CAPTURE THE FLAG
WRITE UP

Dibuat oleh :
PORT80
(Johan Wahyudi)

COMNETS CTF SEASON 2
2015

CHALLENGE **: *FORENSIC***
CASE **: *FORENSIC01 - "Saint Epic"***
FLAG **: COMNETS{InD0N3s1Aku_jAY4}**

1. Executive Summary

Image Steganography
Tools : Stepic

2. Technical Report

Pada soal ini, kita di beri sebuah file yg isi di dalamnya adalah file gambar, tidak ada yang aneh dari file gambar tersebut, baik dari tampilan maupun dari meta datanya, karena ini satu-satunya file soal yg dikasih, maka kemungkinan besar petunjuk ada di file gambar ini, sekarang kita coba dengan teknik steganografi...

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia
Pada soal ini kita di berikan sebuah gambar, tidak ada keanehan dari file tersebut, baik dari tampilan maupun dari metadata-nya,

(Gambar : soal forensic01)

Stepic (Stegano Picture) adalah tools untuk unhide pesan yang tersembunyi pada sebuah gambar/image, ok kita coba..

Command : python stepic [options]

python stepic -i 1.png -d

Ket :

-i = input file

-d = decode, given an image, write out the hidden data file

3. Conclusion

Flag : COMNETS{InD0N3s1Aku_jAY4}

4. Reference

https://stepic.org/

CHALLENGE **: *Forensic***
CASE **: *Forensic03 - "Trololo Face"***
FLAG **: COMNETS{jaY4_bAy4}**

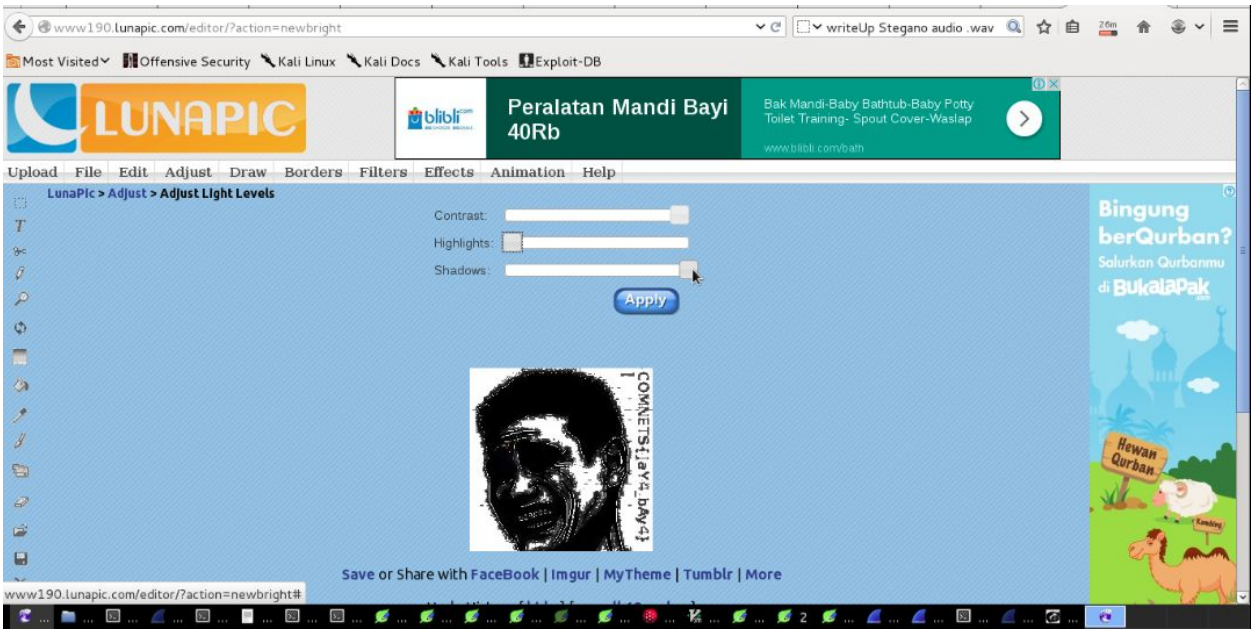
1. Executive Summary

Image Thresholding
Tools : GIMP, lunapic

2. Technical Report

Diberikan sebuah file gambar berekstensi tar.gz, setelah di buka ada file gambar, ini gambarnya

Tidak ada yang aneh dari metadata file gambar ini, karena hint dari soal ini adalah image threshold, sekarng kita coba threshold dulu image ini (apa itu threshold searching di google aja ya ^_^), saya pake tools online(http://lunapic.com), kita upload file gambarnya disana, sekarang kita coba mainkan panel editornya sampe karakter yang tersembunyi itu muncul..



Upss... Ada text yang mulai muncul, kita mainkan terus panelnya sampai textnya jelas..

