TUGAS KOMPUTER FORENSIK

1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?

* Joe Jacob’s supplier : Jimmy Jungle
* Supplier address : 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 krusial yang terdapat pada coverpage.jpg adalah bukti yang menguatkan mengenai siapa supplier dari Joe Jacob, dan pada file tersebut juga terdapat sebuah password yang digunakan untuk membuka file Schedule visits.exe

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

Ada beberapa sekolah lainnya yang sering dikunjungi oleh Joe Jacob, yaitu :

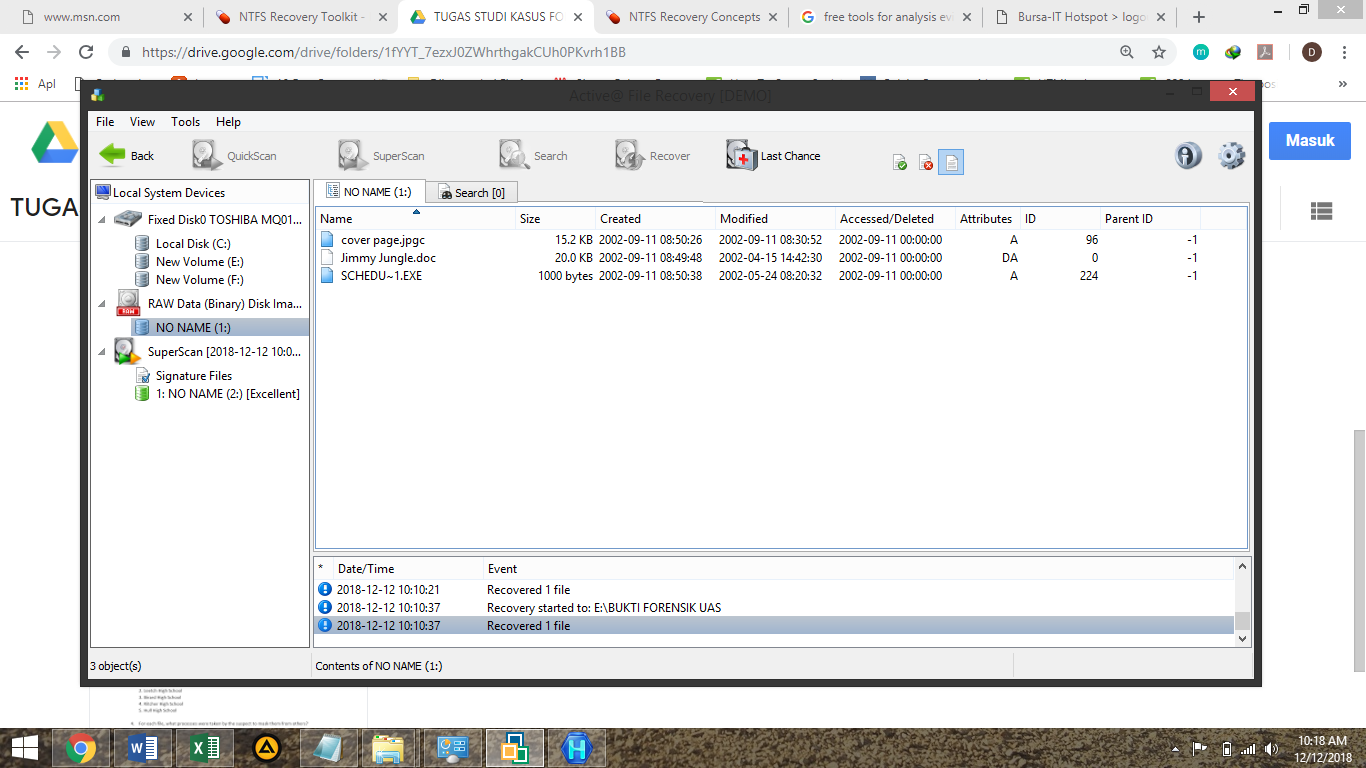
* Key High School
* Leetch High School
* Birard High School
* Richter High School
* Hull High School

