Descripción

Nombre: Try 3v3r1Tb1ng (https://twitter.com/Hackers4F/status/1079687437251559424)

Related: Zootopia (https://en.wikipedia.org/wiki/Zootopia)

Fecha de liberación: 8 de junio de 2018

Autor: 1v4n

Objetivo

Formato de flag: H4F{md5}

Resumen:

Descargamos con gdown el archivo R3t0_11_TryEverything_R34dm3.png (a9f6295bfb8f8ad9a4899078e6452c26) y lo identificamos como imagen PNG.

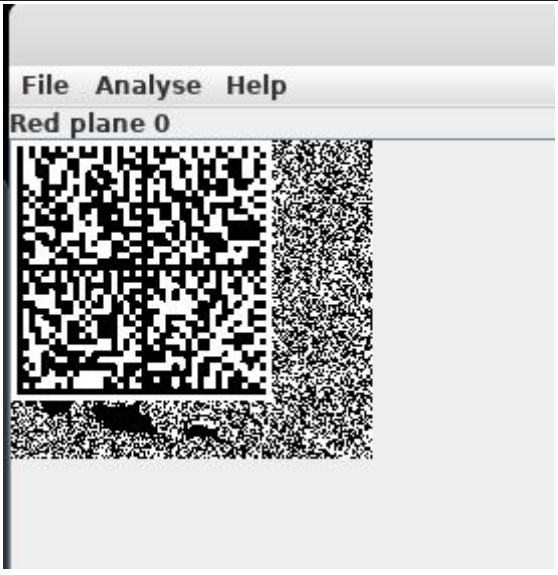
```
root@1v4n:~/CTF/Hackers4Fun/Reto11# gdown
https://drive.google.com/uc?id=1YpY7op2uADukV6hhV6n10VbaxpjerwE0
Downloading...
From: https://drive.google.com/uc?id=1YpY7op2uADukV6hhV6n10VbaxpjerwE0
To: /root/CTF/Hackers4Fun/Reto11/R3t0_11_TryEverything_R34dm3.png
100%|
| 58.4k/58.4k [00:00<00:00, 1.57MB/s]
root@1v4n:~/CTF/Hackers4Fun/Reto11# md5sum R3t0_11_TryEverything_R34dm3.png
a9f6295bfb8f8ad9a4899078e6452c26  R3t0_11_TryEverything_R34dm3.png
root@1v4n:~/CTF/Hackers4Fun/Reto11# file R3t0_11_TryEverything_R34dm3.png
R3t0_11_TryEverything_R34dm3.png: PNG image data, 180 x 159, 8-bit/color RGBA,
non-interlaced
```

Realizamos un análisis forense preliminar donde no encontramos con exiftool, strings y binwalk nada positivo. WTF

