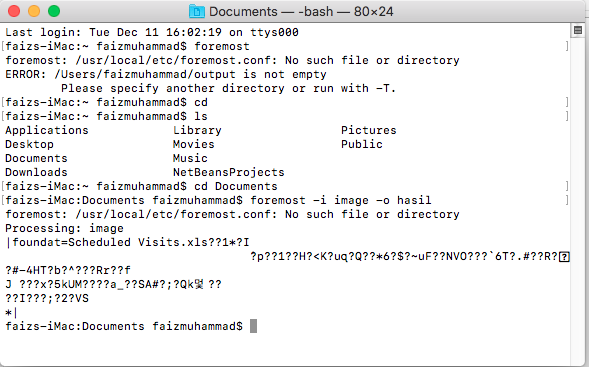
1. Kasus joe Jacob

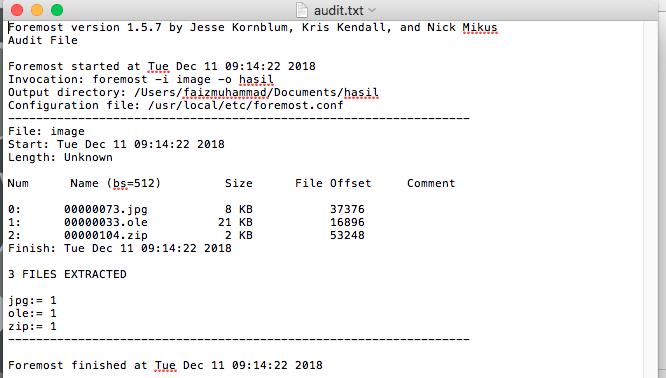
Alat yg digunakan : foremost, iHex, Autopsy

OS : MacOs High Sierra

* Gunakan foremost untuk melihat data2 dalam file image, output disimpan dalam folder “hasil”