3. Conclusion

Flag : COMNETS{jaY4_bAy4}

4. Reference

http://lunapic.com

CHALLENGE **: *FORENSIC***
CASE **: *FORENSIC04* - “Easy To Hide”**
FLAG **: COMNETS{Patriot_Bangsa}**

2. Executive Summary

Analisa Packet
Tools : XZ Compresser

5. Technical Report

Pada soal kali ini, filenya tidak ada ekstensi, kita lihat dulu tipe filenya menggunakan command : file <nama file>

```
File  Edit  View  Search  Terminal  Help
root@kali:/media/root/MY-LIB/HACKING/CTF/CTF ILKOM/CTF SESASON 2/FORENSIC/forensic04 (3)# file forensic04
forensic04: XZ compressed data
root@kali:/media/root/MY-LIB/HACKING/CTF/CTF ILKOM/CTF SESASON 2/FORENSIC/forensic04 (3)#
```

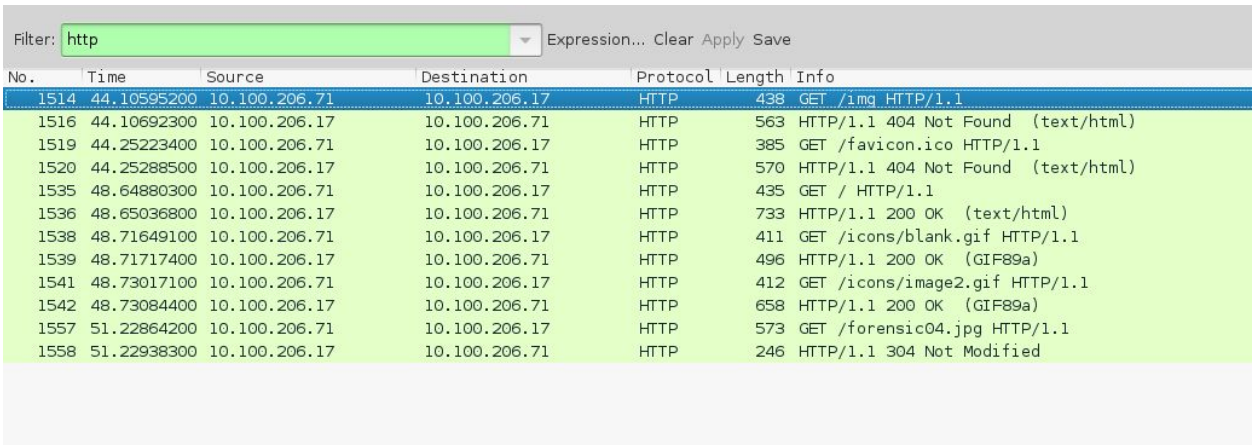
Ternyata file tersebut aslinya adalah file XZ compressed (di kompress dengan ekstensi XZ), ok kita coba decompress dulu filenya untuk melihat isi dari file tersebut,.

```
root@kali:/media/root/MY-LIB/HACKING/CTF/CTF ILKOM/CTF SESASON 2/FORENSIC/forensic04 (3)# mv forensic04 forensic04.xz
root@kali:/media/root/MY-LIB/HACKING/CTF/CTF ILKOM/CTF SESASON 2/FORENSIC/forensic04 (3)# ls
forensic04.xz
root@kali:/media/root/MY-LIB/HACKING/CTF/CTF ILKOM/CTF SESASON 2/FORENSIC/forensic04 (3)# xz -d forensic04.xz
root@kali:/media/root/MY-LIB/HACKING/CTF/CTF ILKOM/CTF SESASON 2/FORENSIC/forensic04 (3)# ls
forensic04
root@kali:/media/root/MY-LIB/HACKING/CTF/CTF ILKOM/CTF SESASON 2/FORENSIC/forensic04 (3)#
```

Setelah di decompress, ternyata hasilnya juga file yg tidak memiliki ekstensi juga, -,- , ok kita cek lagi type filenya..

```
root@kali:/media/root/MY-LIB/HACKING/CTF/CTF ILKOM/CTF SESASON 2/FORENSIC/forensic04 (3)# file forensic04
forensic04: pcap-ng capture file - version 1.0
root@kali:/media/root/MY-LIB/HACKING/CTF/CTF ILKOM/CTF SESASON 2/FORENSIC/forensic04 (3)#
```

Ternyata file pcap tohh.. Ok sekarang coba kita buka filenya menggunakan aplikasi wireshark atau tshark, sama saja, disini saya menggunakan wireshark, karena tshark menurut saya sulit untuk menganalisa paket sebanyak ini (ada 1500an paket yg capture), ok.. Untuk memudahkan kita menganalisa, coba kita filter, jadi yg di tampilkan hanya untuk paket protokol http (karena biasanya flagnya berada di paket protokol ini..



