Nama : ISNAINI RIZKI ATIKA

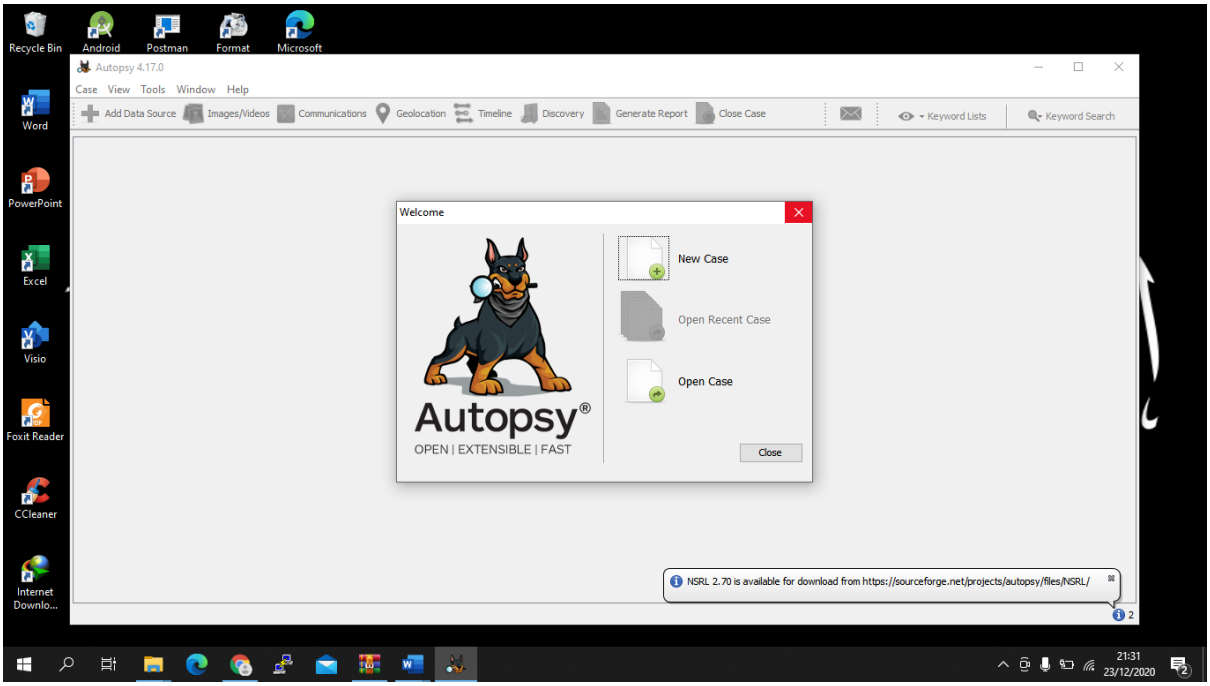
NIM :17102130

Kelas :TI2

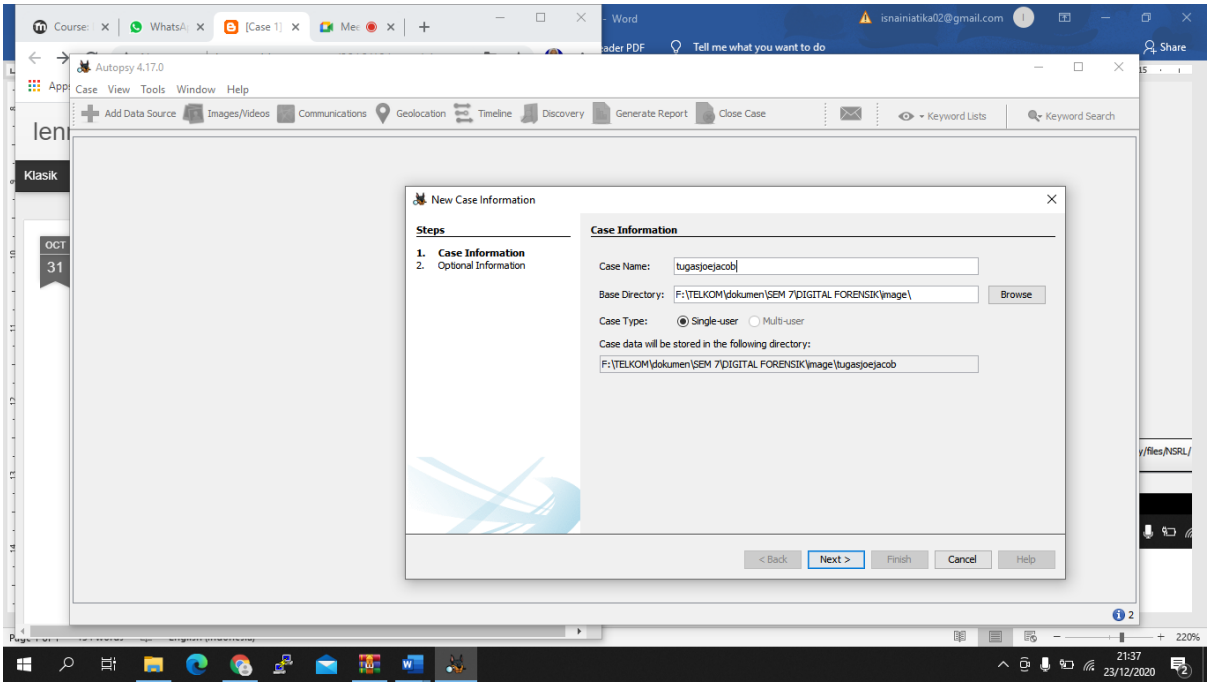
TUGAS DIGITAL FORENSIK

Untuk menggerjakan tugas ini saya menggunakan aplikasi autopsy yang saya gunakan untuk menganalissi data digital dari kasus Joe Jacob, saya juga menggunakan aplikasi NTFS Data recovery untuk menganalisis masalah dengan partisi dan file dan aplikasi bimtek untuk mencari file yang dicurigai sebagai password.

