**Nama : Ima Sintia**

**Nim : 09021181520132**

**Kelas : IF REG**

**LAPORAN HASIL ANALISA**

1. Menganalisa Studi Kasus dari file Image.Zip
2. Who is Joe Jacob’s supplier of marijuna and what is the address listed for rhe supplier?

Jawab :

* Supplier of marijuana : **Jimmy Jungle**
* address listed for rhe supplier : 626 Jungle Ave Apt 2 , Jungle, NY 11111

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

Jawab :

* Didalam file coverpage.jpg terdapat **“pw = goodtimes”** dimana password ini sepertinya digunakan untuk membuka file ScheduledVisits.exe

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

Jawab :

Sekolah yang didatangi Joe Jacob :

* Key High School
* Leetch High Shcool
* Birard High Shcool
* Ritcher High School
* Hull High School

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

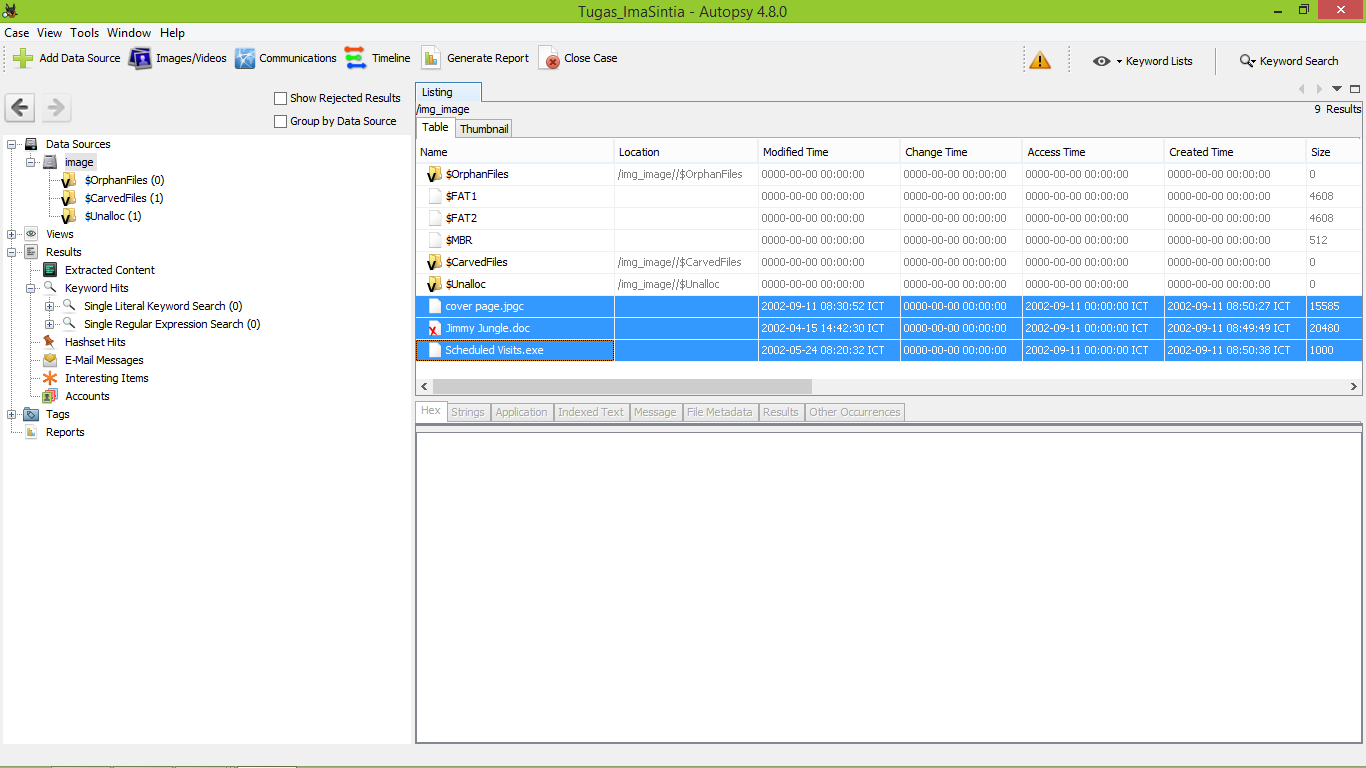
Jawab :

* Pertama, file JimmyJungle.doc yang sengaja dihapus
* Kedua, file coverpage.jpgc yang diubah ektensinya dengan memanipulasi hex-nya
* Ketiga, file ScheduledVisit.exe yang seharusnya merupakan file .zip dan dimanipulasi hex-nya serta dilindungi dengan sebuah password

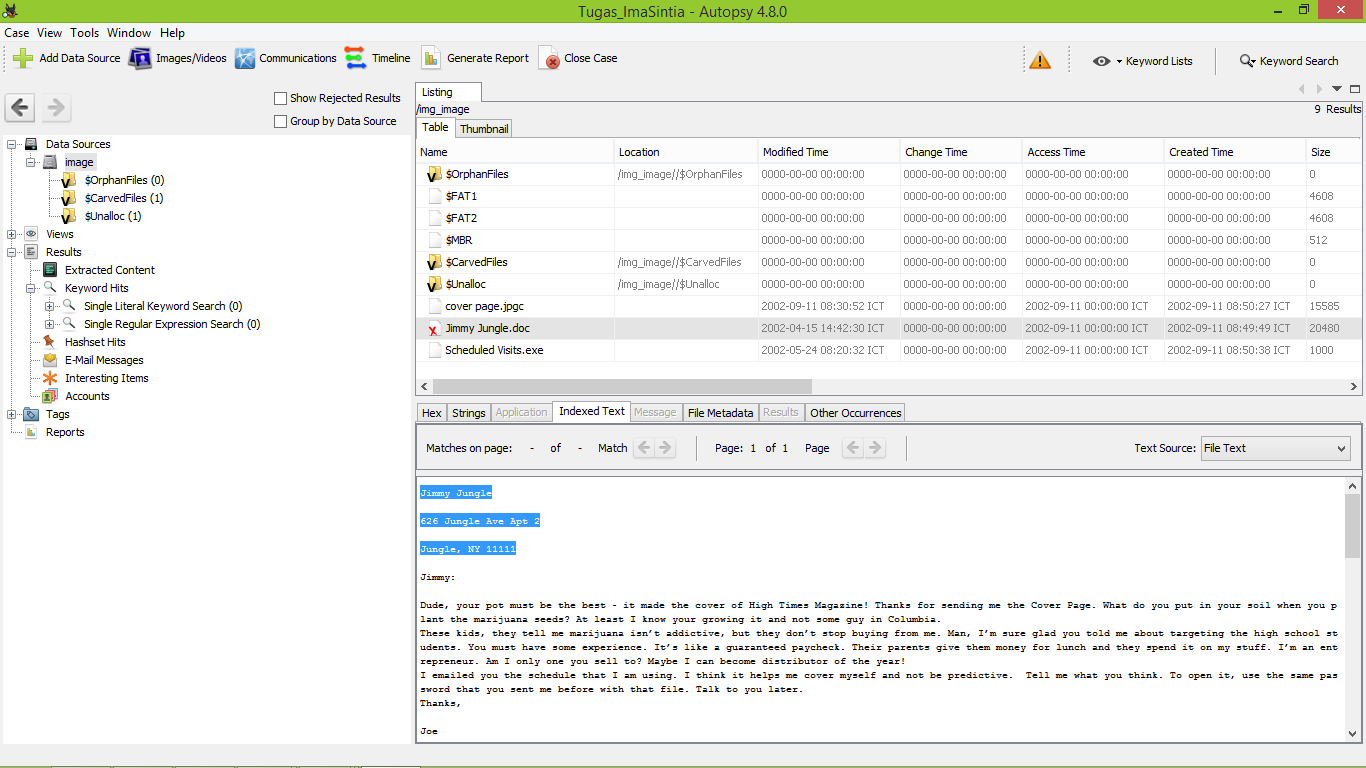
1. What processes did you use to successfully examine the entire contents of each file ?

