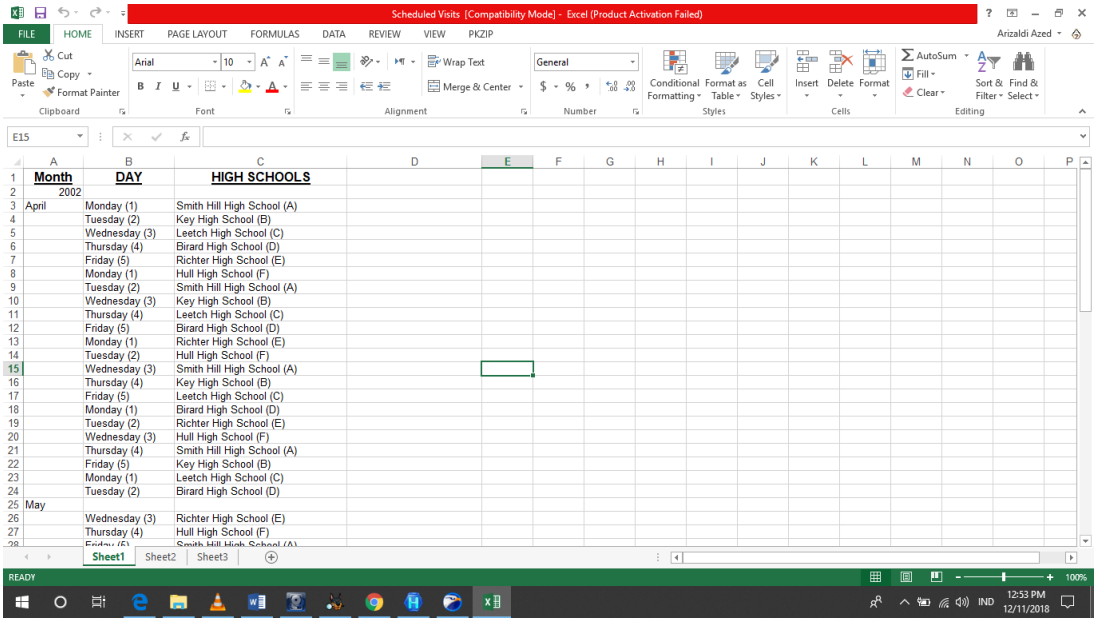
1. Analisa Forensik Image File
   a. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?
      Jimmy Jungle, 626 Jungle Ave Apt 2 Jungle NY 11111

   b. What crucial data is available within the coverpage.jpg file and why is this data crucial?
      File ini berisi kata sandi untuk membuka file sched~1.exe yang sudah dikunci didalam zip

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

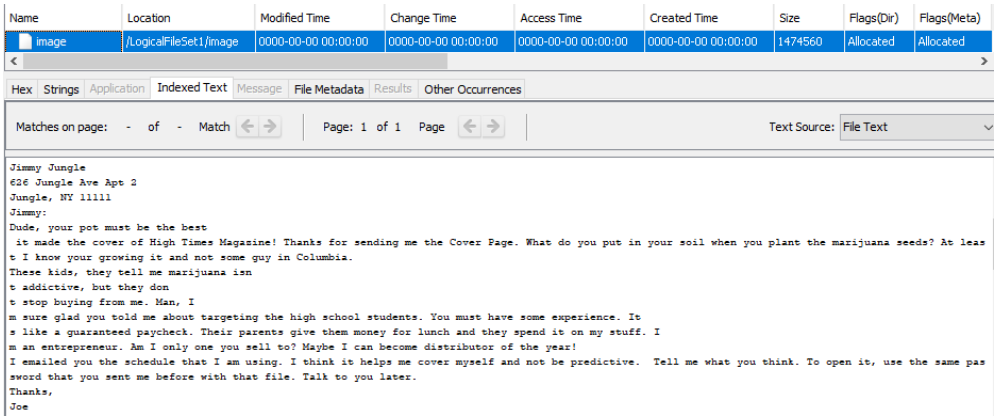


Month	DAY	HIGH SCHOOLS
2002		
April	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leetch High School (C)
	Thursday (4)	Birard High School (D)
	Friday (5)	Richter High School (E)
	Monday (1)	Hull High School (F)
	Tuesday (2)	Smith Hill High School (A)
	Wednesday (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)

