El siguiente contenido está publicado con fines académicos y de concienciación. No nos hacemos responsables de las actividades que se lleven a cabo con la información mostrada a continuación.

El siguiente post forma parte de una serie de posts dedicados a mostrar las soluciones a los retos presentados en el **Evento de CiberSeguridad de Secuma 2018** celebrado en **Málaga el 15 de Noviembre de 2018.**

Cabe destacar que vamos a proceder a publicar el código fuente de cada uno de los retos (de los retos de Web) para que todo el mundo pueda bajarselo, modificarlo y conseguir así customizarlo a su gusto para lograr nuevas variantes procedientes del mismo reto que puedan inspirar a la creación de nuevos retos y/o soluciones. Así que estar atentos al **Gitlab**.

Tan sólo pedimos que siempre que se modifique el código se mencione al autor del mismo así como que se ponga a disposición del público el resultante. Dicho esto vamos a proceder a explicar, de forma detallada los pasos que seguimos así como consejos que puedan ayudar al lector y/o aclarar conceptos. Empecemos!

FASE DE CONTACTO.

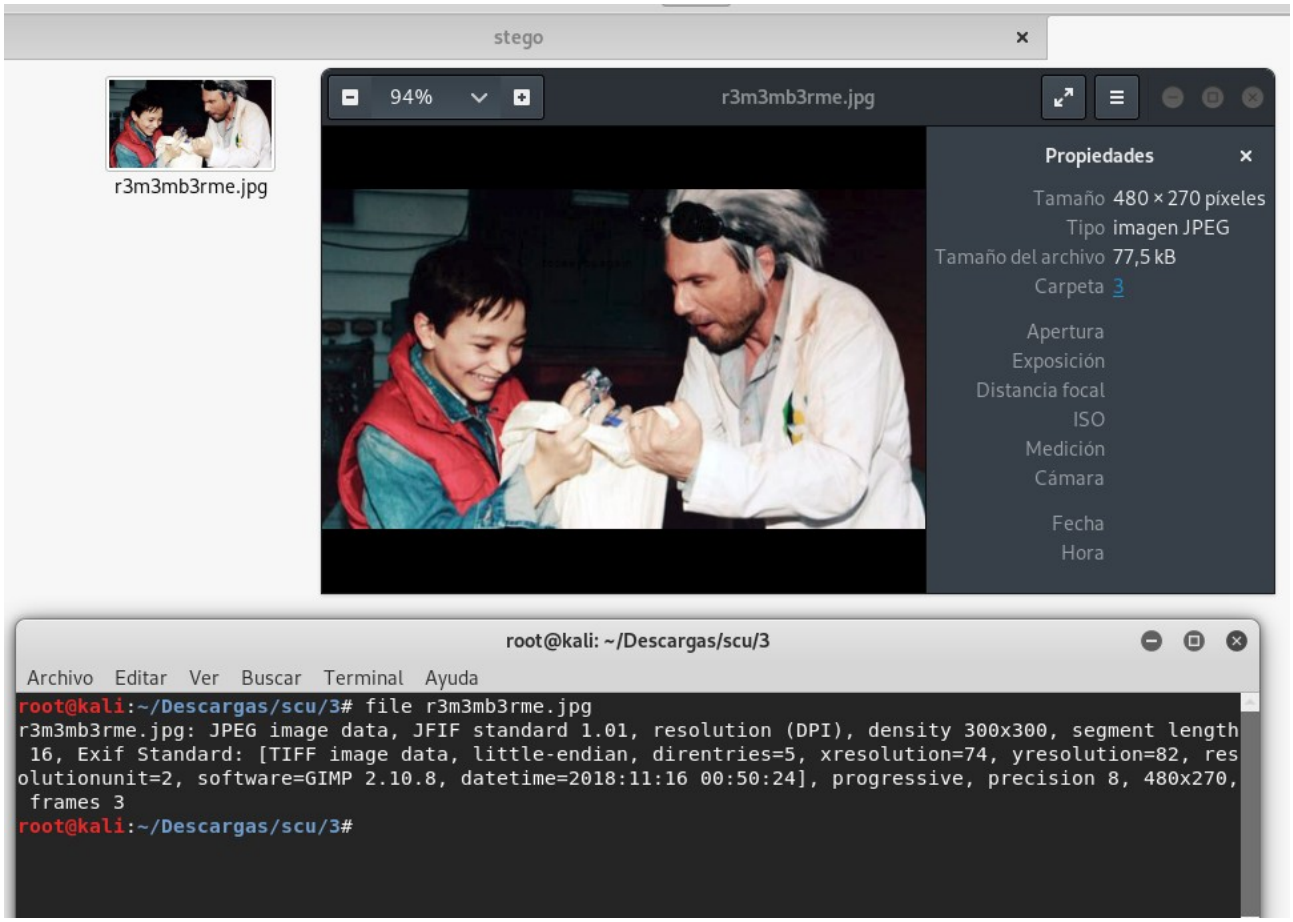
Inicialmente nos descargamos el la imagen adjunta después de leer la descripción, que la vamos a poner aquí pues es muy importante para este reto:

