Descripción

Nombre: _ L0aD1ng 2019 (https://twitter.com/Hackers4F/status/1079687437251559424)
Related: The Good Doctor (https://en.wikipedia.org/wiki/The_Good_Doctor_(TV_series))
Fecha de liberación: 31 de diciembre de 2018
Autor: 1v4n

A fan of #Thegooddoctor has sent us a secret, you help us find out? He likes one the countries where it was filmed.

Objetivo

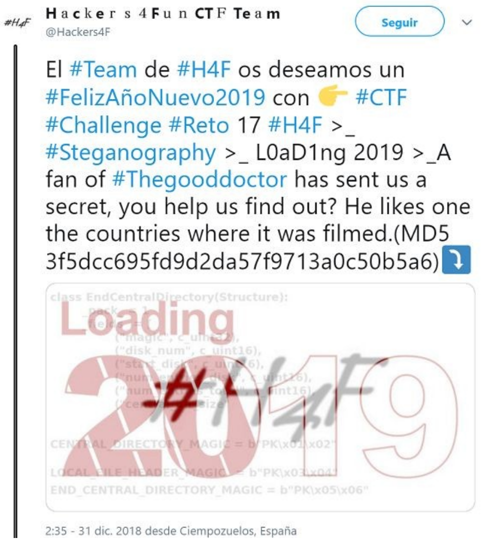
Formato de flag: H4F{md5}

Herramientas utilizadas

Firefox V. 60.5.1 https://www.mozilla.org/en-US/firefox/60.5.1/releasenotes/
Wget 1.20.1 https://www.gnu.org/software/wget/
Strings 2.31.1 https://www.gnu.org/software/binutils/
Binwalk v2.1.2 https://github.com/ReFirmLabs/binwalk
7-Zip [64] 16.02 https://www.7-zip.org/download.html
Unicode Text Stego https://www.irongeek.com/i.php?page=security/unicode-steganography-homoglyph-encoder
MP3Stego http://www.petitcolas.net/fabien/software/MP3Stego_1_1_18.zip

Resumen:

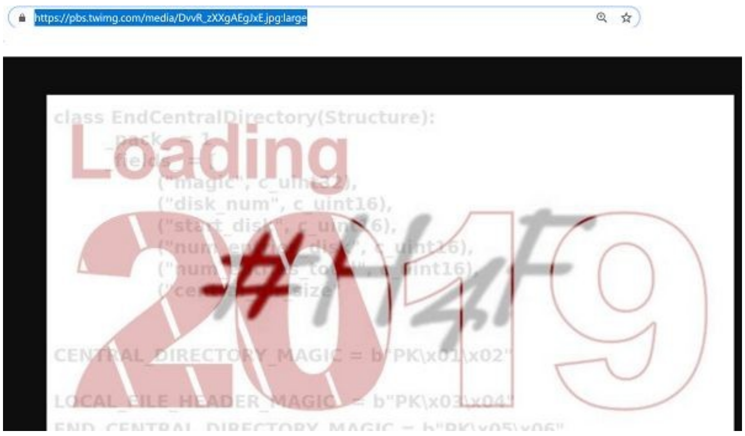
Visitamos el tuit publicado y visualizamos la imagen que aloja https://pbs.twimg.com/media/DvvR_zXXgAEgJxE.jpg



Hackers4Fun CTF Team
@Hackers4F

El #Team de #H4F os deseamos un #FelizAñoNuevo2019 con 👉 #CTF #Challenge #Reto 17 #H4F >_ #Steganography >_ L0aD1ng 2019 >_A fan of #Thegooddoctor has sent us a secret, you help us find out? He likes one the countries where it was filmed.(MD5 3f5dcc695fd9d2da57f9713a0c50b5a6)⤵️

2:35 - 31 dic. 2018 desde Ciempozuelos, España



https://pbs.twimg.com/media/DvvR_zXXgAEgJxE.jpg:large

Loading
2019
#H4F
class EndCentralDirectory(Structure):
("disk_num", c_uint16),
CENTRAL_DIRECTORY_MAGIC = b"PK\x01\x02"
LOCAL_FILE_HEADER_MAGIC = b"PK\x03\x04"
END_CENTRAL_DIRECTORY_MAGIC = b"PK\x05\x06"

```
root@1v4n:~/CTF/Hackers4Fun/Reto17# curl 'https://pbs.twimg.com/media/DvvR_zXXgAEgJxE.jpg' > output
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  153k  100  153k    0     0   295k      0 --:--:-- --:--:-- --:--:--  295k
```