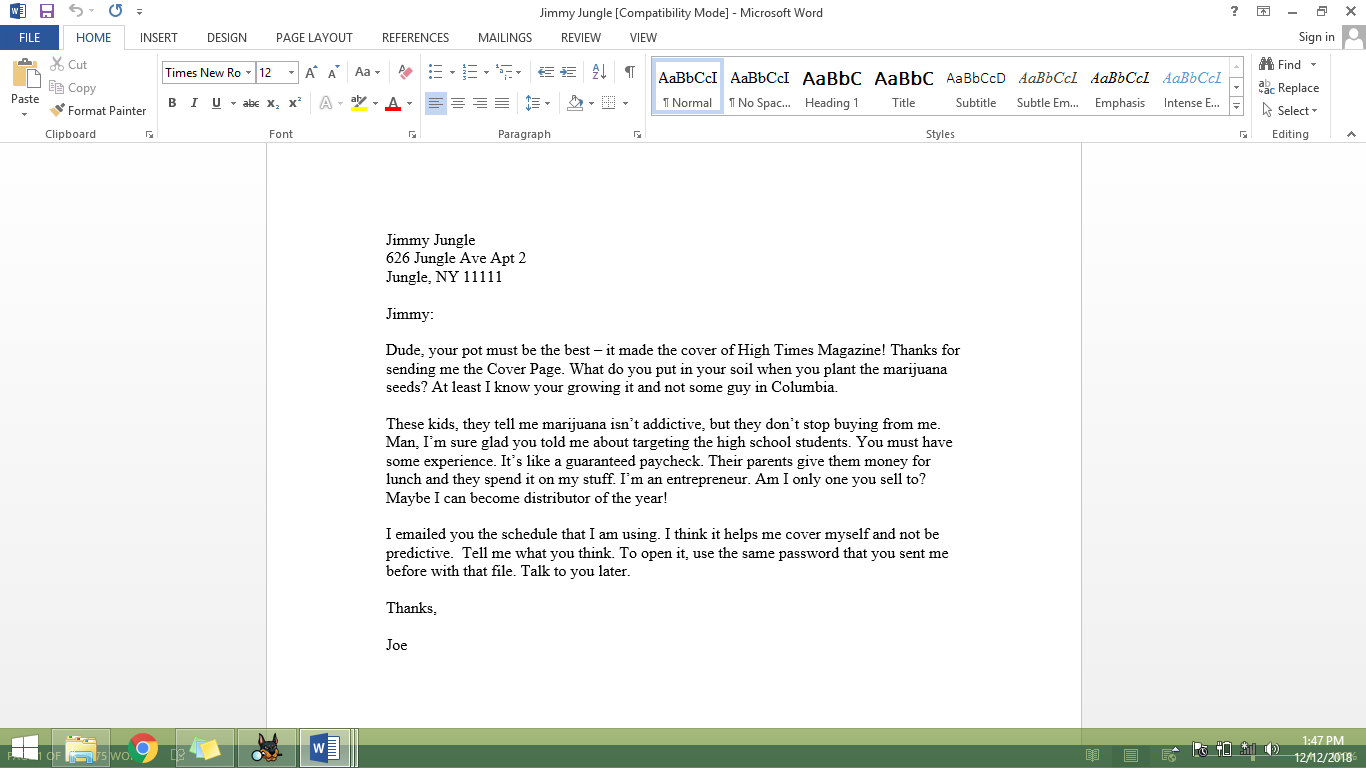
Jawab :

* Membuka file image.zip menggunakan aplikasi Autopsy

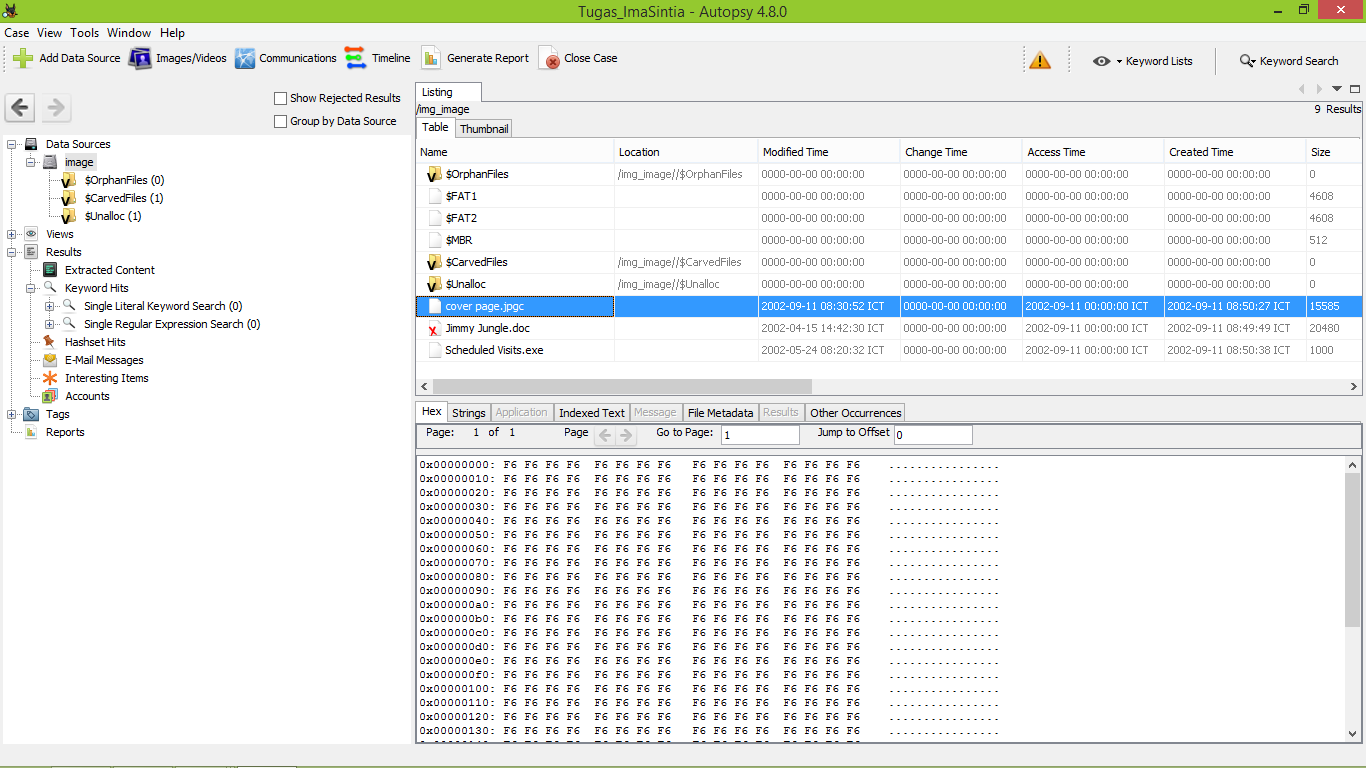


* Terdapat beberapa informasi yang mencurigakan didalam file image.zip dan salah satu dari file tersebut telah dihapus

