



II. OSINT, Esteganografía y Forense

Inés Martín, Carlos Barahona, Clara Contreras y Sergio Pérez

Índice

1. OSINT

1. OSINT Básico
2. IMINT
3. HUMINT

2. Esteganografía (*stego*)

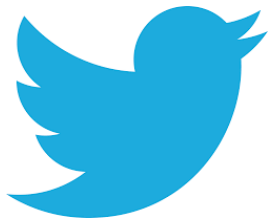
1. Exiftool, binwalk, foremost...
2. *Guess the tool*
3. *Stego-toolkit*

3. Forense

1. Magic bytes
2. Strings
3. Volatility: primeros pasos

1. OSINT

- Se trata de descubrir información de fuentes abiertas (*Open Source Intelligence*)
- Normalmente, tirando del hilo llegaremos a la flag
- Hay muchas formas de dar la información en estos retos



1. OSINT



<https://osintframework.com/>



1. OSINT

- Habrá ocasiones que las páginas web que queremos visitar ya no están disponibles
- ¿Significa que han desaparecido de Internet?
- Recuerda que Internet, normalmente, es para siempre



[WayBackMachine:http://archive.org/](http://archive.org/)

1. OSINT

EJEMPLO DE UNO DE ESTOS RETOS

Tengo un amigo que acaba de empezar a jugar al CS:GO y se cree que es un pro player. Tanto que en algunas de sus redes sociales se hace llamar Pr0g4m3rCSG0. Incluso le ha dado por grabar vídeos con sus kills...

El otro día se dejó su cuenta abierta en mi PC y escondí una flag en su contenido, además de hacer alguna publicación en su nombre. ¿Puedes recuperar la flag?

1. IMINT

- Otras veces la información no es tan clara
- Pueden darnos una imagen de la que partir para encontrar otra información:
 - En qué ciudad/calle/país/lugar se hizo la imagen
 - Obtener información de una persona a partir de la imagen
 - Encontrar un número de vuelo, número de teléfono, etc.



1. IMINT

Geolocation Estimation

<https://labs.tib.eu/geoestimation/>



Instructions


Image Selection

Open (47/48)


Annotated (1/48)

Upload

Choose Random



We are working on an improved visualization, since currently it could fail on some examples.



Reference

For details on the deep learning approach please check our publication:

Müller-Budack E., Pustu-Iren K., Ewerth R. (2018) Geolocation Estimation of Photos Using a Hierarchical Model and Scene Classification. In: Ferrari V., Hebert M., Sminchisescu C., Weiss Y. (eds) Computer Vision – ECCV 2018. ECCV 2018. Lecture Notes in Computer Science, vol 11216. Springer, Cham

This work is financially supported by the German Research Foundation (DFG project number 388420599).

Guess Location

Leaflet | © Mapbox © OpenStreetMap Improve this map

Marker:

User

Model

Ground truth

EXIF (if available)

Statistics

Reset

Annotated images: 1

Rate of success: 0 / 1 (0%)

Your mean error: 7165 km

Model's mean error: 0 km

Result

Distance to ground truth or EXIF location:

You: 7164.97 km

Model: 0.26 km

Scene Classification

Probability indoor: 2.36%

Probability nature: 3.25%

Probability urban: 94.39%

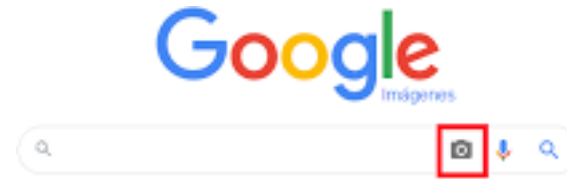
Predicted scene: urban

7

Inés Martín, Carlos Barahona, Clara Contreras y Sergio Pérez

1. IMINT

- Google imágenes
- TinEye (<https://tineye.com/>)
- Yandex (<https://yandex.com/>)
- Google Lens
- Otros buscadores
 - DuckDuckGo, Bing...



