

Descripción

Nombre: Gr33tings Pr0F3s0R F4lk3n (Related <https://www.imdb.com/title/tt0086567/>)

Fecha de liberación: 8 de Noviembre de 2018

Autor: 1v4n (<https://twitter.com/1r0Dm480> // <https://twitter.com/hackers4f>)

Categoría: Misc

Dificultad: Medio-Bajo

NORAD COC analysts detect unusual traffic. The incident is transferred to the FBI, they make arrests to a teenager named David. You can help us discover secrets.

Objetivo

Formato de la flag: flag{md5}

Resumen:

Método 1:

Herramientas utilizadas

Versión Versión 70.0.3538.102 (Build oficial) (64 bits) <https://www.google.com/chrome/>

<https://www.virustotal.com>

<https://www.onlinehexeditor.com>

<https://hexed.it>


<https://md5hashing.net>

<https://gchq.github.io/CyberChef>

<https://www.coordenadas-gps.com/convertidor-de-coordenadas-gps>

<https://console.cloud.google.com>

Comenzamos por visitar el reto y descargamos el archivo adjunto *RetoH4F_16_Gr33tings_Pr0F3s0R_F4lk3n* [MD5:afe112fe88a60e7129a6b18a279bdce8] https://drive.google.com/file/d/1XgxybBOHreSlzbQTHg6osC-4g_J17oP6/view sin extensión. Analizándolo en Virustotal detectamos datos Exif Metadata y compresión JPEG.



No engines detected this file

SHA-256: eeeab405555c9db82496f713441748de84cebef9c7831515778c09fcc9c097

File name: RetoH4F_16_Gr33tings_Pr0F3s0R_F4lk3n

File size: 118.98 KB

Last analysis: 2018-11-08 11:04:31 UTC

0 / 56

Detection

Details

Community

Basic Properties

MD5: afe112fe88a60e7129a6b18a279bdce8

SHA-1: abb5e08768f960a656a877f95b1156097bdcf99

File Type: unknown

Magic: data

SSDeep: 1536:9p1EL+g7G+/mg4TKaQ0/6H1weKVqH/EZIQq70/ET5E1CCa5OG7IHXPQMGAYD7Z9QG0uTK/66j5f5mTlz7yPkg1p

File Size: 118.98 KB

File Names

RetoH4F_16_Gr33tings_Pr0F3s0R_F4lk3n

ExifTool File Metadata

Compression: JPEG (old-style)

ExifByteOrder: Big-endian (Motorola, MM)

ImageDescription: -L4_hjurnal file Metadata

Make: Pana Camaras

ResolutionUnit: None

ThumbnailImage: (Binary data 67584 bytes, use -b option to extract)

ThumbnailLength: 67584

ThumbnailOffset: 260

Warning: Processing TIFF-like data after unknown 30-byte header

XResolution: 1

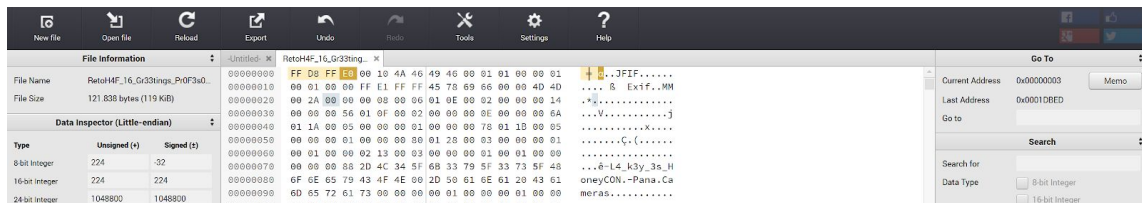
YCbCrPositioning: Centered

YResolution: 1

Pasamos a identificar el archivo con la web tool de <https://www.onlinehexeditor.com/> y nos arroja que el File Signature ha sido alterado con 00 00 00 00 confirmándose que estamos ante la estructura de un archivo de imagen JPG con ayuda de <https://filesignatures.net>

2 Results Found For JFIF File Extension		
Extension	Signature	Description
☆ JFIF	FF D8 FF E0	JPEG IMAGE
	ASCII	Size: 4 Bytes Offset: 0 Bytes
☆ JFIF	FF D8 FF E0	JFIF IMAGE FILE - jpeg
	ASCII	Size: 4 Bytes Offset: 0 Bytes

