FORENSIK GAMBAR - ANALISA METADATA UNTUK PEMBUKTIAN GAMBAR ASLI / EDITTING

VICKO BHAYYU / 09011181520036

KEAMANAN JARINGAN KOMPUTER / 2018

Forensik merupakan bidang ilmu pengetahuan yang digunakan untuk membantu proses penerapan ilmu atau sains. (Wikipedia – Ilmu Forensik)

Forensik computer merupakan salah satu dari cabang ilmu forensic yang berkaitan dengan bukti legal yang ditemui pada computer dan media penyimpanan digital. Tujuan dari forensic computer adalah untuk menjabarkan keadaan kini dari suatu artefak digital. Istilah artefak digital bisa mencakup sebuah sistem computer, media penyimpanan, sebuah dokumen elektronik baik sebuah pesan email atau gambar jpeg, atau bahkan sederet paket yang berpindah dalam jaringan computer. (Wikipedia – Forensik Komputer)

Pada kali ini penulis akan mencoba menulis apa yang dilakukan penulis dalam mencoba melakukan sebuah forensic gambar. Studi kasus sederhana kali ini untuk pembuktian sederhana apakah gambar tersebut merupakan asli atau telah mengalami proses editing dengan analisa sederhana metadata yang terdapat pada gambar.

Diberikan 4 gambar berikut.



Gambar b.jpg

Gambar a.jpg



Gambar d.jpg

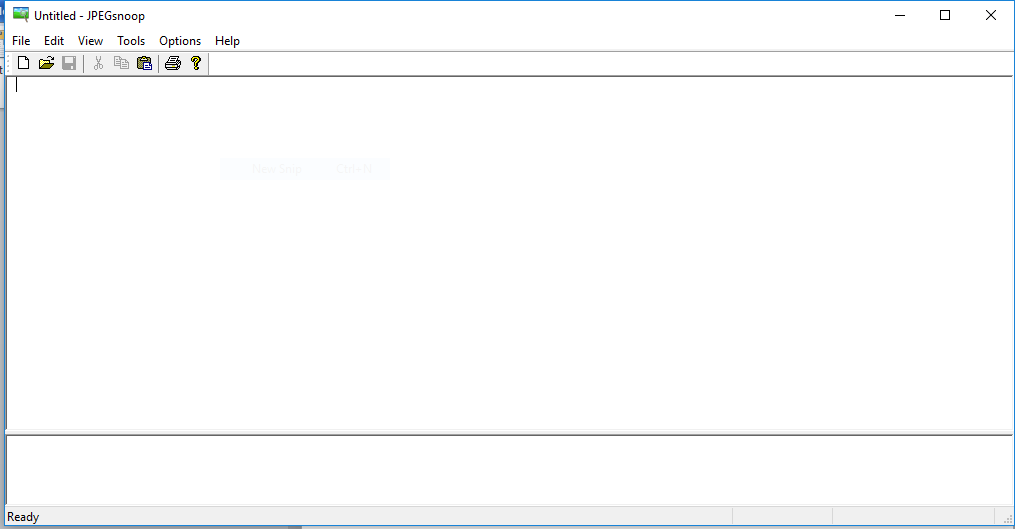
Gambar c.jpg

Jika kita lihat ke 4 gambar tersebut merupakan gambar yang sama, namun dari ke 4 itu manakah gambar yang merupakan gambar asli yang diambil dari kamera tanpa proses editing ?

Disini penulis menggunakan :