Yandex



Google Lens



Microsoft Bing



1.HUMINT

- Otro de los casos más comunes es que nos den (o encontremos durante nuestra investigación) algún dato personal de nuestro objetivo
- Tenemos entonces que empezar a utilizar otros mecanismos
 - Si es un mail: cuentas asociadas (<https://tools.epieos.com>), leaks asociados a esas cuentas (<https://haveibeenpwned.com/>) ...
 - Si es un número de teléfono: cuentas asociadas en RRSS, herramientas abiertas
 - Si es un nombre: LinkedIn, Freelancer, TripAdvisor... redes donde se utiliza el nombre real
 - Si es un usuario: redes sociales/plataformas como Twitter, Github, Instagram...
<https://github.com/sherlock-project/sherlock>









□ ☆ [Redacted]

⌵ Filtrar las URL
|| 🔍 ⓧ
Todos
HTML
CSS
JS
XHR
Tipografía
Imágenes
Medios
WS
Otros
☐ Desactivar caché
Sin limitación ⌵
⚙️

```
1
2
3
4 b4CbAwV89nhZabFPUuhh3tD_YB3llmV-FQA\",1],\"10
5
6
7
```

1.HUMINT

Con este dato ahora podemos acceder a mucha de la información asociada a su cuenta de Google

- API de Google
 - <https://developers.google.com/people/api/rest/v1/people/get>
- Google Fotos
 - <https://get.google.com/albumarchive/{userID}>
- Google Maps
 - <https://www.google.com/maps/contrib/{userID}>

1. OSINT

OTRO EJEMPLO

Hemos rastreado a un usuario que nos robó el número de tarjeta de crédito hace algún tiempo. Él no sabía que éramos hackers, y ha intentado cazar a un cazador. Sabemos que utiliza el pseudónimo de 3lMu10 y que tiene un curso de carding en la darknet. ¿Podrías ayudarnos a encontrar el dominio onion en el que se aloja?

Hint: No es necesario navegar por la deep web para encontrar el dominio de 3lMu10.

TOOLS

<https://osintframework.com/>

Histórico Web: <http://archive.org/>

Localización Imágenes: <https://labs.tib.eu/geoestimation/>

Imágenes: Google imágenes, TinEye (<https://tineye.com/>),
Yandex (<https://yandex.com/>), Google Lens

Emails: <https://tools.epieos.com>, <https://haveibeenpwned.com/>

Usuarios: Redes sociales, <https://github.com/sherlock-project/sherlock>

1. Esteganografía

¿Qué es la esteganografía?

La **esteganografía** trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos dentro de otros, de modo que no se perciba su existencia.



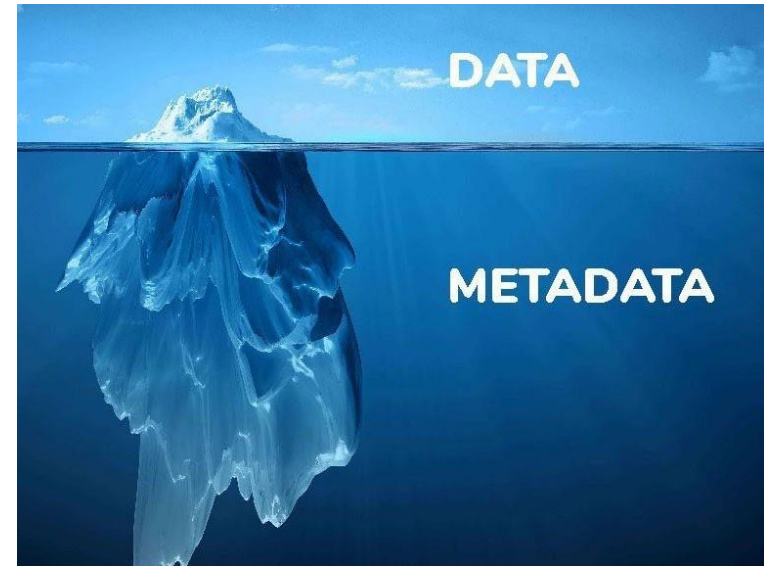
1. Esteganografía

¿Qué son los metadatos?

“Datos acerca de los datos”

Es información que caracteriza datos, describen el contenido, calidad, condiciones, historia, disponibilidad y otras características de estos.