Filter: http — Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1514	44.10595200	10.100.206.71	10.100.206.17	HTTP	438	GET /img HTTP/1.1
1516	44.10692300	10.100.206.17	10.100.206.71	HTTP	563	HTTP/1.1 404 Not Found (text/html)
1519	44.25223400	10.100.206.71	10.100.206.17	HTTP	385	GET /favicon.ico HTTP/1.1
1520	44.25288500	10.100.206.17	10.100.206.71	HTTP	570	HTTP/1.1 404 Not Found (text/html)
1535	48.64880300	10.100.206.71	10.100.206.17	HTTP	435	GET / HTTP/1.1
1536	48.65036800	10.100.206.17	10.100.206.71	HTTP	733	HTTP/1.1 200 OK (text/html)
1538	48.71649100	10.100.206.71	10.100.206.17	HTTP	411	GET /icons/blank.gif HTTP/1.1
1539	48.71717400	10.100.206.17	10.100.206.71	HTTP	496	HTTP/1.1 200 OK (GIF89a)
1541	48.73017100	10.100.206.71	10.100.206.17	HTTP	412	GET /icons/image2.gif HTTP/1.1
1542	48.73084400	10.100.206.17	10.100.206.71	HTTP	658	HTTP/1.1 200 OK (GIF89a)
1557	51.22864200	10.100.206.71	10.100.206.17	HTTP	573	GET /forensic04.jpg HTTP/1.1
1558	51.22938300	10.100.206.17	10.100.206.71	HTTP	246	HTTP/1.1 304 Not Modified

Diatas adalah paket protokol http yg berhasil tertngkap, sekarang kita coba lihat isinya, dengan cara klik salah satu paket dan pilih > Follow TCP Stream,

$

```
GET /img HTTP/1.1
Host: 10.100.206.17:5123
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.85 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8

HTTP/1.1 404 Not Found
Date: Tue, 13 Oct 2015 03:57:04 GMT
Server: Apache/2.4.7 (Ubuntu)
Content-Length: 281
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /img was not found on this server.</p>
<hr>
<address>Apache/2.4.7 (Ubuntu) Server at 10.100.206.17 Port 5123</address>
</body></html>
GET /favicon.ico HTTP/1.1
Host: 10.100.206.17:5123
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.85 Safari/537.36
Accept: */*
Referer: http://10.100.206.17:5123/img
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8

HTTP/1.1 404 Not Found
Date: Tue, 13 Oct 2015 03:57:04 GMT
Server: Apache/2.4.7 (Ubuntu)
```

Bisa kita lihat file di atas, banyak sekali http headernya, sekarang kita ambil satu saja untuk kita tampilkan ke browser,

```
File  Edit  Search  Options  Help
HTTP/1.1 404 Not Found

Date: Tue, 13 Oct 2015 03:57:04 GMT

Server: Apache/2.4.7 (Ubuntu)

Content-Length: 281

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html; charset=iso-8859-1



<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /img was not found on this server.</p>
<hr>
<address>Apache/2.4.7 (Ubuntu) Server at 10.100.206.17 Port 5123</address>
</body></html>
```

Tampilan di browser

Bisa kita lihat diatas, direktori yg ingin diakses adalah direktori /img yg berada di alamat 10.100.206.17:5123 (port 5123) dan muncul peringatan not found.. Sekarang coba kita akses direktori tersebut dari browser (http://10.100.206.17:5123/img)..

(maaf saya tidak bisa menampilkan screenshot dari hasil pencarian, karena server lagi down ketika saya menulis ini :/),

Ternyata ada file di direktori http://10.100.206.17:5123/img.. Ini filenya :

Tidak ada yang aneh dari gambar diatas, coba kita lihat meta datanya dulu..

```
root@kali:/media/root/MY-LIB/HACKING/CTF/CTF ILKOM/CTF SESASON 2/FORENSIC/forensic04# exiftool forensic04.jpg
ExifTool Version Number         : 9.74
File Name                       : forensic04.jpg
Directory                       : .
File Size                       : 56 kB
File Modification Date/Time     : 2015:10:28 01:59:33+07:00
File Access Date/Time           : 2015:11:12 10:18:21+07:00
File Inode Change Date/Time     : 2015:10:28 10:40:43+07:00
File Permissions                : rw-------
File Type                       : JPEG
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Comment                         : Created with GIMP md5 "77a7c9d8d87a29cb23106315f537e5fd"
Image Width                     : 540
Image Height                    : 335
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
root@kali:/media/root/MY-LIB/HACKING/CTF/CTF ILKOM/CTF SESASON 2/FORENSIC/forensic04#
```

Di bagian coment ada text menarik.. “Created with GIMP md5 "77a7c9d8d87a29cb23106315f537e5fd"", sepertinya itu adalah encrypt md5, sekarang coba kita decrypt, disini saya menggunakan tools online untuk mendecrypt, (http://md5decrypt.net/en/)

6. Conclusion

Flag : **COMNETS{Patriot_Bangsa}**

7. Reference

http://md5decrypt.net/en/