TUGAS

KEAMANAN JARINGAN KOMPUTER

Nama : **Randa Fratelli Junaedi**

NIM : **0901118419006**

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

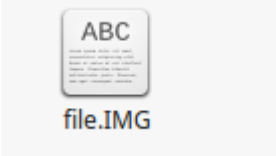
UNIVERSITAS SRIWIJAYA

2018

TUGAS FORENSIK PADA SUATU FILE IMAGE

Komputer forensik dapat diartikan sebagai proses pengumpulan dan analisis data dari berbagai sumber daya komputer yang mencakup sistem komputer, baik itu jaringan komputer, jalur komunikasi, dan berbagai media penyimpanan yang layak untuk diajukan dalam sidang pengadilan. Secara singkat tujuan dari komputer forensik adalah untuk menjabarkan keadaan terkini dari suatu catatan digital. Istilah catatan digital bisa mencakup sebuah sistem komputer, media penyimpanan (seperti flash disk, hard disk, atau juga CD-ROM), sebuah dokumen elektronik (misalnya sebuah pesan email atau gambar JPEG), atau bahkan sederetan paket yang berpindah dalam jaringan komputer.

Pada tahap ini saya akan mengeforensikan suatu file image, dimana pada saat melakukan pengecekan awal jenis file yang ada pada file image.img menggunakan utilitas file, berikut hasil pengecekan file image.img




```
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK $ file File.Img
File.Img: Zip archive data, at least v1.0 to extract
```

hasil dari pengecekan tersebut menghasil bahwa file tersebut merupakan jenis file dari archive data Zip dan dimana isi dari file tersebut memiliki 3 file :

```
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK $ unzip File.Img
Archive:  File.Img
 extracting: BENAR.7z
  inflating: file
  inflating: new megapro.jpg
```

- BENAR.7z
- File
- New megapro.jpg

Tahap selanjutnya saya akan mengidentifikasi apa maksud dari file New megapro.jpg

```
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK $ file new\ megapro.jpg
new megapro.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, se
gment length 16, progressive, precision 8, 1080x810, frames 3
```

dalam pengecekan jenis file dapat dihasilkan bahwa file tersebut memang benar berjenis file jpg ((Gambar).

Untuk mencari informasi lebih lanjut, disini saya menggunakan strings, dimana hasil dari file tersebut mendapatkan informasi bahwa “siapa pemilik kendaraan pada gambar file tersebut,

```
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK $ strings new\ megapro.jpg
```

```
$l!WEbU
kap?
 Permasalahan : Siapakah Pemilik Motor NewMegapro 2011 ini ?
```

Gambar file new megapro.jpg

Pada tahap ini saya akan menuju file BENAR.7z, pada saat untuk mengekstrak file tersebut. Ternyata memiliki berupa password untuk mengakses file tersebut. Disini saya melewatkan tahap ini untuk menuju tahap pencarian sebuah password file ini.

```
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK $ file BENAR.7z
BENAR.7z: 7-zip archive data, version 0.3
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK $ 7z x BENAR.7z

7-Zip [64] 9.20  Copyright (c) 1999-2010 Igor Pavlov  2010-11-18
p7zip Version 9.20 (locale=id_ID.UTF-8,Utf16=on,HugeFiles=on,4 CPUs)

Processing archive: BENAR.7z


Enter password (will not be echoed) :
Extracting  Flag     Data Error in encrypted file. Wrong password?
Extracting  data.jpg     Data Error in encrypted file. Wrong password?

Sub items Errors: 2
```

Pada tahap mengidentifikasi sebuah File yang hanya bernama “file” tanpa ada jenis dari file tersebut, saya melakukan pencarian jenis file tersebut dengan menggunakan utilitas file seperti tahap pertama.

```
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK $ file file
file: data
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK $ binwalk file

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
1             0x1             JPEG image data, EXIF standard
13            0xD             TIFF image data, big-endian, offset of first image di
rectory: 8

dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK $ foremost file
Processing: file
|*|
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK $ ls
BENAR.7z  data.jpg  file  File.Img  Flag  new megapro.jpg  output
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK $ cd output/
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK/output $ ls
audit.txt  jpg
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK/output $ file audit.txt
audit.txt: ASCII text
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK/output $ cd jpg/
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK/output/jpg $ ls
00000000.jpg
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK/output/jpg $ open 00000000.jpg
```

Bahwa dapat dihasilkan hanya berupa data, pada tahap ini tidak dapat petunjuk apa pun dalam pencarian identifikasi file tersebut dengan utilitas file, untuk lebih mengetahui apa maksud dari file tersebut, saya menggunakan sebuah tools binwalk.

Binwalk adalah alat untuk mencari gambar biner yang diberikan untuk file yang disematkan dan kode yang dapat dieksekusi. Secara khusus, dirancang untuk mengidentifikasi file dan kode yang tertanam di dalam suatu file.

Dengan binwalk file tersebut merupakan suatu file jpeg dan untuk mendapatkan isi dalam file tersebut saya menggunakan tool foremost, dan bahwa isi file tersebut berupa gambar yang berisi tulisan “Menujuskon” dari analisa, kemungkinan tulisan dalam gambar tersbut berupa password untuk membuka file BENAR.7z.

Foremost adalah sebuah tools Linux yang digunakan untuk melakukan pemeriksaan forensik untuk *recovery files* berdasarkan pada header, footer dan internal struktur data.

Setelah diekstrak, file tersebut memiliki 2 file dimana berupa :

- File Flag
- File data.jpg

```
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK $ 7z x BENAR.7z

7-Zip [64] 9.20  Copyright (c) 1999-2010 Igor Pavlov  2010-11-18
p7zip Version 9.20 (locale=id_ID.UTF-8,Utf16=on,HugeFiles=on,4 CPUs)

Processing archive: BENAR.7z


Enter password (will not be echoed) :
Extracting  Flag
Extracting  data.jpg

Everything is Ok

Files: 2
Size:       2427592
Compressed: 1871338
```

Gambar data.jpg, disini saya belum mengetahui siapa dari 3 orang tersebut pemilik sepeda motor tersebut.

Untuk lebih mengetahui informasi yang sebenarnya saya melanjutkan siapa sebenarnya dari 3 orang yang ada pada gambar data.jpg tersebut pemilik sepeda motor sebenarnya. Dengan mengidentifikasikan file yang bernama Flag ini.

```
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK $ file Flag
Flag: ASCII text, with very long lines, with no line terminators
dha_fra@Anonymous ~/Unduhan/BENAR/FORENSIK $ cat Flag | base64 -d > data1
```

Dari pencarian jenis file flag dalam hasil utilitas file, berupa sebuah berkas dalam enkripsi base64. Dan didecode merupakn proses mengembalikan chiper text ke dalam plain text yang sebelumnya di encode.

Data1 : hasil dari file Flag dimana dari analisa saya, orang pada gambar ini merupakan pemilik motor new megapro tersebut.