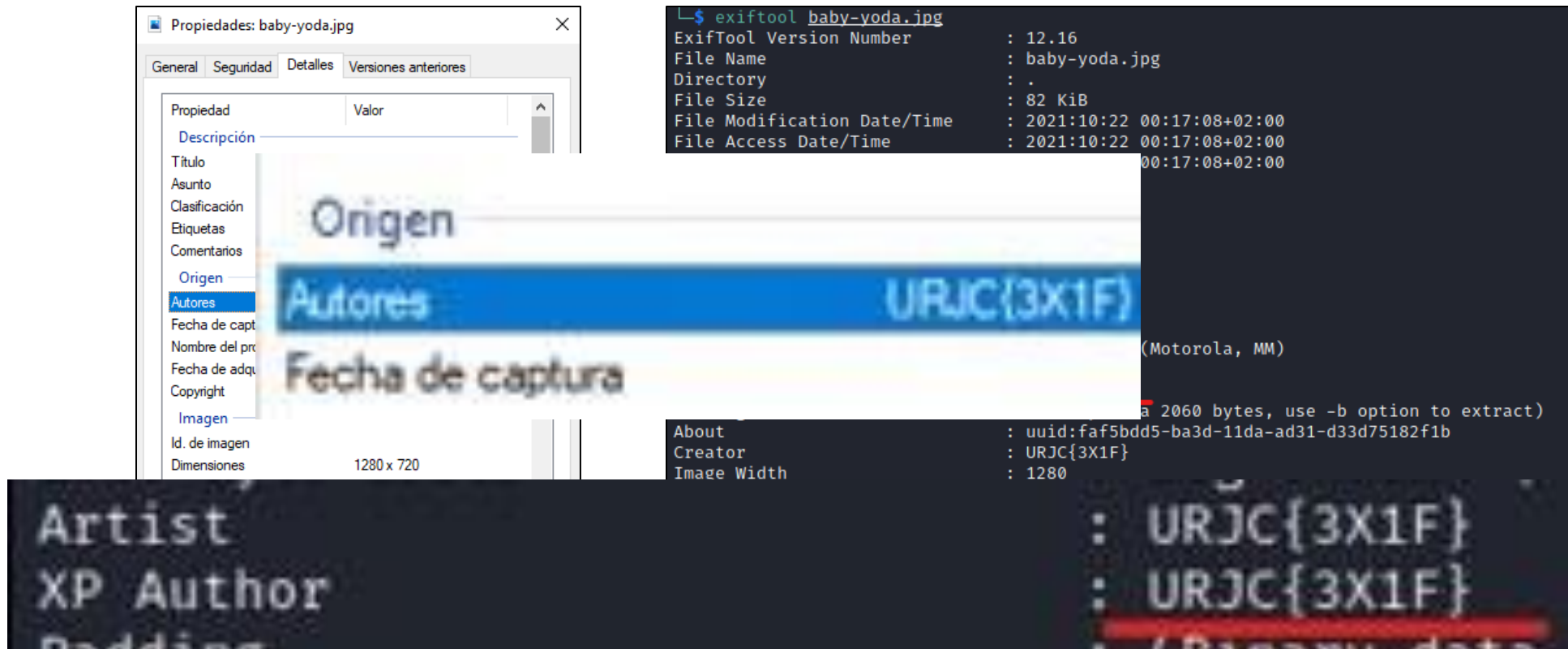
En los metadatos podremos encontrar información relevante.



1. Esteganografía

Exiftool

Herramienta utilizada para extraer los metadatos de los archivos.



The image shows two side-by-side screenshots. The left screenshot is a Windows 'Propiedades: baby-yoda.jpg' window, with the 'Detalles' tab selected. It displays a list of properties on the left and their values on the right. The 'Origen' (Origin) property is highlighted, showing the value 'URJC{3X1F}'. Other visible properties include 'Autores', 'Fecha de captura', 'Id. de imagen', and 'Dimensiones' (1280 x 720). The right screenshot is a terminal window showing the command `exiftool baby-yoda.jpg` and its output. The output lists various EXIF metadata fields and their values, including 'ExifTool Version Number: 12.16', 'File Name: baby-yoda.jpg', 'File Size: 82 KiB', 'File Modification Date/Time: 2021:10:22 00:17:08+02:00', 'File Access Date/Time: 2021:10:22 00:17:08+02:00', 'About: uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b', 'Creator: URJC{3X1F}', 'Image Width: 1280', 'Artist: URJC{3X1F}', 'XP Author: URJC{3X1F}', and 'Padding: (Binary data)'. The 'URJC{3X1F}' value is highlighted in blue in the terminal output.