My father and I were very close. He was an example to follow for me.

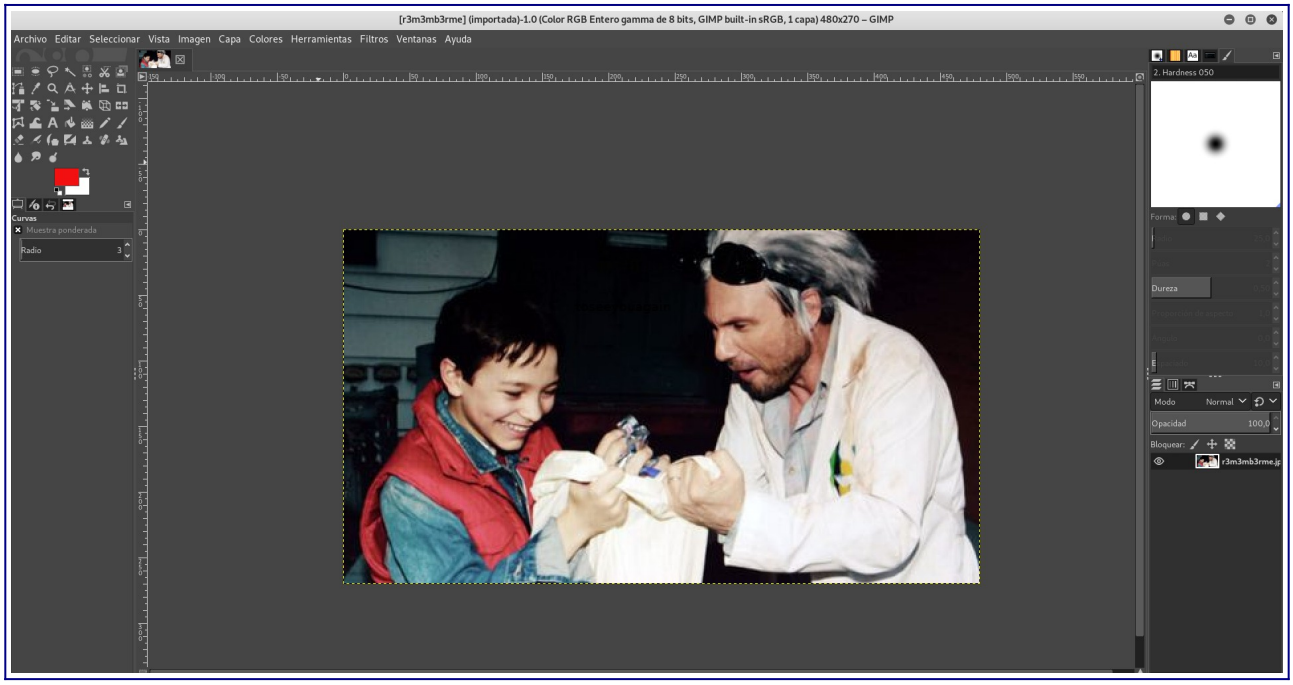
But ... one day I failed him. And from that day he stopped talking to me and looking at me, even the night he died. He did not say anything to me.

