INFORMATION AND SYSTEMS SECURITY SOCIETY

UTCTF 2020

Forensics : Observe Closely

Value : 50 Pts

Description : A simple image with a couple of twists...

Attachment : Griffith_Observatory.png

Solutions :

Downloading the attachment «**Griffith_Observatory.png**» and we got this picture bellow.

Running «**strings**» against the picture and i discovered an hidden file in it «**hidden_binary**».

```
root@kali:~/Téléchargements# strings Griffith_Observatory.png
IHDR
IDATx
0^z!
14Ms
```

```
;V<C
hidden_binaryUT
B>X^ux
```

Running «**binwalk**» for extract the data from the picture and we get our hidden binary.

```
root@kali:~/Téléchargements# binwalk -e Griffith_Observatory.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 320 x 155, 8-bit/color RGBA, non-interlaced
41            0x29            Zlib compressed data, default compression
127759        0x1F30F         Zip archive data, at least v2.0 to extract, compressed size: 2587,
uncompressed size: 16664, name: hidden_binary
130500        0x1FDC4         End of Zip archive, footer length: 22
```

Going into the extracted directory, and running the binary give us the flag.

```
root@kali:~/Téléchargements# cd _Griffith_Observatory.png.extracted/
root@kali:~/Téléchargements/_Griffith_Observatory.png.extracted# ls
1F30F.zip  29  29.zlib  hidden_binary
root@kali:~/Téléchargements/_Griffith_Observatory.png.extracted# ./hidden_binary
Ah, you found me!
utflag{2fbe9adc2ad89c71da48cabe90a121c0}
```

Flag : utflag{2fbe9adc2ad89c71da48cabe90a121c0}