Obtenemos un archivo de imagen JPEG y con hash MD5 7cdbcada4458b8c9ffaa32f019902804. Si observamos en la publicación del reto los servidores de la Tw han modificado el archivo original.

```
root@1v4n:~/CTF/Hackers4Fun/Reto17# file output
output: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8,
600x320, components 3
root@1v4n:~/CTF/Hackers4Fun/Reto17# md5sum output
7cdbcada4458b8c9ffaa32f019902804  output
root@1v4n:~/CTF/Hackers4Fun/Reto17# mv output output.jpg
```

Ejecutamos exiftool para analizar nuestra imagen JPEG

```
root@1v4n:~/CTF/Hackers4Fun/Reto17# exiftool output.jpg
ExifTool Version Number         : 11.16
File Name                       : output.jpg
Directory                       : .
File Size                       : 153 kB
File Modification Date/Time     : 2019:04:07 12:31:26-04:00
File Access Date/Time           : 2019:04:07 12:40:08-04:00
File Inode Change Date/Time     : 2019:04:07 12:35:54-04:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Profile CMM Type                : Unknown (<!--)
Profile Version                 : 4.0.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2017:07:07 13:22:32
Profile File Signature          : acsp
Primary Platform                : Unknown ()
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             :
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 :
Profile ID                      : 0
Image Width                     : 600
Image Height                    : 320
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 600x320
Megapixels                      : 0.192
```

Seguimos con el análisis básico forense del archivo con *strings* y *binwalk -e* extrayendo archivos *embebidos*

```
root@1v4n:~/CTF/Hackers4Fun/Reto17# strings output.jpg > strings.txt
root@1v4n:~/CTF/Hackers4Fun/Reto17# nano strings.txt
```

```
JFIF
ICC_PROFILE
<!--
...
.H1nT-Un1-C0d3-St3g0UT
...
ICC_PROFILE
H4F_St3g0_The_GD_MP35
...
```

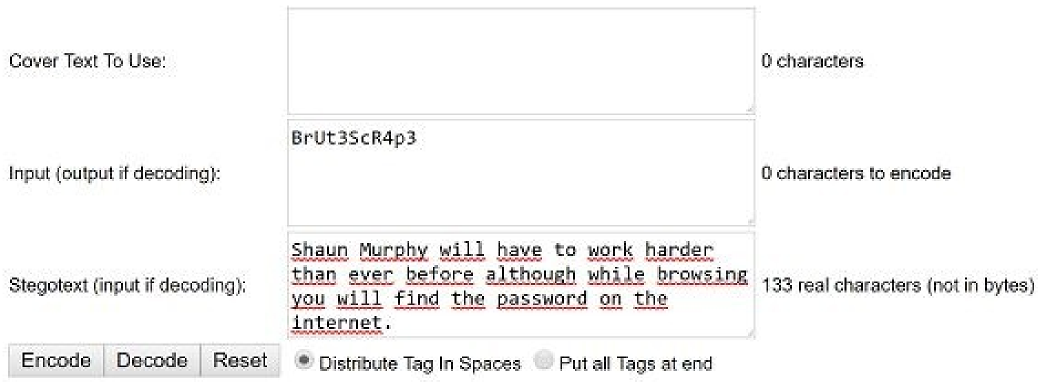
```
root@1v4n:~/CTF/Hackers4Fun/Reto17# binwalk -e output.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
182           0xB6            Zip archive data, at least v2.0 to extract, compressed size: 161, uncompressed size: 290, name: .H1nT-Un1-C0d3-St3g0
65576         0x10028         Zip archive data, at least v2.0 to extract, compressed size: 110, uncompressed size: 198, name: H4F_St3g0_The_GD_MP3
131307        0x200EB         End of Zip archive, footer length: 22
```

