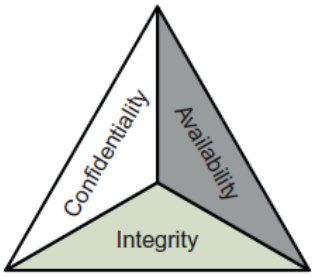
Nama : Ahmad Akbar Tanjung
NIM : 1310651209
Kelas : A

## 1. Resume

Akses Kontrol

**Confidentiality, Integrity, dan Availability**




Confidentiality, Integrity, dan Availability adalah konsep landasan keamanan informasi.

**Confidentiality**

mencegah pengungkapan yang tidak sah, dan berusaha untuk mencegah akses yang tidak sah.

**Integrity**

mencegah modifikasi data yang tidak sah dari informasi. Dengan kata lain, integritas berusaha untuk mencegah akses tulis tidak sah ke data.

**Availability**

Ketersediaan memastikan bahwa informasi yang tersedia bila diperlukan.

Disclosure, alteration, dan destruction

CIA juga dapat dijelaskan oleh kebalikannya:

Disclosure, alteration, dan destruction (DAD).

*Disclosure* adalah pengungkapan yang tidak sah terhadap suatu informasi

*Alteration* adalah modifikasi yang tidak sah dari data.

*Destruction* adalah membuat sistem tidak tersedia.

**Identitas dan otentikasi**

Identitas adalah data user yang akan mengakses data.

otentikasi yaitu proses mengkonfirmasi keabsahan (user) tersebut benar.

**Otorisasi**

Otorisasi adalah sebuah proses pengecekan kewenangan user dalam mengakses sumberdaya.

**Akuntabilitas**

Akuntabilitas yaitu pertanggung jawaban pengguna terhadap apa yang mereka lakukan. Dan dapat dikenakan sangsi apabila melanggar kebijakan yang ada.

**Non-repudiation**

Non-repudiation (menolak penyangkalan), adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman suatu informasi.

**Least privilege and need to know**

Maksudnya adalah user diberikan akses yang minimun dan user tersebut harus tahu bagian-bagian tertentu dari sebuah informasi sebelum informasi tersbut diakses.

**Subyek dan obyek**

Sebuah subjek merupakan entitas yang aktif pada sistem data dan Objek adalah data pasif dalam suatu sistem.

**Defense-in-depth**

Defense-in-depth yaitu pertahanan berlapis yang berlaku beberapa perlindungan untuk menguragi resiko.

**MODEL ACCESS CONTROL**

Model akses kontrol terdiri dari Discretionary Access Control (DAC), Mandatory Access Control (MAC), and nondiscretionary access control.

**Discretionary Access Controls**

Discretionary Access Control (DAC) yaitu memberikan akses penuh terhadap data yang mereka miliki yaitu berbagi, mengubah ataupun menghapusnya.

**Mandatory Access Controls**

Mandatory Access Control (MAC) yaitu kebijakan membatasi akses ke sistem dikendalikan untuk objek sumber daya (seperti file data, perangkat, sistem, dll) berdasarkan tingkat otorisasi atau izin dari entitas mengakses, baik itu orang, proses, atau perangkat.

**Role-Based Access Control (RBAC)**

Role-Based Access Control (RBAC) sebuah metode untuk mengatur akses kesumber daya komputer atau jaringan yang didasarkan pada peran pengguna individu.

**Centralized Access Control**

Centralized access control berkonsentrasi kontrol akses di satu titik logis untuk sistem atau organisasi. Alih-alih menggunakan database kontrol akses lokal, sistem mengotentikasi melalui server otentikasi pihak ketiga. Kontrol akses terpusat dapat digunakan untuk menyediakan Single Sign-On (SSO), di mana subjek dapat mengotentikasi sekali, dan kemudian mengakses beberapa sistem

**Access Control Lists**

Access control lists yaitu Metode yang digunakan untuk menyeleksi paket yang keluar masuk.

