HackLabs.id Weekly Mini CTF

Problem : Bu Tejo

Difficulty : Easy

ProbSetter : Aseng

Challenge ini diawali seperti challenge sebelum sebelumnya di mana kita diarahkan ke gdrive dari hacklabs.id dan dari situ kita dapat mengunduh file .zip bernama whatsapp.zip yang berisikan file png

Setelah memastikan bahwa file tersebut merupakan file gambar dengan extension png, menggunakan command *file* pada linux, saya mencoba melihat apakah terdapat file lain di dalam foto tersebut menggunakan *binwalk*

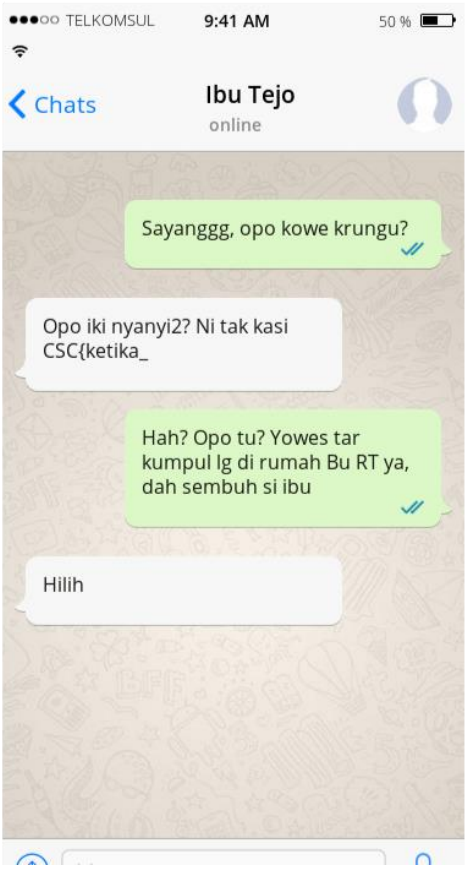
```
root@opacite:~# binwalk whatsapp1.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 391 x 734, 8-bit/color RGBA, non-interlaced
41            0x29            Zlib compressed data, default compression

root@opacite:~#
```

Dari foto di atas, dipastikan bahwa file tersebut hanya file png biasa hal ini karna Zlib compressed data, merupakan bawaan dari suatu file image dengan extension png

Kemudian saya mengecek metadata dari file whatsapp1.png tersebut menggunakan command *exiftool*

```
root@opacite:~# exiftool whatsapp1.png
ExifTool Version Number         : 12.06
File Name                       : whatsapp1.png
Directory                       : .
File Size                       : 143 kB
File Modification Date/Time     : 2020:09:18 13:01:22+07:00
File Access Date/Time           : 2020:09:25 20:33:23+07:00
File Inode Change Date/Time     : 2020:09:25 20:33:02+07:00
File Permissions                : rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 391
Image Height                    : 734
Bit Depth                       : 8
Color Type                      : RGB with Alpha
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Warning                         : [minor] Trailer data after PNG IEND chunk
Image Size                      : 391x734
Megapixels                      : 0.287
root@opacite:~#
```

Dari data yang didapatkan, saya tidak melihat sesuatu yang mencurigakan, saatnya membuka file tersebut



Dari file gambar tersebut, saya mendapatkan setengah dari flagnya, CSC{ketika_

Lalu saya terpikirkan untuk mengecek hex yang ada pada foto tersebut, menggunakan command *xxd*

```
root@opacite:~# xxd -u whatsapp1.png
```

```
00023be0: 0000 0049 454E 44AE 4260 8265 6D61 6B5F  ...IEND.B`.emak_
00023bf0: 656D 616B 5F63 7962 6572 5F67 6869 6261  emak_cyber_ghiba
00023c00: 687D                                     h}
root@opacite:~#
```

Llau dari hashil tersebut, didapatkan full flagnya

CSC{ketika_emak_emak_cyber_ghibah}