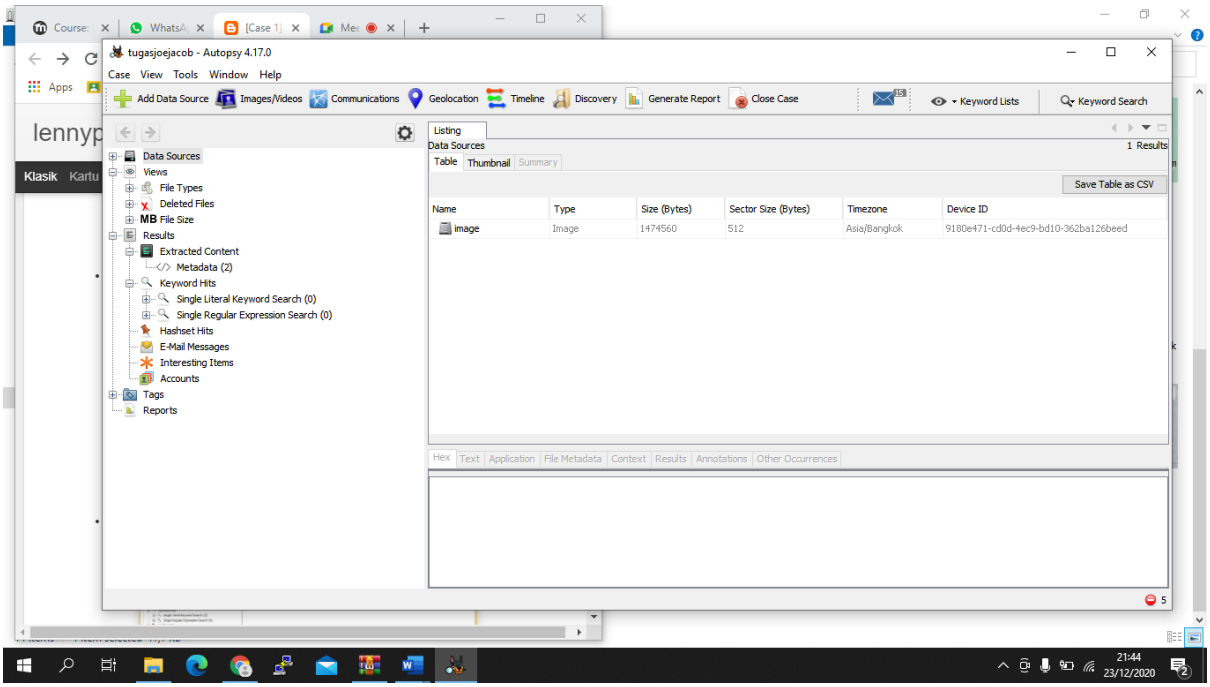
1. Langkah awal adalah menganalisis file dengan menjalankan aplikasi autopsy



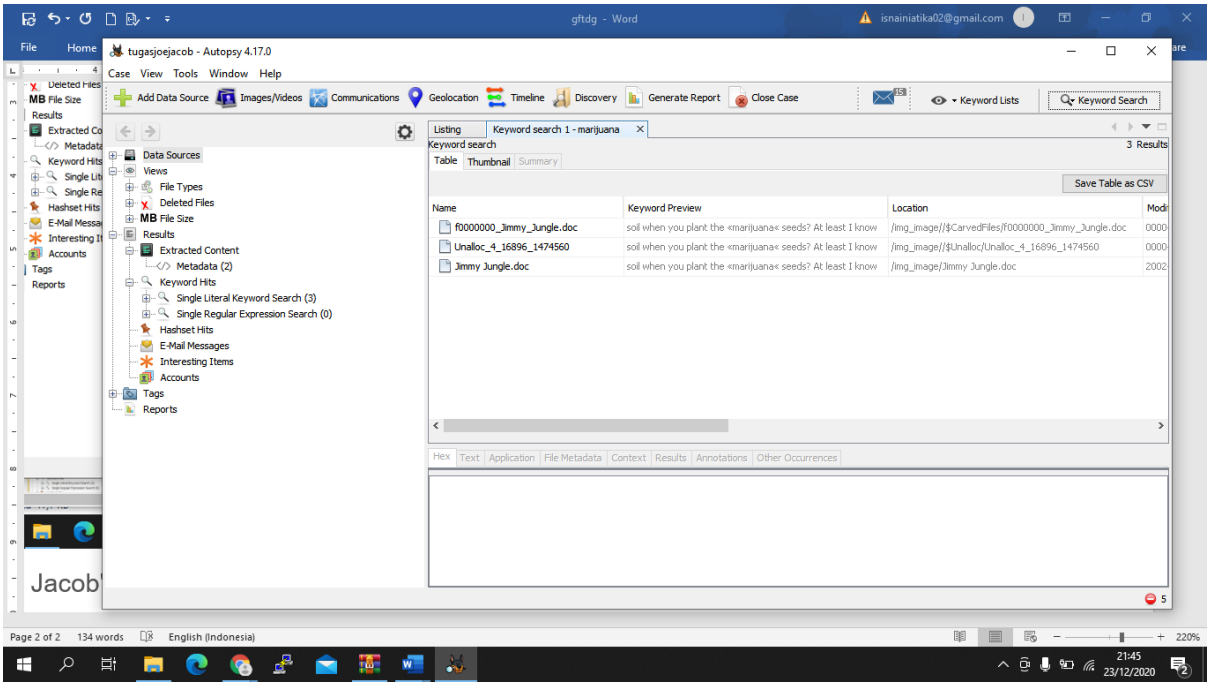
Selanjutnya buat case dan sesuaikan dengan kebutuhan.



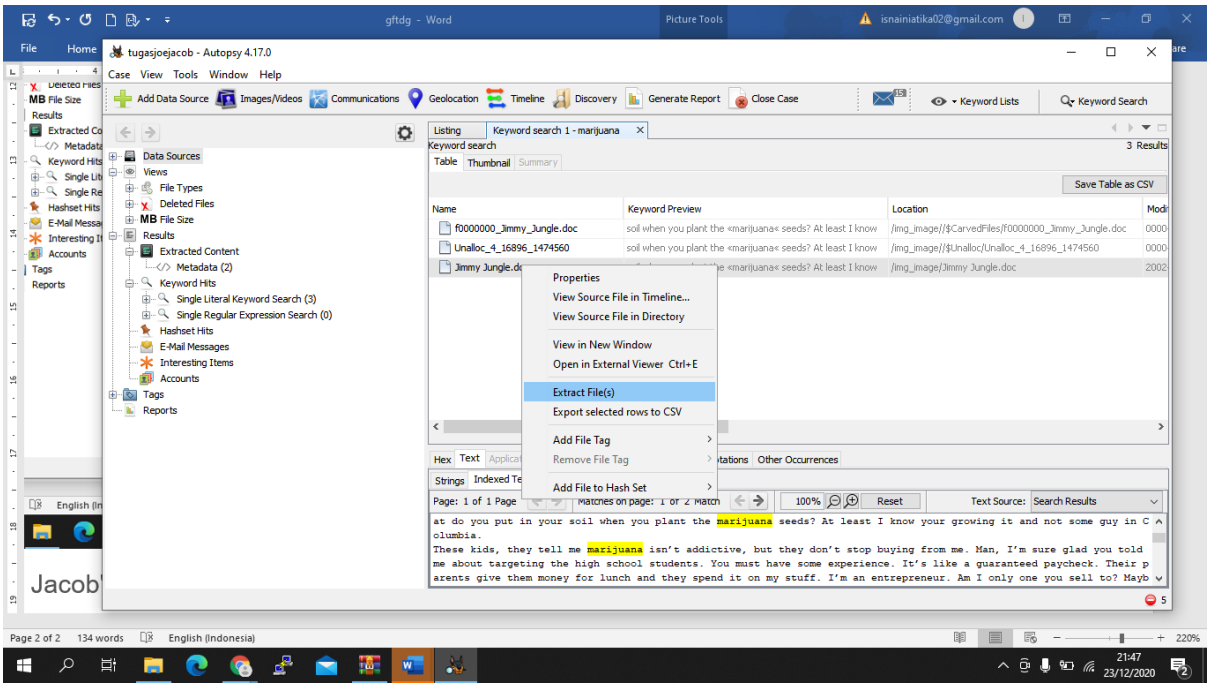
Setelah selesai, open image maka keluar tampilan seperti ini.