Modificamos el Magic Number (File Signature) de 00 00 00 00 a FF D8 FF E0 con la web tool <https://hexed.it/> que es la correspondiente a una imagen JFIF o JPEG y exportamos obteniendo el archivo *RetoH4F_16_Gr33tings_Pr0F3s0R_F4lk3n.jpeg* [MD5 54cc9bf888206cd863d1fde52e3c4349]



Ahora ya podemos ejecutar y abrir el archivo de imagen que esconde el artefacto inicial. En el que visualmente observamos un fotograma de la película de WarGames (1983) en el que se ambientará el reto https://es.wikipedia.org/wiki/Juegos_de_guerra



Con lo que vamos a extraer la información oculta con la web tool de Jeffrey's <http://exif.regex.info/exif.cgi>

Basic Image Information

Target file: RetoH4F_16_Gr33tings_Pr0F3s0R_F4lk3n.jpeg

Description:	L4_k3y_3s_HoneyCON
Camera:	-Pana Camera
File:	630 x 346 JPEG 121,838 bytes (119 kilobytes)
Color Encoding:	WARNING: No color-space metadata and no embedded color profile: Windows and Mac web browsers treat colors randomly. Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

Extracted 720 x 400 66-kilobyte "EXIF:ThumbnailImage" JPG
Displayed here at 62% width (52% the area of the original)

Click image to isolate; click this text to show histogram

Main JPEG image displayed here at 71% width (51% the area of the original)

Click image to isolate; click this text to show histogram

XMP

XMP Toolkit:	Image:ExifTool 11.16
Event:	-46 69 6c 6d
Person In Image:	kcaM refinneJ namthgiL divaD
Subject:	Blaise de Vigenere
Type:	57 61 72 47 61 6d 65 73 20 69 73 20 61 20 31 39 38 33
Instructions:	Qcflsc

JFIF

JFIF Version:	1.01
Resolution:	1 pixels/None

File — basic information derived from the file.

File Type:	JPEG
MMIO Type:	image/jpeg
Exif Byte Order:	Big-endian (Motorola, MM)
Encoding Process:	Baseline DCT, Huffman coding
Bits Per Sample:	8
Color Components:	3
File Size:	119 kB
File Type Extension:	jpg
Image Size:	630 x 346
Y Cb Cr Sub Sampling:	YCbCr4:2:0 (2 2)

Composite
This block of data is computed based upon other items. Some of it may be wildly incorrect, especially if the image is not a standard JPEG.

megapixels:	0.218
-------------	-------

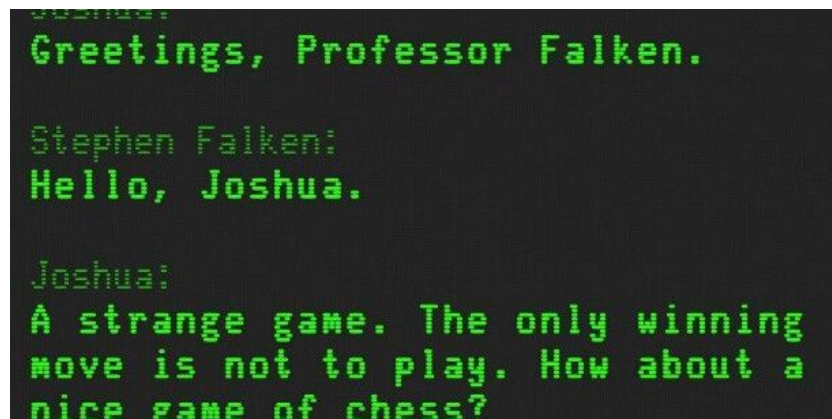
EXIF

Image Description:	L4_k3y_3s_HoneyCON
Make:	-Pana Camera
Compression:	JPEG (old-style)
Resolution:	1 pixels/None
Y Cb Cr Positioning:	Centered
X Resolution:	72
Y Resolution:	72
Resolution Unit:	inches
Thumbnail Length:	67,584
Thumbnail Image:	(67,584 bytes binary data)

Detectamos que la imagen de la etiqueta “ThumbnailImage” es diferente a la imagen principal y además nos arroja datos que no son los esperados en los metadatos como “L4_k3y_3s_HoneyCON”, “46 69 6c 6d”, “kcaM refinneJ namthgiL divaD”, “Blaise de Vigenere”, “57 61 72 47 61 6d 65 73 20 69 73 20 61 20 31 39 38 33” y “Qcflsc”.