**Access Control Protocols And Frameworks**

Access control protocols and frameworks yaitu sentralisasi dan desentralisasi dapat mendukung pengguna jauh otentikasi untuk sistem lokal. Protokol yang dapat digunakan yaitu RADIUS, Diameter, TACACS / TACACSþ, PAP, dan CHAP.

*Radius* Remote Authentication Dial-In Service Pengguna (RADIUS) protokol adalah pihak ketiga sistem otentikasi. RADIUS menggunakan User Datagram Protocol (UDP) port 1812 (authentication) dan 1813 (accounting).

*Diameter* penerus Radius yang dirancang untuk peningkatan Authentication.

*TACACS dan TACACS1(Terminal Access Controller Access Control System)* adalah sistem kontrol akses yang mengharuskan pengguna mengirim ID dan statis (reusable) password untuk otentikasi.

*PAP dan CHAP*

Password Authentication Protocol (PAP) pengguna memasukkan password dan dikirim melalui jaringan. Lalu dikonfirmasi dan divalidasi. server PAP

**Tipe dan Kategori Akses Kontrol**

Terdapat 6 tipe akses aontrol yaitu :

- Pencegahan
- Detektif
- Corrective
- Pemulihan
- Pencegah
- Kompensasi

**METODE AUTHENTIKASI**

Sebuah konsep kunci untuk melaksanakan jenis kontrol akses mengendalikan tepat otentikasi subyek dalam sistem.

Type 1 authentication: something you know.

Subjek diberikan akses atas dasar sesuatu yang mereka tahu, seperti password atau PIN (Personal Identification Number, password nomor-based). Ini adalah bentuk paling mudah, dan sering lemah, otentikasi.

- Passwords
- Password hashes and password cracking
- Dictionary attacks
- Hybrid attacks
- Brute-force attacks
- Rainbow tables
- Salts

Type 2 authentication: something you have

Otentikasi ini mengharuskan pengguna memiliki sesuatu yang membuktikan mereka adalah pengguna dikonfirmasi.

- Synchronous dynamic token
- Asynchronous dynamic token

Type 3 authentication: something you are

Otentikasi ini yang menggunakan karakteristik fisik sebagai sarana identifikasi atau otentikasi. Biometrics dapat digunakan untuk membentuk identitas atau untuk otentikasi.

**TECHNOLOGIES ACCESS CONTROL**

Beberapa teknologi yang digunakan untuk implementasi akses kontrol.

- Single sign-on
- Federated identity management
- Kerberos
- SESAME

**MENILAI ACCESS CONTROL**

proses yang ada untuk menilai efektivitas pengendalian akses. Tes dengan lingkup sempit meliputi tes penetrasi, penilaian kerentanan, dan keamanan audit.

Pengujian penetrasi

Sebuah tester penetrasi adalah hacker topi putih yang menerima otorisasi untuk mencoba masuk ke perimeter fisik atau elektronik organisasi

Pengujian kerentanan

Kerentanan pemindaian scan jaringan atau sistem untuk daftar kerentanan yang telah ditetapkan seperti sistem misconfiguration, usang perangkat lunak, atau kurangnya patch.

Audit keamanan

Sebuah audit keamanan adalah tes terhadap standar diterbitkan. Organisasi dapat diaudit untuk PCI-DSS kepatuhan. Penilaian keamanan adalah pendekatan holistik untuk menilai efektivitas akses control. Alih-alih mencari sempit di tes penetrasi atau penilaian kerentanan, penilaian keamanan memiliki lingkup yang lebih luas.