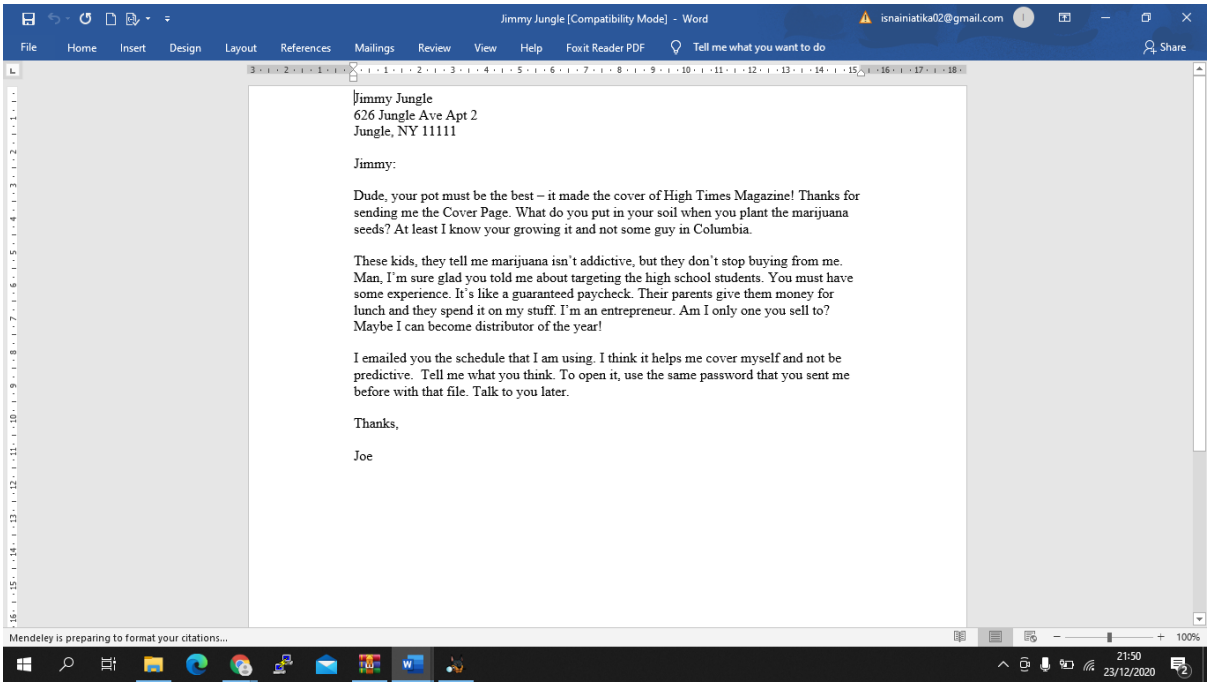
Untuk mencari jawaban nomer satu maka cari menggunakan kata kunci “marijuana”



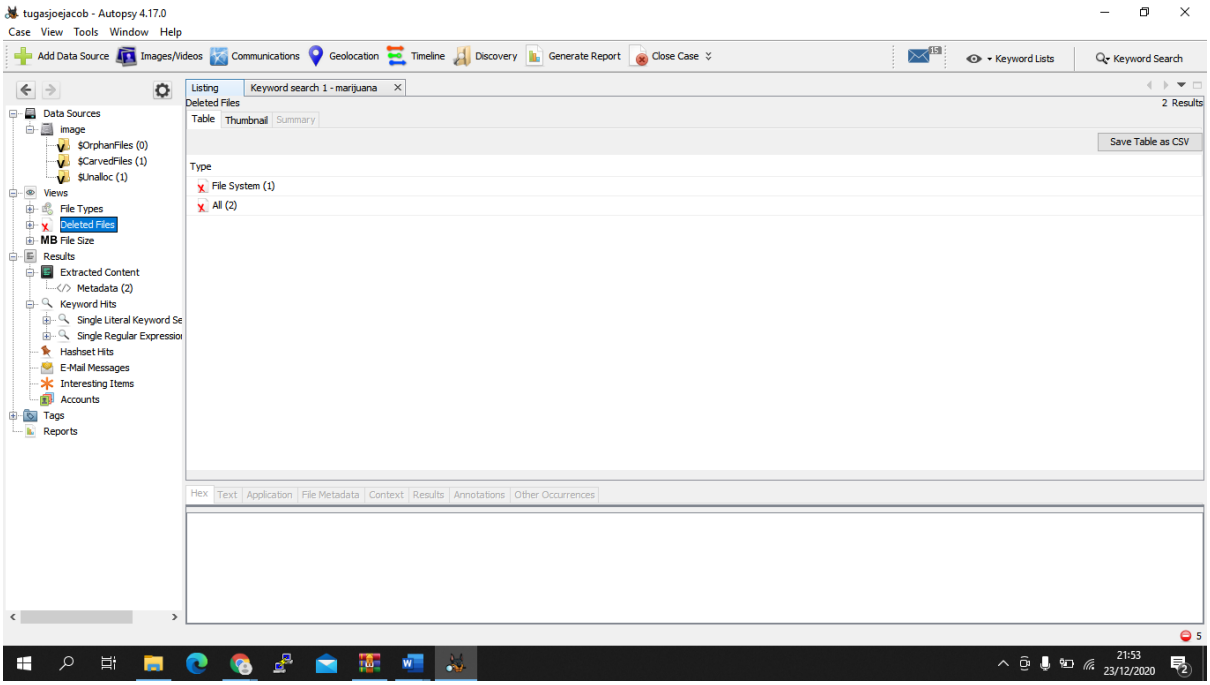
Selanjutnya jika ada file dalam bentuk word, ini di curigai terdapat berbagai informasi penting tentang kasus ini, maka eksport file word agar pelacakan lebih mudah.