El primer dato nos da una clave que es HoneyCON, el segundo dato codificado en Hexadecimal que nos encontramos es “Film”, el tercer dato es “David Lightman Jennifer Mack” en reverse, el cuarto es el nombre del criptógrafo al cual se le otorgó el nombre del cifrado Vigenere, el quinto dato es otro Hexadecimal

“WarGames is a 1983” y el sexto es un texto cifrado. Sospechamos que es un Vigenere y que la key que necesitamos es HoneyCON, resultando ser el nombre de **Joshua** (nombre de la AI del WOPR).



```
Joshua:
Greetings, Professor Falken.

Stephen Falken:
Hello, Joshua.

Joshua:
A strange game. The only winning
move is not to play. How about a
nice game of chess?
```

A partir de aquí nos quedaría descartar que el archivo de imagen no esconde más secretos en forma de esteganografía. Con lo que nos ayudaremos de <https://futureboy.us/stegano> y detectamos que nos nos guarda un secreto escondido de 2,7 KB:

Steganographic Encoder

This form uses steganography techniques to hide a secret message (or even another file) in a JPEG image, or a WAV or AU audio file. submit, you should be prompted to save your modified file.

If the payload is too large, (more than about 10% the size of the image for small images, closer to 20% for larger images) this may fail to data in it.

Select a JPEG, AU or WAV file to upload:

Seleccionar archivo Ningún archivo seleccionado

Password (may be blank):

Payload (select the appropriate radio button to either enter payload text directly or upload a file):

☒ Just find capacity of this file

☐ Text

☐ File payload: Seleccionar archivo Ningún archivo seleccionado

Enviar

"steganoin803.jpg":
format: jpeg
capacity: 2.7 KB

Pasamos a descubrir el secreto con la password **Joshua** en <https://futureboy.us/stegano/decinput.html>

arrojándonos como resultado la siguiente cadena en base64 que pasamos a decodificar:

VHJZX0g0ckQzcl9IM3lzXzFzX04wdGgxbmdfaHR0cHM6Ly93d3cueW91dHViZS5jb20vd2F0Y2g/dj1PcWVGQ2RYe
HF5RQ > TrY_H4rD3r_H3r3_1s_N0th1ng_https://www.youtube.com/watch?v=OqeFCdXxqyE

Steganographic Decoder

This form decodes the payload that was hidden in a JPEG image or a WAV or AU audio file using the [encoder form](#). When you submit, you will help you guess at what the payload is and its file type...

Select a JPEG, WAV, or AU file to decode:

Seleccionar archivo RetoH4F_16...F4k3n.jpeg

Password (may be blank):

Joshua

☒ View raw output as MIME-type: text/plain

☐ Guess the payload

☐ Prompt to save (you must guess the file type yourself.)

Enviar

Con el resultado que obtenemos, un clip video con música muy acorde para el reto, pensamos que queda camino por andar y pasamos a extraer la imagen 54cc9bf888206cd863d1fde52e3c4349.jpg [MD5: a6433d86bfb7f78353fb8f95dd753c31] que nos encontramos embebida en “ThumbnaillImage”.