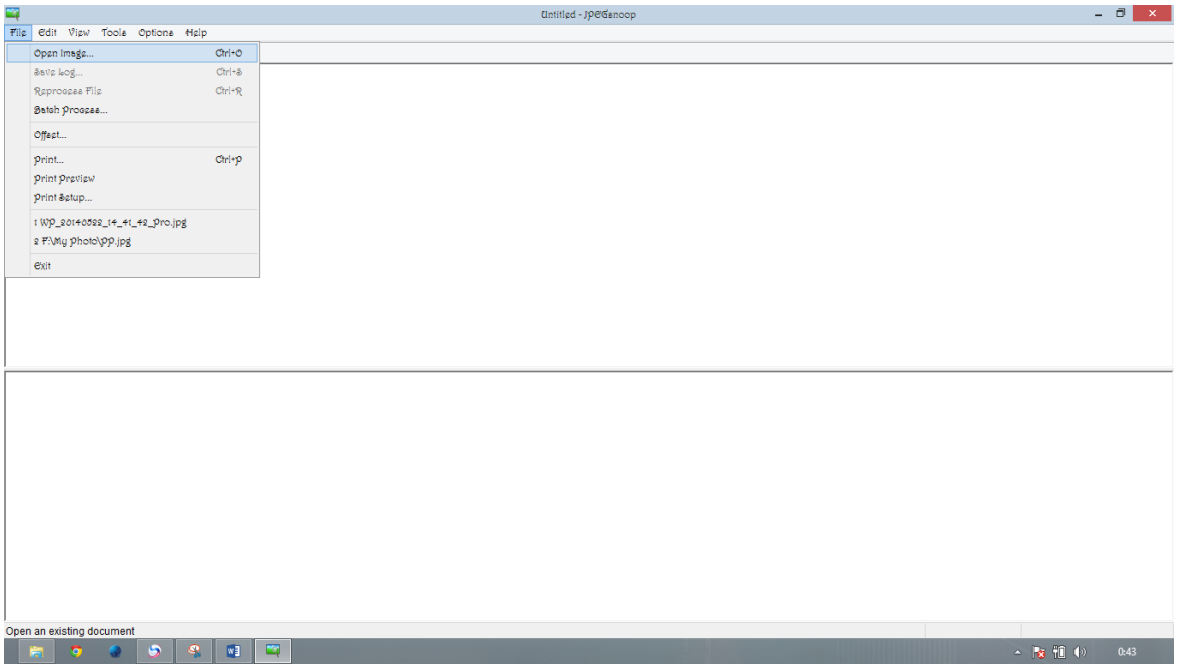
Cari software atau tools pendukung keamanan informasi kemudian cobalah fungsional software tersebut untuk menangani kasus tertentu. Buatlah step by step yang terdiri dari screenshot, keterangan gambar, dan analisis. Misalnya penggunaan wireshark dalam melakukan analisis paket data jaringan (pcap file), penggunaan ftk forensic untuk mengetahui file steganografi, dan lain sebagainya. Review software boleh sama, akan tetapi kasusnya harus berbeda dengan temen-temennya.

