II. OSINT, Esteganografía y Forense

Ismael Gómez, Alejandro Bermejo, Inés Martín y Sergio Pérez

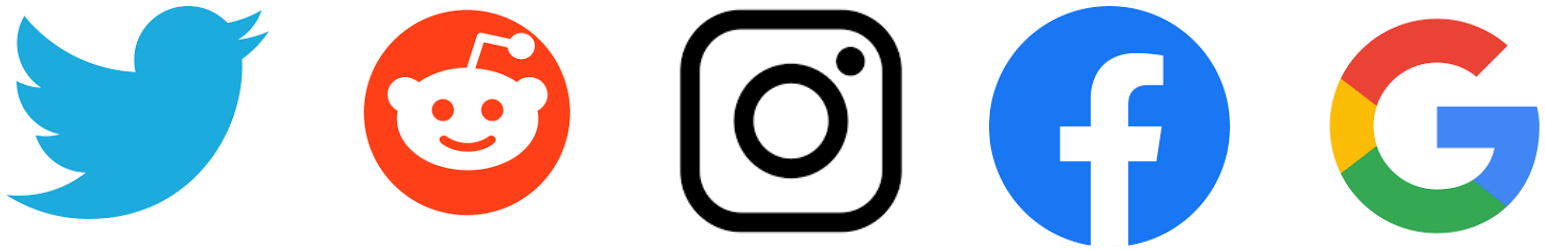
Universidad
Rey Juan Carlos

Universidad Rey Juan Carlos

Índice

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



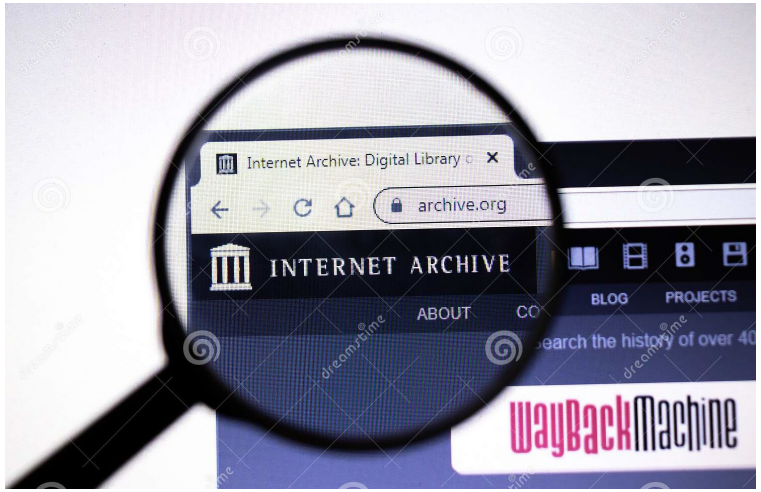
EJEMPLO DE UNO DE ESTOS RETOS

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. 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/

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 3IMu10 y que tiene un curso de carding en la darknet. ¿Podrías ayudarnos a encontrar el dominio onion en el que se aloja?

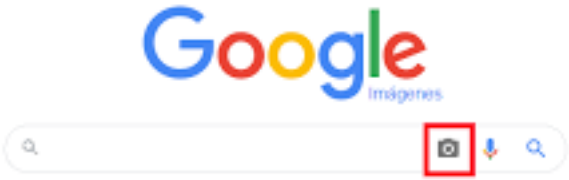
Hint: No es necesario navegar por la deep web para encontrar el dominio de 3IMu10.