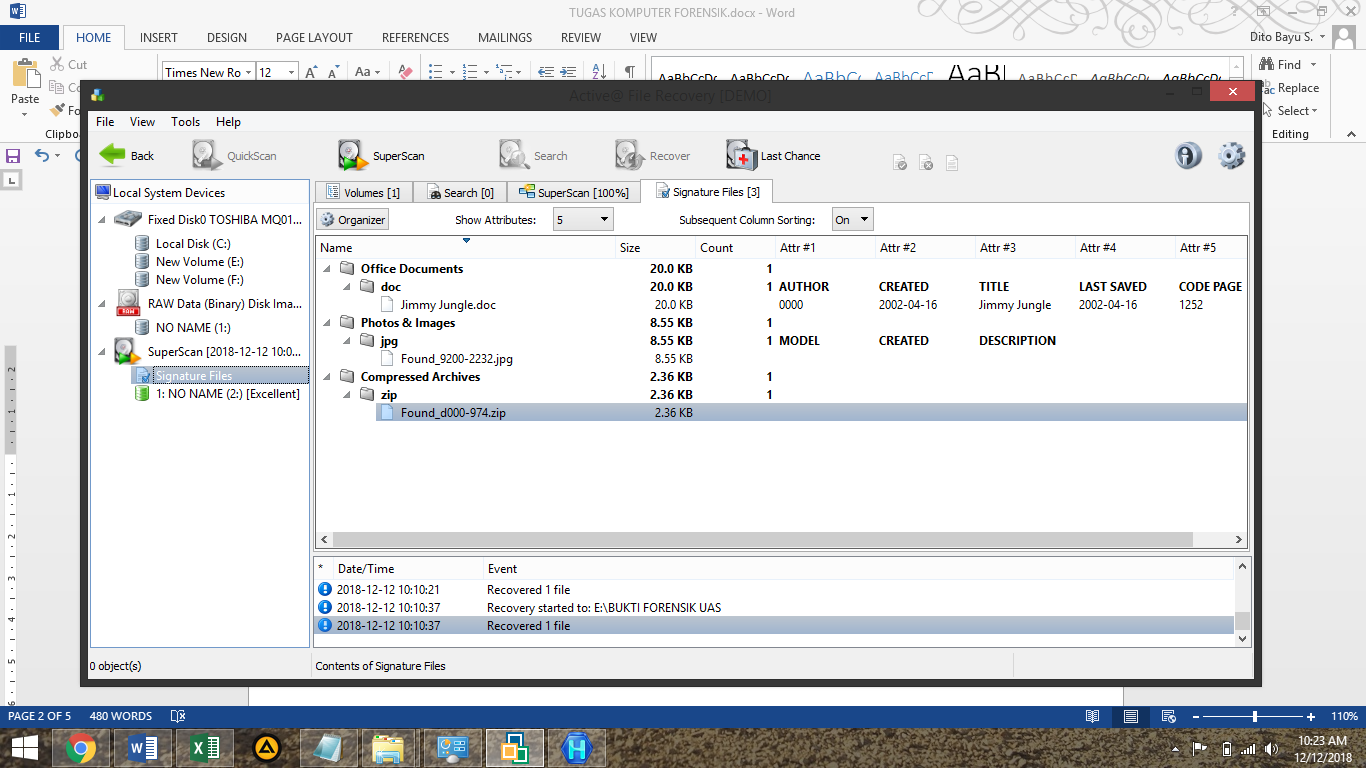
1. For each file, what processes were taken by the suspect to mask them from others?

* Jimmy Jungle.doc
* File ini dihapus
* Coverpage.jpg
* Extensi filenya dirubah
* Schedule Visist.zip
* Extensi filenya diganti menjadi exe, dan dilindungi oleh password

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

Proses yang dilakukan, seperti berikut :