Propiedad	Valor
Origen	URJC{3X1F}
Autores	
Fecha de captura	
Id. de imagen	
Dimensiones	1280 x 720

```
exiftool baby-yoda.jpg
ExifTool Version Number      : 12.16
File Name                    : baby-yoda.jpg
Directory                    : .
File Size                    : 82 KiB
File Modification Date/Time  : 2021:10:22 00:17:08+02:00
File Access Date/Time       : 2021:10:22 00:17:08+02:00
About                        : uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b
Creator                      : URJC{3X1F}
Image Width                  : 1280
Artist                       : URJC{3X1F}
XP Author                    : URJC{3X1F}
Padding                      : (Binary data)
```

1. Esteganografía

Técnicas y herramientas comunes

Binwalk

Es una herramienta que detecta y extrae archivos que se encuentran ocultos dentro de otros.

```
william@ubuntu:~/Documents$ binwalk -Me fw.bin
 8F9BB0
 8F9BB0.7z
 8F9BB0.extracted
 68A180
 68A180.7z
 72C1B0
 72C1B0.7z
 72C1B0.extracted
  DC39.crt
  E161.crt
  EBAF.crt
  F224.crt
736648
```



<https://github.com/ReFirmLabs/binwalk>



1. Esteganografía

Técnicas y herramientas comunes

Steghide

Es una herramienta que, dada una contraseña, permite esconder archivos dentro de otros.



<http://steghide.sourceforge.net/>



Stegseek

Realiza un ataque por diccionario a la contraseña de la herramienta steghide.



<https://github.com/RickdeJager/stegseek>



1. Esteganografía

```
root@kali:~/Escritorio# steghide embed -ef texto.txt -cf imagen.jpg -N
Enter passphrase:
Re-Enter passphrase:
embedding "texto.txt" in "imagen.jpg"... done
root@kali:~/Escritorio#
root@kali:~/Escritorio# steghide extract -sf imagen.jpg -xf archivo.txt
Enter passphrase:
wrote extracted data to "archivo.txt".
root@kali:~/Escritorio# ls
archivo.txt  imagen.jpg  texto.txt
root@kali:~/Escritorio#
```

Stegseek version 0.1

=== Stegseek Help ===

To crack a stegofile;

stegseek --crack -sf [stegofile.jpg] -wl [wordlist.txt]

Cracking options:

-sf, --stegofile	select stego file
-wl, --wordlist	select the wordlist file
-t, --threads	set the number of threads. Defaults to the number of cores.
-v, --verbose	display detailed information
-q, --quiet	skip performance metrics (slightly increases performance)

Use "stegseek --help -v" to include steghides help.

```
stegseek --crack -sf pic.jpg -wl rockyou.txt
```

```
[i] Read the entire wordlist (14344391 words), starting cracker
```

```
[ 14344392 / 14344391 ] (100,00%)
```

```
[i] --> Found passphrase: "      1"
```

```
[i] Original filename: "secret.txt"
```

```
[i] Extracting to "pic.jpg.out"
```