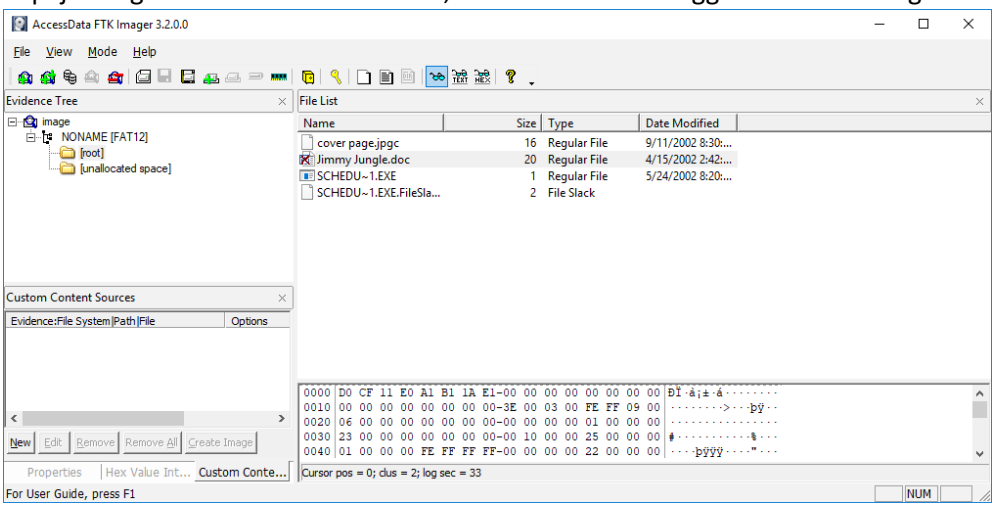
      Key High School (B)
      Leetch High School (C)
      Birard High School (D)
      Richter High School (E)
      Hull High School (F)

   d. For each file, what processes were taken by the suspect to mask them from others?
      Dalam file Jimmy Jungle.doc, Joe berbicara tentang dua file yang sudah ditukar dengan Jimmy
      Jadi urutan waktu file yang benar adalah
      -. cover page.jpgc
      -. sched~1.exe
      -. Jimmy Jungle.doc

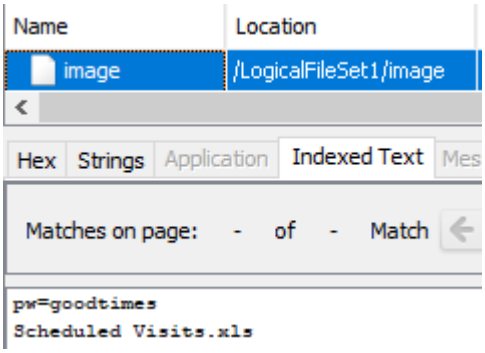
   e. What processes did you (the investigator) use to successfully examine the entire contents of each file
      Didalam image.file yang dibuka menggunakan Autopsy Tools, terdapat beberapa keterangan tanpa harus membuka atau merecovery file tersebut, diantaranya terdapat isi file Jimmy Jungle.doc dan juga password untuk membuka file excel yang berisi Schedule Visit.



Tapi jika ingin memerika file tersebut, bisa di recover menggunakan FTK Imager Tools