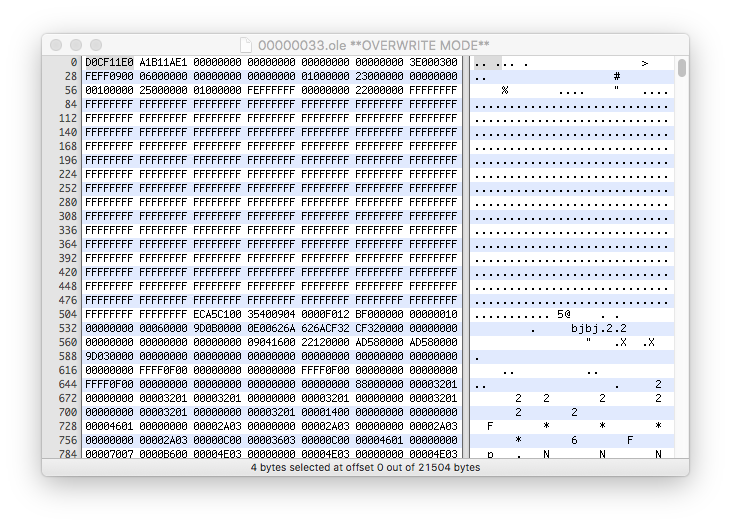


* Terdapat 3 file dalam image

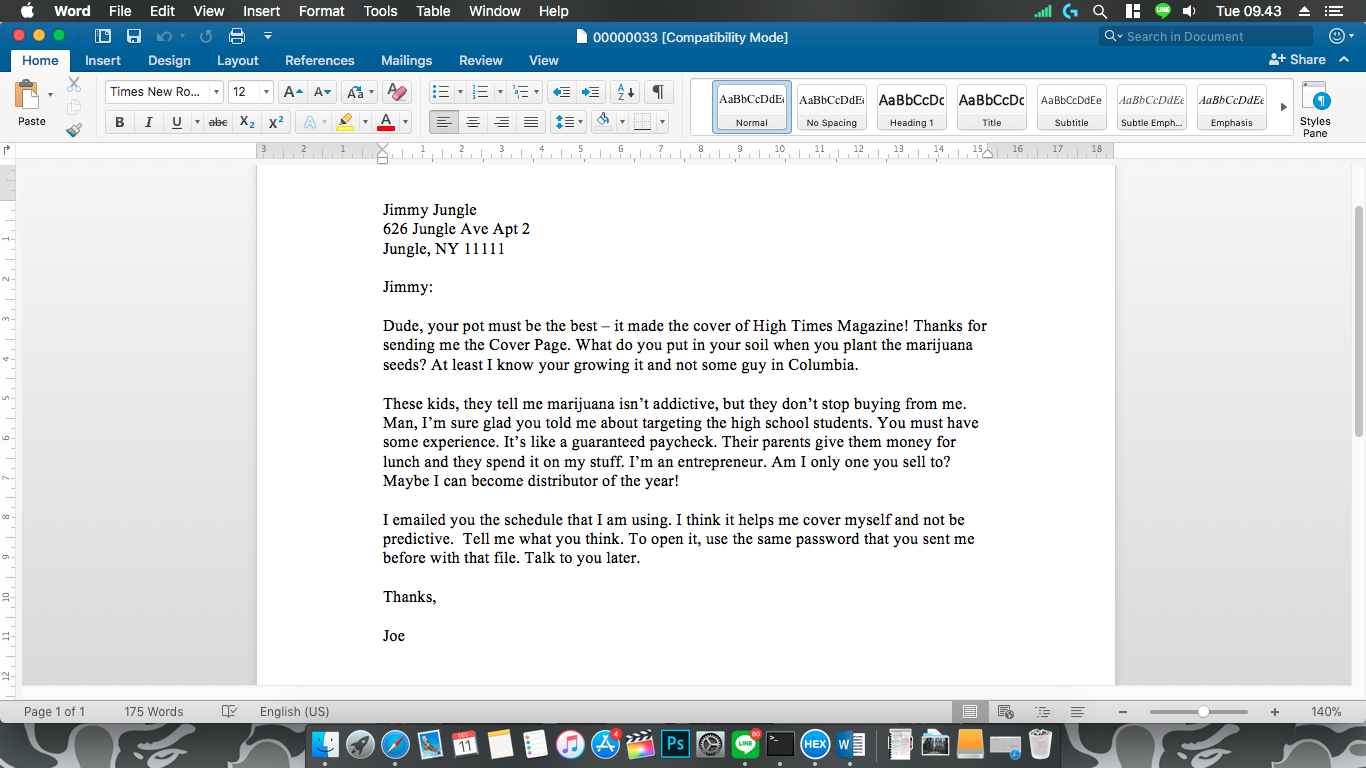


* Karena file .ole tidak tidak dapat dibuka, maka dilihat dlu

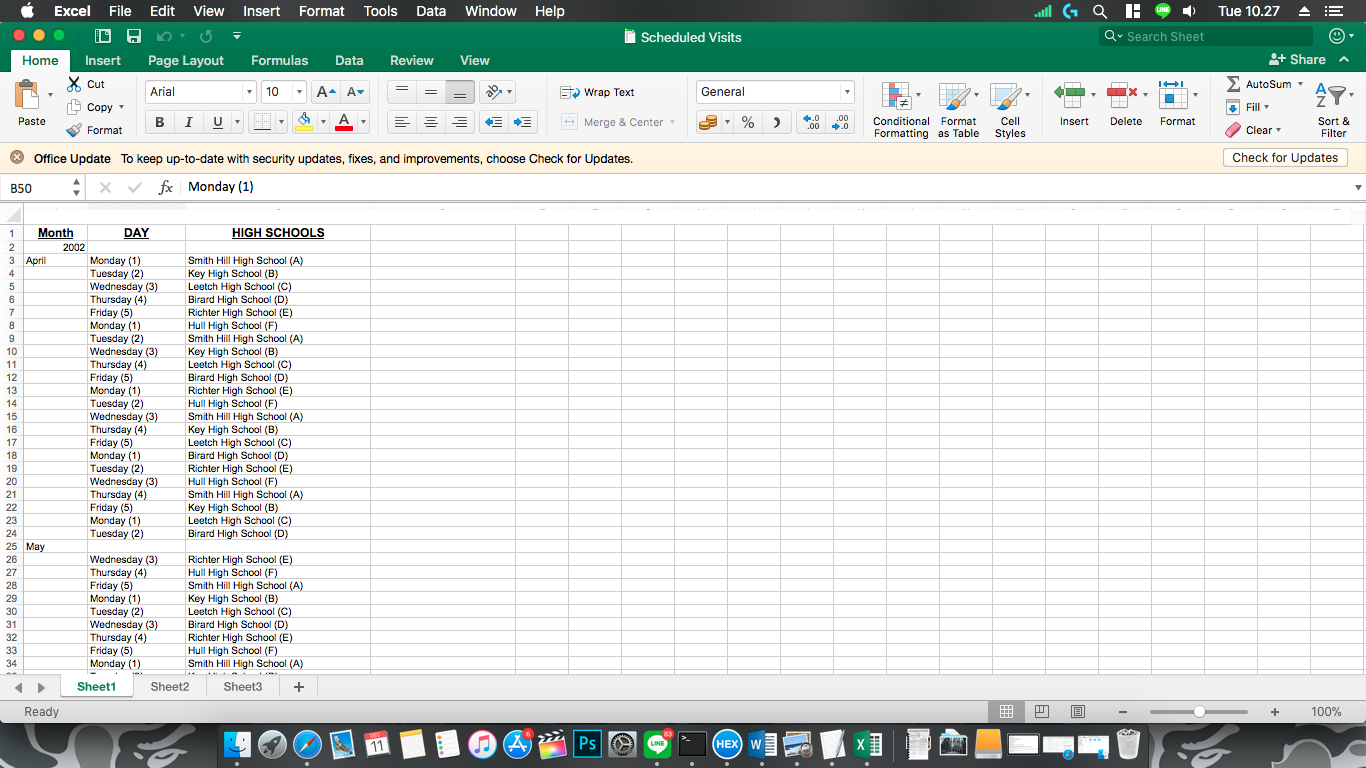
File signaturenya menggunakan iHex.