1. Esteganografía



1. Esteganografía

Técnicas y herramientas comunes

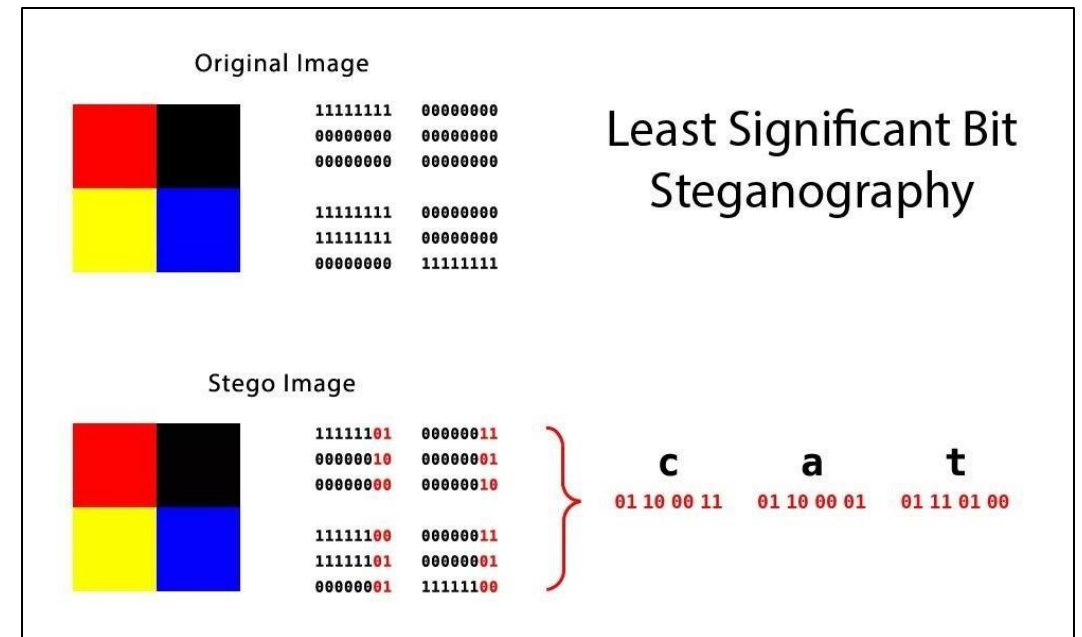
LSB (Least Significant Bit)

Es una técnica que oculta datos en los bits menos significantes de cada pixel de una imagen.

También se podría aplicar a otros archivos como por ejemplo vídeos.



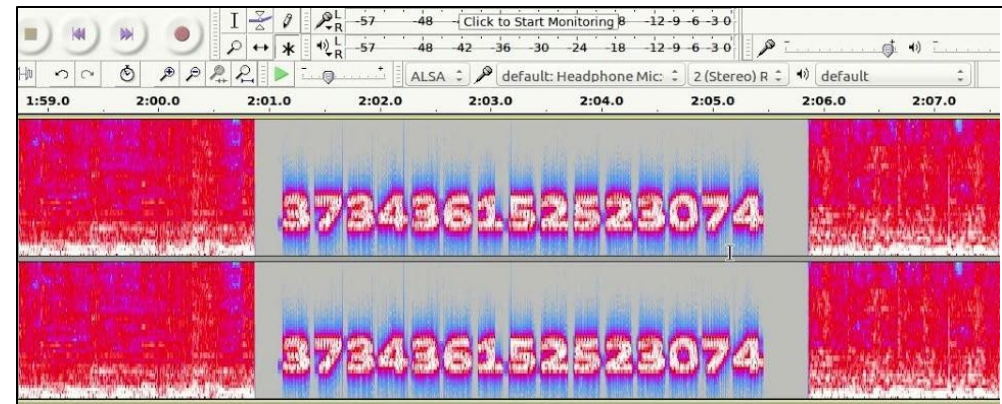
<https://pypi.org/project/stego-lsb/>



1. Esteganografía

Archivos de audio/vídeo

Suele ser interesante ver el **espectrograma** a de los archivos de audio/vídeo para buscar mensajes ocultos (texto, código morse...)



Audacity
Sonic Visualizer

<https://academo.org/demos/spectrum-analyzer/>



1. Esteganografía

Stego Toolkit

- Es una colección de herramientas de esteganografía de gran utilidad para los CTF.
- Contiene una lista detallada de las herramientas que podríamos utilizar según los distintos casos, y el uso de cada una de ellas.
- `check_jpg.sh` y `check_png.sh`