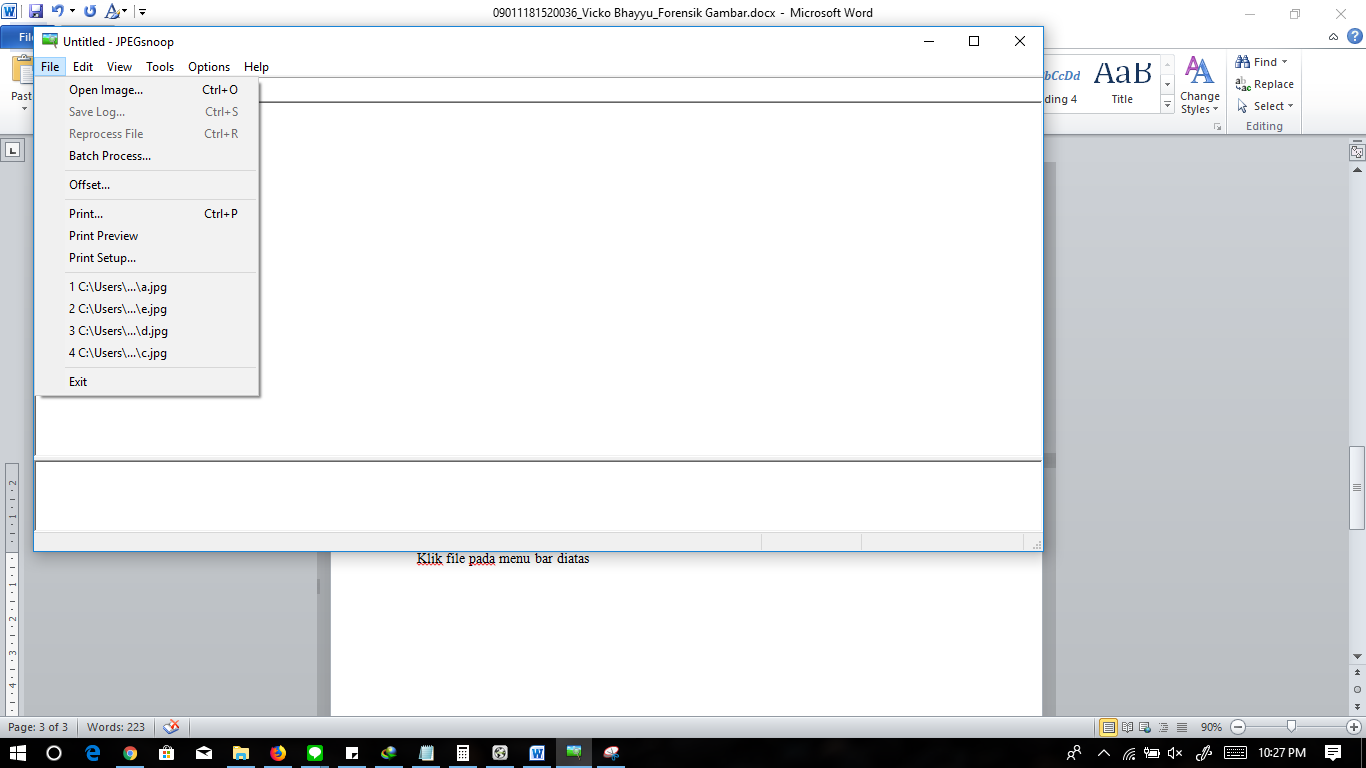
* Software : JPEGSNOOP
* OS : Windows 10