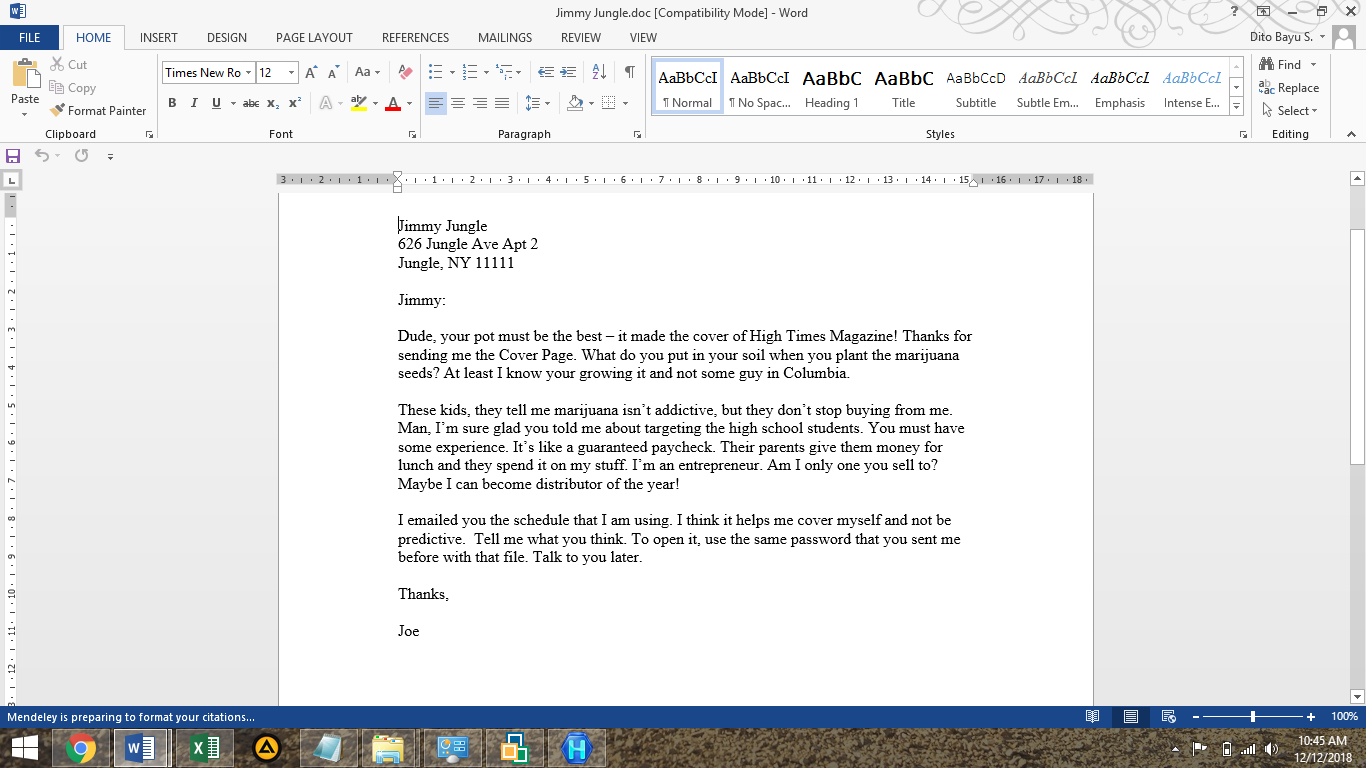
1. Meload atau membuka file image yang akan dianalisis pada aplikasi NTFS Recovery
2. Kemudian setelah mendapatkan file apa saja yang ada pada evidence kita lakukan proses superscan untuk mengetahui file signature sebenarnya dari file yang ada



1. Setelah mendapatkan file apa saja yang ada didalam evidence, kemudian kita merecover file yang diduga memiliki butki tersebut
2. Menganalisis setiap file yang ada :

