Arfah Anggraina
09021281520140

1. Analisis 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!

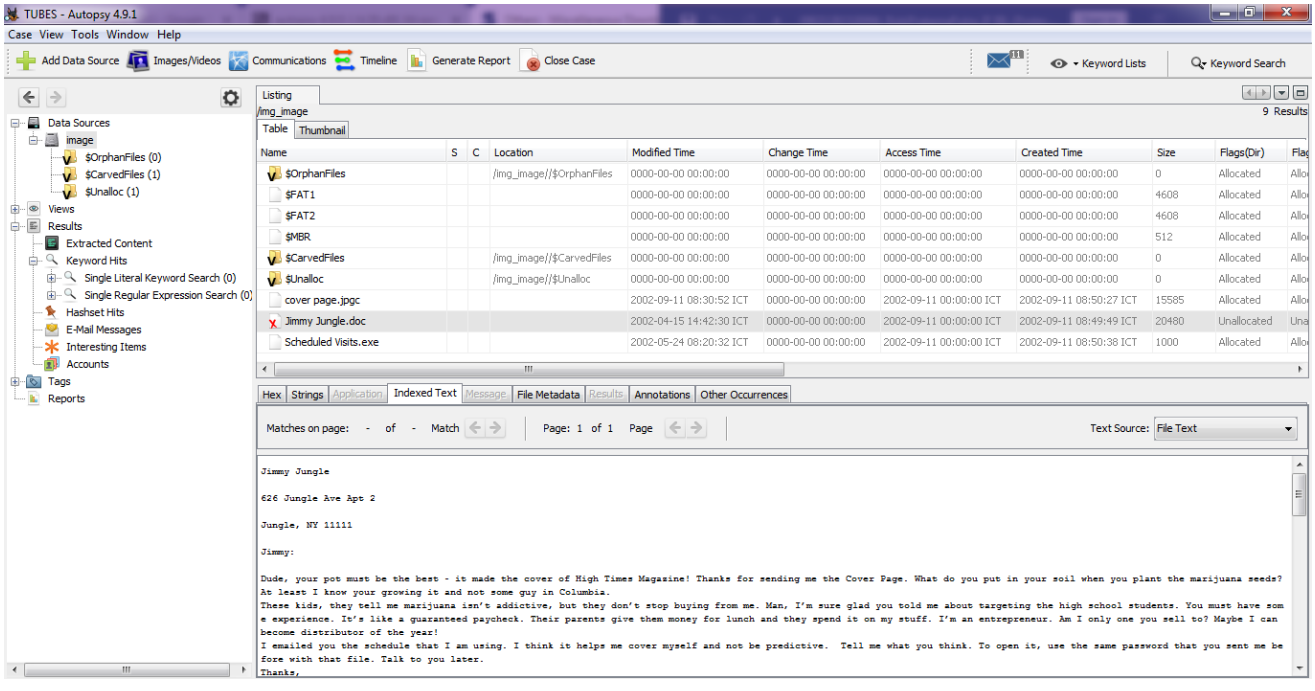
Any names, locations, and situations presented are completely made up. Any resemblance to any name, locations and/or situation is purely coincidence.

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

   Jawab:

   Supplier dari Joe Jacob adalah Jimmy Jungle dan alamatnya 626 Jungle Ave, Apt 2. Jungle, NY 11111

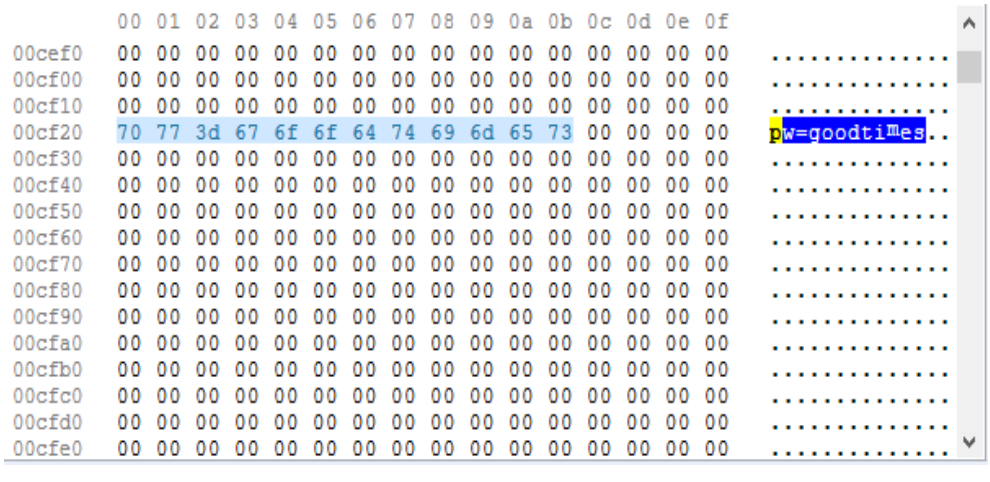
Arfah Anggraina
09021281520140



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

Jawab:

Data itu penting karena setelah dianalisis terdapat sting "pw=goodtimes" yang berguna untuk membuka file Scheduled Visits.exe dimana file Scheduled Visits.exe akan diubah jadi file Scheduled Visits.zip



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

Jawab:

Setelah dianalisis dan file Scheduled Visits.exe diubah menjadi Scheduled Visits.zip, terdapat file Scheduled Visits.xls yang berisikan jadwal kunjungan Jae Jacob ke beberapa sekolah, seperti Key High School, Leetch High School, Birard High School, Richter High School, Hull High School.