Sebelumnya penulis akan menampilkan cara memasukkan gambar pada JPEGSNOOP

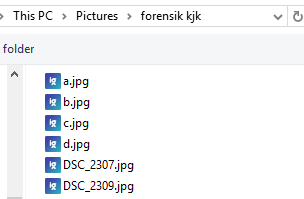


Gambar diatas merupakan tampilan awal saat membuka jpegsnoop

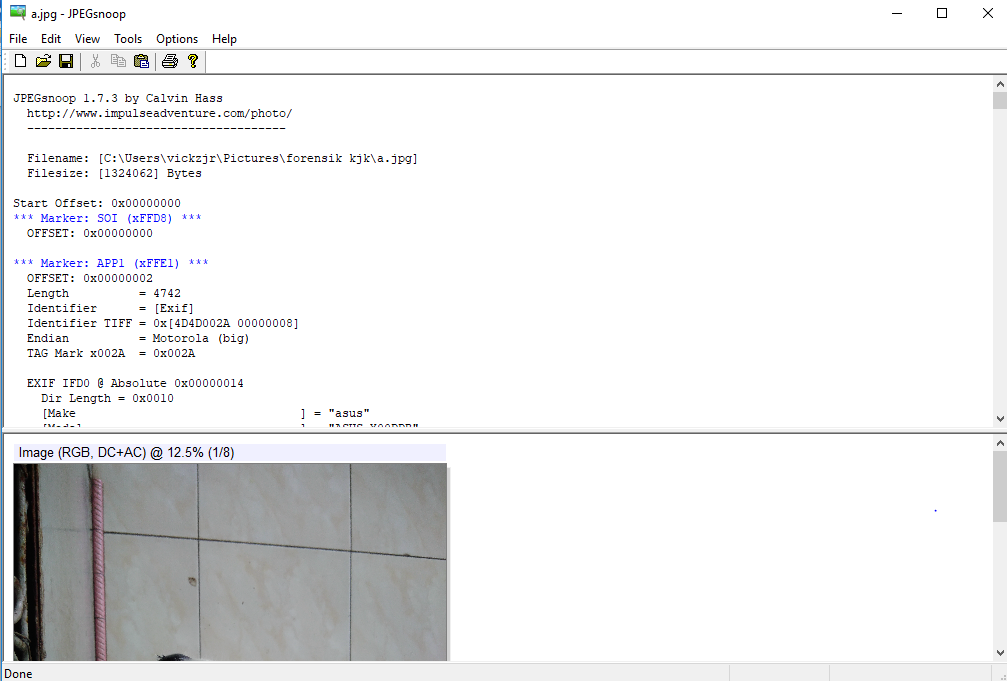
Klik file pada menu bar diatas



Klik Open image, arahkan ke direktori folder gambar yang diinginkan

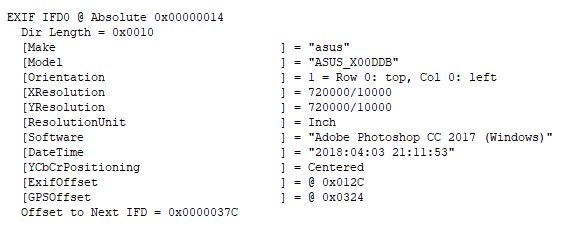


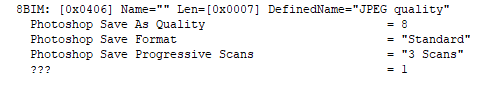
Pilih file yang diingin dilihat metadatanya

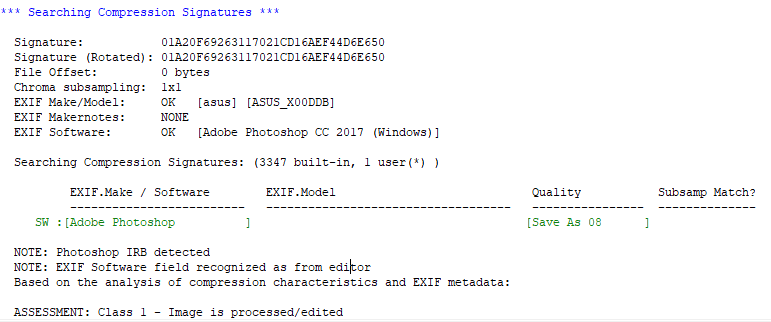


Tampilan setelah dimasukkan gambar..

Berikut merupakan potongan metadata dari gambar a.jpg



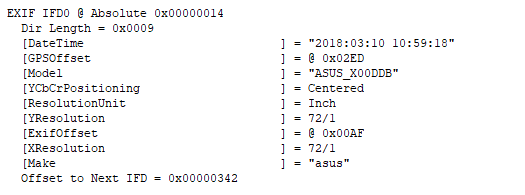


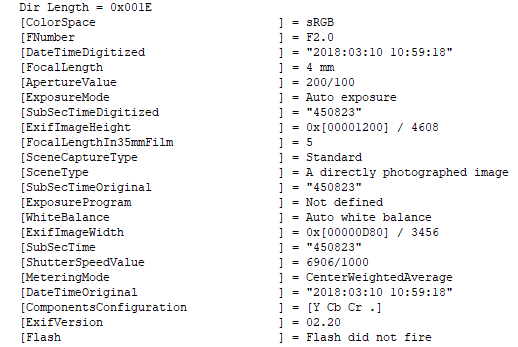


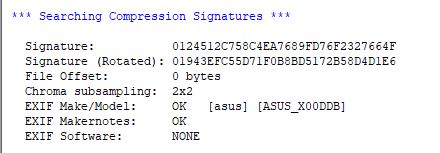
Terlihat adanya software Adobe Photoshop CC 2017 (Windows) yang menandakan bahwa gambar ini telah melalui serangkaian proses pada Adobe Photoshop CC 2017. Maka jpegsnoop menyimpulkan bahwa gambar ini merupakan gambar yang diambil dari kamera ASUS\_X00DDB dan telah dilakukan proses editing menggunakan software Adobe Photoshop CC 2017.