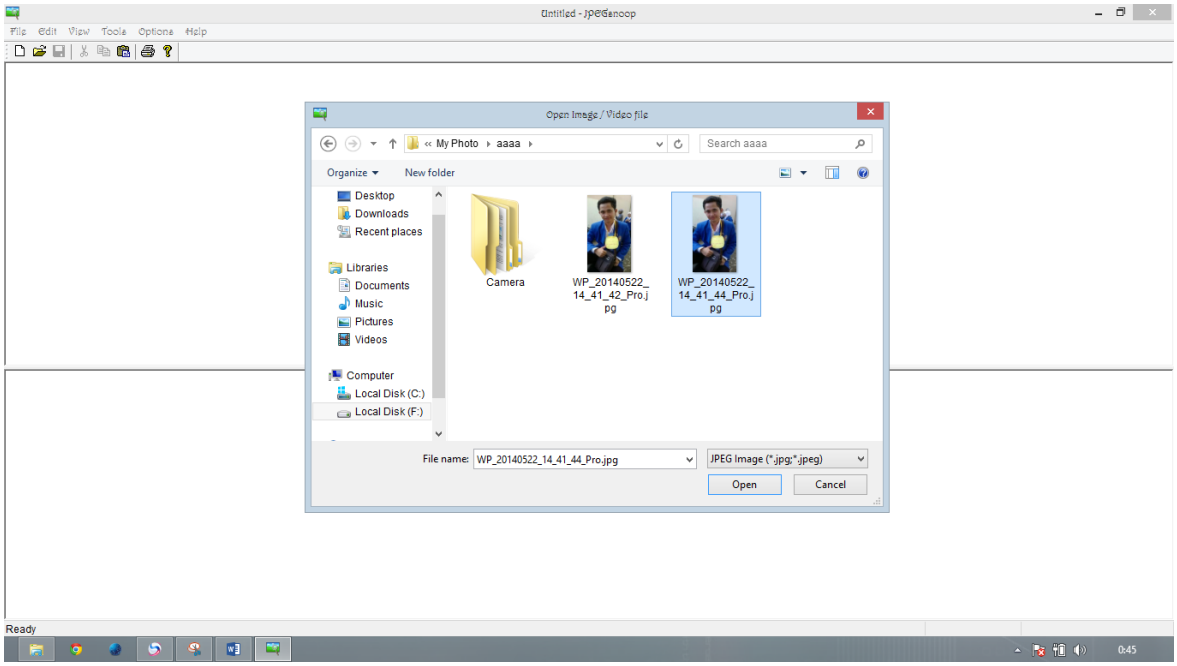
## 2. Step by step penggunaan JPEGsnop untuk membedakan foto asli dan palsu.