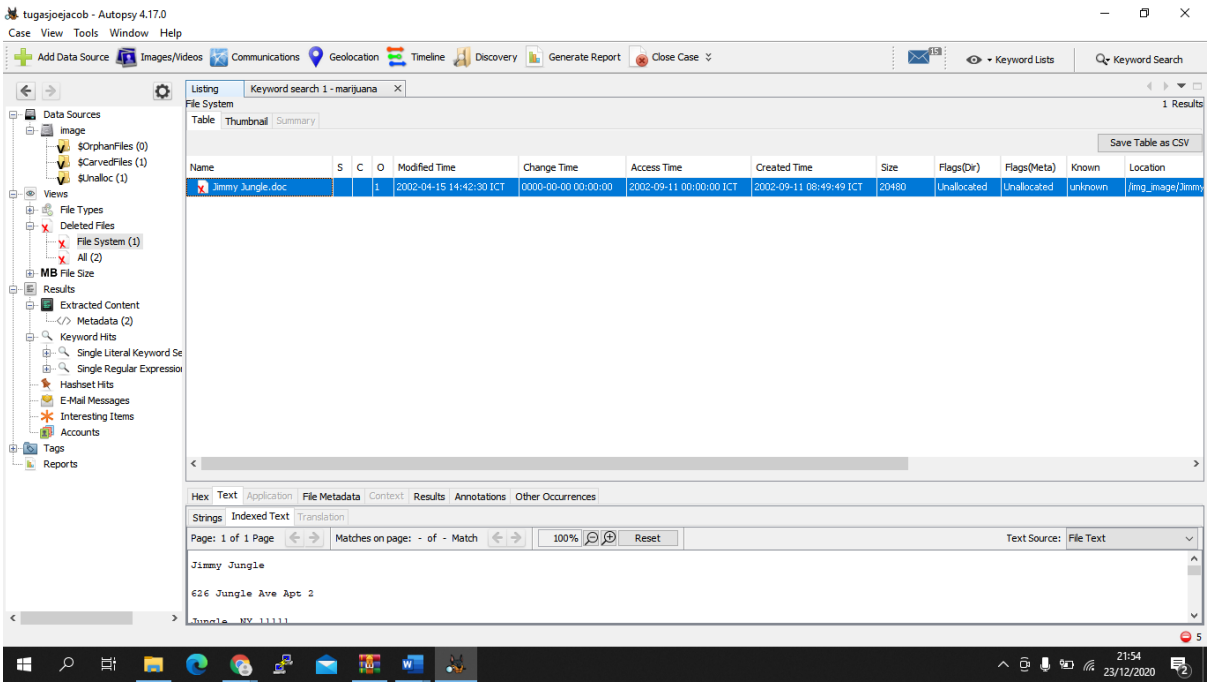


Pada dokumen berikut ini da[at diketahui bahwa Jimmy Jungle terlibat dalam kasus ini sebagai pemasok, kemungkinan menjadi distributor terbesar Joe Jacob.

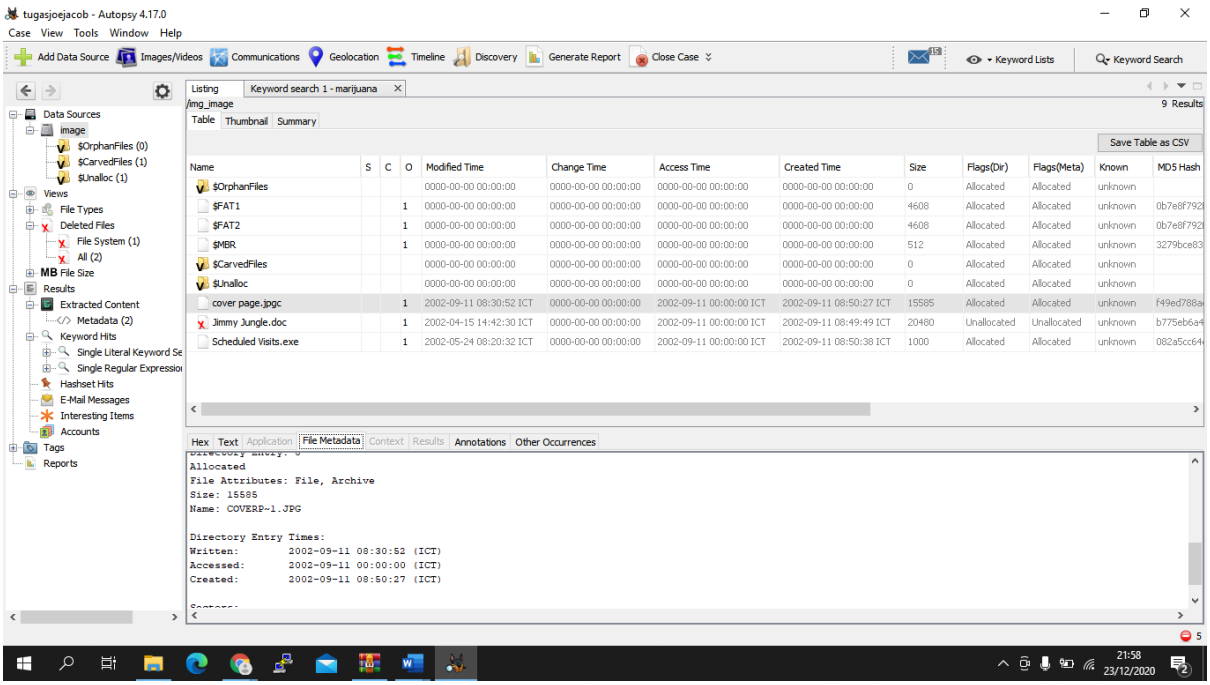


Pada file ini dapat diketahui bahwa file jimmy jungle merupakan file yang sudah di hapus.