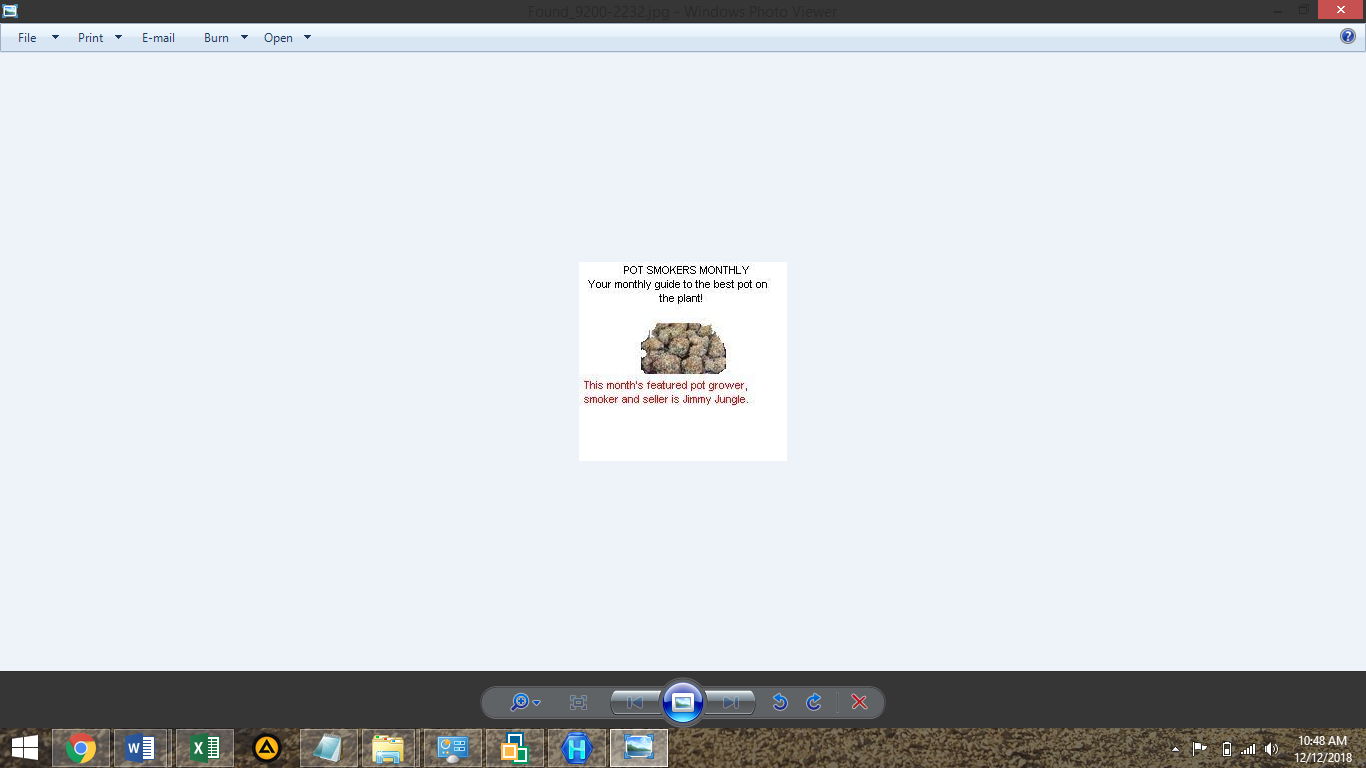
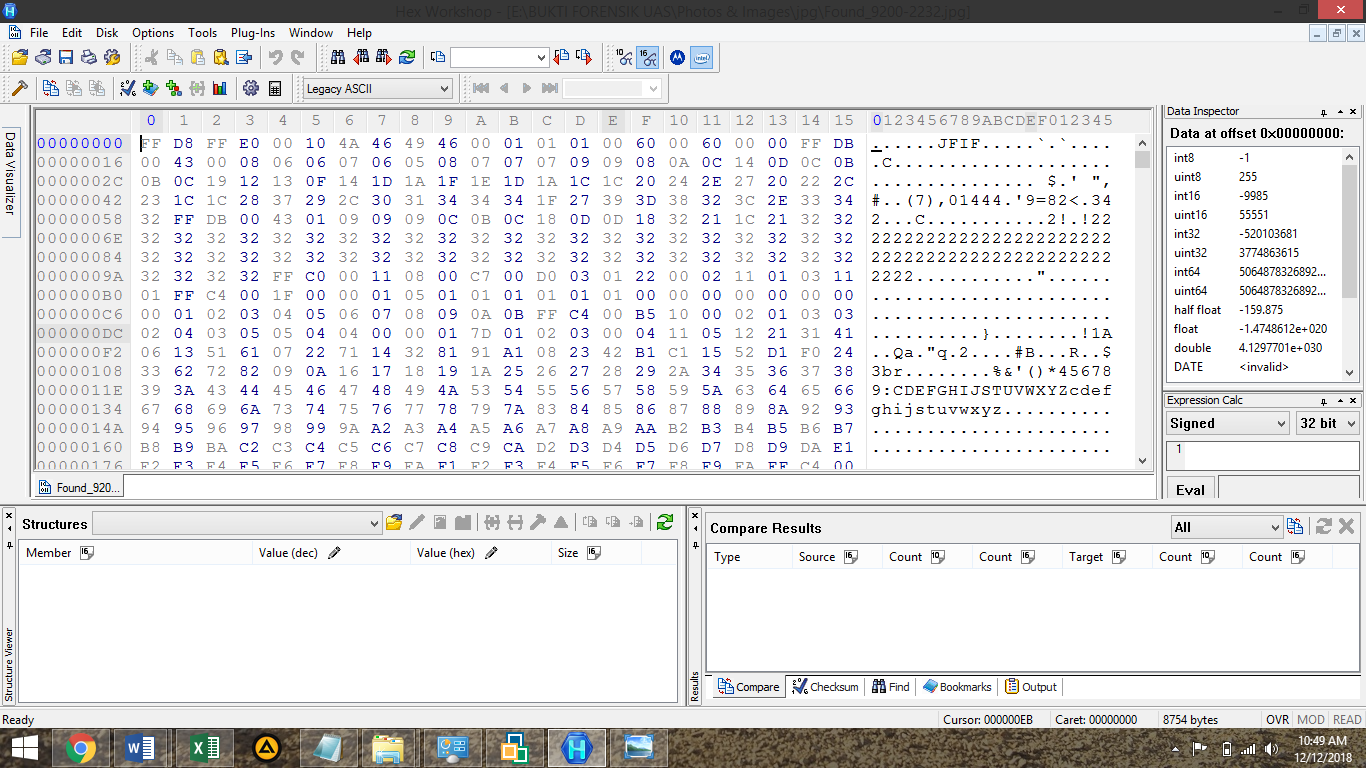
* File Jimmy Jungle.doc

Pada file ini hanya dilakukan proses recovery saja, dan dilakukan analisis terhadap isi file ini. Pada file ini terdapat informasi mengenai supplier Joe Jacob