I remember ... he always told me that people try hard to hide their fears and shadows, but with a little light, everything is discovered.

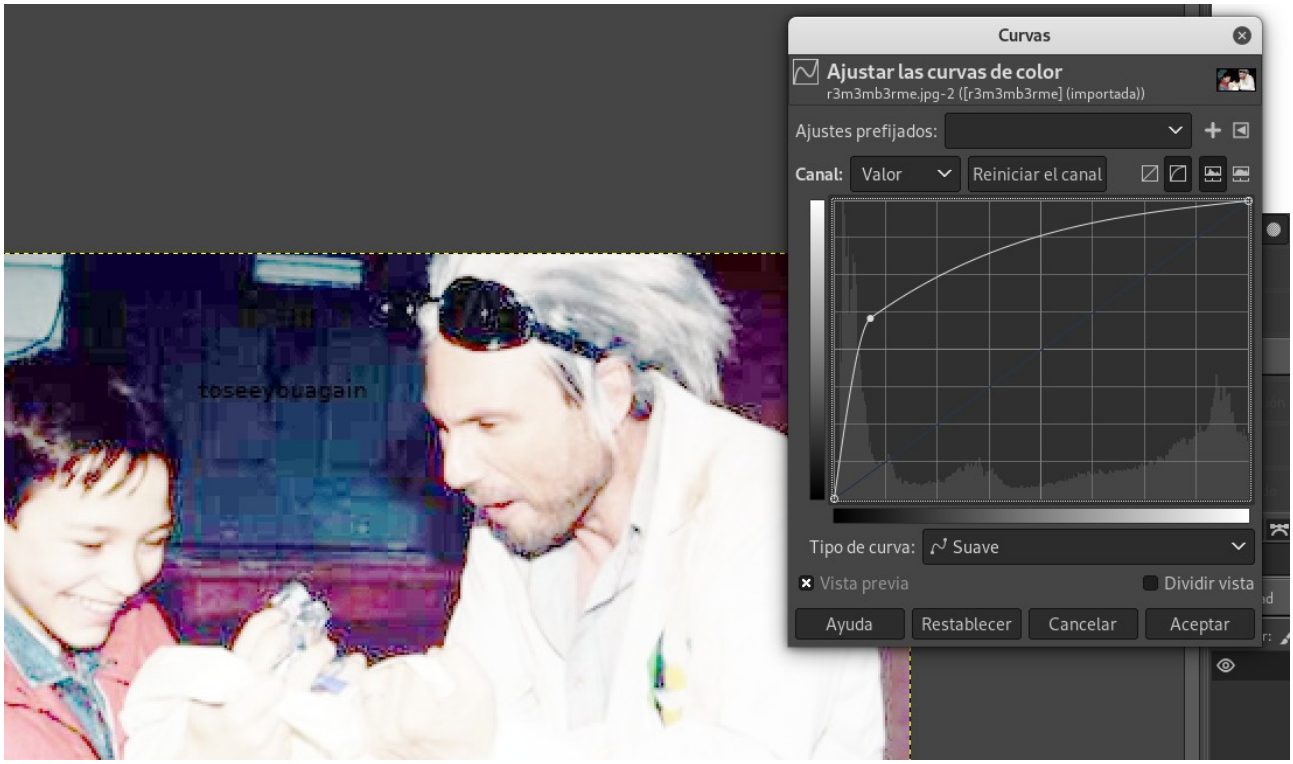
En especial debemos quedarnos con el último párrafo, pues es el que menos se ajusta a lo que dice Elliot en ese capítulo. Destacamos las palabras "**shadows**" y "**little light**". Pero vamos a verificar primero que efectivamente es una imagen y no nos la estan colando con nada:



Podemos apreciar que es un JPEG, pero sobretodo que se ha utilizado el software **GIMP** sobre dicha foto, esto nos puede dar una pista, pues seguramente habrán modificado algo con la imagen:



Y una vez la tenemos abierta, es cuando volvemos a pensar en esas dos palabras: luces y sombras… ¿Por qué no probamos a jugar con las curvas? De esta forma podemos ajustar la imagen y revelar información coincidente con determinados tonos de color.