* File tersebut memiliki header untuk file office, maka dicoba untuk dibuka menngunakan word



* Terdapat pesan dari supplier joe, termasuk nama dan alamatnya.
* Selanjutnya pada cover page.jpg ketika dibuka dengan ihex terdapat “pw=goodtimes” yg kemungkinan adalah password yg disebutkan pada surat diatas.
* Selanjutnya file scheduled visit, ketika dicek signaturenya dengan ihex ternyata merupakan file zip.
* Ketika mencoba membuka file zip tsb, terdapat password, kemudian dicoba menggunakan password “goodtimes”
* Setelah dibuka, didalam file zip tsb diketahui sekolah2 lain tempat joe berjualan marijuana



soal:

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?

**Password : goodtimes, karena pass itu merupakan password untuk file zip yg berisi jadwal tempat berjualan joe**

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

**Leetch High School, Birard High School, Richter High School, Key High School, dan Hull High School**

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

**Jimmyjungle.doc -> dihapus**

**Cover page.jpgc - > sebenarnya merupakan file jpg**

**Scheduled visits.exe -> sebenarnya merupakan file zip yg dipassword yang didalamnya terdapat file xls.**

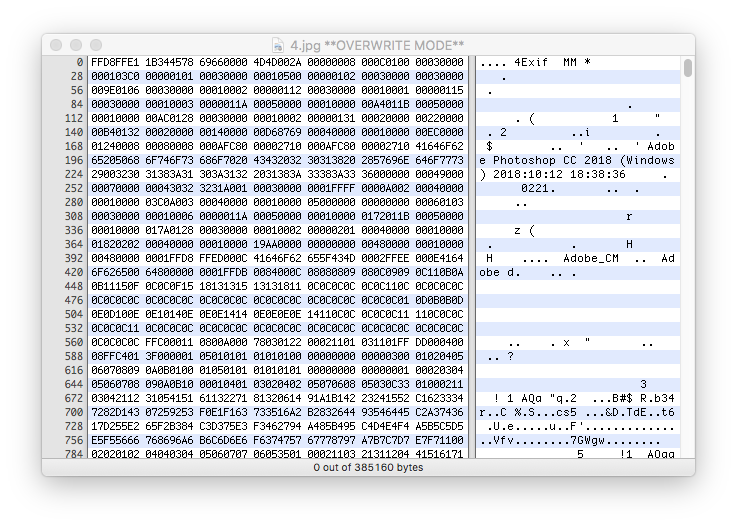
1. What processes did you (the investigator) use to successfully examine the entire contents of each file?

**Dijelaskan diatas**

1. Soal analisis foto

Alat yang digunakan : iHex

Operating system : MacOS High Sierra

Kedua file dibuka menggunakan iHex, terlihat bahwa file foto 4.jpg merupakan hasil editan dengan photoshop CC 2018 dengan operating system windowsSedangkan foto 3.jpg merupakan foto asli yang diambil menggunakan iPhone 8 plus