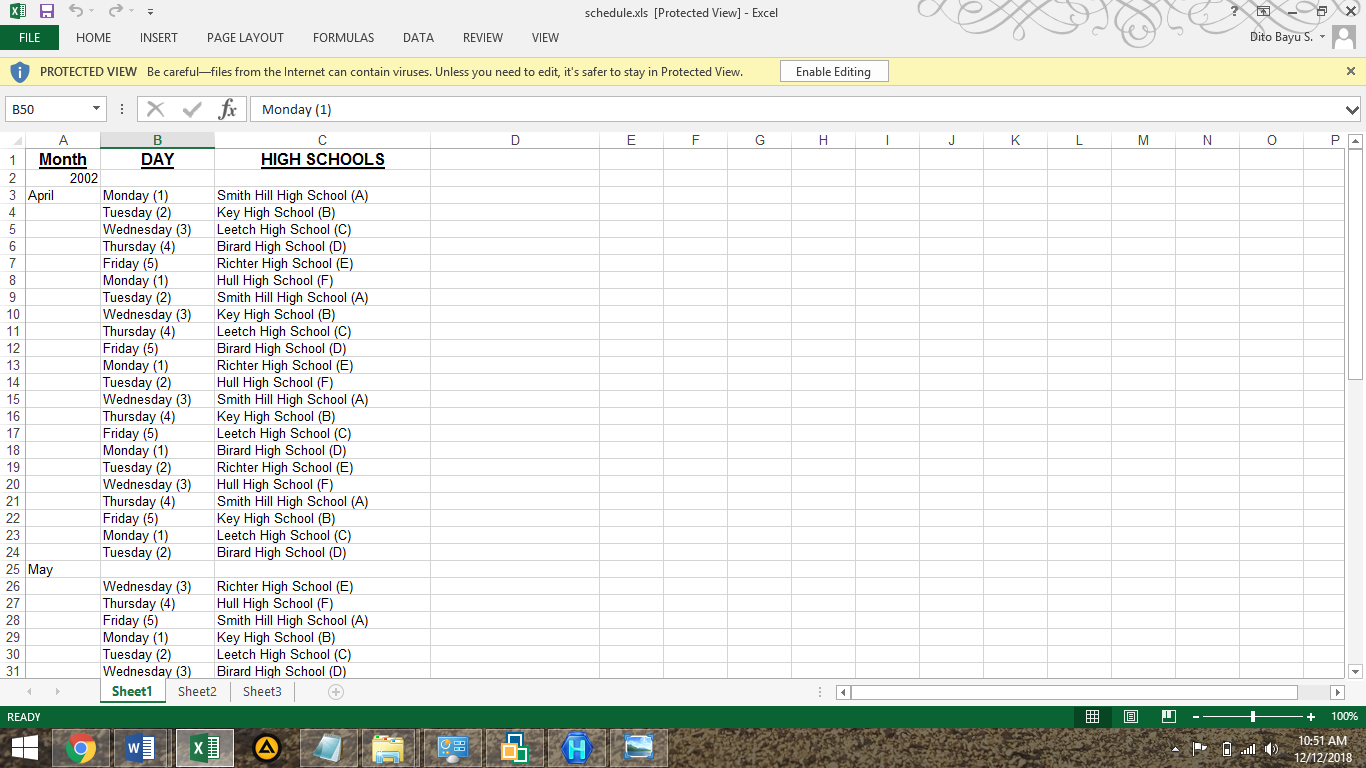
* File coverpage.jpg

Setelah dilakukan proses recovery, kemudian file ini dianalisis foto yang ada pada filenya dan meteadatanya menggunakan hex editor. Pada file ini terdapat informasi yang menguatkan mengenai supplier dari Joe Jacob, dan juga terdapat sebuah password, yaitu pw=goodtimes ketika dianailis menggunakan hex editor.



* File Schedule visits.zip

Setelah melakukan proses recovery, kemudian dilakukan analisis pada file ini. Ternyata pada file ini dilindungi oleh password, dan ketika dimasukan password yang didapatkan dari file coverpage.jpg file Schedule visits.zip ini dapat diekstrak. Didalam file zip didaptkan sebuah file Schedule visits.xls yang merupakan bukti mengenai sekolah mana saja yang dikunjungi oleh Joe Jacob selain sekolah Smith Hill.



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





Gambar 4.JPG

Gambar 3.JPG

Analisa Metadata :