Arfah Anggraina
09021281520140

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?

Jawab:

- File cover page.jpgc telah dimanipulasi sehingga upaya untuk menganalisis file ini akan menmapilkan byte yang disetel ke “F6”.
- Untuk file Jimmy Jungle.doc telah dihapus.
- Untuk file Scheduled Visits.exe sebenarnya jenis file .zip yang telah diubah sebelumnya serta file tersebut dilingungi dengan kata sandi.

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

Jawab:

Dengan menggunakan **Autopsy 4.9.1**, lakukan otopsi file image dari hasil ekstraksi image.zip menggunakan aplikasi ini. Terdapat 3 file yang dicurigai yaitu file cover page.jpgc, Jimmy Jungle.doc dan Scheduled Visits.exe. Untuk file Jimmy Jungle.doc, diklakukan ekstraksi file sehingga terdapat isi pesan yang ditujukan kepada Jimmy Jungle oleh Joe Jacob. Kemudian analisis berikutnya yaitu file cover page.jpgc yang hex valuenya sudah di manipulasi. Setelah dianalisis file file cover page.jpgc ini, terdapat string ”pw=goodtimes”. Kemudian analisis terakhir dilakukan pada file Scheduled Visits.exe. Hasil analisisnya, file tersebut ternyata file yang berformat .zip yang apabila diekstrak akan diminta password. Password yang digunakan yaitu password yang telah ditemukan pada hasil analisis dari file cover page.jpgc. Setelah file Scheduled Visits.zip berhasil di ekstraksi, terdapat file Scheduled Visits.xls yang berisikan jadwal dan tempat yang dikunjung.

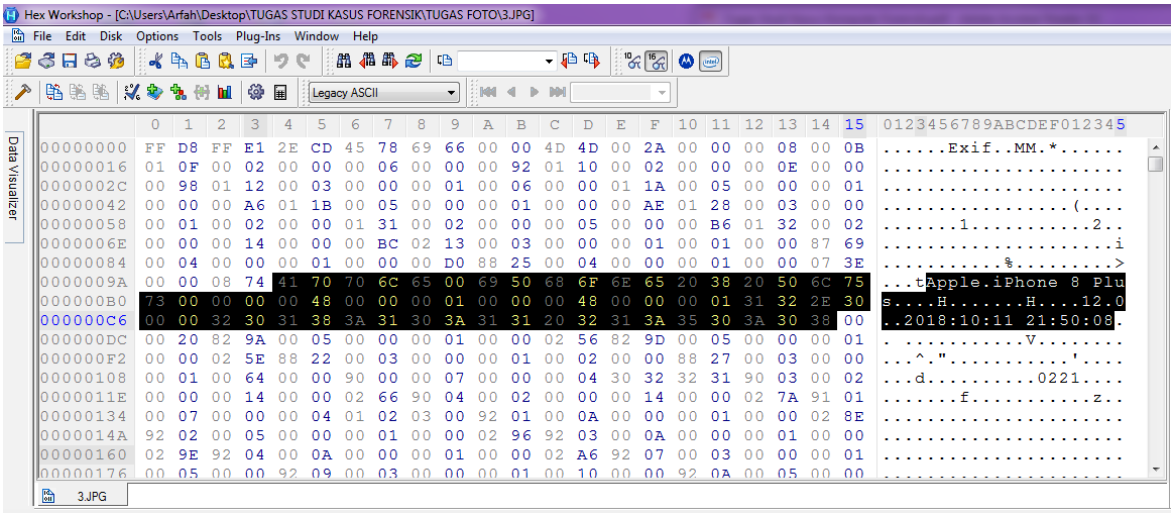
2. Analisa Forensik Gambar/Foto

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

Arfah Anggraina
09021281520140

Jawab:

Setelah dilakukan analisis pada file 3.jpg dan file 4.jpg. file 3.jpg menunjukan bahwa gambar tersebut diambil dengan menggunakan kamera **Apple iPhone 8 Plus** dan waktu pengambilan pada tanggal **11 Oktober 2012 pukul 21:50:08** sehingga file 3.jpg ini merupakan gambar **ASLI**.



Hasil analisa dari file 4.jpg menunjukkan bahwa gambar tersebut telah diubah dengan menggunakan aplikasi **Adobe Photoshop CC 2018** dan waktu diubahnya gambar ini pada tanggal **12 Oktober 2018 Pukul 18:38:36**. Serta pada tampilan gambar 4.jpg dapat dilihat perubahan yang terjadi yaitu terjadi pada nomor remote 0 tetapi telah dihapus sehingga nomor 0 sudah tidak ada dan juga perubahan yang terjadi pada kata “SONY” diganti menjadi “ONY”, sehingga gambar 4 merupakan gambar **PALSU**.