

[Página principal](#)



lunes, 25 de junio de 2018

Writeup Reto H4F Stegano: Try 3v3r1Tb1ng



Nuevo reto de Stegano/OSINT, donde tendremos que ayudar a Judy H. (Conejita de Zootrópolis) y a Nick W. (el zorro estafador) a investigar las desapariciones.

Manos a la obra

Nos descargamos la imagen del enlace de Google Drive.

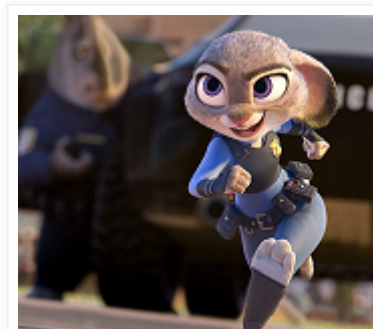
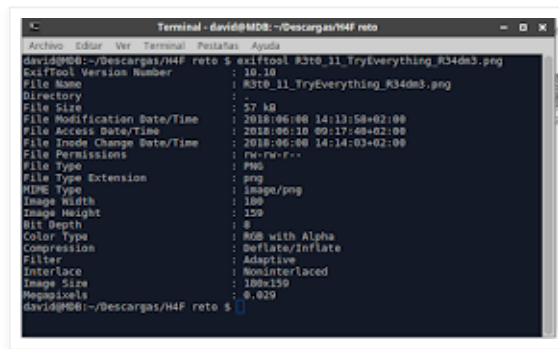


Imagen del reto

La analizamos con exiftool, una de mis herramientas favoritas:



No se observa ninguna evidencia o pista que nos pueda ayudar, vamos a usar "Stegsolve", vamos pasando por los diferentes tipos de planos y.....Bingo! tenemos un código de barras.



Exactamente, es un código de barras del tipo **Data Matrix**, usamos un lector de códigos online y lograremos leer su contenido.

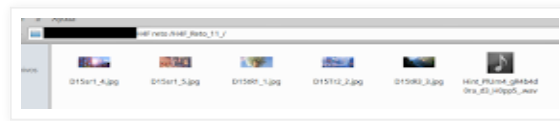


Una vez leído, nos muestra un código en **base64**, podemos usar para ello **ASCII to Hex**:



Otro link! Está claro que no nos lo iban a poner fácil....(abriendo otra caja de Paracetamol de 1g)

Entramos en el enlace y nos descargamos el archivo "H4F_Reto_11_.7z", lo descomprimos y nos aparecerá una carpeta con los siguientes ficheros:



Tenemos 5 imágenes y un archivo de audio en formato .wav. La inercia me lleva a reproducir el archivo de audio, en él se encuentra las instrucciones para resolver el reto (eso sí, el audio está en inglés):

Texto del audio:

Speaker 1: Congratulations the flag you are looking for is hidden in this file through it to a widely used in CTF challenges.
Speaker 2: But Judy H. in NYC W. need your help to solve the mystery of the disappearances and discover the five districts they must investigate in the five images they have obtained.
Speaker 2: Important for this they must use reverse image.
Speaker 2: The password is number imagine distrito one number imagine just treated to number imagine distrito three number imagine distrito for number imagine Distrito to five.
Speaker 1: All names together and in lowercase letters not exceeding thirty seven characters.
Speaker 2: For example champ Martin and Senati Campamento renal.
Speaker 1: Good luck and don't use brute force.

Analizando el texto:

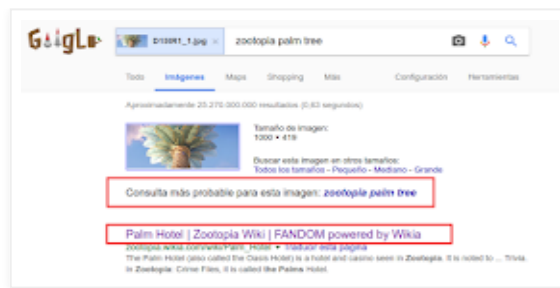
1. Nos dice que tenemos el flag "oculta" en este fichero (en el .wav, claro).
2. Indica como "pista" que es **importante** que usemos "reverse image".
3. También nos dice que la contraseña es cada uno de los distritos, todo junto, en minúsculas y sin exceder los 37 caracteres.

Pues empecemos, para hacer "reverse image" existen varias **OSINT TOOLS**, pero yo usé "Google Images".