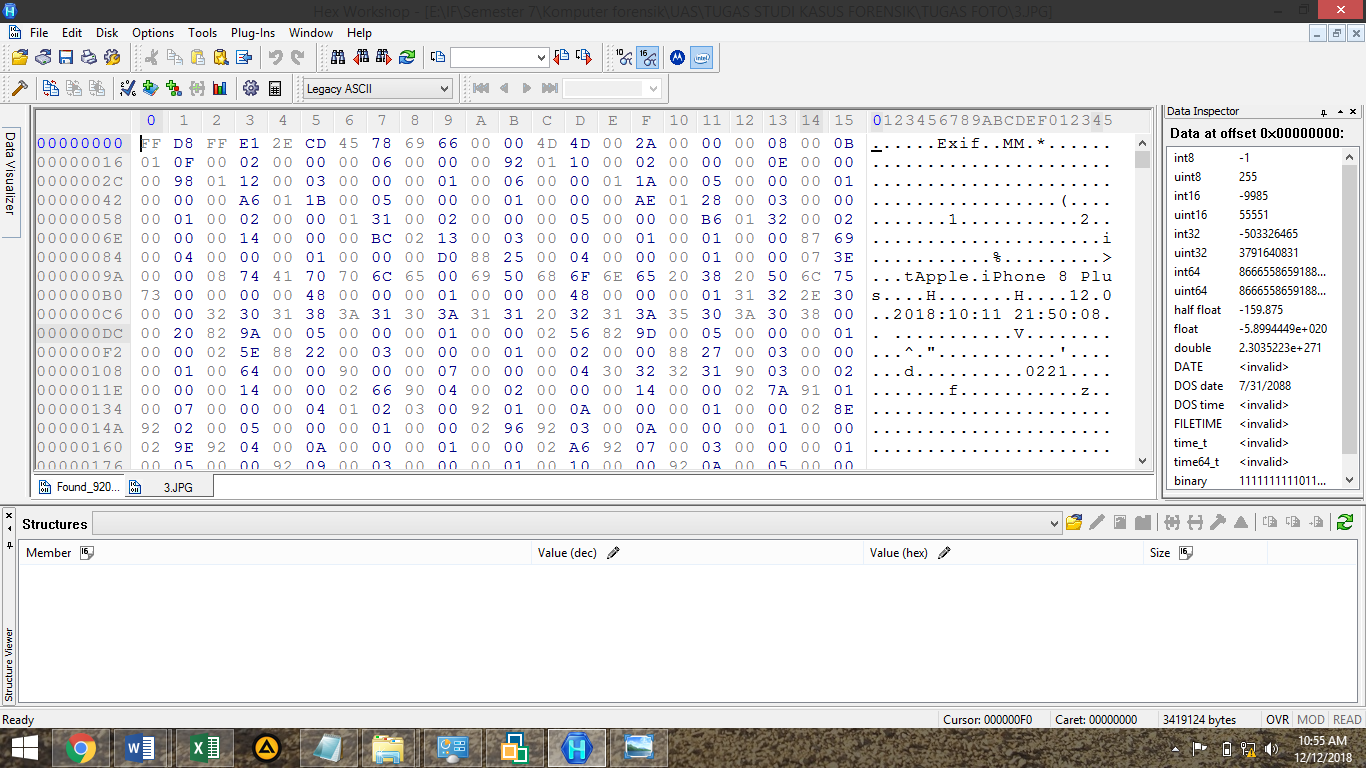


Foto 3.JPG

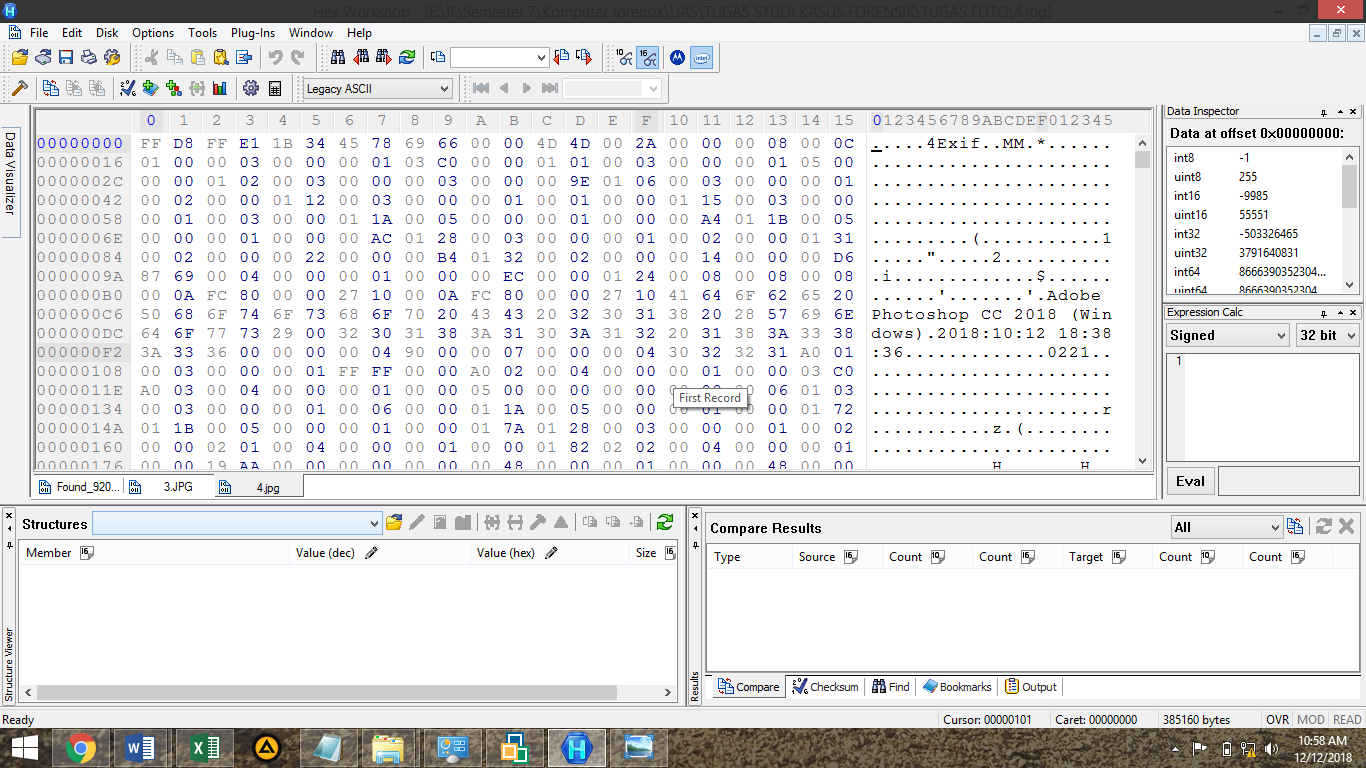


Foto 4.JPG

Dari metadata masing-masing foto, dapat kita lihat bahwa foto 3.JPG diambil melalui smartphone iPhone 8 plus, dan pada foto 4.JPG terlihat bahwa foto tersebut pernah diolah menggunakan software Adobe Photoshop CC 2018. Untuk kesimpulan sementara berdasarkan metadata foto 3.JPG dianggap asli dan foto 4.JPG kemungkinan telah dimodifikasi. Dan untuk bukti yang lainnya dapat kita lihat berdasarkan ELA (Error Level Analysis). Berikut ini gambar ELA dari masing-masing foto :

