Tugas

Keamanan Jaringan Komputer

Disusun Oleh :

Nama : Sigit Wijaya Pramono

NIM : 09011181419012

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

Forensic Pada File JPG Dalam ZIP Yang Terkunci

Pada tugas ini membuat sebuah analisis data forensic dengan jenis data yang beragam, yang bertujuan mencari dan melihat informasi dari sebuah data forensic yang menjadi objek. Jenis data yang digunakan dalam tugas ini yaitu dalam bentuk JPG, dimana file JPG tersebut tersimpan dan terkunci dalam betuk ZIP. Maka rules yang dilakukan pertama kali yaitu mencari kunci/password dari file ZIP tersebut unutk dapat mendapatkan dan mengolah file JPG di dalamnya.

Berikut merupakan langkah-langkah dalam melakukan tugas ini :

1. Pertama kali memproses file ZIP yang mana file tersebut terkunci sebuah password, maka harus melakukan cracking password terlebih dahulu.
   - Menggunakan command `fcrackzip -l 3-5 -c aA1 -u` *(nama file ZIP)*

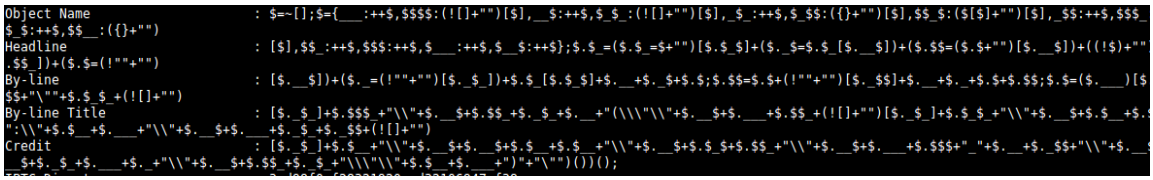
     ```
     massgt@SK ~/Downloads/KJK $ fcrackzip -l 3-5 -c aA1 -u mautau.zip


     PASSWORD FOUND!!!!: pw == CaeG
     massgt@SK ~/Downloads/KJK $
     ```

     Seperti gambar diatas dengan menggunakan command tersebut kita akan mendapatkan password, dari hasil tersebut didapatkan password *CaeG*.
2. Setelah mendapatkan password, selanjutnya yaitu mengekstrak file ZIP guna mendapatkan file JPG yang dimaksud.
   - Menggunakan command `unzip` *(nama file ZIP)*

     ```
     massgt@SK ~/Downloads/KJK $ unzip mautau.zip
     Archive:  mautau.zip
     [mautau.zip] mautau.jpg password:
       inflating: mautau.jpg
     massgt@SK ~/Downloads/KJK $
     ```
3. Selanjutnya setelah melakukan ekstrak file ZIP, buka folder yang di ekstrak dan terdapat file JPG yang bernama mautau.jpg. Lalu kita melihat *EXIF* yang berarti metadata/informasi yang terdapat dalam sebuah foto atau gambar.
   - Menggunakan command `exiftool` *(nama file JPG)*

     ```
     massgt@SK ~/Downloads/KJK $ exiftool mautau.jpg
     ExifTool Version Number         : 10.10
     File Name                       : mautau.jpg
     Directory                       : .
     File Size                       : 33 kB
     File Modification Date/Time     : 2014:10:13 14:38:30+07:00
     File Access Date/Time           : 2014:10:13 14:38:30+07:00
     File Inode Change Date/Time     : 2018:04:10 00:00:05+07:00
     File Permissions                : rw-rw-r--
     File Type                       : JPEG
     File Type Extension             : jpg
     MIME Type                       : image/jpeg
     JFIF Version                    : 1.02
     Exif Byte Order                 : Big-endian (Motorola, MM)
     Image Description               : Hayo Di Mana Hayo X___X
     Make                            : Camera Kodak
     Camera Model Name               : Nokia 3315
     Orientation                     : Horizontal (normal)
     X Resolution                    : 96
     Y Resolution                    : 96
     Resolution Unit                 : inches
     Software                        : Adobe Photoshop CS3 Windows
     Modify Date                     : 2012:12:28 16:33:00
     ```

Dari gambar diatas terlihat sebagian dari hasil exiftool dari hasil tersebut kita menggunakan beberapa data didalam nya, antara mail seperti dibawah ini :



Seperti gambar diatas, isi potongan baris kode dari object name, headline, by-line, by-line title, credit, di edit / di gabung menjadi satu baris seperti berikut ini :

$=~[];$={___:++$,$$$$:(![]+"")[$],__$:++$,$_$_:(![]+"")[$],_$_:++$,$_$$:({}+"")[$],$$_$:($[$]+"")[$],_$$:++$,$$$_:(!""+"")[$],$__:++$,$_$:++$,$$__:({}+"")[$],$$_:++$,$$$:++$,$___:++$,$__$:++$};$.$_=($.$_=$+"")[$.$_$]+($._$=$.$_[$.__$])+($.$$=($.$+"")[$.__$])+((!$)+"")[$._$$]+($.__=$.$_[$.$$_])+($.$=(!""+"")[$.__$])+($._=(!""+"")[$._$_])+$.$_[$.$_$]+$.__+$._$+$.$;$.$$=$.$+(!""+"")[$._$$]+$.__+$._+$.$+$.$$;$.$=($.___)[$.$_][$.$_];$.$($.$($.$$+"\""+$.$_$_+(![]+"")[$._$_]+$.$$$_+"\\"+$.__$+$.$$_+$._$_+$.__+"(\\\"\\"+$.__$+$.___+$.$$_+(![]+"")[$._$_]+$.$_$_+"\\"+$.__$+$.$$_+$._$_+$.__+"\\"+$.__$+$.___+":\\"+$.$__+$.___+"\\"+$.__$+$.___+$._$_+$._$$+(![]+"")[$._$_]+$.$__+"\\"+$.__$+$.__$+$.$__+$.$__+"\\"+$.__$+$.$_$+$.$$_+"\\"+$.__$+$.___+$.$$$+"_"+$.__+$._$$+"\\"+$.__$+$.$_$+$.$_$+"\\"+$.__$+$._$_+$.___+$._+"\\"+$.__$+$.$$_+$._$_+"\\\"\\"+$.$__+$._+")"+"\"")()();

4. Setelah mendapat kan script kode nya yang telah digabung, selanjutnya Ambil beberapa potongan baris dan paste di google dengan keyword "$=~[];$={___:++$,$$$$:(![]+"") decode", didapatkan link: http://utf-8.jp/public/jjencode.html. Paste pada kolom bawah dan klik Eval.

5. Setelah masuk ke link yang terdapat pada gambar diatas, dan sudah memasukkan baris kode yang telah digabungkan tadi maka akan mendapatkan hasil informasi yaitu *flag* dengan isi *B3l4L4nG_t3mPur* seperti terlihat pada gambar dibawah :