Langkah 1

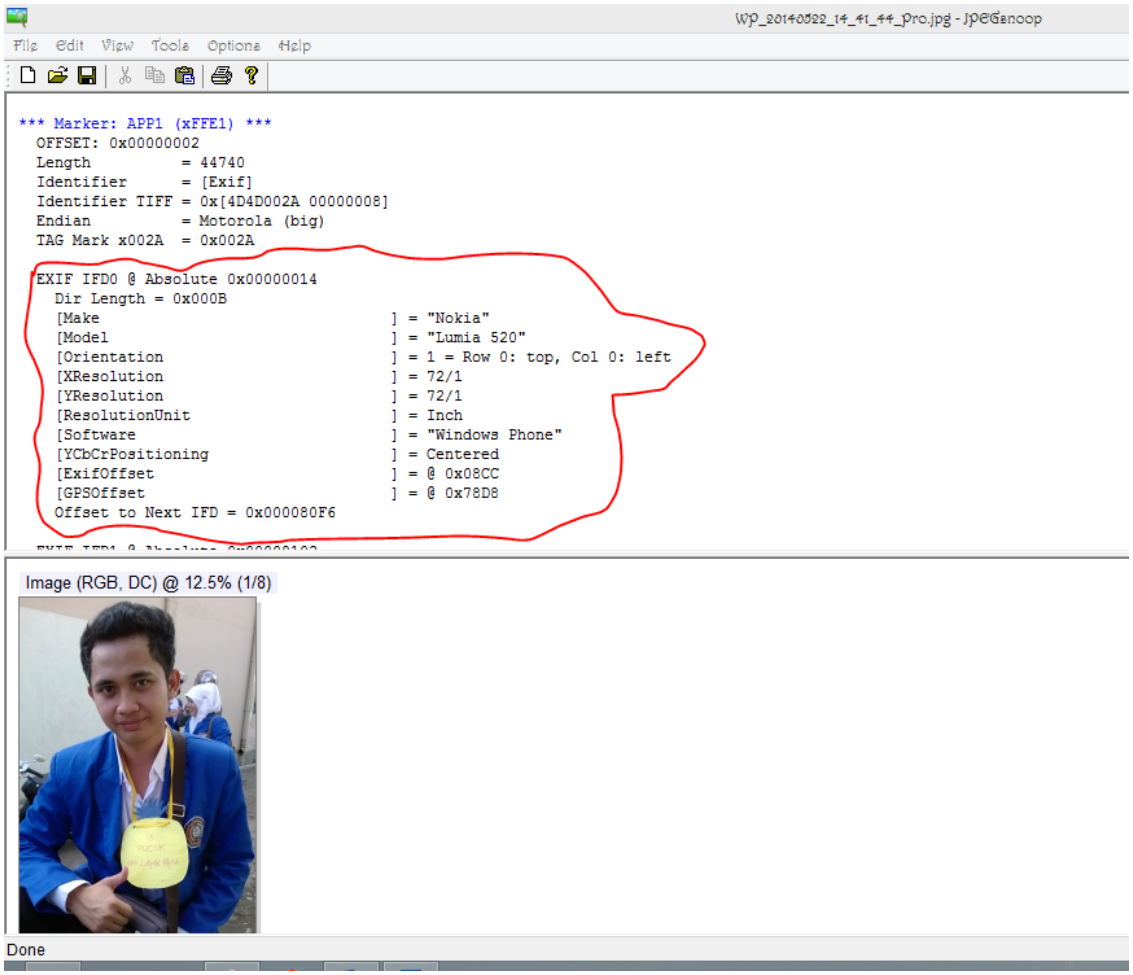
Buka aplikasi JPEGsnop

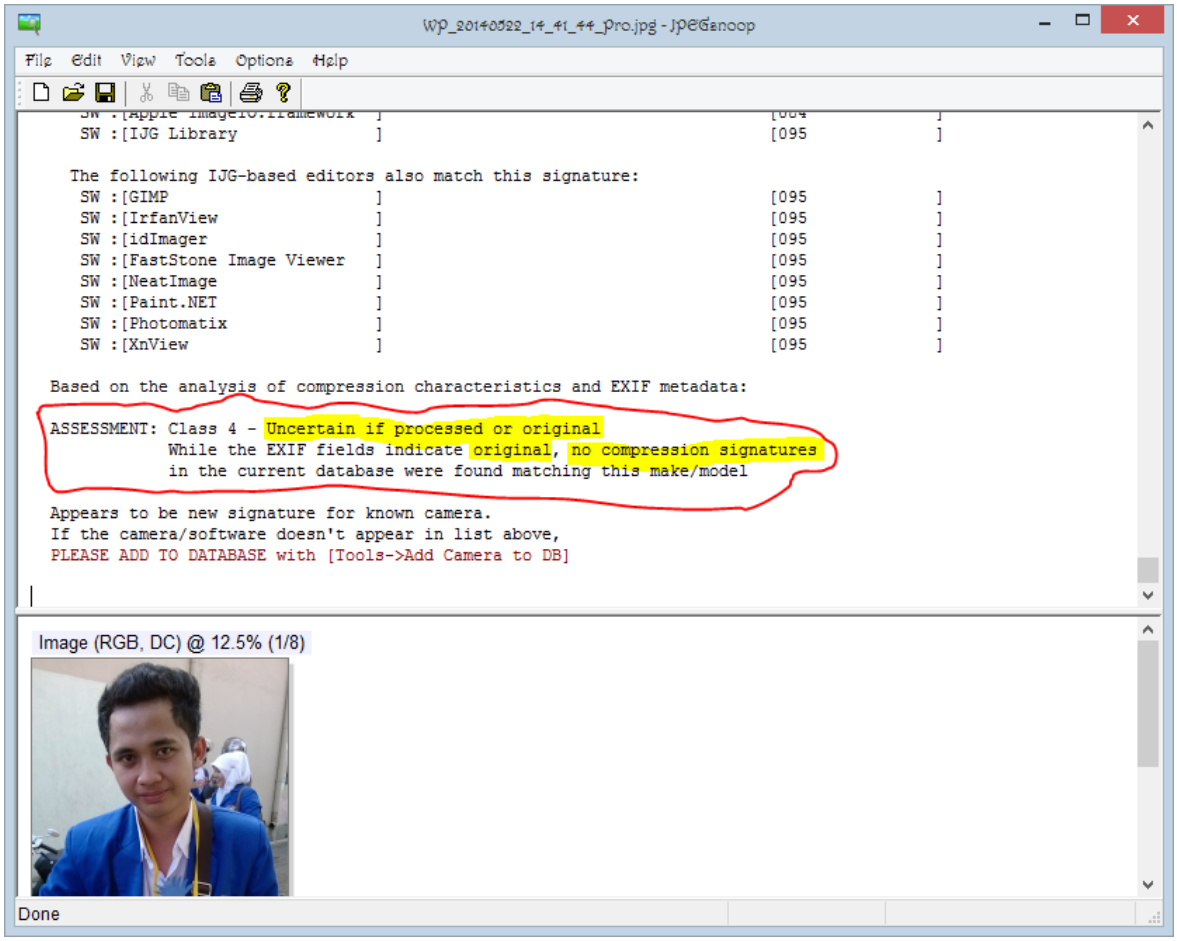

2. Setelah terbuka. Buka foto yang mau di ujicoba.