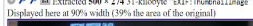
Volviendo a repetir los pasos anteriores en la web tool <http://exif.regex.info/exif.cgi> obtenemos de nuevo otra imagen embebida y datos codificados:

Basic Image Information

Target file: 54c9388396c863411d675c43492.jpg

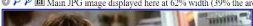
Copyright:	
File:	720 × 400 JPEG 67,584 bytes (66 kilobytes)
Color Encoding:	<p>WARNING: No color-space metadata and no embedded color profile: Windows and Mac web browsers treat colors randomly.</p> <p>Images for the web are most widely viewed when in the sRGB color space and with an embedded color profile. See my Introduction to Digital Image Color Spaces for more information.</p>

Extracted 500 × 274 (1) kilobyte "DGP/ThumbnailImage" JPG
Displayed here at 90% width (39% the area of the original)



Click image to isolate; click this text to show homepage

Main JPG image displayed here at 62% width (39% the area of the original)



Click image to isolate; click this text to show homepage

XMP

XMP Toolkit	Image::ExifTool 11.16
Instructions	-L4_F14G_N0s_3c0Nd3_S3cR3T0s_Y_Su_F0rM4T0_eS_H4F{md5}

EXIF

Y Cb Cr Positioning	Centered
Copyright	© 1999-2000 Sony Electronics Inc. All rights reserved. Sony, the Sony logo, "Walkman" and "Image" are registered trademarks of Sony Electronics Inc. in the U.S. and other countries. "Walkman" and "Image" are also registered trademarks of Sony Electronics Inc. in the U.S. and other countries. "Walkman" and "Image" are also registered trademarks of Sony Electronics Inc. in the U.S. and other countries.
GPS Version ID	2.3.0.0
GPS Longitude	118.326258 degrees
Compression	JPEG (old-style)
Resolution	72 pixels/inch
Software	-Hs4Oo_D3_4_t4N3
Thumbnail Length	31,602
Thumbnail Image	(31,602 bytes binary data)

[illegible]

El primer dato nos vuelve a recordar “L4_Fl4G_N0s_3sC0nD3_S3cR3T0s_Y_Su_F0rM4T0_eS_H4F{md5}”, el segundo nos arroja decodificando el Morse “[HTTPS://TWITTER.COM/DAVIDLIGHTMAN83](https://twitter.com/DAVIDLIGHTMAN83)” el perfil de twitter creado en octubre de 2017 de @davidlightman83 (parece una pista falsa xD), seguimos con la Longitud de una coordenada GPS con valor 118.326258 y finalmente una codificación Atbash “Sh4LI_W3_4_g4M3”



De nuevo a partir de aquí nos quedaría descartar que el archivo de imagen no esconde más secretos en forma de esteganografía. Que vuelve a ser afirmativo.

Steganographic Encoder

This form uses steganography techniques to hide a secret message (or even another file) in a JPEG image, or a WAV or AU audio file. The submitter you should be prompted to save your modified file.

If the payload is too large, (more than about 10% the size of the image for small images, closer to 20% for larger images) this may fail silent data in it.

Select a JPEG, AU or WAV file to upload:
 54cc9b88820...e3c4349.jpg

Password (may be blank):

Payload (select the appropriate radio button to either enter payload text directly or upload a file):

☒ Just fit capacity of this file

☐ Text

☐ File payload: Ningún archivo seleccionado

Enviar:

"steganoin10736.jpg":
format: jpeg
capacity: 1.8 KB

Intentamos descubrir el secreto sin password en <https://futureboy.us/stegano/decinput.html> pero esta vez sin éxito. Probamos con posibles contraseñas comunes pero no conseguimos nada. Por lo tanto seguiremos adelante sin atascarse ya que no encontramos pistas de un posible ataque de diccionario. :(

Pasamos, de nuevo, a extraer la imagen a6433d86bfb7f78353fb8f95dd753c31.jpg [MD5: fb665a8c32385667aa63ca62637810c6] que nos encontramos en “ThumbnailImage”. Y volviendo a repetir los pasos anteriores en la web tool <http://exif.regex.info/exif.cgi> sin obtener finalmente ninguna imagen embebida pero sí datos codificados:

Basic Image Information

Target file: a6433d86bfb7f78353fb8f95dd753c31.jpg

Description:	1DRfUDRzU19sNF8zBkMwblRSNHl0U18zb18zTF9NMHYxM19DbDFwXzNTX0RETU1BQUFBX1dIRU5fSVRfV0FTX0xPQURFRF95XzRudDNzX0QzX1V0MWwxejRybGFfUk9DS3lvdQ
File:	500 x 274 JPEG 31,602 bytes (31 kilobytes)
Color Encoding:	WARNING: No color-space metadata and no embedded color profile: Windows and Mac web browsers treat colors randomly. Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