<https://github.com/DominicBreuker/stego-toolkit>

Tool	Description	How to use
file	Check out what kind of file you have	<code>file stego.jpg</code>
exiftool	Check out metadata of media files	<code>exiftool stego.jpg</code>
binwalk	Check out if other files are embedded/appended	<code>binwalk stego.jpg</code>
strings	Check out if there are interesting readable characters in the file	<code>strings stego.jpg</code>
foremost	Carve out embedded/appended files	<code>foremost stego.jpg</code>
pngcheck	Get details on a PNG file (or find out is actually something else)	<code>pngcheck stego.png</code>
identify	GraphicMagick tool to check what kind of image a file is. Checks also if image is corrupted.	<code>identify -verbose stego.jpg</code>
ffmpeg	ffmpeg can be used to check integrity of audio files and let it report infos and errors	<code>ffmpeg -v info -i stego.mp3 -f null -</code> to recode the file and throw away the result

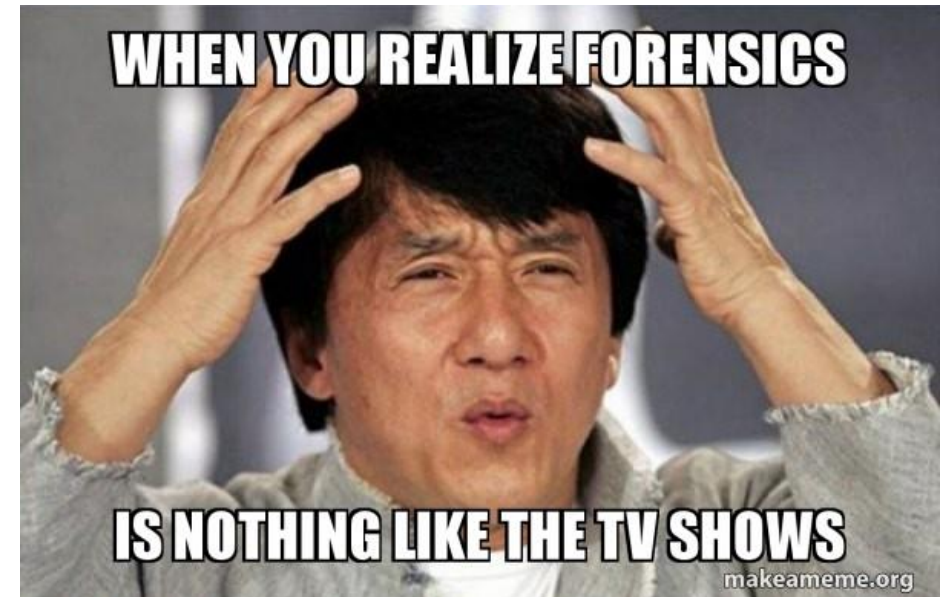


III. Forense

¿Qué es el análisis forense?

El análisis forense informático comprende el conjunto de técnicas pensadas para extraer la información de cualquier soporte sin alterar su estado. Esto permite buscar datos ocultos, dañados o eliminados.

El resultado del análisis de la información puede ser una prueba determinante en un proceso judicial.



III. Forense

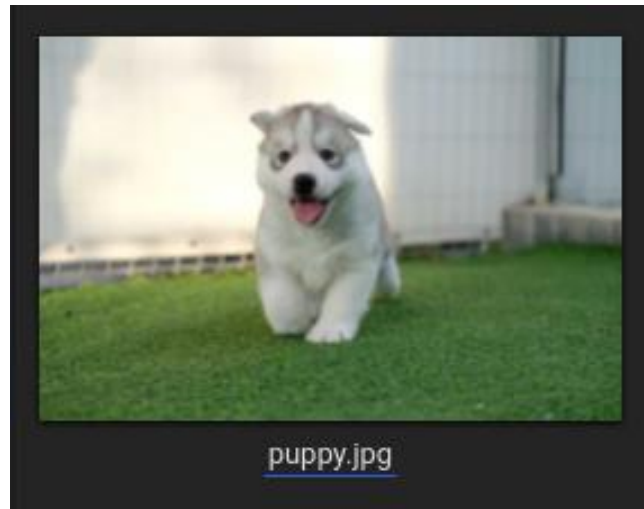
Análisis forense

- Análisis de archivos
- Análisis de discos duros
- Análisis de memoria RAM
- Análisis de tráfico de red
- Otros: logs, emails, *mobile*, tráfico USB...



III. Forense - Archivos

¿Cómo sabe el sistema que un archivo que parece una fotografía es una fotografía de verdad?

