CTF: La taberna del "Patito Modosito"

Reto 9 Hackers4Fun CTF Team / Reto 24 Hack Players

*Solución de **KerosenoDev***

Descripción

Este CTF (capture the flag) trata de **esteganografía**, por lo que tendremos que descubrir el mensaje que oculta la siguiente **imagen** de la entrada a la taberna del "Patito Modosito":

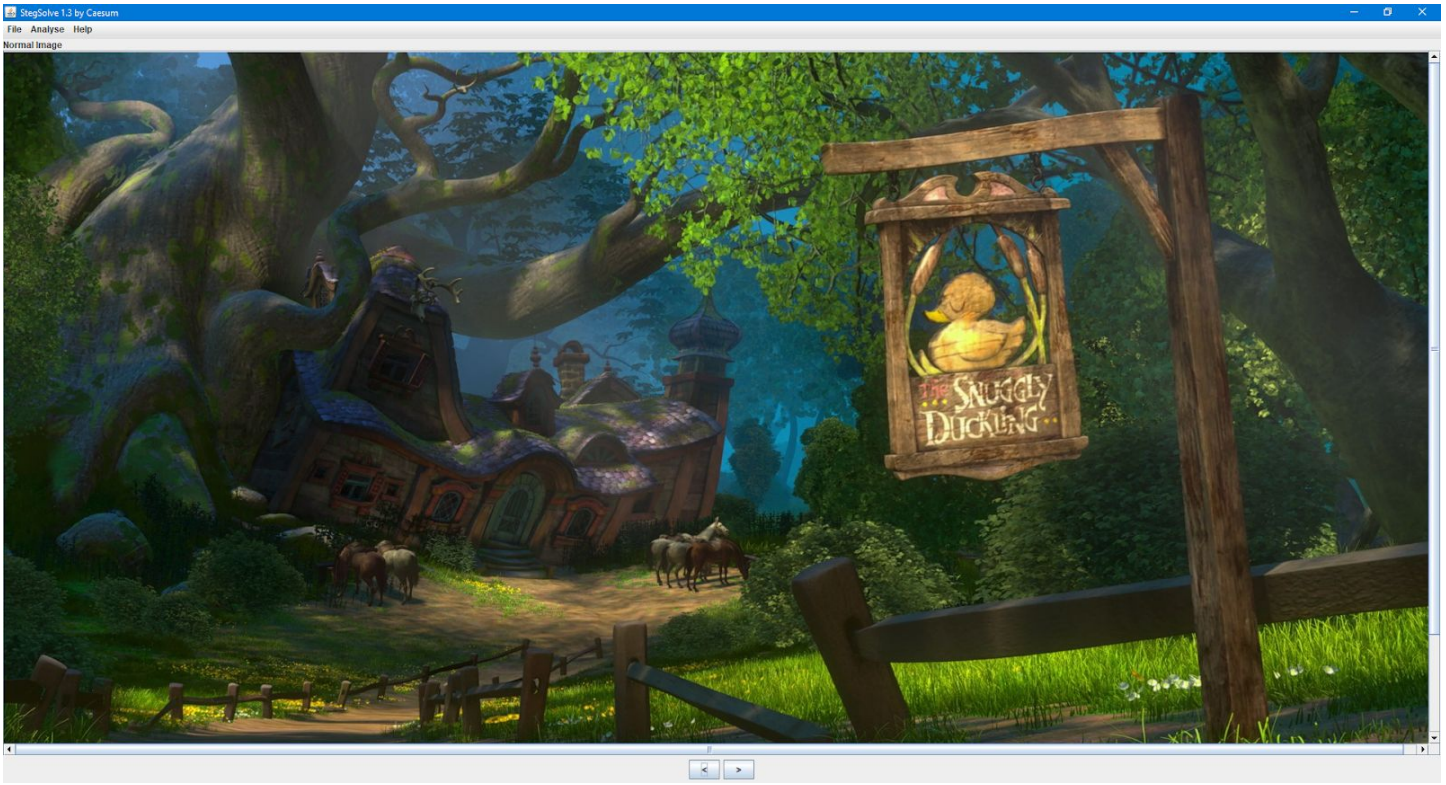
Para analizar la imagen, hay que **descargarla** del enlace original:

https://drive.google.com/file/d/1NTdlOWcVpbdwe6RnMcW6KFcEZXKMxrGf/view

Pista: el reto trata de princesas 👸 que nos desvelarán un buen consejo 👍

Pasos

Abrimos la imagen original descargada con **Stegsolve** (en este caso la **versión 1.3**), una herramienta, que entre otras cosas, nos da una vista rápida de diferentes planos de bits y algunas transformaciones simples de la imagen.