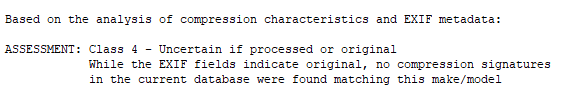
Kenyataannya memang gambar ini merupakan gambar asli yang diambil kamera namun penulis mencoba melakukan sedikit editing dan kemudian kompresi gambar menggunakan software Adobe Photoshop CC 2017.

Berikut potongan metadata gambar b.jpg





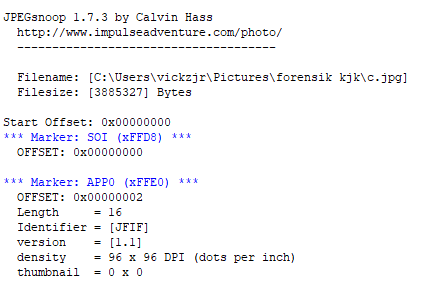


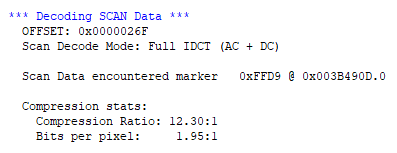


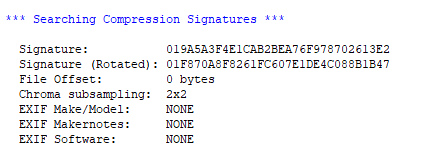
Dari metadata diatas, tidak terdapat informasi mengenai software editing, maka jpegsnoop menyimpulkan tidak yakin bahwa telah dilakukan editing atau merupakan gambar asli, namun pada database jpegsnoop tidak terdapat data mengenai model kamera yang digunakan.

Kenyataannya memang gambar b.jpg merupakan gambar asli yang diambil langsung dari kamera ASUS\_X00DDB.

Berikut metadata gambar c.jpg





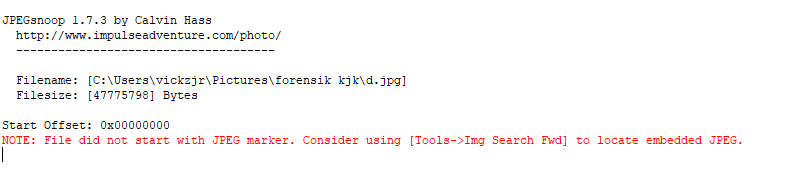




Terlihat hanya sedikit informasi yang dapat ditampilkan oleh jpegsnoop, gambar ini telah melalui proses kompresi gambar. Dengan informasi ini, jpegsnoop menyimpulkan bahwa gambar c.jpg telah melalui proses perubahan / editing.

Kenyataannya bahwa gambar c.jpg merupakan gambar keluaran yang dihasilkan oleh software quick stego dengan format bmp, penulis mencoba memasukkan sebuah steganografi namun jpegsnoop hanya dapat melihat metadata gambar dengan format jpeg saja. Oleh dari itu maka penulis menggunakan software Paint bawaan dari Windows lalu melakukan save as ke format jpg.

Berikut potongan metadata gambar d.jpg



Jpegsnoop tidak dapat mendapatkan metadata dari gambar d.jpg.

Kenyataannya,sama seperti gambar c.jpg, gambar d.jpg merupakan keluaran dari software quickstego dengan format bmp. Lalu penulis mencoba untuk mengubah langsung format bmp ke jpg melalui fitur rename file beserta ekstensinya. Yang awalnya merupakan d.bmp menjadi d.jpg. Maka dari itu jpegsnoop tidak dapat mengambil metadata dari d.jpg karena pada awalnya bukan merupakan gambar jpeg.

Inilah serangkaian proses yang dilakukan penulis. Penulis juga mendapatkan informasi bahwa software jpegsnoop hanya mengambil informasi metadata yang terdapat pada gambar. Apabila gambar tersebut diubah terlebih dahulu metadatanya dengan bantuan software lain, maka jpegsnoop tetap menampilkan metadata tersebut. Ini merupakan kelemahan dari software ini.

Sekian dan terima kasih.