KEAMANAN JARINGAN KOMPUTER

TOOLS FORENSIK DART UNTUK MELIHAT KEASLIAN SEBUAH GAMBAR

M Nizal

(09011181419025)

FAKULTAS ILMU KOMPUTER

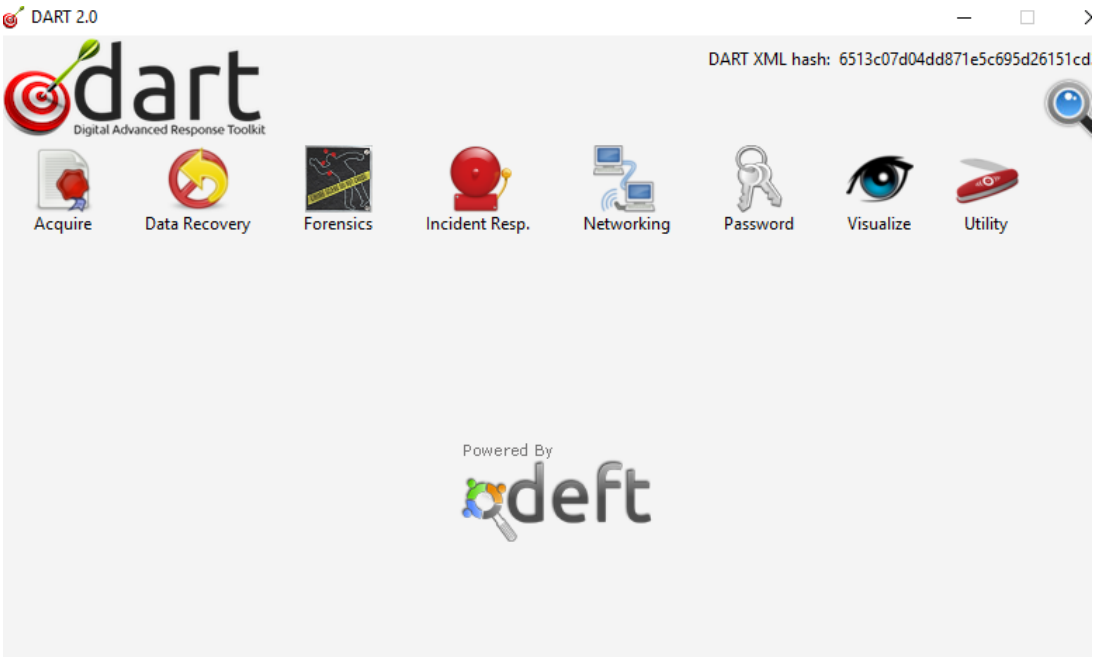
JURUSAN SISTEM KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

TOOLS FORENSIK DART UNTUK MELIHAT KEASLIAN SEBUAH GAMBAR

Pada tugas forensik kali ini saya menggunakan tools forensik DART dimana tools ini dapat di download secara gratis di internet, berikut tampilan dari forensik DART



Dilihat dari tampilan forensik DART terdapat berbagai tools seperti Acquire, Data Recovery, Forensics, Networking, Password, Visualize, dan Utility. Tetapi dari berbagai tools diatas saya mengambil contoh dari Tools JPEGSNOOP yang digunakan untuk melihat keaslian dari sebuah foto berupa metadata dari sebuah foto tersebut seperti contoh dari mana foto tersebut serta bisa melihat ASSEMENT dari foto tersebut yang terbagi dalam beberapa CLASS untuk melihat foto tersebut asli atau sudah di edit .

Berikut jenis class dari beberapa foto

- Class 1 : File gambar bisa dipastikan pernah diedit.
- Class 2 : File kemungkinan besar pernah diedit.
- Class 3 : Kemungkinan besar asli.
- Class 4 : Gambar bisa dianggap asli.