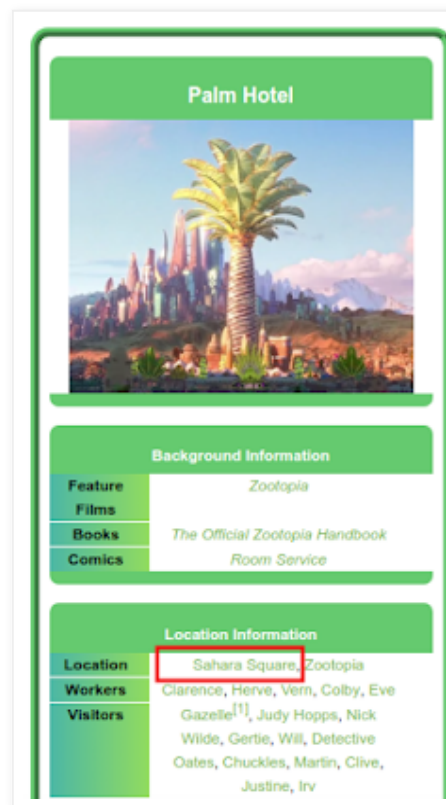


Nota: Para no hacer muy largo, este paso sólo lo haré con la primera imagen, pero son los mismos pasos para el resto de fotos.

Analizamos la primera imagen:



Hacemos clic a cualquiera de los dos enlaces (nos lleva al mismo sitio) y veremos una "wiki" con toda la información del sitio, incluyendo la foto completa de la torre y la localización de esta.



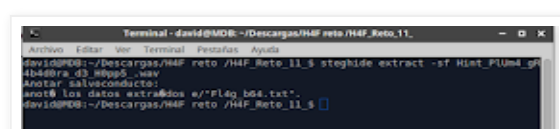
La primera imagen nos lleva al distrito: **Sahara Square**.

Continuamos usando los mismos pasos con el resto de imágenes y se nos debería de quedar así:

1. Sahara Square
2. Tundratwon
3. Rainforest
4. Savanna
5. Little Rodentia

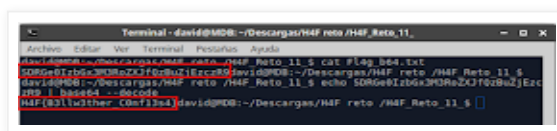
Por lo tanto, la clave para obtener nuestra flag es: **saharatundrarainforestsavannarodentia**

Nos dirigimos a la terminal para ejecutar "**Steghide**" y extraemos el archivo del .wav.



Ahora si, leemos el archivo "**Fl4g_b64.txt**" y nos dará otro código en base64, decodeamos y nos

dará la flag.

A terminal window titled 'Terminal - david@MDQ: ~/Descargas/H4F reto /H4F_Reto_11_'. The prompt is 'david@MDQ:~/Descargas/H4F reto /H4F_Reto_11_ \$'. The user enters 'cat flag_b64.txt'. The output is 'SORGe0IzGx3MReZxJfQzBzEzCjR9_1_h4f0d --dec0de'. The user then enters 'echo SORGe0IzGx3MReZxJfQzBzEzCjR9_1_h4f0d --dec0de'. The output is 'H4F{B3llw3ther_C0nf13s4}'. The flag is highlighted in red in the original image.

```
Terminal - david@MDQ: ~/Descargas/H4F reto /H4F_Reto_11_
david@MDQ:~/Descargas/H4F reto /H4F_Reto_11_ $ cat flag_b64.txt
SORGe0IzGx3MReZxJfQzBzEzCjR9_1_h4f0d --dec0de
david@MDQ:~/Descargas/H4F reto /H4F_Reto_11_ $ echo SORGe0IzGx3MReZxJfQzBzEzCjR9_1_h4f0d --dec0de
H4F{B3llw3ther_C0nf13s4}
```

La flag es: **H4F{B3llw3ther_C0nf13s4}**

Caso cerrado, como diría el gran John "Hannibal" Smith (Team A)....*"Me encanta que los planes salgan bien"* ("purito" incluido, por supuesto).



Hasta otra hackers!!!

David en 15:30

Compartir

No hay comentarios:

[Publicar un comentario](#)



[Página principal](#)



[Ver versión web](#)

Con la tecnología de [Blogger](#).