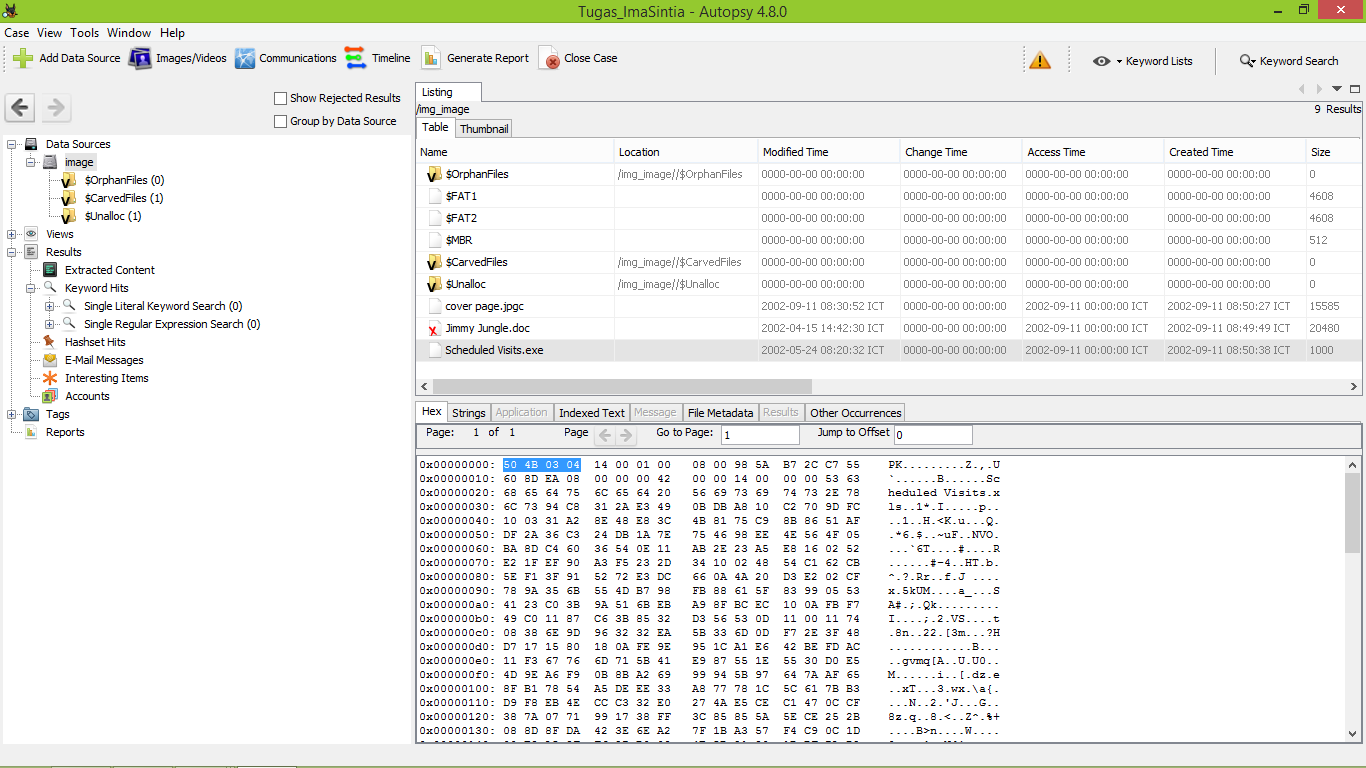




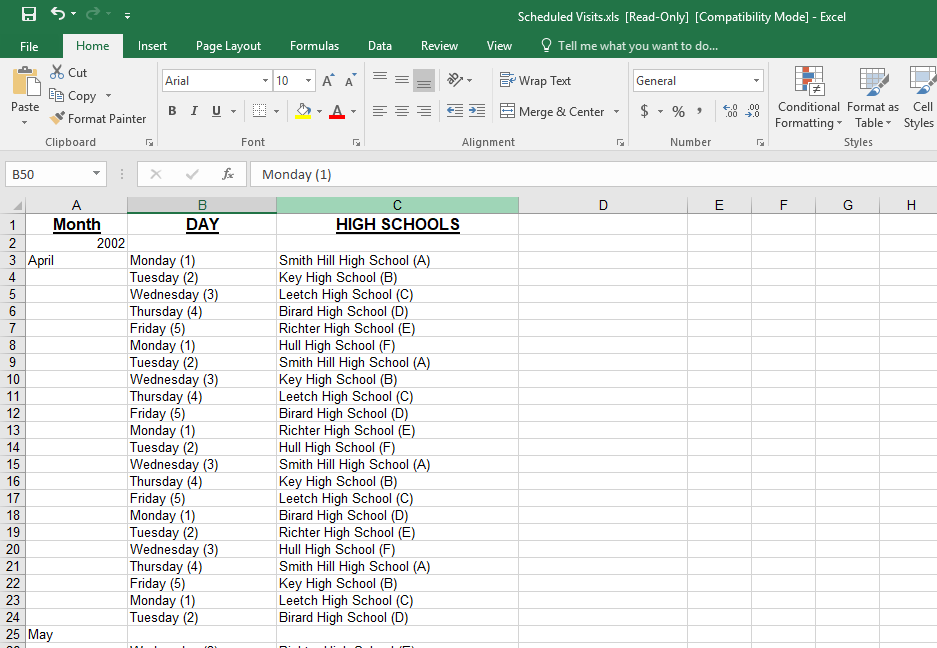
* Setelah itu kita buka file yang telah dihapus yaitu file Jimmy Jungle.doc dapat kita lihat terdapat sebuah pesan yang dikirimkan Joe Jacob kepada supplier marijuana.