3. Perhatikan Kode seperti yang ada di gambar

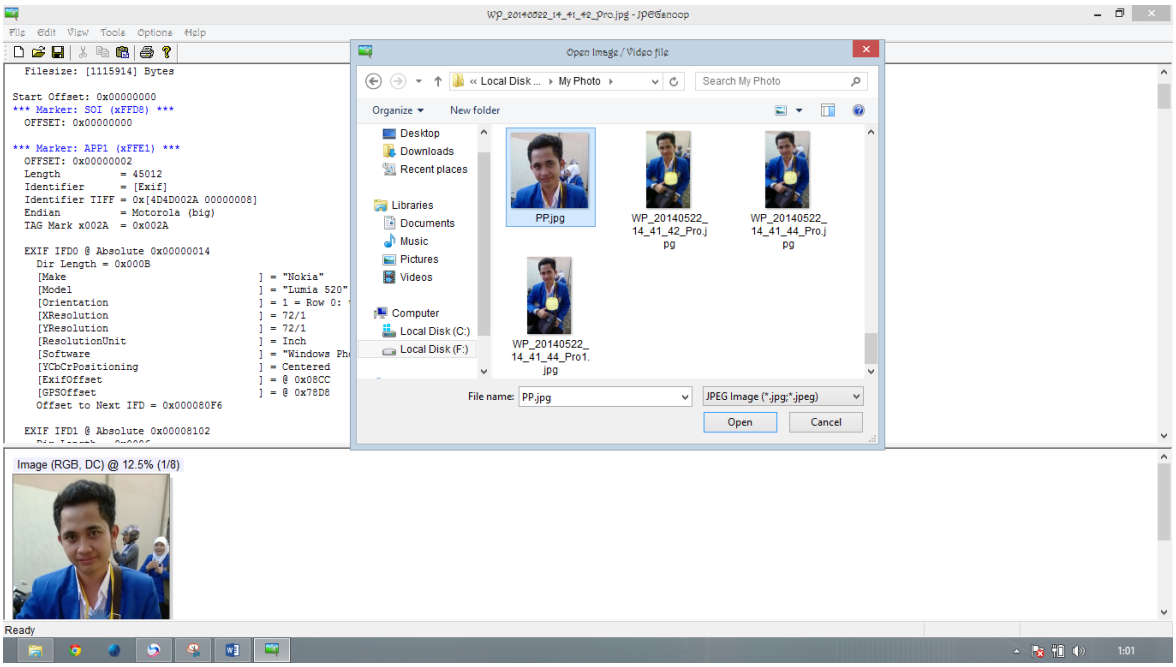


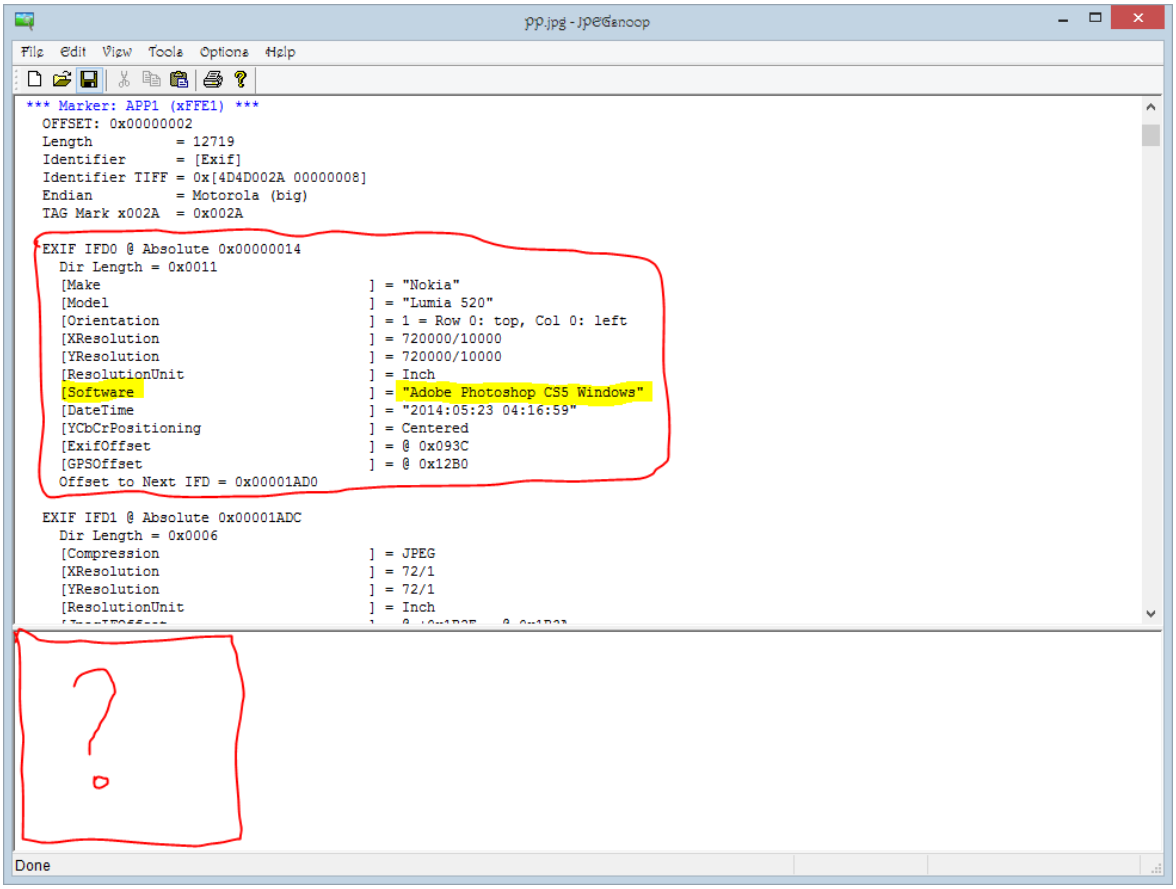



Bisa disimpulkan bahwa foto di atas adalah asli, bisa dilihat dalam kotak merah bahwa foto tersebut original(asli)

Untuk selanjutnya kita bandingkan dengan foto yang sudah di edit.