XMP

XMP Toolkit	Image::ExifTool 11.36
Person In Image	D4v1D 1Mo41 8000 WOPR
Instructions	07ba59a1bdccf263e2e3a12c5b097d47

EXIF

Image Description	Encoded as: 1DRfUDRzU19sNF8zBkMwblRSNHl0U18zb18zTF9NMHYxM19DbDFwXzNTX0RETU1BQUFBX1dIRU5fSVRfV0FTX0xPQURFRF95XzRudDNzX0QzX1V0MWwxejRybGFfUk9DS3lvdQ
Y Cb Cr Positioning	Centered
GPS Version ID	2.3.0.0
GPS Latitude	34.067933 degrees
Resolution	1 pixels/None

JFIF

JFIF Version	1.01
Resolution	1 pixels/None

File — basic information derived from the file:

File Type	JPEG
MIME Type	image/jpeg
File Byte Order	Big-endian (Motorola, MM)
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
File Size	31 KB
File Type Extension	jpg
Image Size	500 x 274
Y Cb Cr Sub Sampling	YCbCr4:4:4 (1:1)

Los datos no esperados en los metadatos son “TDRfUDRzU19sNF8zBkMwblRSNHl0U18zb18zTF9NMHYxM19DbDFwXzNTX0RETU1BQUFBX1dIRU5fSVRfV0FTX0xPQURFRF95XzRudDNzX0QzX1V0MWwxejRybGFfUk9DS3lvdQ”, un Hash MD5 b7ba59a1bdccf263e2e3a12c5b097d47” y “GPS Latitude 34.067933 degrees”.

El primer dato nos arroja despues de decodificar el base64 “L4_P4s_I4_3nC0nTR4r4S_3n_3L_M0v13_C1p_3S_DDMMAAAA_WHEN_IT_WAS_LOADED_y_4nt3s_D3_Ut1l1z4rla_ROCKyou” (tenemos que arrojar rockyou primero, posiblemente en la esteganografía) y el segundo lo obtenemos haciendo reverse al MD5 “https://www.youtube.com/watch?v=KXzNo0vR_dU” un clip de video del que nos están pidiendo el **DDMMAAAA** de cuando fue cargando en YouTube. En este caso fue **30072013**.

WarGames (3/11) Movie CLIP - Shall We Play a Game? (1983) HD

364.222 visualizaciones 1,1 MIL 35 COMPARTIR GUARDAR

Movieclips ©
Publicado el 30 jul. 2013

WarGames: movie online: <http://tiny.cc/mn1hGFr9Q>

No nos olvidamos del último dato que es “GPS Latitude 34.067933 degrees” que con el datos obtenidos en la anterior imagen “GPS Longitude 118.326258 degrees”, utilizamos la herramienta online <https://www.coordenadas-gps.com/convertidor-de-coordenadas-gps> y nos geolocaliza un lugar en China. :o

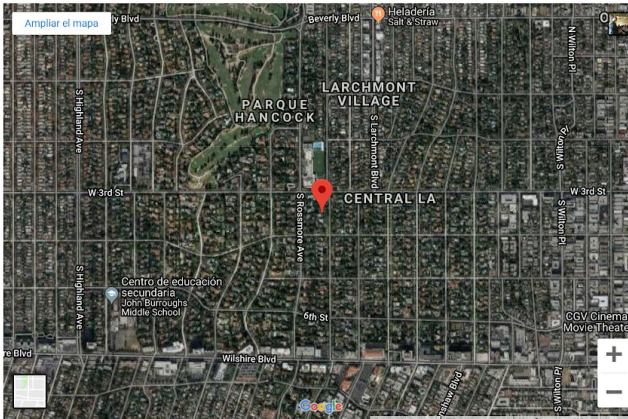
Vamos a jugar con los signos de la Longitud y buscamos en (34.0679329, -118.326258) y nos geolocaliza el **333 S Arden Blvd, Los Angeles, CA 90020, EE. UU.** localización de la casa de nuestro protagonista dónde se rodó en 1982 la película WarGames. <http://www.themoviedistrict.com/wargames/>

Dirección

Obtener coordenadas GPS

GD (grados decimales)*
Latitud
Longitud
Obtener Dirección
Ver el mapa

GMS (grados, minutos, segundos)*
Latitud☐ N ☐ S
Longitud☐ E ☐ O



De nuevo a partir de aquí nos quedaría descartar que el archivo de imagen no esconde más secretos en forma de esteganografía. Que vuelve a ser afirmativo.