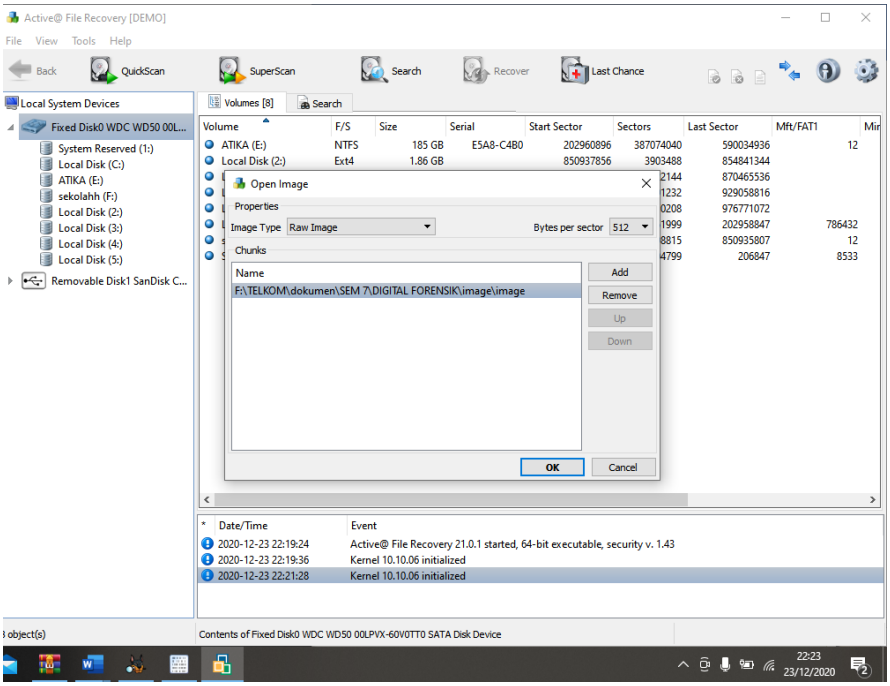




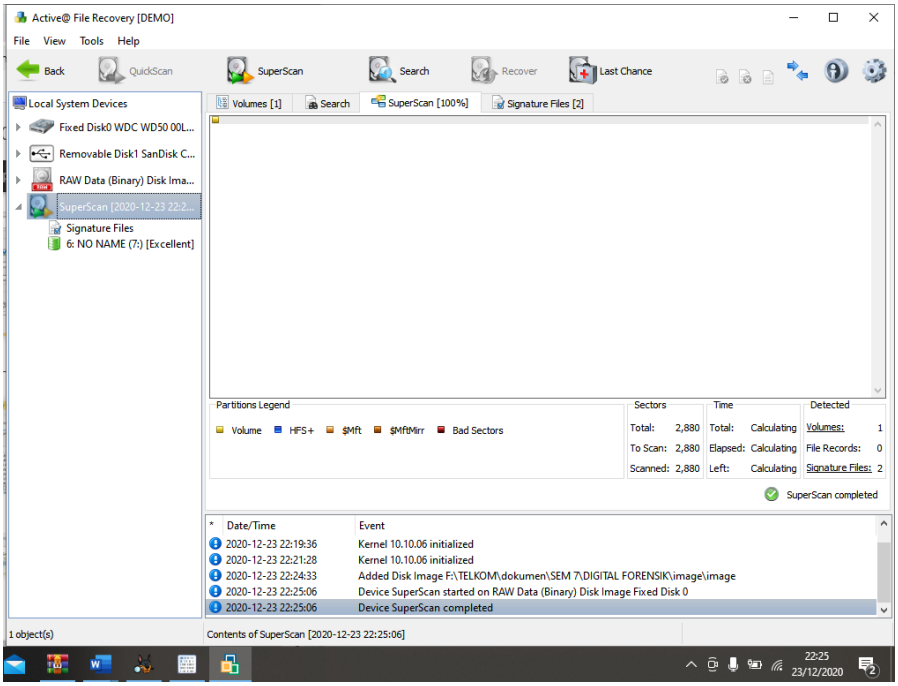
Analisis kedua adalah dengan melihat data source pada hal ini file image dilihat kembali dan mencoba melihat file cover.jpgc (file ini di duga sebenrmya berformat jpg). Ketika dilakukan pencarian, maka ditemukan metadata dari file in dan terlihat bahwa file berformat jpg.



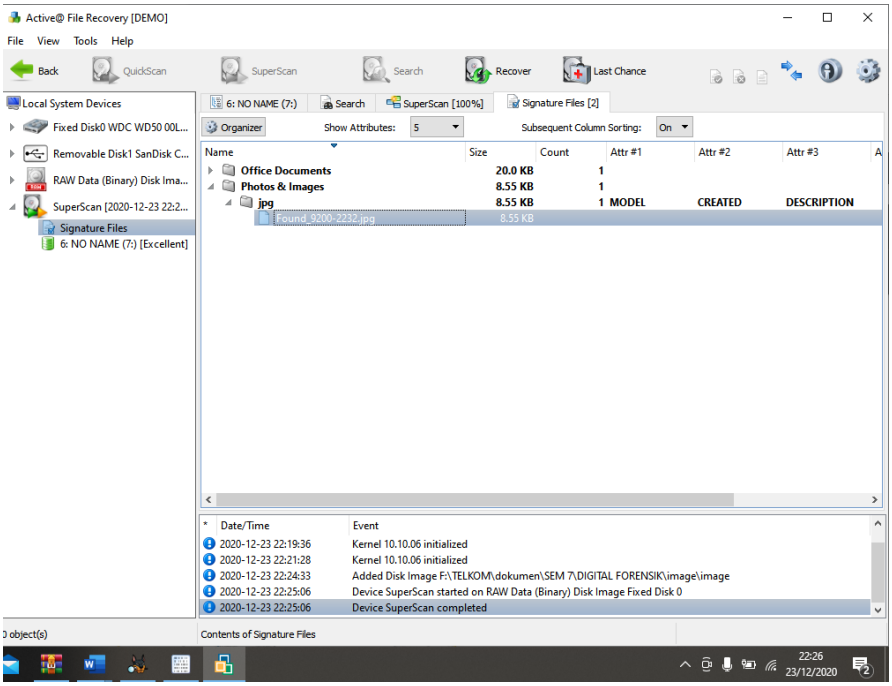
Analisis selanjutnya yaitu menggunakan software NTFS Data Recovery toolkit. Berikut merupakan tampilan open image-> dan tambahkan row image dari file image



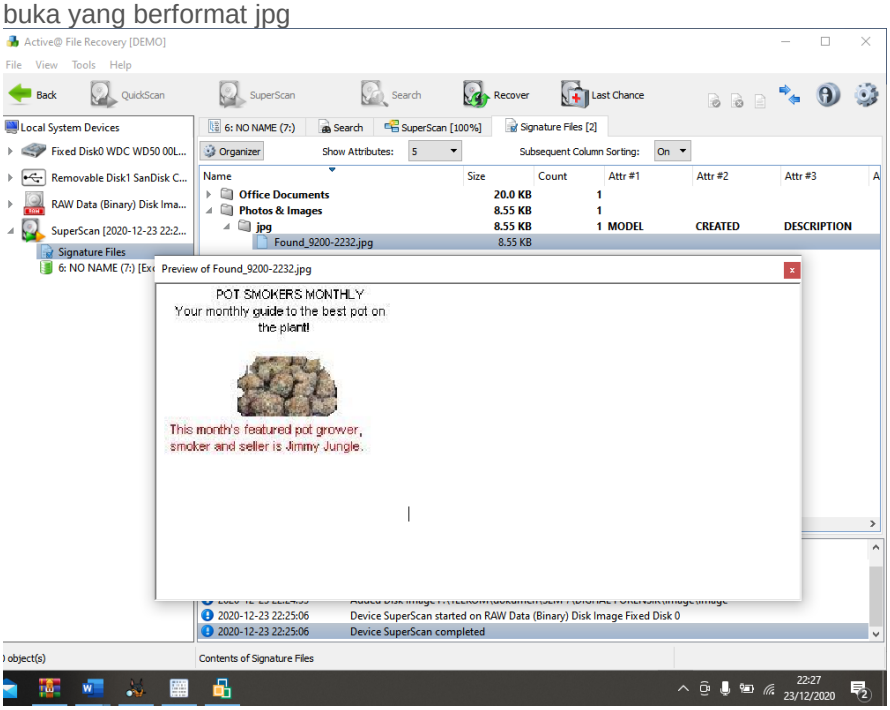
Selanjutnya klik super scan dan keluar seperti ini