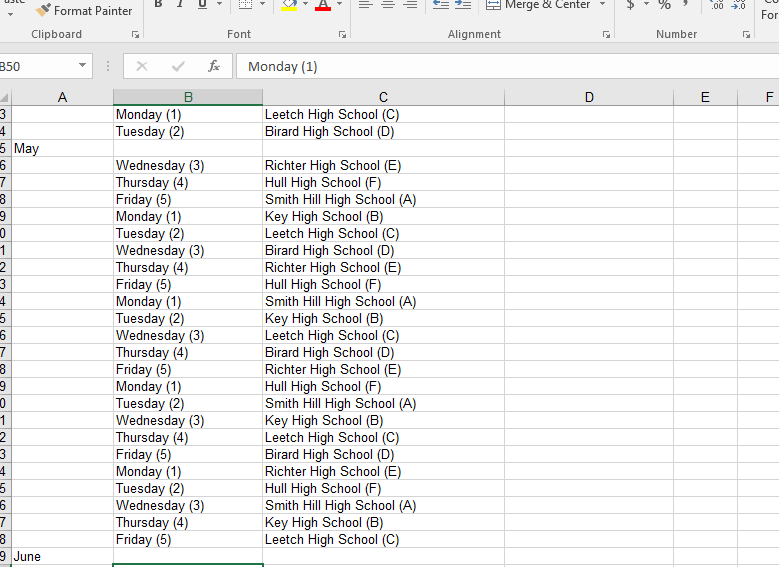


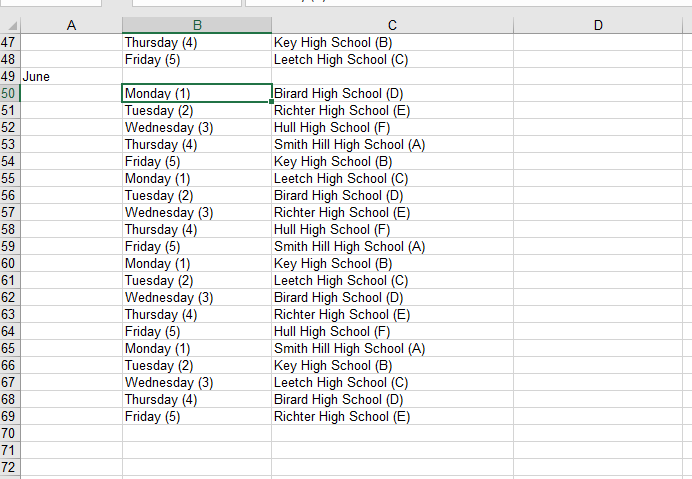
* Setelah itu kita buka file coverpage.jpgc dan kita ubah file ektensi coverpage.jpg, dan didalam file tersebut terdapat data berupa password **“pw=goodtimes”** yang mungkin akan digunakan untuk membuka file Scheduled Visit.exe



* Selanjutnya kita buka file Scheduled Visit.exe dan kita lihat dari bilangan Hex yang terdapat pada file tersebut dengan membuka website <https://www.garykessler.net/library/file_sigs.html> dan kita lihat bilangan Hex tersebut merupakan bilangan untuk file ekstensi file.zip
* Setelah itu ubah file Scheduled Visit.exe ke file .zip kemudian kita exstraksi file .zip tersebut. Dan setelah dibuka ternyata file tersebut dilindungi oleh password dan kita gunakan password yang telah kita temukan difile coverpage.jpg tadi yaitu **“pw = goodtimes”**
* Didalam file Scheduled Visit terdapat file excel dan kita buka menggunakan excel dan terdapat beberapa informasi, seperti tampilan dibawah ini :







1. Menganalisa Foto

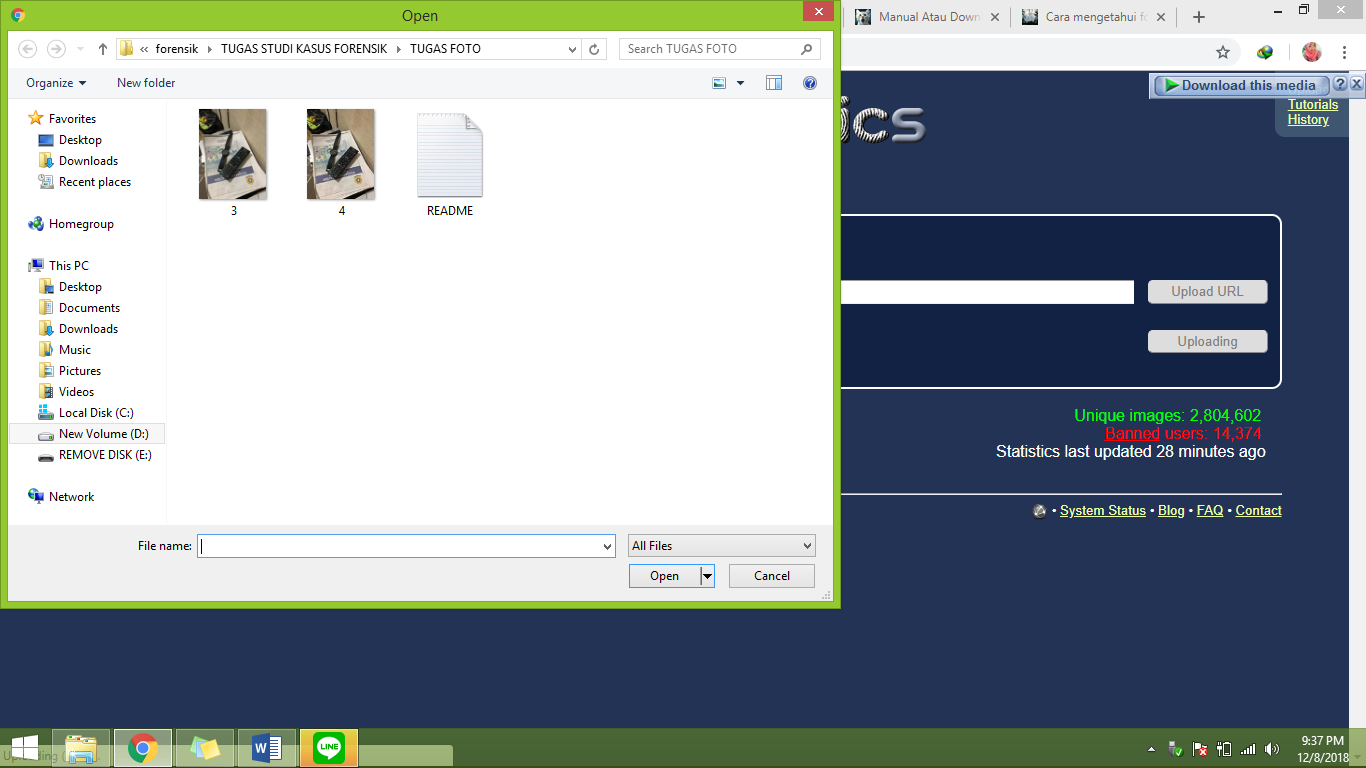
* Untuk hasil analisa mana foto asli dan mana foto palsu ada dibagian paling bawah.

