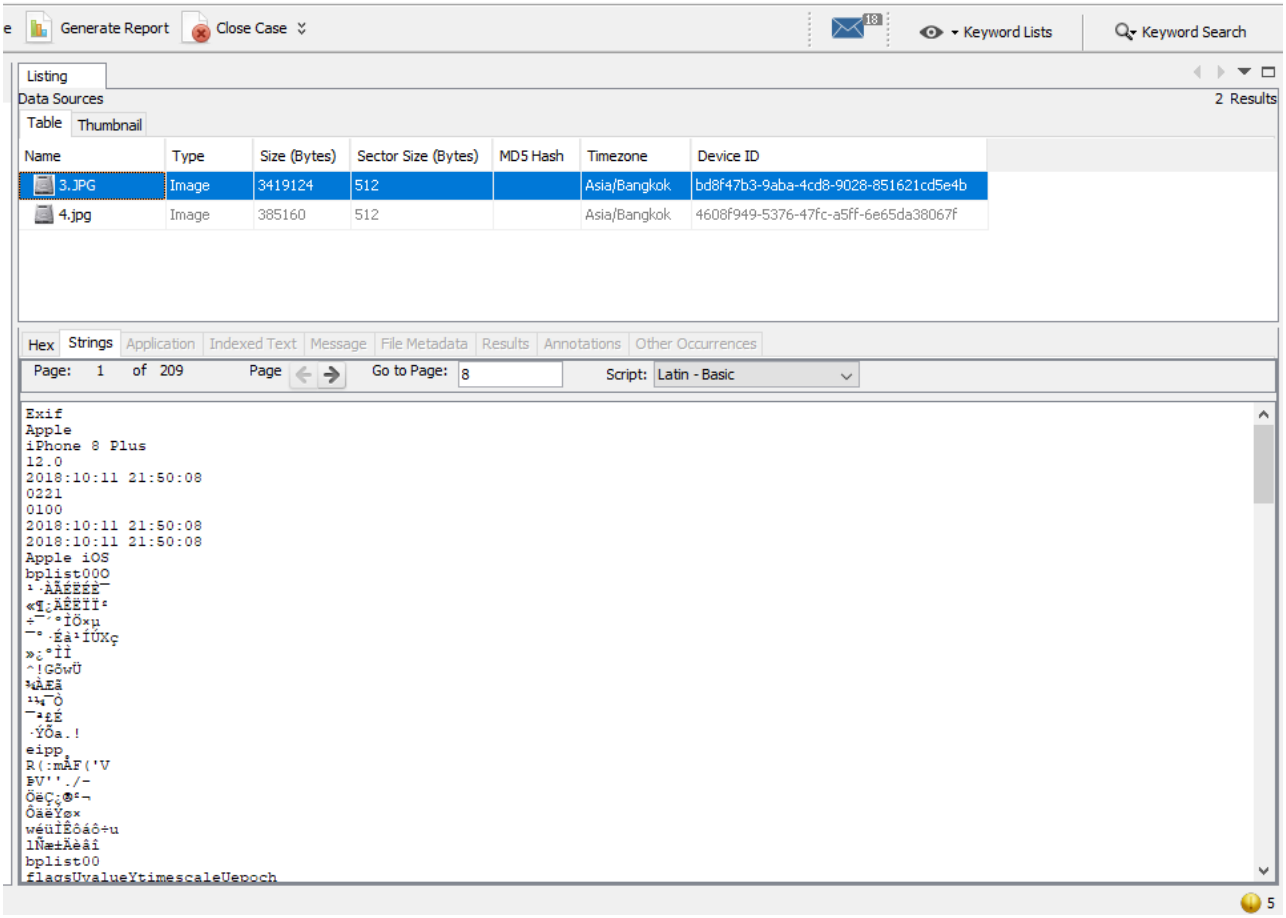
0221

0100

2018:10:11 21:50:08

2018:10:11 21:50:08

Apple iOS



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