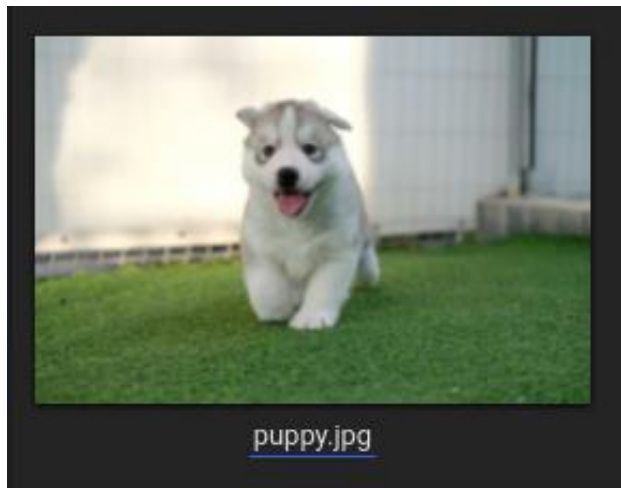


III. Forense - Archivos

Magic Bytes

Conjunto de bytes que se utilizan para identificar el formato de los archivos.

Normalmente se encuentran al principio de estos, pero también podrían encontrarse al final.



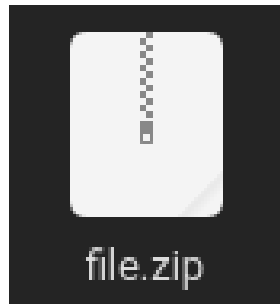
FF D8 FF DB	yøÿÜ	0	jpg
-------------	------	---	-----

```
~/Documents/URJC-CTF xxd puppy.jpg | head
00000000: ffd8 ffdb 0043 0010 0b0c 0e0c 0a10 0e0d .....C.....
00000010: 0e12 1110 1318 281a 1816 1618 3123 251d .....(.....1#%.
00000020: 283a 333d 3c39 3338 3740 485c 4e40 4457 (:3=<9387@H\N@DW
00000030: 4537 3850 6d51 575f 6267 6867 3e4d 7179 E78PmQW_bghg>Mqy
00000040: 7064 785c 6567 63ff db00 4301 1112 1218 pdx\egc...C....
00000050: 1518 2f1a 1a2f 6342 3842 6363 6363 6363 ../../cB8Bccccccc
00000060: 6363 6363 6363 6363 6363 6363 6363 6363 cccccccccccccccc
00000070: 6363 6363 6363 6363 6363 6363 6363 6363 cccccccccccccccc
00000080: 6363 6363 6363 6363 6363 6363 ffc2 0011 cccccccccccc....
00000090: 0803 5505 0003 0122 0002 1101 0311 01ff ..U....".....
```

[Lista de magic bytes](#)

III. Forense - Archivos

¿Es un ZIP de verdad?



```
~/Documents/URJC-CTF file file.zip
file.zip: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1
```

```
~/Documents/URJC-CTF sudo binwalk file.zip
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01

```
~/Documents/URJC-CTF exiftool file.zip
```

ExifTool Version Number	: 12.44
File Name	: file.zip
Directory	: .
File Size	: 10 kB
File Modification Date/Time	: 2022:10:16 17:32:52-04:00
File Access Date/Time	: 2022:10:16 17:33:13-04:00
File Inode Change Date/Time	: 2022:10:16 17:32:52-04:00
File Permissions	: -rw-r--r--
File Type	: JPEG
File Type Extension	: jpg
MIME Type	: image/jpeg
JFIF Version	: 1.01
Resolution Unit	: None
X Resolution	: 1
Y Resolution	: 1
Image Width	: 200
Image Height	: 252
Encoding Process	: Baseline DCT, Huffman coding
Bits Per Sample	: 8
Color Components	: 3
Y Cb Cr Sub Sampling	: YCbCr4:4:4 (1 1)
Image Size	: 200x252
Megapixels	: 0.050

III. Forense - Archivos

Strings

Herramienta que muestra las cadenas de caracteres imprimibles que están contenidas en un fichero.