Langkah-langkah menganalisa foto :

1. Membuka website fotoforensics.com
2. Setelah itu muncul tampilan website tersebut. Seperti tampilan dibawah :



1. Setelah muncul tampilan website fotoforensics, maka ada 2 pilihan cara untuk menganalisa foto yang ingin kita analisa. Yang pertama menyalin image URL dari foto yang ingin kita analisa atau upload file dari media penyimpanan kita.
2. Disini saya memilih upload file untuk menganalisa foto. Saya ingin mengupload satu persatu dari file foto dari tugas tersebut, saya meng-upload foto (3.JPG) dan foto 4.JPG untuk dianalisa, dengan cara meng-klik *Choose File* setelah itu kita pilih gambar 3 lalu kita klik tombol open setelah itu kita upload, untuk gambar 4 caranya sama, seperti tampilan dibawah :



* Upload foto 3.JPG



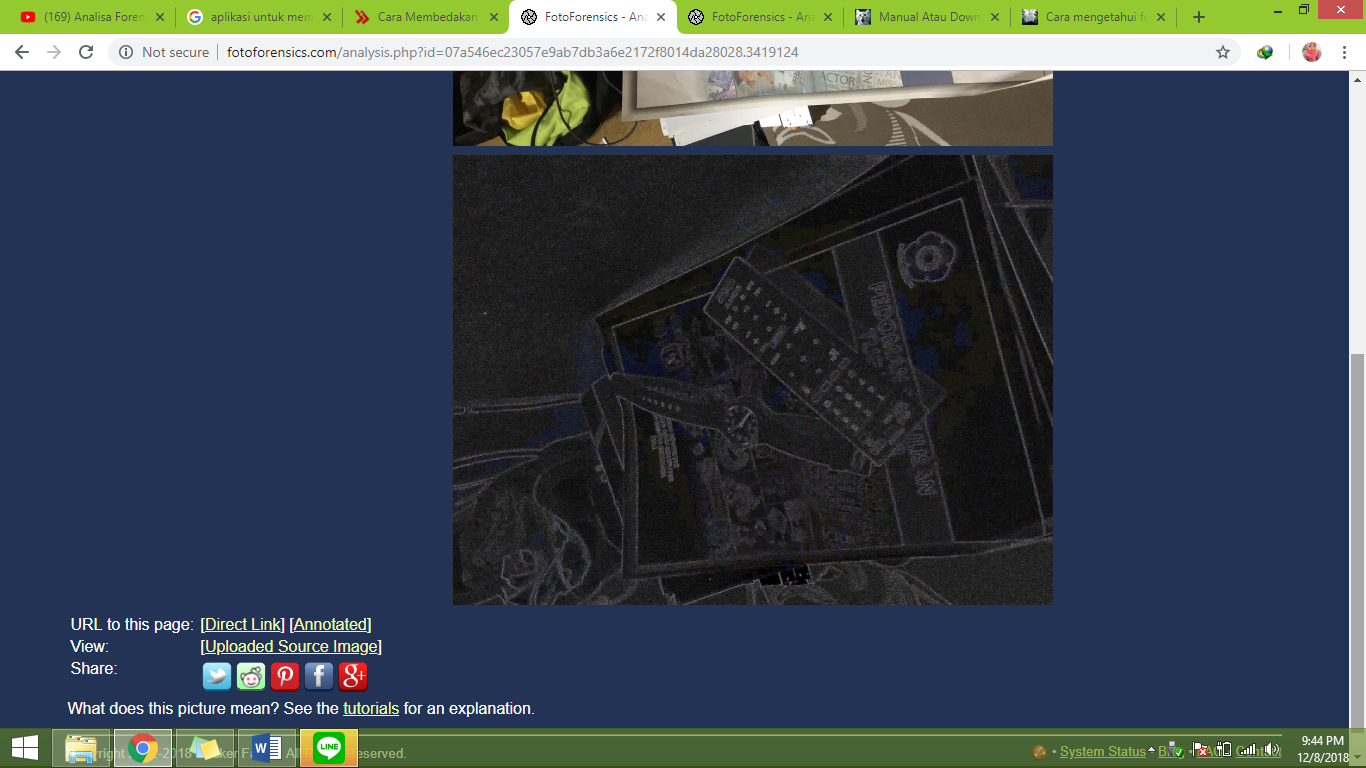
* Upload foto 4.JPG



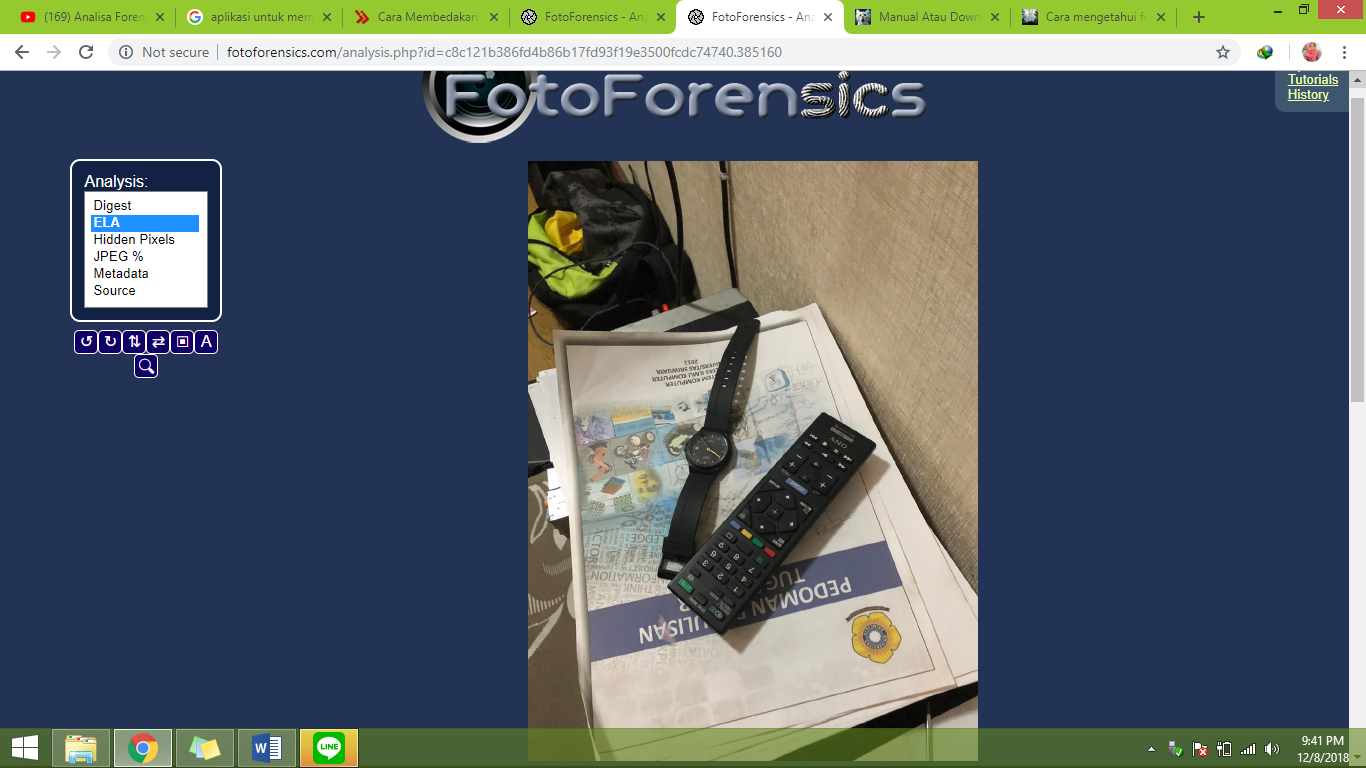
1. Tunggu sampai uploading selesai, setelah uploading selesai, maka website tersebut akan menampilkan hasil analisa seperti tampilan dibawah :