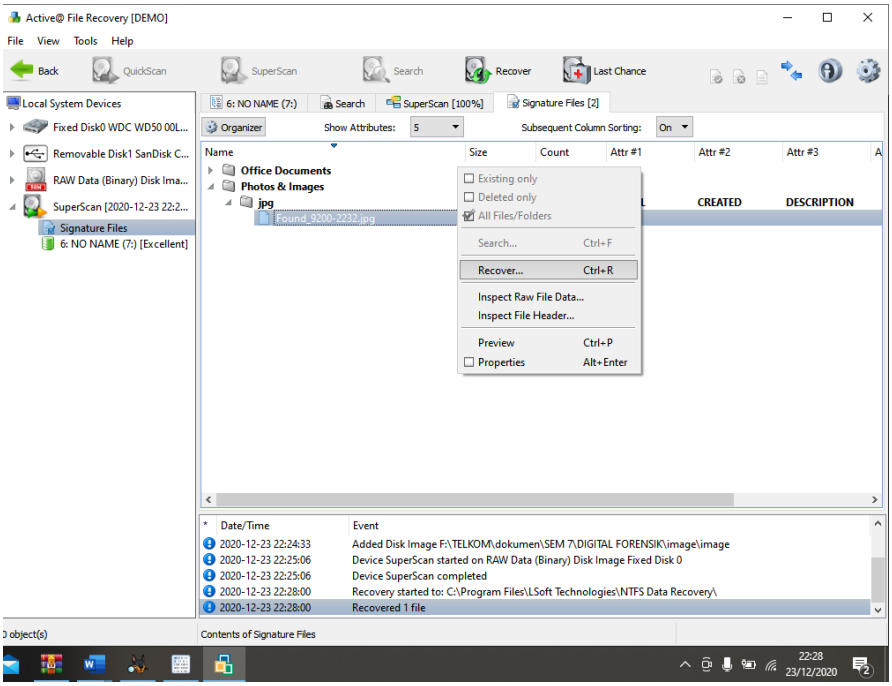
Pada bagian signature files terlihat file file yang terdapat pada image