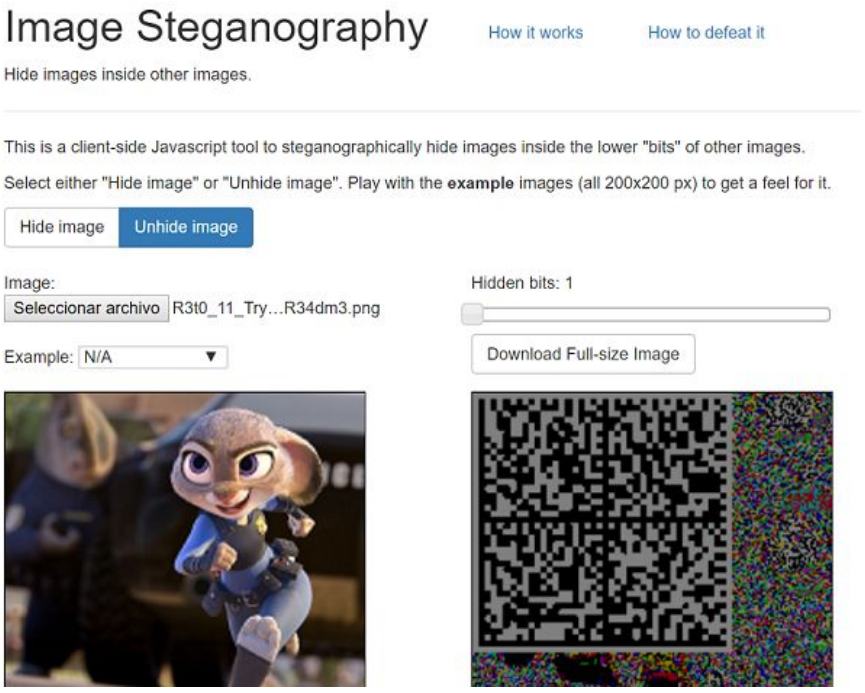
```
root@1v4n:~/CTF/Hackers4Fun/Reto11# pngcheck R3t0_11_TryEverything_R34dm3.png
OK: R3t0_11_TryEverything_R34dm3.png (180x159, 32-bit RGB+alpha, non-interlaced,
48.9%).
root@1v4n:~/CTF/Hackers4Fun/Reto11# strings R3t0_11_TryEverything_R34dm3.png
IHDR
IDATx^l
x$gu&
vuuuuu
.$!Y
B!gb
t:.\
3y<?
ywz,r
spr9
^.^@
V@F@
cn32
zht\4
aZz1
w1xn
VmYHg2
-FR`
...
3LLL
?hWl
QB)-
1~M(U
t"B)U
?"14a
G7^(
(UA)
bR%[4
s?4a
.:ESl.A
r1j~
IDAT
jlL/!
Tr!D
:"D2UL
Z^F&
TfS#
HNV7Xnk:
LWU:
21Q)
IEND
root@1v4n:~/CTF/Hackers4Fun/Reto11# binwalk R3t0_11_TryEverything_R34dm3.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 180 x 159, 8-bit/color RGBA, non-interlaced
41            0x29            Zlib compressed data, compressed
```

Damos por hecho que nuestra imagen nos esconde un *secreto*. Indagando con ***zsteg*** existe stego que confirmamos con ***Stegsolve o Incoherency***

```
root@1v4n:~/CTF/Hackers4Fun/Reto11# zsteg R3t0_11_TryEverything_R34dm3.png
imagedata           .. file: MIPSEB MIPS-II ECOFF executable not stripped - version
248.248
b2,r,msb,xy         .. text: "?\"hu=i[z"
b2,rgb,lsb,xy       .. text: "U_}U]W}W"
b4,g,lsb,xy         .. text: "sUuUU133151"
.root@1v4n:~/CTF/Hackers4Fun/Reto11# ./stegsolve.jar
```