* Hasil analisa ELA dari foto 3.JPG





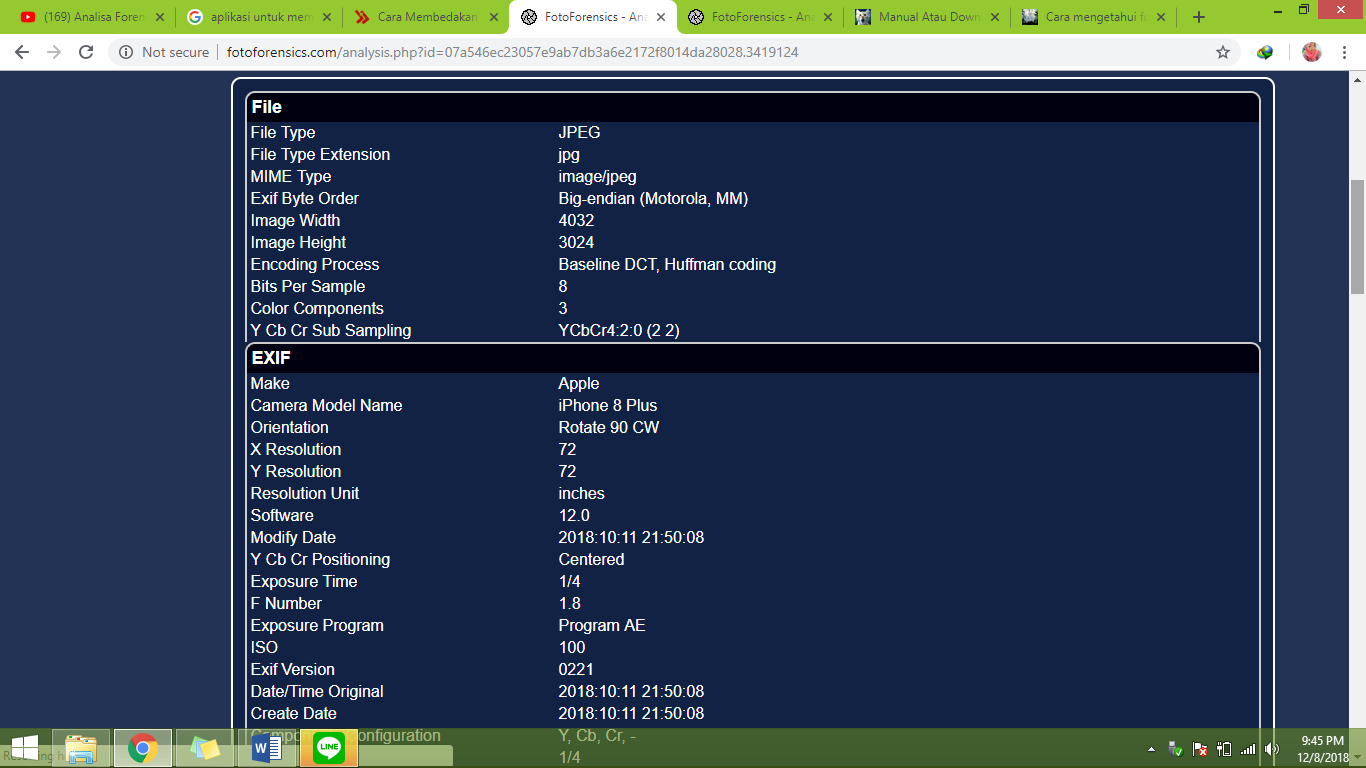
* Hasil analisa ELA dari foto 4.JPG

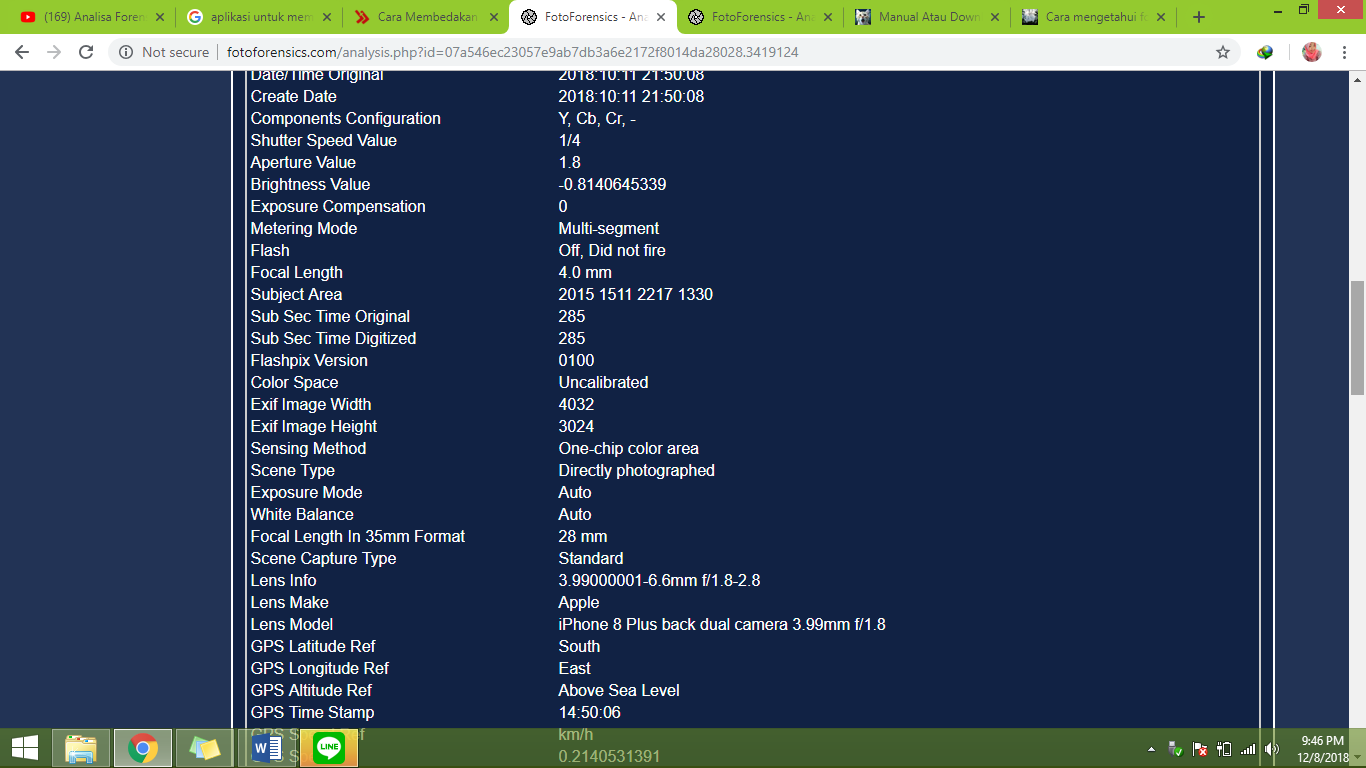


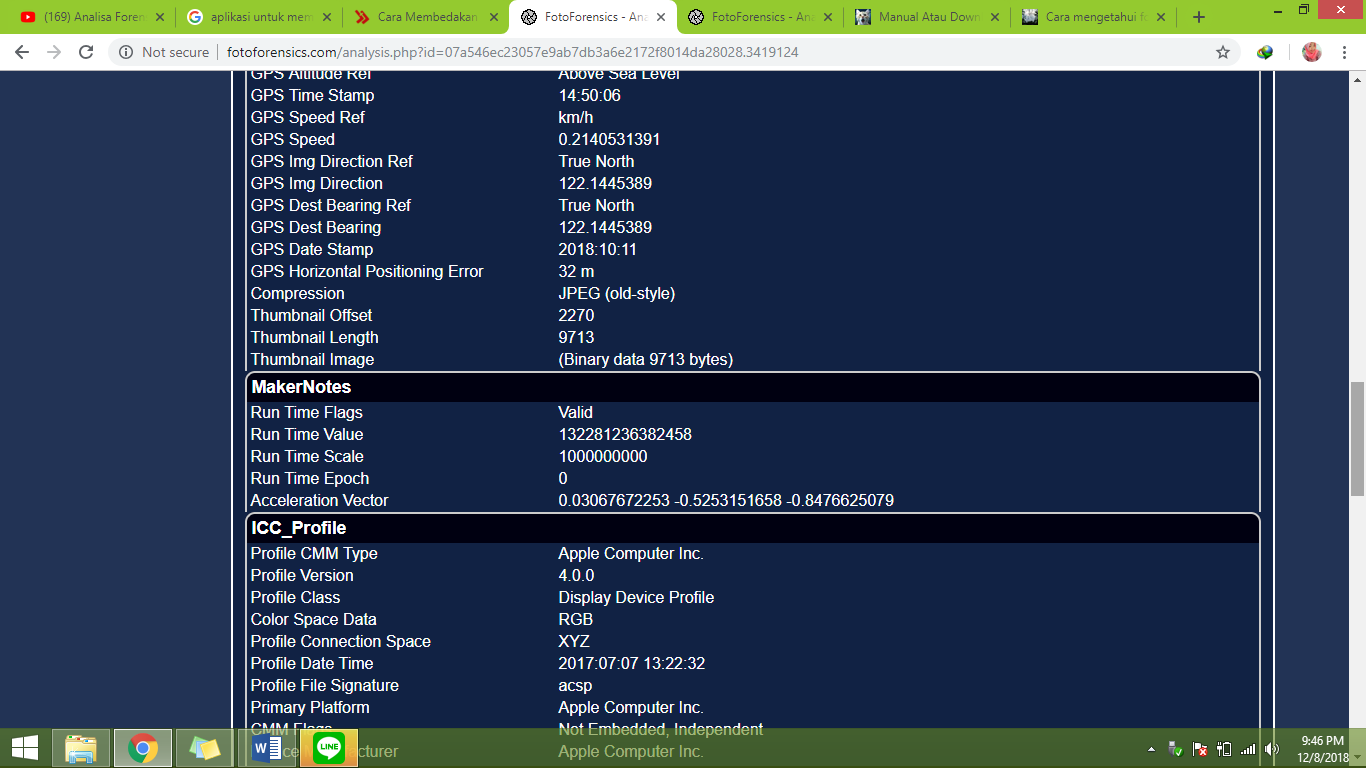


1. Setelah kita menganalisa hasil ELA dari foto 3.JPG dan 4.JPG tersebut, maka kita harus melakukan analisa Metadata dari foto tersebut. Tampilan dibawah ini adalah tampilan analisa Metadata dari foto 3.JPG dan 4.JPG :