Examinamos el contenido extraído. Encontrando un archivo comprimido .zip del cual obtenemos decodificando HEX una URL y un archivo oculto *.H1nT-Un1-C0d3-St3g0* que porta ***Unicode Tags Stego*** de cual obtenemos una clave ***BrUt3ScR4p3***

```
root@1v4n:~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted# ls -la
total 168
drwxr-xr-x 2 root root   4096 abr  7 12:50 .
drwxr-xr-x 4 root root   4096 abr  7 12:50 ..
-rw-r--r-- 1 root root 156730 abr  7 12:50 B6.zip
-rw-r--r-- 1 root root    290 dic 30 19:23 .H1nT-Un1-C0d3-St3g0
root@1v4n:~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted# file .H1nT-Un1-C0d3-St3g0
.H1nT-Un1-C0d3-St3g0: Little-endian UTF-16 Unicode text, with no line terminators
root@1v4n:~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted# cat .H1nT-Un1-C0d3-St3g0
"Shaun @'B'Murphy @'r'will @'U'have @'t'to @'3'work @'S'harder @'c'than @'R'ever @'4'before @'p'although @'3'while browsing you will find the password on the internet.root@1v4n:~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted#
root@1v4n:~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted# file B6.zip
B6.zip: Zip archive data, at least v2.0 to extract
root@1v4n:~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted# 7z x B6.zip
...
root@1v4n:~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted# ls -la
total 172
drwxr-xr-x 2 root root   4096 abr  7 12:56 .
drwxr-xr-x 4 root root   4096 abr  7 12:50 ..
-rw-r--r-- 1 root root 156730 abr  7 12:50 B6.zip
-rwxr--r-- 1 root root    290 dic 30 19:23 .H1nT-Un1-C0d3-St3g0
-rw-r--r-- 1 root root    198 dic 30 20:31 H4F_St3g0_The_GD_MP3
root@1v4n:~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted# file H4F_St3g0_The_GD_MP3
H4F_St3g0_The_GD_MP3: ASCII text
root@1v4n:~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted# cat H4F_St3g0_The_GD_MP3
68 74 74 70 73 3a 2f 2f 64 72 69 76 65 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 6f 70 65 6e 3f 69 64 3d 31 62 36 46 4c 52 52 4d 7a 51 44 51 63 33 69 39 71 37 79 5a 64 2d 72 36 56 5f 46 30 5a 74 69 4b 36
```

```
root@1v4n:~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted# cat H4F_St3g0_The_GD_MP3 | xxd -r -p
https://drive.google.com/open?id=1b6FLRRMzQDQc3i9q7yZd-r6V_F0ZtiK6
```



Cover Text To Use: 0 characters

Input (output if decoding): BrUt3ScR4p3 0 characters to encode

Stegotext (input if decoding): Shaun Murphy will have to work harder than ever before although while browsing you will find the password on the internet. 133 real characters (not in bytes)

Continuamos descargando el audio MP3 de la URL de GDrive obtenida del reversing del HEX anterior con un clip del la sintonía de la serie #Thegooddoctor que nos ambienta el Reto pero no solo esconde audio.

```
root@1v4n:~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted# gdown
https://drive.google.com/uc?id=1b6FLRRMzQDQc3i9q7yZd-r6V_F0ZtiK6
Downloading...
From: https://drive.google.com/uc?id=1b6FLRRMzQDQc3i9q7yZd-r6V_F0ZtiK6
To: /root/CTF/Hackers4Fun/Reto17/_output.jpg.extracted/H4F_Reto_17_St3g0_The_GD.mp3
100%|████████████████████████████████████████████████████████████|
560k/560k [00:00<00:00, 1.19MB/s]
root@1v4n:~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted# file
H4F_Reto_17_St3g0_The_GD.mp3
H4F_Reto_17_St3g0_The_GD.mp3: MPEG ADTS, layer III, v1, 128 kbps, 44.1 kHz, Monaural
```