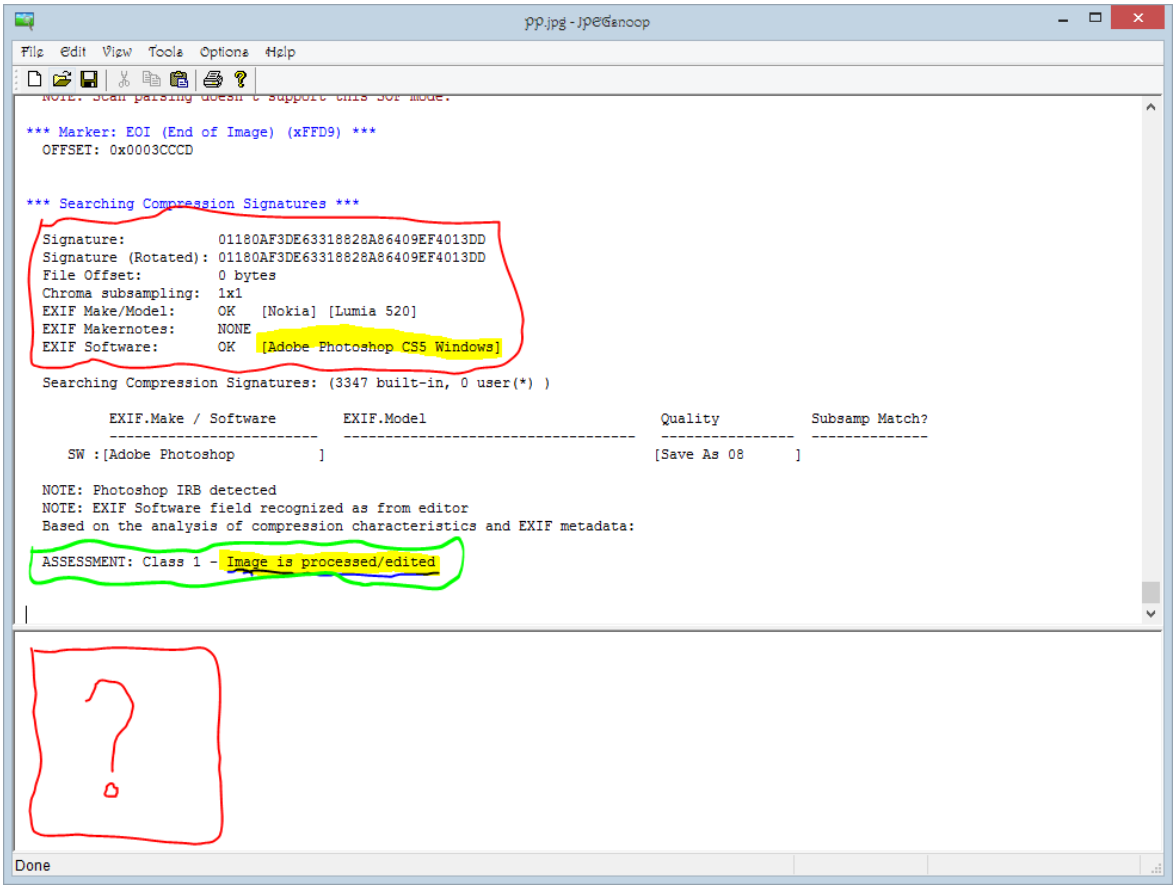
1. Buka foto yang akan kita uji.(ulangi langkah ke-2 di atas)






Dari data di atas sudah terlihat degan jelas bahwa foto tersebut sudah pernah di edit(yang saya tandai kuning) menggunakan “Adobe Photoshop CS5 Windows”.

Dan Preview fotonyapun tidak muncul yang saya kasi tanda (tanya). Dapat dibandingkan dengan foto asli yang diatas.




Aplikasi tersebut sudah menyimpulkan bahwa foto tersebut sudah pernah di edit(kotak hijau dan garis bawah biru).

Aplikasi tersebut sangat berguna, karena pada zaman sekarang banyak foto-foto editan yang dapat menjatuhkan hargadiri seseorang, dari aplikasi ini kita dapat membuktikan bahwa foto tersebut asli atau palsu.