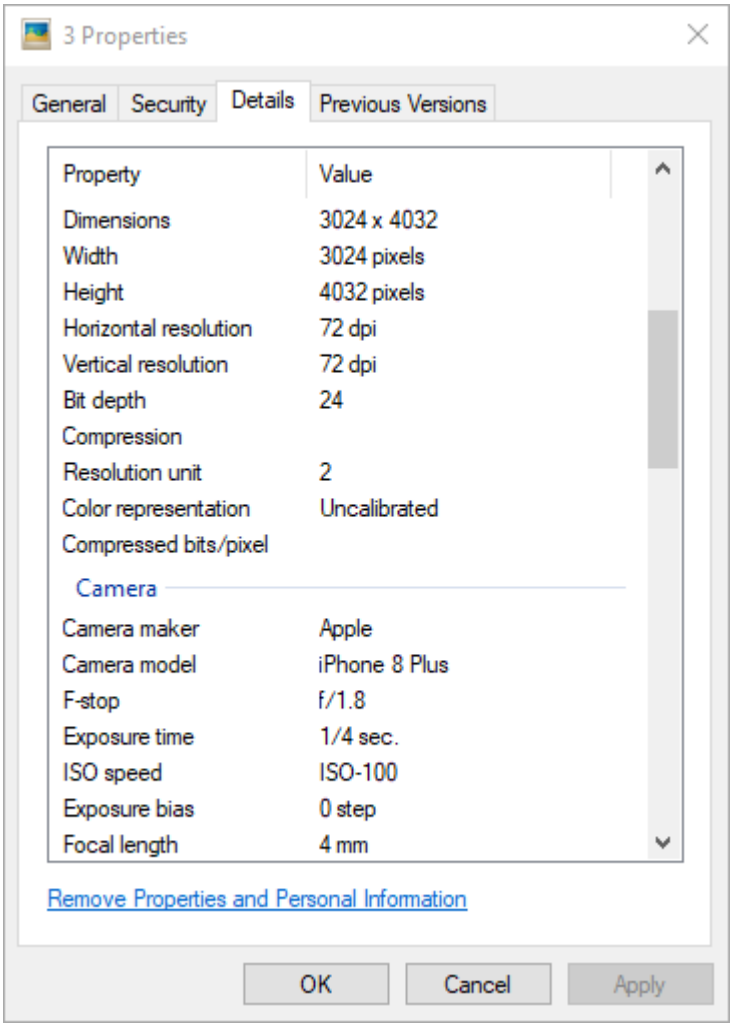


Untuk mendapatkan file .excel dari file SCHEDU~1.EXE, buka file tersebut menggunakan hexworkshop tools. Dalam file tersebut terdapat PK pada awalan string yang menandakan bahwa file tersebut berformat .zip. selanjutnya save as file tersebut dengan ekstensi .zip. didalam file .zip tersebut membutuhkan password untuk membuka file Schedule Visit.xlsx. Password yang dibutuhkan bisa didapatkan dengan cara yang mudah tanpa harus recover file cover page.jpgc karena passwordnya bisa dilihat didalam index text image.file dengan menggunakan Autopsy Tools

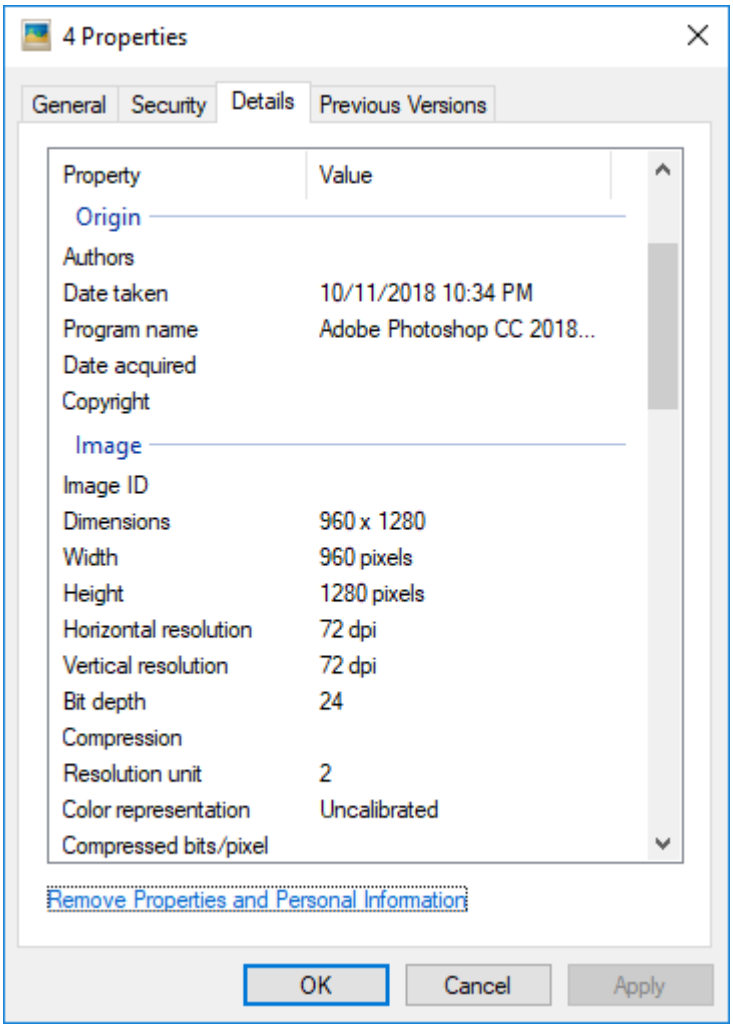


Setelah dibuka dengan menggunakan password “goodtimes”, voila kita dapat jadwal kunjungannya (jawaban nomor 1c)

2. Analisa Forensik Foto



Metadata Foto 3.JPG



Metada Foto 4.JPG

Dilihat dari bentuk kedua foto, jelas terlihat perbedaan signifikan, yaitu terdapat hal yang hilang pada file 4.jpg. Dilihat keterangan foto, tanpa menggunakan forensic tools, terdapat perbedaan diantara kedua foto, foto pada file 3.jpg diambil menggunakan perangkat Apple iPhone 8 Plus, dengan ukuran 3024 x 4032 pixels. Sedangkan file 4.jpg keterangan perangkat pengambil foto sudah hilang, berubah menjadi Adobe Photoshop CC 2018, pada sistem operasi Windows.

Kesimpulan yang didapat adalah file 3.jpg merupakan file asli, sedangkan file 4.jpg adalah palsu atau sudah dirubah dari bentuk aslinya.