Steganographic Encoder

This form uses steganography techniques to hide a secret message (or even another file) in a JPEG image, or a WAV or AU : casual observer. Once you submit, you should be prompted to save your modified file.

If the payload is too large, (more than about 10% the size of the image for small images, closer to 20% for larger images) this below before embedding data in it.

Select a JPEG, AU or WAV file to upload:

Seleccionar archivo: a6433d86bfb...d753c31.jpg

Password (may be blank):

Payload (select the appropriate radio button to either enter payload text directly or upload a file):

☒ Just find capacity of this file

☐ Text

File payload: Seleccionar archivo Ningún archivo seleccionado

Enviar

"steganoin13196.jpg":
format: jpeg
capacity: 1.5 KB

Como nos aconsejaron anteriormente que utilizáramos el diccionario rockyou (

<https://www.scrapmaker.com/data/wordlists/dictionaries/rockyou.txt>)

"L4_P4sS_I4_3nC0nTR4r4S_3n_3L_M0v13_Cl1p_3S_DDMMAAAA_WHEN_IT_WAS_LOADED_y_4nt3s_D3_Ut1l 1z4rla_ROCKyou". Si filtramos el diccionario con el término "wargame" y obtendremos que **wargame123** es la password que nos revelará la esteganografía una URL acertada que nos dirigirá a la segunda parte del reto:

<https://goo.gl/oAdWFn> > Reto_16H4F_HB_AFS101.7z [MD5: 71ff799128e00e1a4a4b04a3a6d456df]

El archivo comprimido nos solicita una contraseña que obtuvimos en la última imagen **30072013**, y pasamos a obtener otro archivo comprimido **N0r4D.tar** [MD5: d7dff2e29a49f86a441b7381214105db] que descomprimos y obtenemos finalmente un archivo de audio hint_modem.wav [MD5: adc9599695c1ae757218525824ba5963] y el archivo comprimido FI4g.rar [edbe186b80fa0708a85cf1bee0a3ab9b] que nos pide una password para conseguir nuestra FLAG.

Investigando encontramos cómo interpretar el sonido del modem con \$minimodem

(<http://www.whence.com/minimodem/minimodem.1.html>) para ello necesitaremos una consola online en

<https://console.cloud.google.com> y con los siguientes comandos:

```
sudo apt-get install minimodem

minimodem --rx 100 -f hint_modem.wav
### CARRIER 100 @ 1250.0 Hz ###
GREETINGS PROFESSOR FALKEN.
Hello.
```

HOW ARE YOU FEELING TODAY?

I'm fine. How are you?

EXCELLENT. IT'S BEEN A LONG TIME. CAN YOU EXPLAIN
THE REMOVAL OF YOUR USER ACCOUNT NUMBER ON 6/23/73?

People sometimes make mistakes

YES THEY DO. SHALL WE PLAY A GAME?

Love to. How about Global Thermonuclear War?

WOULDN'T YOU PREFER A GOOD GAME OF CHESS?

Later. Lets play Global Thermonuclear War....

...THANK YOU FOR PLAYING THIS GAME THE PASSWORD TO FIND THE FLAG IS THE NUMBER
OF THE HOUSE WHERE DAVID LIVES

```
### NOCARRIER ndata=511 confidence=9.499 ampl=0.936 bps=100.00 (rate perfect)
###
```

La password es el número de la casa donde vive David L. nuestro protagonista y que ya obtuvimos en el pasos anteriores> **333** . Pasamos a descomprimir el archivo Fl4g.rar y obtenemos la escondida FLAG en el archivo **Fl4G_R3t0_16**.

Y la solución es **H4F{05dfb621cdca15c190334d3b2eedcceb}**

Autor: 1v4n a.k.a. @1r0Dm4480

Twitter: <https://twitter.com/Hackers4f> // <https://twitter.com/1r0Dm4480>