Nama : Henzo Sabiq

NiM : 09021281520111

**Tugas Forensik**

1. 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

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

Data penting yang tersimpan dalam file tersebut adalah password untuk mengakses file lain yang dicurigai, yakni Scheduled Visits.exe yang ternyata adalah file berekstensi .zip
2. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?

Berdasarkan data yang diperoleh dari file Scheduled Visits.xls, dapat diketahui bahwa Joe Jacobs rutin mengunjungi sekolah berikut :

1. Key High School
2. Leetch High School
3. Birard High School
4. Ritcher High School
5. Hull High School
3. For each file, what processes were taken by the suspect to mask them from others?

1. Jimmy Jacobs.doc – File dihapus

2. cover page.jpgc – dimanipulasi hex valuenya, setelah dipulihkan diketahui ekstensi aslinya
 (.jpg)

3. Scheduled Visits.exe – Adalah file .zip berpassword, dimana password tersebut disimpan
 didalam cover page.jpg; file .jpgc yang sudah dipulihkan

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

Langkah-langkah yang diambil.

* 1. Mengekstrak file image.zip untuk mendapatkan file image yang merupakan image file
	 yang akan dianalisa dengan Autopsy.

	 Berikut adalah hasil otopsi dari file tersebut :



* 1. Setelah diidentifikasi, ditemukan 3 buah file yang mencurigakan; cover page.jpgc , Jimmy Jungle.doc , dan Scheduled Visit.exe

	
	2. Kemudian, saya mengekstrak Jimmy Jungle.doc. Berikut adalah pesan yang saya temukan :

	
	3. Kemudian, saya mengecek file cover page.jpgc yang ternyata adalah sebuah citra digital yang hex-valuenya sudah dimanipulasi. Setelah berhasil diperbaiki, didapatlah sebuah string “pw=goodtimes” pada header citra digital yang berhasil dipulihkan. String ini tampak seperti sandi dari suatu file.
	4. Lalu, saya analisa file Scheduled Visit.exe. Setelah dicocokkan dengan header file signature di Wikipedia (<https://en.wikipedia.org/wiki/List_of_file_signatures>), saya dapat mengetahui bahwa ini aslinya merupakan file .zip berpassword yang memiliki file Scheduled Visit.xls didalamnya. Ekstensinya saya rubah, lalu saya buka dengan WinRAR.

	
	5. Setelah file berhasil dibuka, didapatlah info berupa sekolah-sekolah yang menjadi target edar narkoba.

	

	
1. Soal Foto

Lakukan analisa pada metadata gambar/foto, membandingkan yang mana asli dan yang mana palsu.

Setelah menganalisa kedua file (3.JPG dan 4.jpg), dapat diketahui bahwa file 3.JPG yang ditangkap menggunakan Apple iPhone 8+ merupakan yang asli, sementara 4.jpg sudah direkayasa menggunakan Adobe Photoshop.

Berikut merupakan header dari kedua file :




Tools yang digunakan :

1. Sistem Operasi Windows 10
2. Autopsy 4.8.0
3. HxD
4. Wikipedia