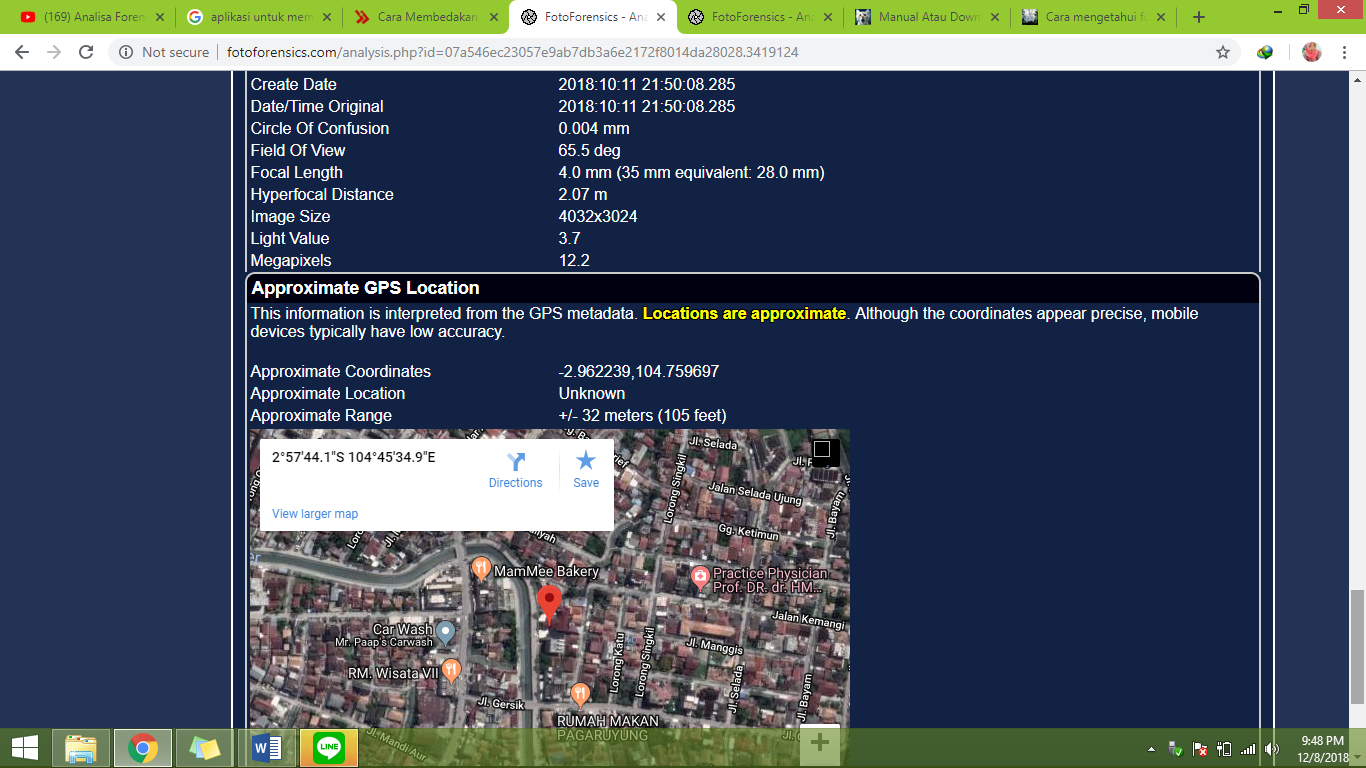
* Hasil analisa Metadata foto 3.JPG



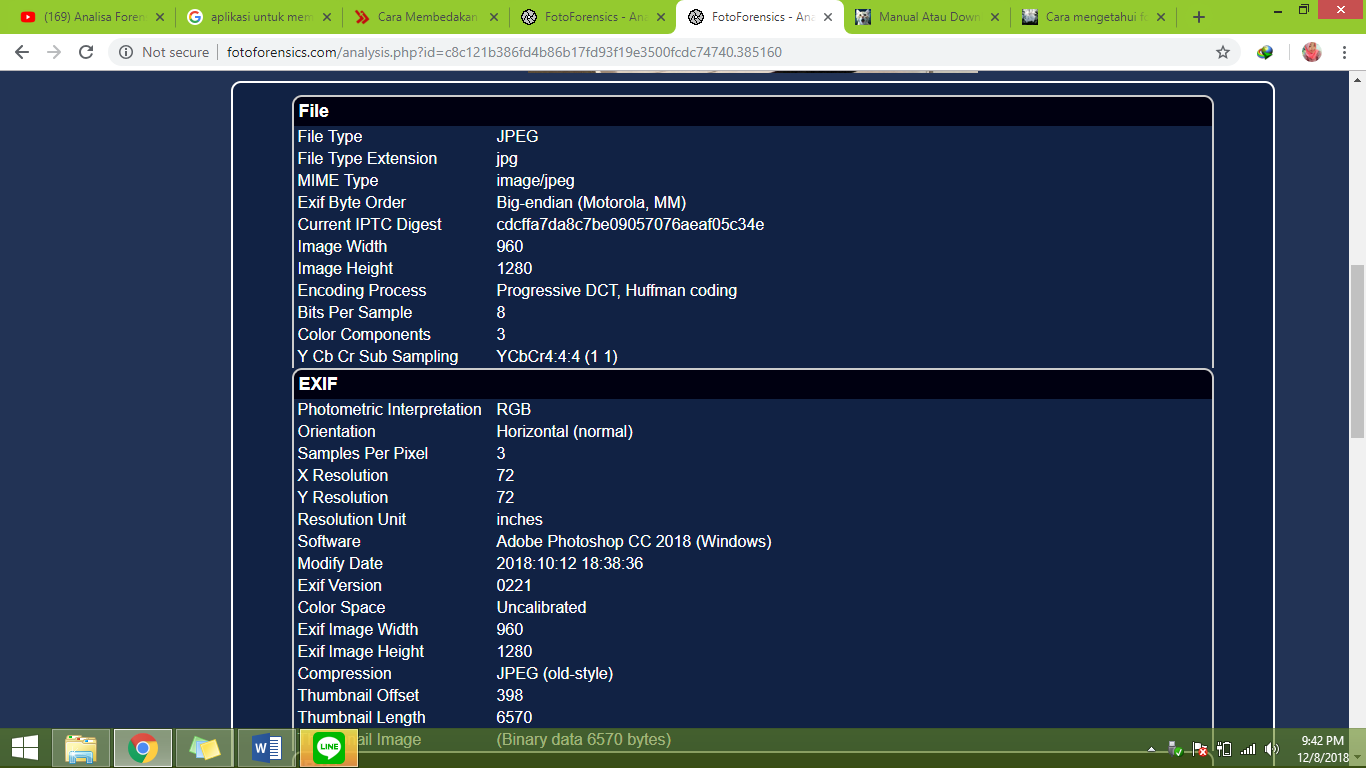


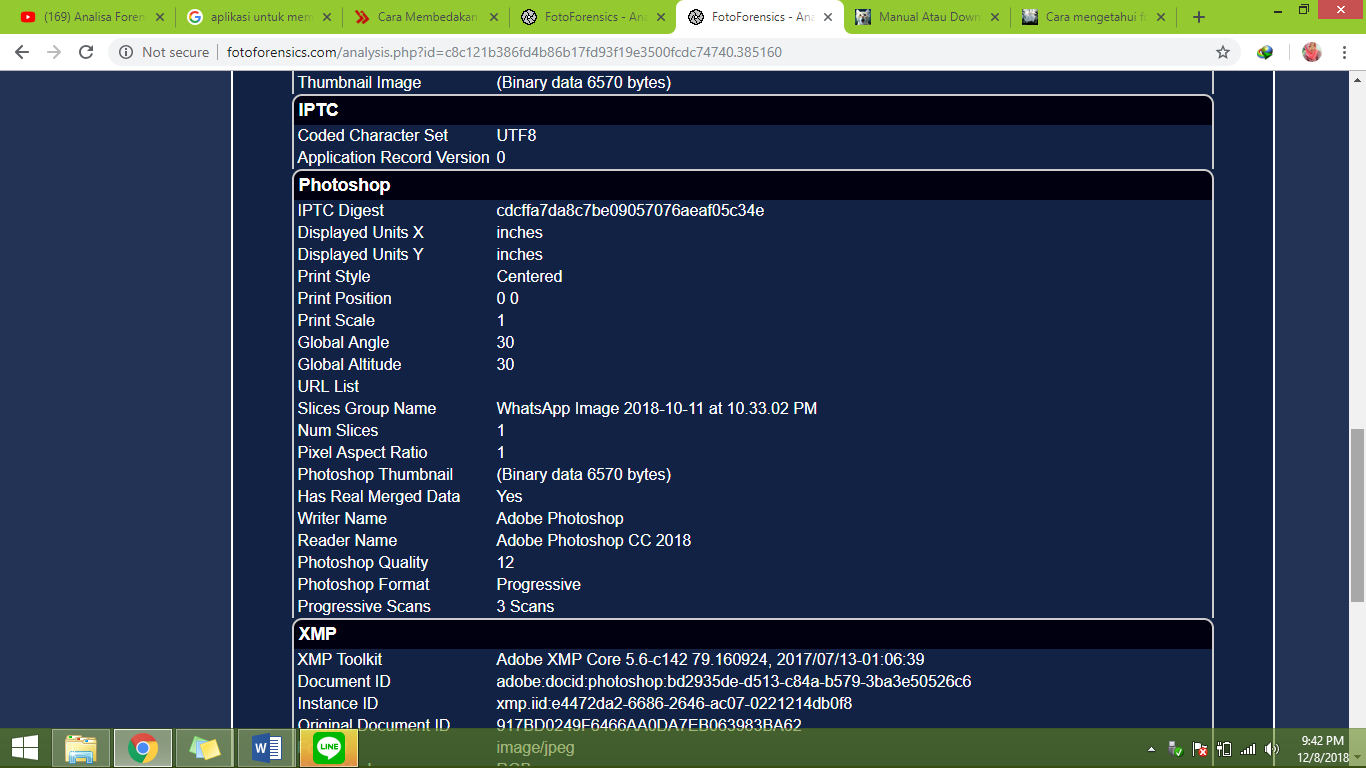






* Hasil analisa Metadata foto 4.JPG







Hasil analisa Metadata dari foto 3.JPG dan 4.JPG :

* Untuk analisa Metadata dari foto 3.JPG setelah melakukan analisa menggunakan *Website* fotoforensics, kita bisa lihat hasil analisa Metadatanya sangat lengkap, dari camera yang dipakai untuk memfoto, terus tanggal dia melakukan foto, dan juga lokasi dia melakukan foto.
* Sedangkan untuk hasil analisa Metadata untuk foto 4.JPG setelah melakukan analisa, kita bisa lihat hasil analisa Metadatanya tidak lengkap, dan lokasi foto tersebut juga tidak ada dihasil analisa Metadatanya.
* Setelah saya melakukan analisa Metadata dari kedua foto tersebut bahwa foto 3.JPG itu adalah foto yang asli dikarenakan hasil Metadatanya lengkap dan hp yang digunakan untuk memfoto menggunakan hp *Iphone 8Plus,* sedangkan foto 4.JPG itu adalah foto yang palsu dikarenakan hasil Metadatanya tidak lengkap dan diedit menggunakan software *Adobe Photoshop CC.2018*.