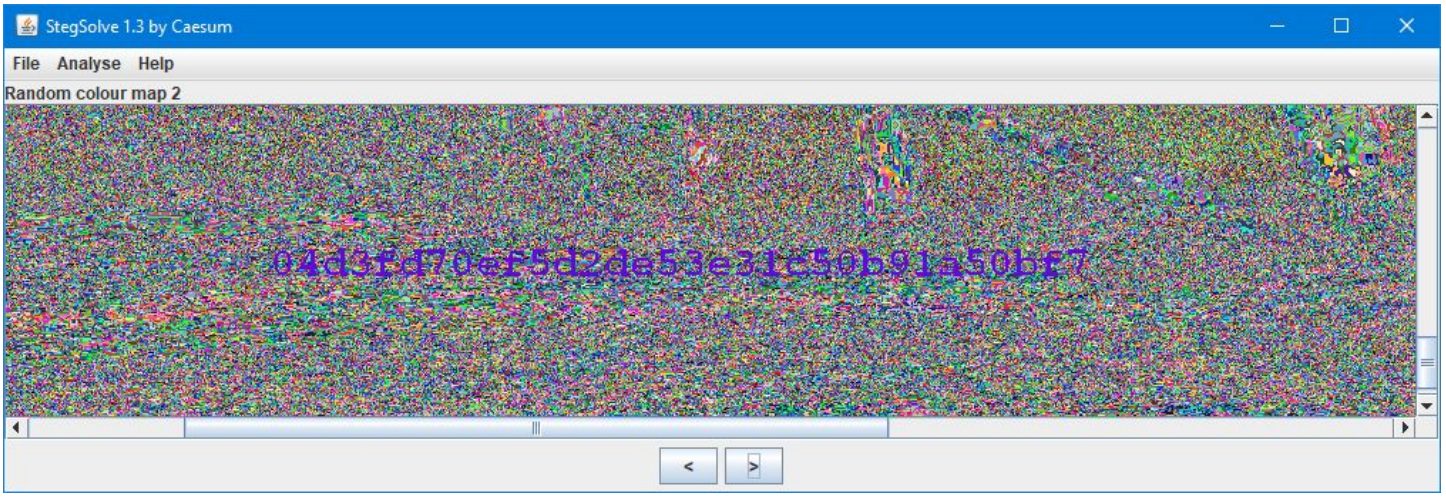


Para ello, una vez abierta la imagen, solo tenemos que ir pasando entre planos usando los botones de anterior o siguiente que se encuentran en la parte inferior, e ir revisando por cada uno si hay algún mensaje oculto.

En este caso, ya vemos como se ve un mensaje oculto en la zona inferior izquierda en los "Red plane", "Green plane", "Blue plane" y "Random colour map". Así que nos quedamos con el que mejor veamos la nota.

Recomiendo poner los "**Random colour map**" tantas veces como sea necesaria ya que cada vez que carga, como su nombre indica, la combinación de colores es aleatoria, por lo que a veces sale el mensaje mucho más claro según qué colores.

Veremos algo como esto:



Es el siguiente **hash MD5**: `04d3fd70ef5d2de53e31c50b91a50bf7`

Para decodificarlo vamos a la herramienta online [MD5Hashing.net](), ponemos el hash en "**Decrypt (search for a match):**" y pulsamos en "**Decode!**".

Obtendremos el siguiente resultado:

Decoded value:

Select Decoded Value

```
goo.gl/48jej6
```

El resultado es un enlace acortado con Google URL Shortener: **goo.gl/48jej6**

Que lleva a la siguiente imagen:

Como ya sabréis, es **Merida**, de la película Brave (indomable) de Disney, lo que encaja con la pista.

Al analizar esta imagen de nuevo con Stegsolve, parece que no tiene ningún mensaje oculto en las capas o planos. También vemos que ahora el formato no es PNG, sino **JPG**, por lo que ahora probamos a analizarla con **Steganographic Decoder**, que sirve para decodificar imágenes JPEG.

Al **subir la imagen** y darle a "**Enviar**", nos devuelve la sigueinte cadena, otro **hash MD5**:

`867a375cec13208995192cd7b61a183b`

Volvemos a decodificarlo con **MD5Hashing.net**, y ahora nos devuelve lo siguiente:

Decoded value:

Select Decoded Value

```
SDRGeyNYMVJlZE1hc1NlZ3VyYV8jWW9RdWVUdUlyaWF9
```

Una cadena en **Base64**: `SDRGeyNYMVJlZE1hc1NlZ3VyYV8jWW9RdWVUdUlyaWF9`

Ahora la decodificamos con cualquier Base64 Decoder, **como este**, donde ponemos el hash, seleccionamos "**Base 64 (descodificar)**" y pulsamos "**Ok**".

Como resultado nos da lo siguiente:

```
TEXTO ORIGINAL:
SDRGeyNYMVJIZE1hc1NIZ3VyYV8jWW9RdWVUdUlyaWF9

TEXTO PROCESADO:
H4F{#X1RedMasSegura_#YoQueTulria}
```

¡Así que ya tenemos el flag! Es:

H4F{#X1RedMasSegura_#YoQueTulria}

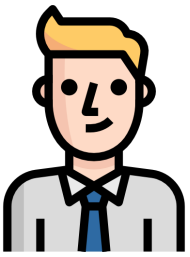
Y ahí está el buen consejo: **ir a X1RedMasSegura**.

Nota

Este es mi primer CTF, no considero que haya sido difícil, pero he tenido que probar muchos caminos para llegar a la solución, lo que me ha servido para aprender y pasar un buen rato con el desafío planteado, por lo que te animo a que hagas lo mismo si tienes la oportunidad y te gusta el tema. Espero que esta solución te sirva para aprender. ¡Un saludo!

Bibliografía

- Hack Players → Reto 24: la taberna del "Patito Modosito"
- Tweet del reto en la cuenta de Twitter de Hackers4Fun CTF Team
- Stegsolve 1.3
- Hash Encryption and Reverse Decryption
- Steganographic Decoder
- Encriptar y Desencriptar Texto Online



KerosenoDev / Francisco Rodríguez G.