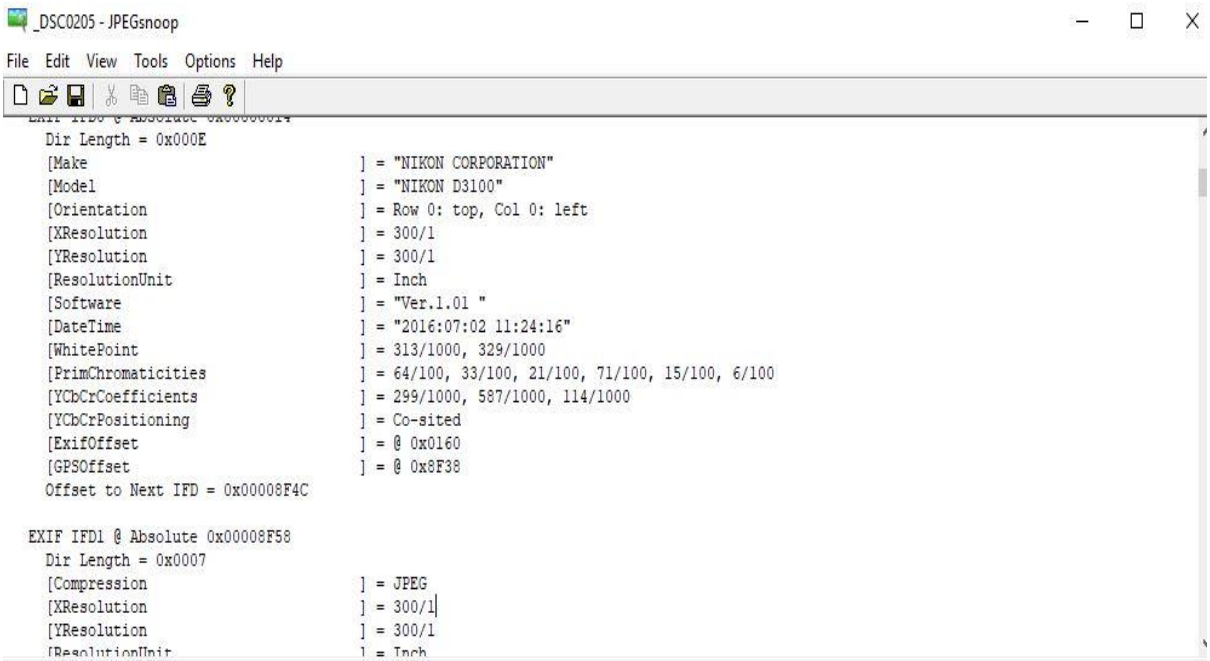
Setelah melakukan penjelasan tentang tools yang saya gunakan, disini saya melakukan percobaan untuk melihat keaslian dari sebuah foto dimana untuk percobaan terdapat 2 foto

dimana foto pertama untuk foto asli yang belum di edit serta foto kedua foto yang saya edit menggunakan photoshop, berikut contoh percobaan yang masih dalam keadaan asli atau tanpa hasil editan.

FOTO ASLI

Berikut hasil forensik menggunakan Tools Forensik DART

Keterangan dari hasil forensik ini dapat dilihat tampilan di atas terdapat fillname, filesize dari foto tersebut.



```
_DSC0205 - JPEGsnoop
File  Edit  View  Tools  Options  Help

   Dir Length = 0x000E
   [Make                          ] = "NIKON CORPORATION"
   [Model                         ] = "NIKON D3100"
   [Orientation                   ] = Row 0: top, Col 0: left
   [XResolution                   ] = 300/1
   [YResolution                   ] = 300/1
   [ResolutionUnit                ] = Inch
   [Software                      ] = "Ver.1.01 "
   [DateTime                      ] = "2016:07:02 11:24:16"
   [WhitePoint                    ] = 313/1000, 329/1000
   [PrimChromaticities            ] = 64/100, 33/100, 21/100, 71/100, 15/100, 6/100
   [YCbCrCoefficients             ] = 299/1000, 587/1000, 114/1000
   [YCbCrPositioning              ] = Co-sited
   [ExifOffset                    ] = @ 0x0160
   [GPSOffset                     ] = @ 0x8F38
   Offset to Next IFD = 0x00008F4C

 EXIF IFD1 @ Absolute 0x00008F58
   Dir Length = 0x0007
   [Compression                   ] = JPEG
   [XResolution                   ] = 300/1
   [YResolution                   ] = 300/1
   [ResolutionUnit                ] = Inch
```