o en la tool online https://incoherency.co.uk/image-steganography/#unhide



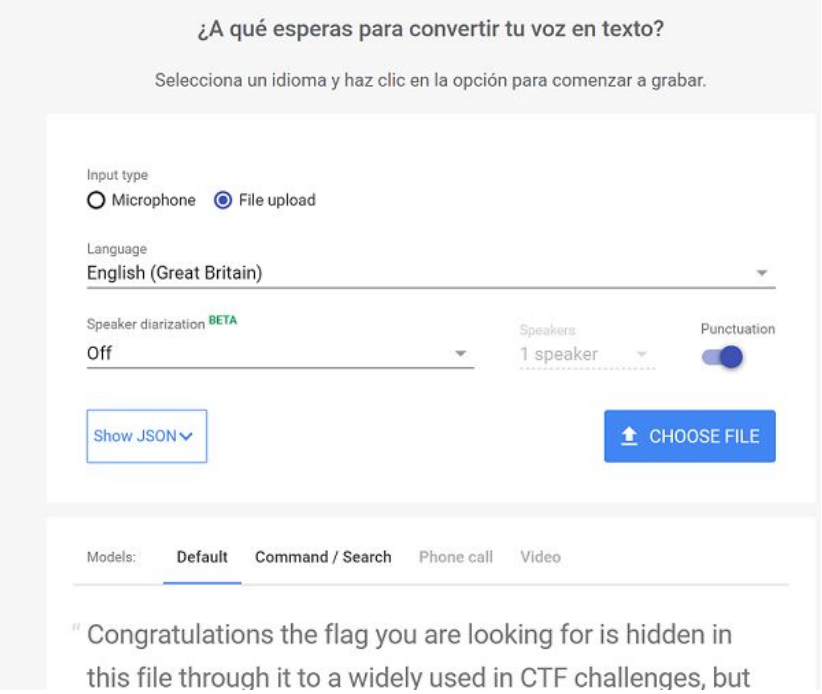
Descargamos el código *qr tipo DATA MATRIX* y pasamos a decodificarlo https://zxing.org/w/decode.jspx . Obtenemos una URL de drive que no lleva a un nuevo artefacto H4F_Reto_11_.7z (35b33709ba1e2f30073c56da8246b3bb)

```
Decode Succeeded
Raw text
aHR0cHM6Ly9kcml2ZS5nb29nbGUuY29tL2ZpbGUvZC8xNW8tR2RldEpvRVRPLWpqZnlWbmVNQkdIWEFfZzZmblQvdmlldz91c3A9c2hhcmluZw==
Raw bytes
62 49 53 31 64 49 4e 37   4d 7a 3a 6c 64 6e 6d 33
5b 54 36 6f 63 9f 6f 63   48 56 76 5a 9f 75 4d 33
5b 71 63 48 56 77 5b 44   39 79 4f 58 39 75 53 33
53 6d 65 46 71 77 53 57   53 51 4d 58 71 72 5b 6f
6d 58 63 6e 57 4f 52 6c   65 4a 58 46 47 67 5b 7b
5b 6e 63 6d 52 77 65 6e   6d 6d 65 7b dd 64 34 42
3a 64 33 69 69 64 6e 6d   76 5b 78 3e 3e 81 e0 77
0f a5
Barcode format      DATA_MATRIX
Parsed Result Type  TEXT
Parsed Result
aHR0cHM6Ly9kcml2ZS5nb29nbGUuY29tL2ZpbGUvZC8xNW8tR2RldEpvRVRPLWpqZnlWbmVNQkdIWEFfZzZmblQvdmlldz91c3A9c2hhcmluZw==
root@1v4n:~/CTF/Hackers4Fun/Reto11# printf
'aHR0cHM6Ly9kcml2ZS5nb29nbGUuY29tL2ZpbGUvZC8xNW8tR2RldEpvRVRPLWpqZnlWbmVNQkdIWEFfZzZmblQvdmlldz91c3A9c2hhcmluZw==' | base64 -d
https://drive.google.com/file/d/15o-GdetJoETO-jjfyVneMBGHXA_g6fnT/view?usp=sharing
root@1v4n:~/CTF/Hackers4Fun/Reto11# gdown
https://drive.google.com/uc?id=15o-GdetJoETO-jjfyVneMBGHXA_g6fnT
Downloading...
From: https://drive.google.com/uc?id=15o-GdetJoETO-jjfyVneMBGHXA_g6fnT
To: /root/CTF/Hackers4Fun/Reto11/H4F_Reto_11_.7z
2.27MB [00:02, 1.10MB/s]
root@1v4n:~/CTF/Hackers4Fun/Reto11# file H4F_Reto_11_.7z
H4F_Reto_11_.7z: 7-zip archive data, version 0.4
root@1v4n:~/CTF/Hackers4Fun/Reto11# md5sum H4F_Reto_11_.7z
35b33709ba1e2f30073c56da8246b3bb  H4F_Reto_11_.7z
root@1v4n:~/CTF/Hackers4Fun/Reto11# 7z x H4F_Reto_11_.7z

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=es_ES.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs Intel(R)
Core(TM) i7-6500U CPU @ 2.50GHz (406E3),ASM,AES-NI)

Scanning the drive for archives:
1 file, 2273853 bytes (2221 KiB)

Extracting archive: H4F_Reto_11_.7z
--
Path = H4F_Reto_11_.7z
Type = 7z
Physical Size = 2273853
Headers Size = 310
Method = Delta LZMA2:21
Solid = +
Blocks = 2

Everything is Ok
```

```
Files: 6
Size:       2963966
Compressed: 2273853
root@1v4n:~/CTF/Hackers4Fun/Reto11# ls -la
total 5196
drwxr-xr-x 2 root root    4096 ago 31 13:07 .
drwxr-xr-x 9 root root    4096 ago 27 21:46 ..
-rw-r--r-- 1 root root  194610 jun  2  2018 D15sr1_4.jpg
-rw-r--r-- 1 root root  235059 jun  2  2018 D15sr1_5.jpg
-rw-r--r-- 1 root root  154030 jun  2  2018 D15tR1_1.jpg
-rw-r--r-- 1 root root  249438 jun  2  2018 D15Tr2_2.jpg
-rw-r--r-- 1 root root  198881 jun  2  2018 D15tR3_3.jpg
-rw-r--r-- 1 root root 2273853 ago 31 13:06 H4F_Reto_11_.7z
-rw-r--r-- 1 root root 1931948 jun  8  2018 Hint_PlUm4_gR4b4d0ra_d3_H0pp5_.wav
-rw-r--r-- 1 root root   58447 ago 28 20:13 R3t0_11_TryEverything_R34dm3.png
root@1v4n:~/CTF/Hackers4Fun/Reto11#
```