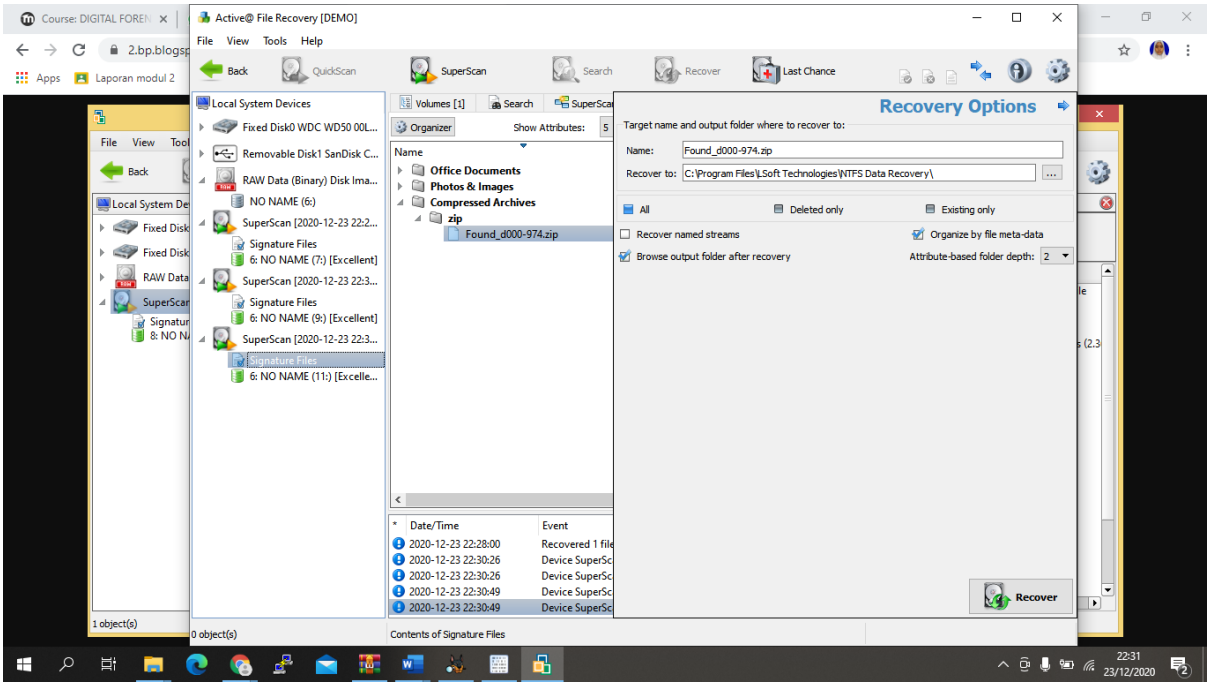


buka yang berformat jpg

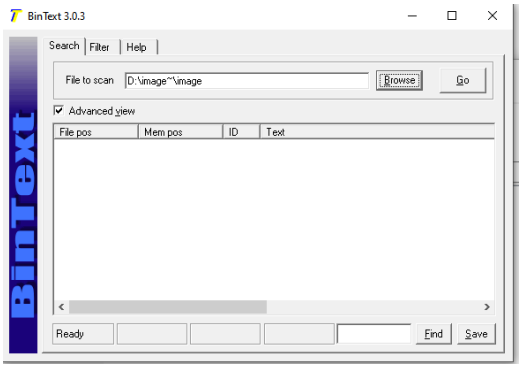


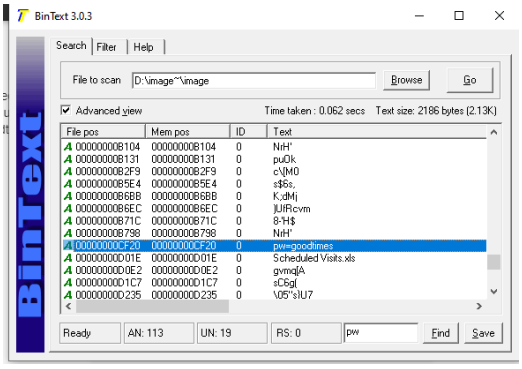
klik kanan file.jpg dan klik recover



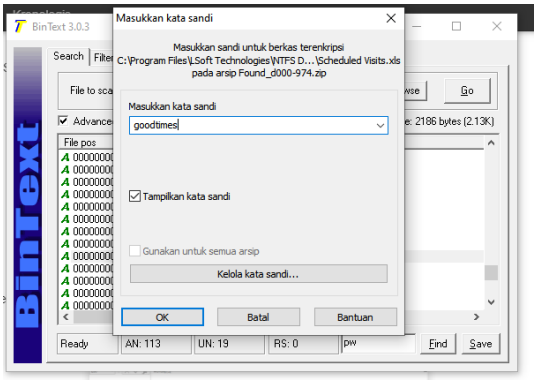


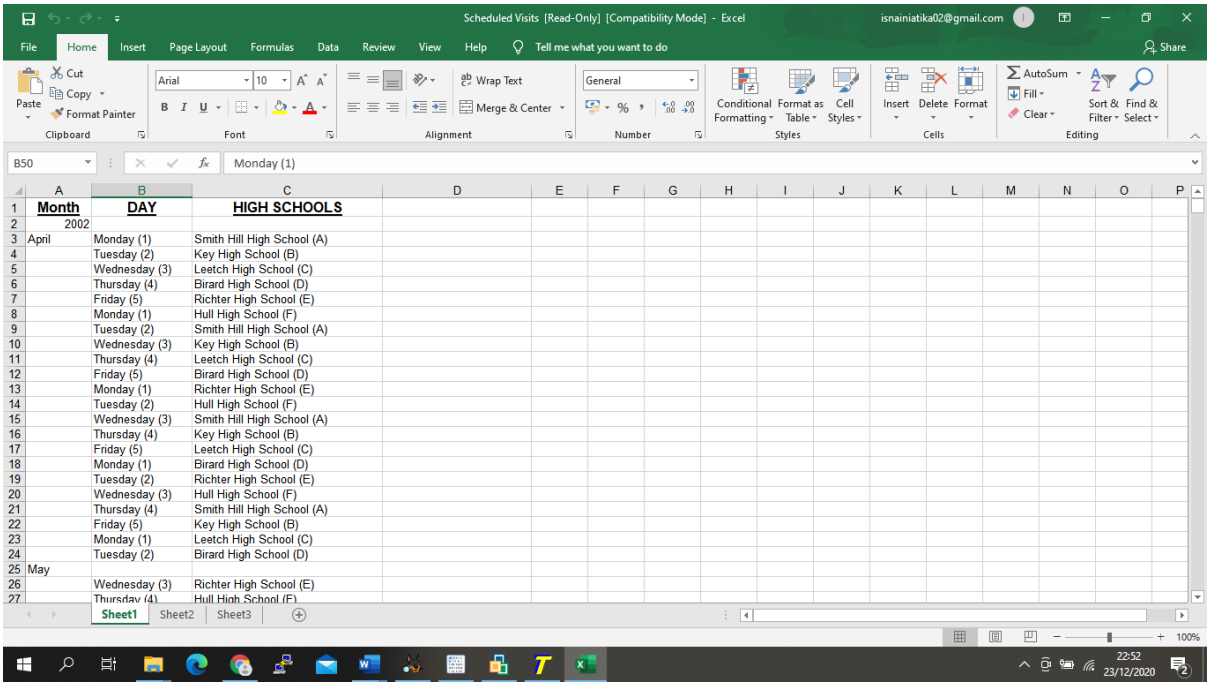
Setelah recover maka akan keluar file berbentuk zip, akan tetapi untuk membuka file.zip ini memerlukan password, untuk mencari password saya menggunakan aplikasi bintext, memasukkan image nya dan mencari kata kata yang berhubungan dengan password pada kolom pencarian dengan kata kunci “ password” ataupun “pw”. Dan keluar kata yang di curigai sebagai password.





Setelah menemukan password maka password dimasukkan dan data dapat diakses.



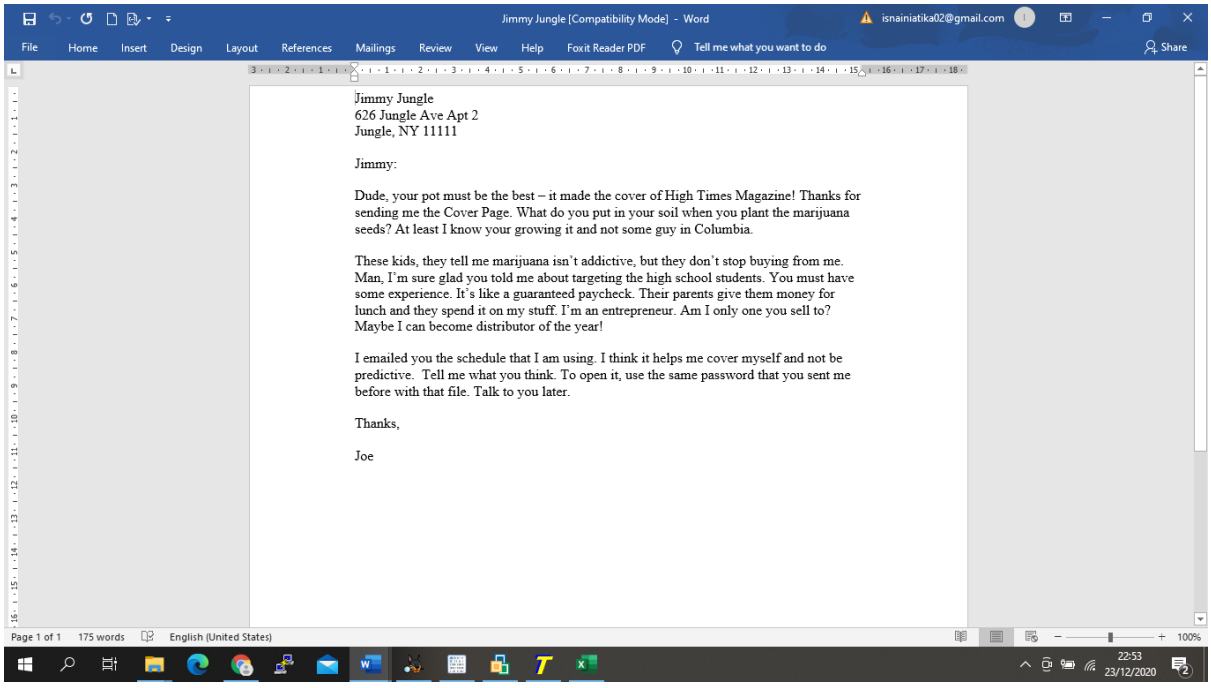


Month	DAY	HIGH SCHOOLS
2002		
April	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leetch High School (C)
	Thursday (4)	Birard High School (D)
	Friday (5)	Richter High School (E)
	Monday (1)	Hull High School (F)
	Tuesday (2)	Smith Hill High School (A)
	Wednesday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

Analisis sesuai soal

1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?
   Pemasok ganja Joe Jacob adalah Jimmy Jungle. Alamat dari Jimmy Jungle adalah di 626 Jungle Ae Apt 2, Jungle, NY 11111.

Bukti:



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.

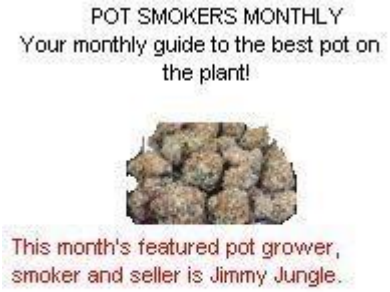
These kids, they tell me marijuana isn't addictive, but they don't stop buying from me. Man, I'm sure glad you told me about targeting the high school students. You must have some experience. It's like a guaranteed paycheck. Their parents give them money for lunch and they spend it on my stuff. I'm an entrepreneur. Am I only one you sell to? Maybe I can become distributor of the year!