```
~/Documents/URJC-CTF strings Archive.zip | tail
9xLd
gt~[
r*X{
"aW) N1
B*yS81
secret.txt
jsf;[
:PU&
puppy.jpg
secret.txt
```

¿Por qué es importante?

Nos puede ayudar a encontrar librerías cargadas en un binario, IPs o dominios maliciosos, firmas de malware, comandos sospechosos, palabras clave...

III. Forense - Retos Cortitos

Vamos a hacer unos ejercicios rápidos que utilizan las herramientas que hemos comentado.

Quedate	Stego
ExifSeal	Stego
Foto misteriosa	Stego
AHHHHH	Forense
Numeritos mágicos	Forense
Test	Forense

III. Forense - Volatility

¿Qué es Volatility?

Es una colección de herramientas que nos ayudan a analizar "dumps" de memoria volátil (RAM)

Fácil de ejecutar ya que está implementada en Python

Preinstalada en la máquina del curso



III. Forense - Volatility (Primer paso)

```
(urjc@ETSICTF)-[~/Documentos/dump]
$ vol.py -f dump.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO      : volatility.debug      : Determining profile based on KDBG search ...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1  : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2  : FileAddressSpace (/home/urjc/Documentos/dump/dump.raw)
PAE type   : No PAE
DTB        : 0x187000L
KDBG       : 0xf80002bfe0a0L
Number of Processors : 8
Image Type (Service Pack) : 1
```

El plugin "imageinfo" nos da información sobre el dump que vamos a comenzar a analizar

Lo más importante es quedarnos con el "profile"

III.Forense - Volatility (pslist)

```
(urjc@ETSIICTF)-[~/Documentos/dump]  
$ vol.py -f dump.raw --profile="Win7SP1x64" pslist
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start
0xfffffa801afe1b30	firefox.exe	3312	3692	33	353	1	1	2020-06-12 16:16:16 UTC+0000
0xfffffa801a811520	firefox.exe	3084	3692	39	381	1	1	2020-06-12 16:16:16 UTC+0000
0xfffffa801af39b30	firefox.exe	2784	3692	25	307	1	1	2020-06-12 16:16:21 UTC+0000
0xfffffa801aa10270	notepad.exe	3060	1928	2	58	1	0	2020-06-12 16:16:34 UTC+0000
0xfffffa8019dc1b30	spsvc.exe	3000	512	5	164	0	0	2020-06-12 16:17:13 UTC+0000
0xfffffa801aff97d0	svchost.exe	3656	512	13	351	0	0	2020-06-12 16:17:13 UTC+0000
0xfffffa8018faf630	7zFM.exe	868	1184	4	149	1	0	2020-06-12 16:17:32 UTC+0000
0xfffffa8018f7e060	SearchProtocol	2256	1036	8	287	1	0	2020-06-12 16:18:24 UTC+0000
0xfffffa801ace08a0	SearchFilterHo	2320	1036	6	103	0	0	2020-06-12 16:18:24 UTC+0000
0xfffffa801a9d5b30	SearchProtocol	1960	1036	8	284	0	0	2020-06-12 16:18:24 UTC+0000
0xfffffa8019011b30	MRCv120.exe	1376	1928	16	319	1	1	2020-06-12 16:18:50 UTC+0000
0xfffffa8019096060	WMIADAP.exe	1184	888	6	98	0	0	2020-06-12 16:19:13 UTC+0000
0xfffffa8019066060	WmiPrvSE.exe	1400	648	8	126	0	0	2020-06-12 16:19:13 UTC+0000

III.Forense - Volatility (cmdline)

```
(urjc@ETSIICTF)-[~/Documentos/dump]  
$ vol.py -f dump.raw --profile="Win7SP1x64" cmdline
```

```
*****  
svchost.exe pid: 3656  
Command line : C:\Windows\System32\svchost.exe -k secsvcs  
*****  
7zFM.exe pid: 868  
Command line : "C:\Program Files\7-Zip\7zFM.exe" "C:\Users\Admin\Desktop\ficheroSecreto.7z"  
*****
```

Con este plugin conseguimos la ruta de un fichero bastante sospechoso





II. OSINT, Esteganografía y Forense

Inés Martín, Carlos Barahona, Clara Contreras y Sergio Pérez