Keterangan dari hasil forensik image tersebut terdapat foto diambil menggunakan kamera NIKON dan ada model dari kamera tersebut yaitu NIKON type D3100 serta terdapat tanggal pengambilan foto tersebut.

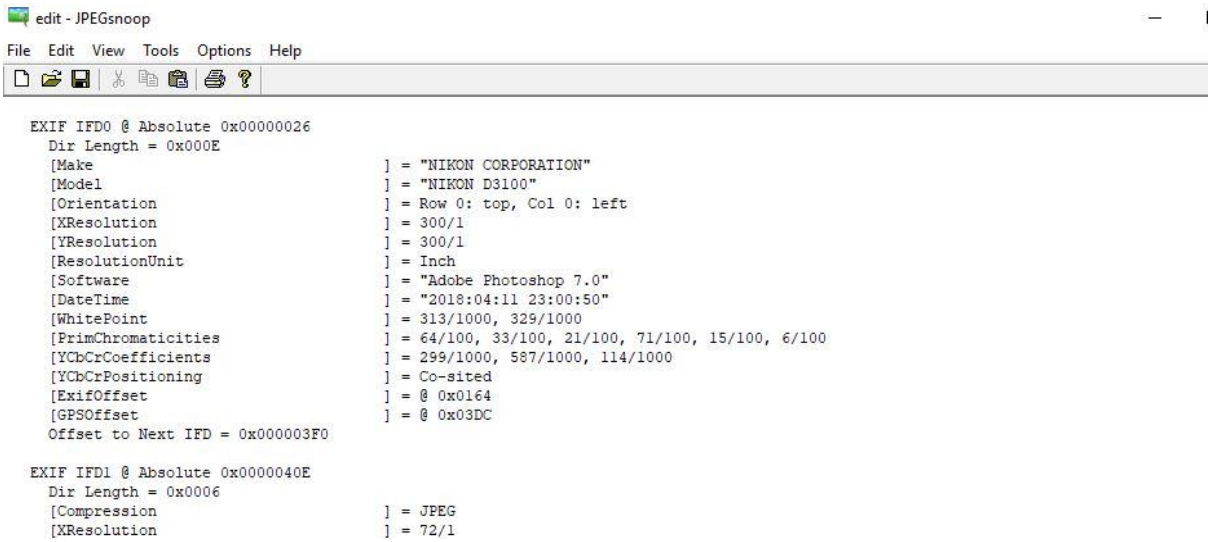
```
   CAM:[NIKON                ] [NIKON D2X                    ] [FINE          ] Yes
   CAM:[NIKON                ] [NIKON D300                   ] [FINE          ] Yes
   CAM:[NIKON                ] [NIKON D40                    ] [FINE          ] Yes
   CAM:[NIKON                ] [NIKON D40X                   ] [FINE          ] Yes
   CAM:[NIKON                ] [NIKON D50                    ] [FINE          ] Yes
   CAM:[NIKON                ] [NIKON D70                    ] [FINE          ] Yes
   CAM:[NIKON                ] [NIKON D70s                   ] [FINE          ] Yes
   CAM:[NIKON                ] [NIKON D80                    ] [FINE          ] Yes
   CAM:[Panasonic            ] [DMC-FX01                     ] [              ] Yes
   CAM:[Panasonic            ] [DMC-LX2                      ] [              ] Yes
   CAM:[Panasonic            ] [DMC-TZ1                      ] [              ] Yes

 Based on the analysis of compression characteristics and EXIF metadata:

 ASSESSMENT: Class 4 - Uncertain if processed or original
             While the EXIF fields indicate original, no compression signatures
             in the current database were found matching this make/model

 Appears to be new signature for known camera.
 If the camera/software doesn't appear in list above,
 PLEASE ADD TO DATABASE with [Tools->Add Camera to DB]
```

Keterangan dari hasil forensik diatas terdapat hasil ASSEMENT CLASS dari foto dimana foto tersebut terdapat pada Class 4, dilihat dari penjelasan sebelumnya bahwa jika sebuah foto tersebut berada di Class 4 berarti foto tersebut masih dalam keadaan asli atau belum pernah di edit sekali pun.