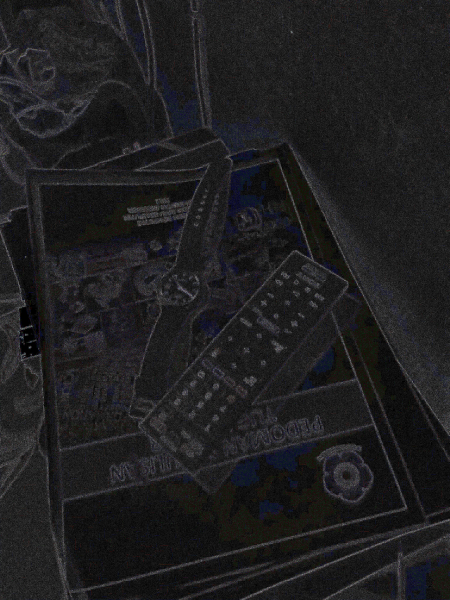


Foto 4.JPG

Foto 3.JPG

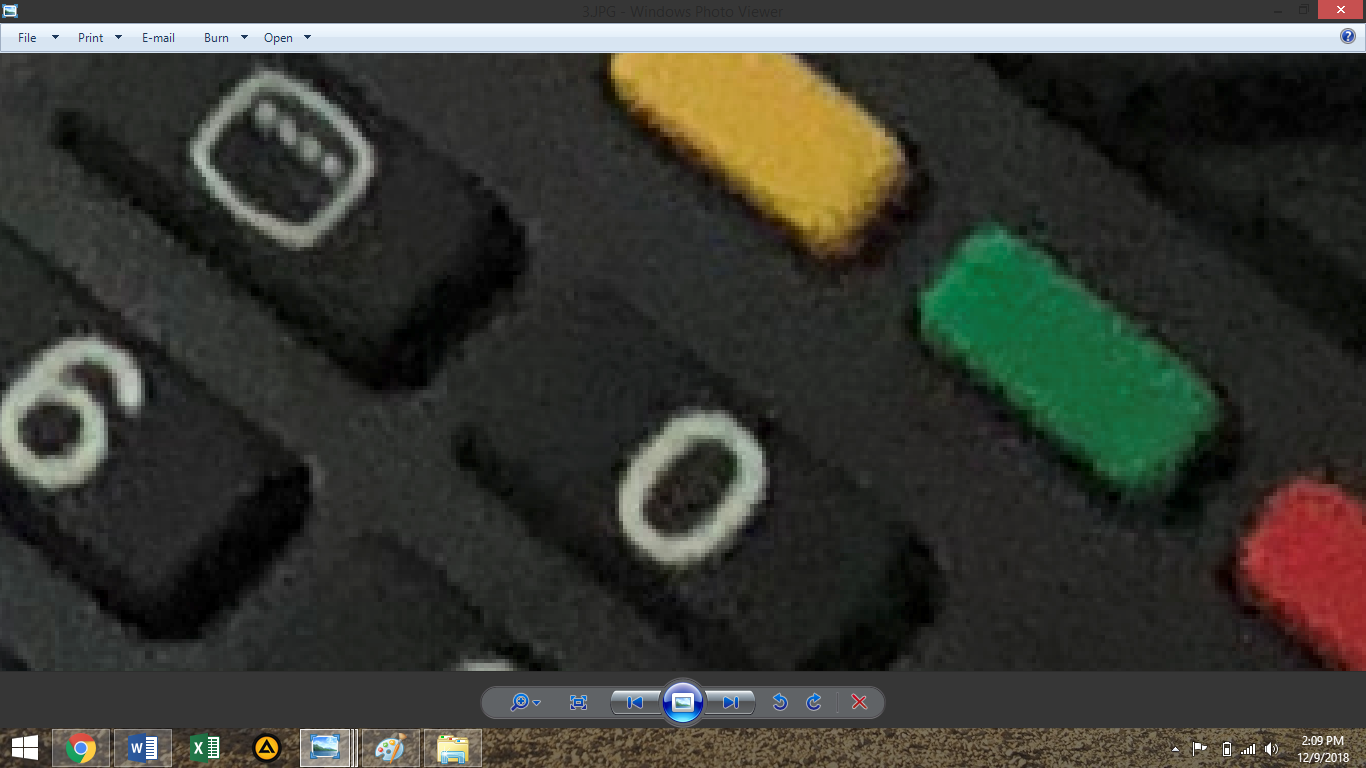
Berdasarkan metode ELA (Error Level Analysis) dapat kita lihat bahwa pada foto 4.JPG (pada bagian merek remote) memiliki kualitas level noise yang berbeda dari foto remotenya, sedangkan pada foto 3.JPG mempunyai kualitas level (noise) yang rata dan tidak ditemukan adanya kejanggalan. Untuk lebih memastikannya lagi dapat kita lihat jika kedua gambar kita lakukan zoom, fotonya akan menjadi seperti berikut :

Foto 3.JPG

Foto 3.JPG

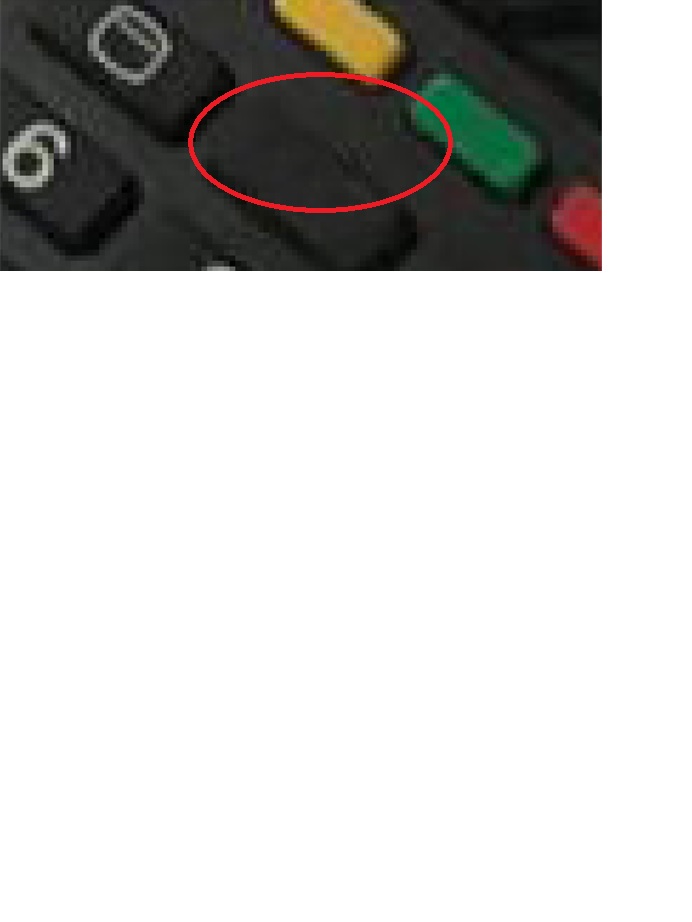


Foto 4.JPG

Dan bila kita melakukan zooming pada kedua gambar terlihat pada foto 4.JPG ada bagian pixel yang terlihat agak blur sedangkan pada foto 3.JPG tidak. Maka dari analisa metadata yang ada dan beberapa bukti tamban yang telah kita lakukan dapat ditarik kesimpulan bahwa foto 4.JPG telah mengalami modifikasi, dan foto 3.JPG merupakan foto yang asli.