Jugando con las curvas, descubrimos un pequeño mensaje oculto entre la cabeza del padre y elliot. Dice algo como: "**toseeyouagain**".

Una vez tenemos esta palabra, podemos intentar buscar mensajes ocultos en la imagen o meterla como flag, pero en ambas fracasaremos, pues ni es el formato, ni hay información oculta dentro de la imagen.

Si probamos a pasarle la herramienta Binwalk y analizamos la imagen en busca de firmas comunes de archivos, nos encontramos con lo siguiente:

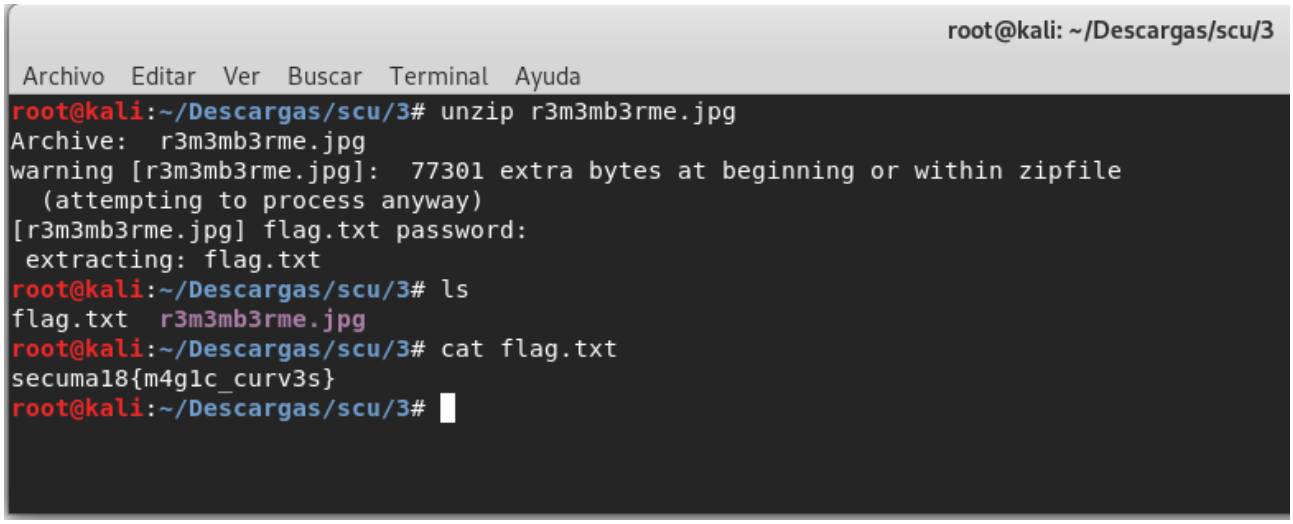
```
root@kali:~/Descargas/scu/3# binwalk -B r3m3mb3rme.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, little-endian offset of first image directory: 8
260           0x104           JPEG image data, JFIF standard 1.01
77301         0x12DF5         Zip archive data, encrypted at least v1.0 to extract, compressed size: 35, uncompressed size: 23, name: flag.txt
77496         0x12EB8         End of Zip archive, footer length: 22

root@kali:~/Descargas/scu/3#
```

Donde encontramos que hay un fichero ***ZIP** embebido junto con la imagen*, con un bonito flag.txt.

Si probamos a descomprimir la imagen, con unzip por ejemplo, nos intentará descomprimir el zip, y nos pide contraseña, para la cual escribimos la frase obtenida con las curvas: “toseeyouagain”.



Y tras extraer los ficheros, obtenemos un txt que contiene la **FLAG**!

by **@Secury**