Pada percobaan kedua disini saya melakukan percobaan mmenggunakan foto yang sama tetapi telah saya edit menggunakan ADOBE PHOTOSHOP berikut foto yang telah saya edit.

FOTO YANG TELAH DI EDIT

Foto diatas kalo dilihat secara kasat mata tidak memiliki perbuhaan signifikan karena saya hanya melakukan pengeditan berupa mengcrop dari foto tersebut. Untuk melihat hasil forensik dari gambar yang saya edit akan saya tampilkan dibawah ini.



Dari hasil tools forensik DART diatas bahwa dapat dilihat dibagian software terdapat tulisan “Adobe Photoshop 7.0”. diamana itu merupakan software yang saya gunakan untuk melakukan pengeditan dari foto tersebut serta dapat dilihat jam dari saya melakukan pengeditan tersebut.

```
*** Marker: APP13 (xFFED) ***
  OFFSET: 0x00003BA2
  length          = 15642
  Identifier      = [Photoshop 3.0]
    8BIM: [0x0425] Name=[] Len=[0x0010]
    8BIM: [0x03ED] Name=[] Len=[0x0010]
    8BIM: [0x0426] Name=[] Len=[0x000E]
    8BIM: [0x040D] Name=[] Len=[0x0004]
    8BIM: [0x0419] Name=[] Len=[0x0004]
    8BIM: [0x03F3] Name=[] Len=[0x0009]
    8BIM: [0x040A] Name=[] Len=[0x0001]
    8BIM: [0x2710] Name=[] Len=[0x000A]
    8BIM: [0x03F5] Name=[] Len=[0x0048]
    8BIM: [0x03F8] Name=[] Len=[0x0070]
    8BIM: [0x0400] Name=[] Len=[0x0002]
    8BIM: [0x0402] Name=[] Len=[0x0004]
    8BIM: [0x0408] Name=[] Len=[0x0010]
    8BIM: [0x041E] Name=[] Len=[0x0004]
    8BIM: [0x041A] Name=[] Len=[0x0345]
    8BIM: [0x0411] Name=[] Len=[0x0001]
    8BIM: [0x0414] Name=[] Len=[0x0004]
```

Tampilan ini merupakan detail dari Marker APP13 atau hasil dari tools forensik DART untuk melihat software mana yang terindtefikasi melakukan pengeditan dari foto tersebut .

Seperti pada keterangan sebelumnya ini merupakan hasil forensik tools DART dimana terdapat hasil ASSEMENT CLASS dari foto dimana foto tersebut yang membedakan dari keterangan sebelumnya foto ini terdapat pada Class 1, dilihat dari penjelasan sebelumnya bahwa jika sebuah foto tersebut berada di Class 1 berarti foto tersebut sudah dipastikan telah di edit walaupun sedikitpun kita mengedit dari foto tersebut.

Kesimpulan dari forensik tools DART JPEGSNOP ini sekecil proses pengeditan jika di teliti menggunakan tools ini akan membaca bahwa foto tersebut telah dilakukan proses pengeditan, dimana pada tools ini bisa dilihat menggunakan aplikasi apa pengeditan nya serta jam dan tanggal pada hasil pengeditan tersebut. Serta pada tools ini bisa melihat keterangan pada foto asli menggunakan kamera apa pengambilan foto tersebut serta tanggal dan jam pengambilan foto tersebut bahkan tersedia di tools JPEGSNOP ini.