Pasamos a decodificar la esteganografía con MP3Stego pero necesitamos una posible password que con ayuda de ***Brutescrape*** y volviendo al enunciado del reto *"He likes one the countries where it was filmed"* nuestra posible password será Canada https://www.imdb.com/title/tt6470478/locations?ref_=tt_ql_dt_5#filming_locations

```
root@1v4n:~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted# mp3stego-decode -X -P Canada
~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted/H4F_Reto_17_St3g0_The_GD.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file =
'/root/CTF/Hackers4Fun/Reto17/_output.jpg.extracted/H4F_Reto_17_St3g0_The_GD.mp3'  output
file =
'/root/CTF/Hackers4Fun/Reto17/_output.jpg.extracted/H4F_Reto_17_St3g0_The_GD.mp3.pcm'
Will attempt to extract hidden information. Output:
/root/CTF/Hackers4Fun/Reto17/_output.jpg.extracted/H4F_Reto_17_St3g0_The_GD.mp3.txt
the bit stream file
/root/CTF/Hackers4Fun/Reto17/_output.jpg.extracted/H4F_Reto_17_St3g0_The_GD.mp3 is a BINARY
file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=3, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=single-ch, sblim=32, jsbd=32, ch=1
[Frame 1339]Avg slots/frame = 417.649; b/smp = 2.90; br = 127.905 kbps
Decoding of
```

```
"/root/CTF/Hackers4Fun/Reto17/_output.jpg.extracted/H4F_Reto_17_St3g0_The_GD.mp3" is
finished
The decoded PCM output file name is
"/root/CTF/Hackers4Fun/Reto17/_output.jpg.extracted/H4F_Reto_17_St3g0_The_GD.mp3.pcm"
WARNING: if you used relative paths, you find your results relative to
"/opt/mp3stego/MP3Stego_1_1_18/MP3Stego/"
root@1v4n:~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted# ls -la
total 3740
drwxr-xr-x 2 root root    4096 abr  7 14:06 .
drwxr-xr-x 4 root root    4096 abr  7 12:50 ..
-rw-r--r-- 1 root root  156730 abr  7 12:50 B6.zip
-rwxr--r-- 1 root root     290 dic 30 19:23 .H1nT-Un1-C0d3-St3g0
-rw-r--r-- 1 root root  560054 abr  7 13:19 H4F_Reto_17_St3g0_The_GD.mp3
-rw-r--r-- 1 root root 3084800 abr  7 14:07 H4F_Reto_17_St3g0_The_GD.mp3.pcm
-rw-r--r-- 1 root root      52 abr  7 14:07 H4F_Reto_17_St3g0_The_GD.mp3.txt
-rw-r--r-- 1 root root     198 dic 30 20:31 H4F_St3g0_The_GD_MP3
root@1v4n:~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted# cat
H4F_Reto_17_St3g0_The_GD.mp3.txt
d2N1TDVmZmY2M2dnZmdmY2FmaGY0NjZlaDYzaGY3aDRlNl8zTg==
```

Decodificamos nuestra cadena con ayuda de audodecoder.py

```
root@1v4n:~/CTF/Hackers4Fun/Reto17/_output.jpg.extracted# python3
~/Crypto/autodecoder/audodecoder.py -l 2 -p H4F -m
d2N1TDVmZmY2M2dnZmdmY2FmaGY0NjZlaDYzaGY3aDRlNl8zTg==



                          (
   (             (        )\ )                  (
   )\       (    )\ )    (()/(     (            )\ )   (   (
((((_)(    ))\  (()/(  (  /(_))   ))\  (   (   (()/(  ))\  )(
 )\ _ )\  /((_)  ((_)) )\(_))_   /((_) )\  )\   ((_))/((_)(()\
 (_)_\(_)(_))(   _| | ((_)|   \ (_))  ((_)((_)  _| |(_))   ((_)
  / _ \  | || |/ _` |/ _ \| |) |/ -_)/ _|/ _ \/ _` |/ -_) | '_|
 /_/ \_\  \_,_|\__,_|\___/|___/ \___|\__|\___/\__,_|\___| |_|

                    Author: oreos | Twitter: @oreos_ES


base64 > rot47: H4F{d777eb8878742797cee69eb97f9c6e0b}
```

Autor: 1v4n a.k.a. @1r0Dm48O
Twitter: https://twitter.com/1r0Dm448O