I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive. Tell me what you think. To open it, use the same password that you sent me before with that file. Talk to you later.

Thanks,

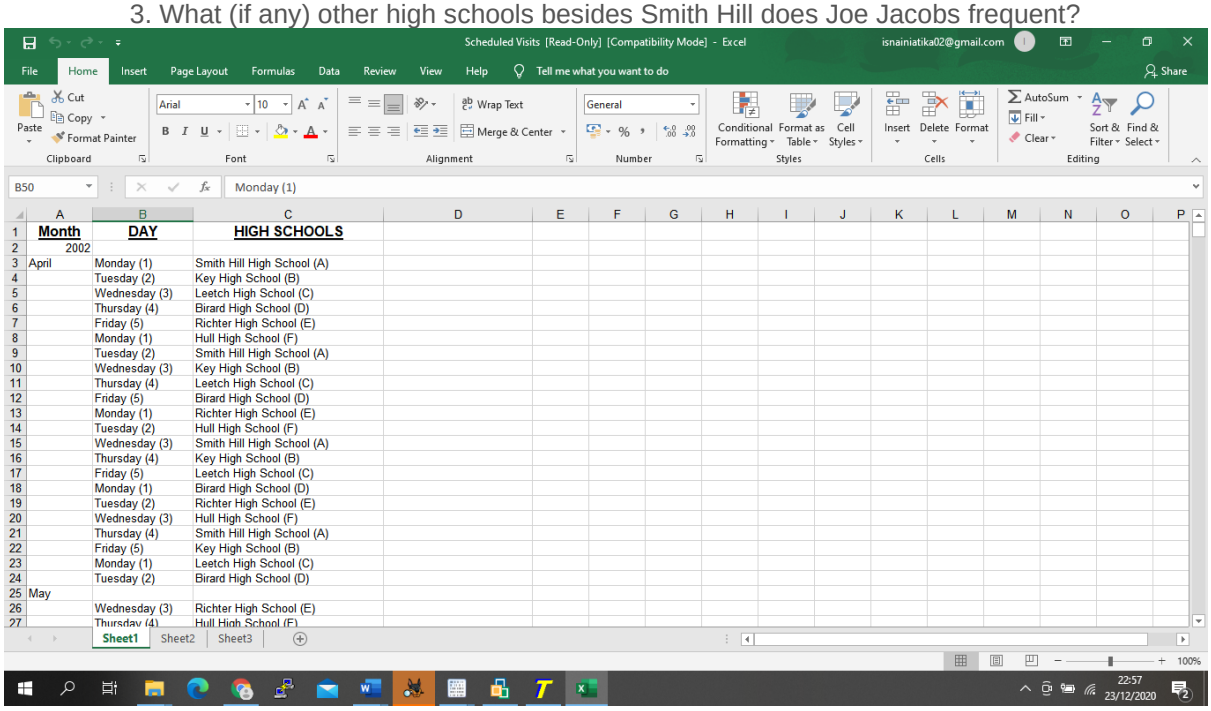
Joe

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



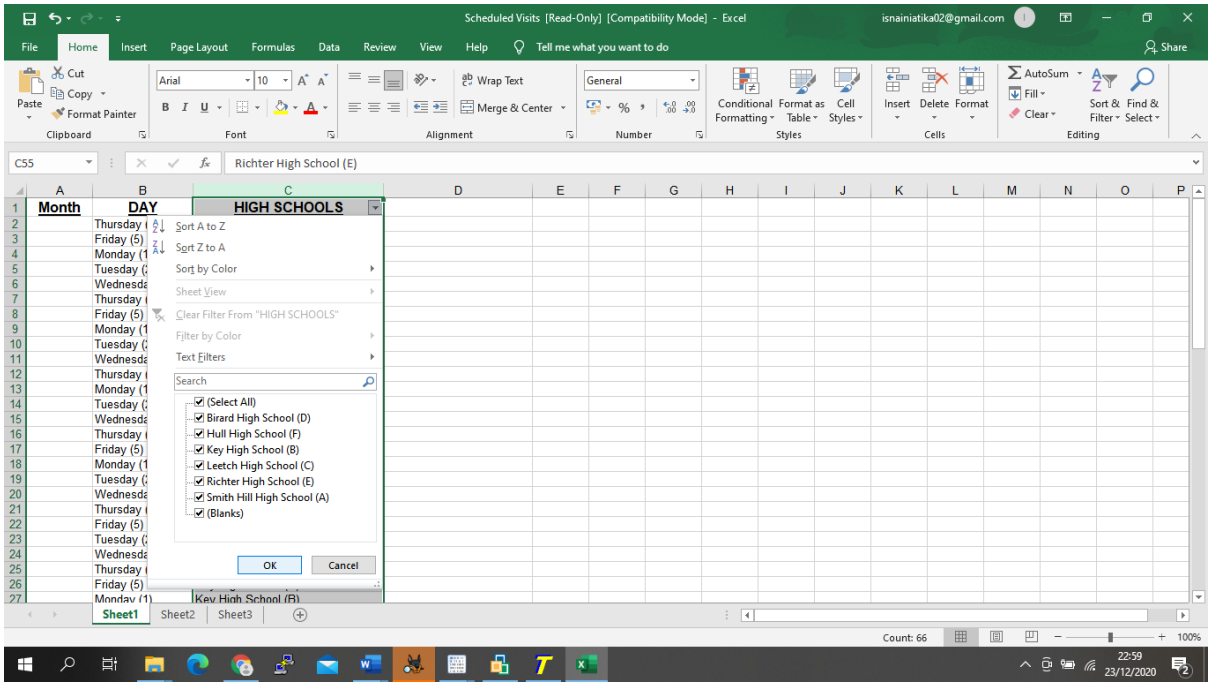
Pada *file*, diduga menggandung kata 'pw=goodtimes'. Data ini bersifat krusial karena kata 'goodtimes' merupakan *password* dari *file* ScheduleVisit.zip.

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



	A	B	C
1	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)

Hasil filter pada kolom High Schools:



Pada *file* Scheduled Visits.xls, didapatkan bahwa terdapat lima sekolah selain Smith Hill High School, yaitu:

a. Key High School (B)
b. Leetch High School (C)
c. Birard High School (D)
d. Richter High School (E)
e. Hull High School (F)

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

- Jimmy Jungle.doc – *file* dihapus tetapi tidak di-*hide* sehingga masih bisa dilihat menggunakan Autopsy
- coverpage.jpgc – nama *file* seharusnya coverpage.jpg tetapi ditulis coverpage.jpc
- Schedule.exe – ekstensi *file* ini seharusnya .zip tetapi ditulis .exe
- Scheduled Visits.xls – *file* diberi *password* dan diletakkan di *file* zip.

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

Proses telah dijelaskan pada bagian atas.