OMG!! Obtenemos 5 archivos de imagen JPG y un archivo WAV con un “speech” en Inglés. Además el archivo WAV porta esteganografía LSB. Pasamos a transcribir el *Hint* con https://cloud.google.com/speech-to-text/

```
root@1v4n:~/CTF/Hackers4Fun/Reto11# steghide info Hint_PlUm4_gR4b4d0ra_d3_H0pp5_.wav
"Hint_PlUm4_gR4b4d0ra_d3_H0pp5_.wav":
  formato: wave audio, PCM encoding
  capacidad: 59,0 KB
'Intenta informarse sobre los datos adjuntos? (s/n) s
Anotar salvoconducto:
steghide: 'no pude extraer ningún dato con ese salvoconducto!
```

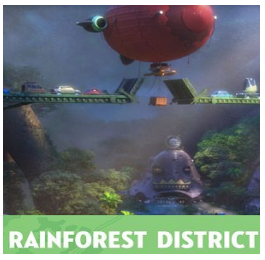


La transcripción nos confirma que la *flag* está escondida en el archivo WAV y que la password que necesitamos está compuesta por el nombre de los 5 distritos ordenados de Zootopia y la conseguiremos a través de OSINT con *"Reverse Image"* (pej. https://www.google.com/imghp). Ademas debera estar en "lowercase" y no deberá superar 37 caracteres.

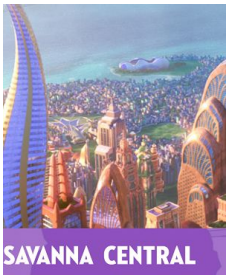
1. Sahara

2. Tundra

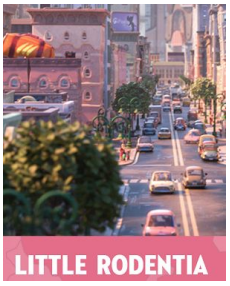
3. Rainforest



4. Savanna



5. Rodentia




```
Password>_ saharatundrarainforestsavannarodentia

>>> len("saharatundrarainforestsavannarodentia")
37
```

```
root@1v4n:~/CTF/Hackers4Fun/Reto11# steghide info Hint_PlUm4_gR4b4d0ra_d3_H0pp5_.wav
"Hint_PlUm4_gR4b4d0ra_d3_H0pp5_.wav":
  formato: wave audio, PCM encoding
  capacidad: 59,0 KB
'Intenta informarse sobre los datos adjuntos? (s/n) s
Anotar salvoconducto:
  archivo adjunto "Fl4g_b64.txt":
    tamaño: 32,0 Byte
    encriptado: rijndael-128, cbc
    compactado: si
root@1v4n:~/CTF/Hackers4Fun/Reto11# steghide extract -sf
Hint_PlUm4_gR4b4d0ra_d3_H0pp5_.wav
Anotar salvoconducto:
anote' los datos extraídos e/"Fl4g_b64.txt".
root@1v4n:~/CTF/Hackers4Fun/Reto11# cat Fl4g_b64.txt
SDRGe0IzbGx3M3RoZXJfQzBuZjEzczR9root@1v4n:~/CTF/Hackers4Fun/Reto11# cat Fl4g_b64.txt |
base64 -d
H4F{B3llw3ther_C0nf13s4}
```

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