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

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



Yandex

TinEye

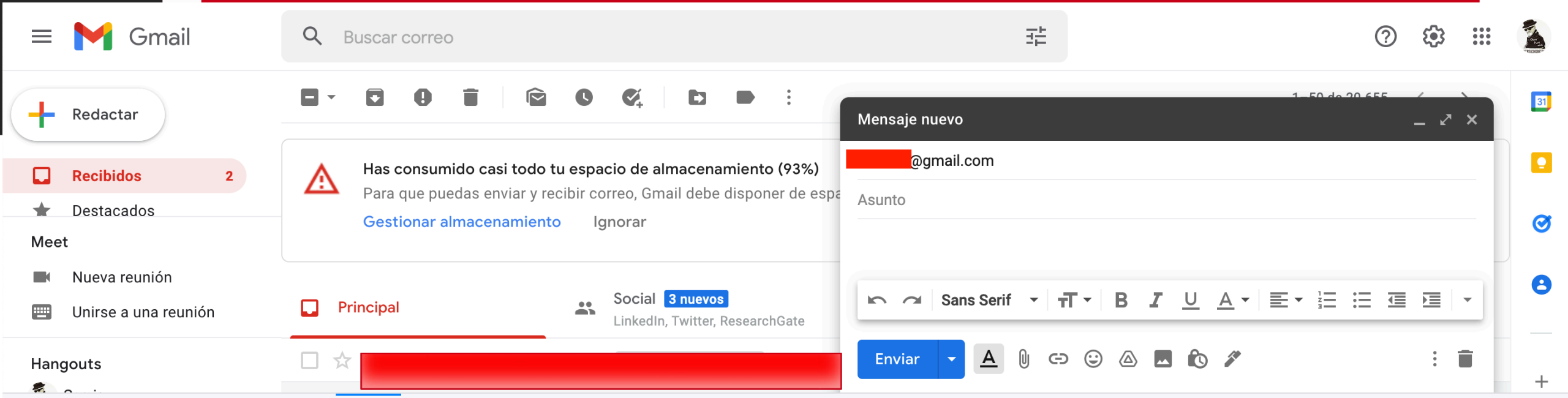
Google Lens

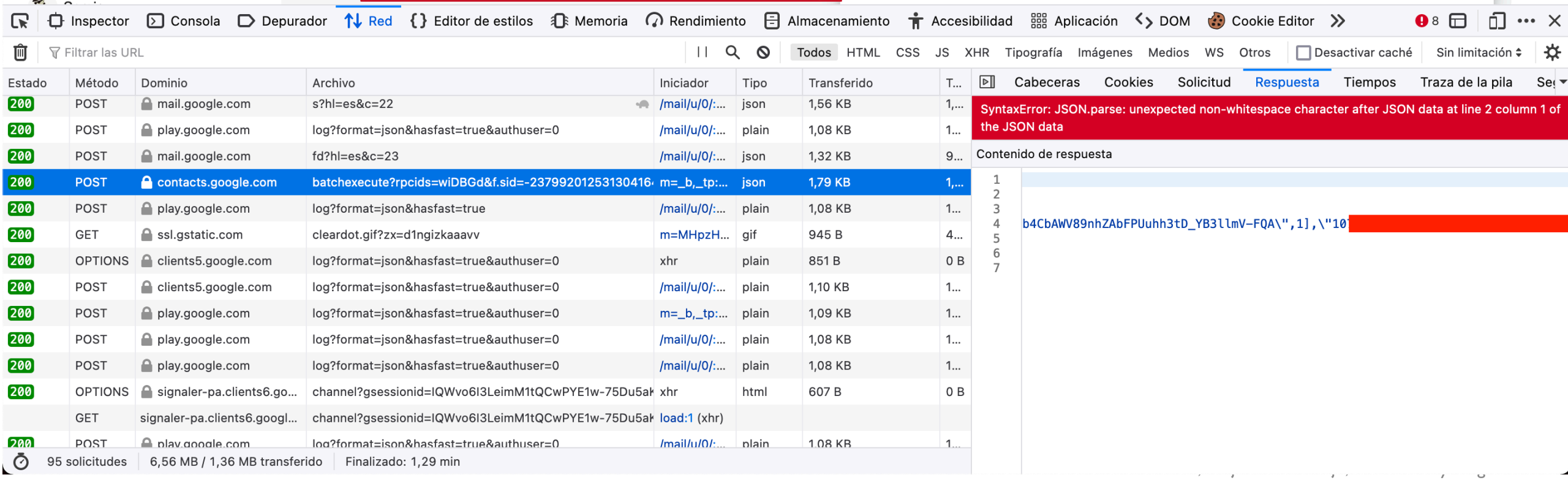
DuckDuckGo

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, 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
- Hay muchas herramientas dedicadas a esta parte


Gmail
Buscar correo
Redactar
Recibidos 2
Destacados
Meet
Nueva reunión
Unirse a una reunión
Hangouts
Has consumido casi todo tu espacio de almacenamiento (93%)
Para que puedas enviar y recibir correo, Gmail debe disponer de espa
Gestionar almacenamiento
Ignorar
Principal
Social 3 nuevos
LinkedIn, Twitter, ResearchGate
Mensaje nuevo
[redacted]@gmail.com
Asunto
Sans Serif
Enviar


Inspector
Consola
Depurador
Red
Editor de estilos
Memoria
Rendimiento
Almacenamiento
Accesibilidad
Aplicación
DOM
Cookie Editor
Filtrar las URL
Todos HTML CSS JS XHR Tipografía Imágenes Medios WS Otros
Desactivar caché
Sin limitación
Estado Método Dominio Archivo Iniciador Tipo Transferido T...
200 POST mail.google.com s?hl=es&c=22 /mail/u/0/:... json 1,56 KB 1,...
200 POST play.google.com log?format=json&hasfast=true&authuser=0 /mail/u/0/:... plain 1,08 KB 1...
200 POST mail.google.com fd?hl=es&c=23 /mail/u/0/:... json 1,32 KB 9...
200 POST contacts.google.com batchexecute?rpcids=wiDBGd&f.sid=-23799201253130416 m=_b,_tp:... json 1,79 KB 1,...
200 POST play.google.com log?format=json&hasfast=true /mail/u/0/:... plain 1,08 KB 1...
200 GET ssl.gstatic.com cleardot.gif?zx=d1ngizkaaavv m=MHpzH... gif 945 B 4...
200 OPTIONS clients5.google.com log?format=json&hasfast=true&authuser=0 xhr plain 851 B 0 B
200 POST clients5.google.com log?format=json&hasfast=true&authuser=0 /mail/u/0/:... plain 1,10 KB 1...
200 POST play.google.com log?format=json&hasfast=true&authuser=0 m=_b,_tp:... plain 1,09 KB 1...
200 POST play.google.com log?format=json&hasfast=true&authuser=0 /mail/u/0/:... plain 1,08 KB 1...
200 POST play.google.com log?format=json&hasfast=true&authuser=0 /mail/u/0/:... plain 1,08 KB 1...
200 OPTIONS signaler-pa.clients6.go... channel?gsessionid=IQWvo6l3LeimM1tQCwPYE1w-75Du5ak xhr html 607 B 0 B
GET signaler-pa.clients6.googl... channel?gsessionid=IQWvo6l3LeimM1tQCwPYE1w-75Du5ak load:1 (xhr)
Cabeceras Cookies Solicitud Respuesta Tiempos Traza de la pila
SyntaxError: JSON.parse: unexpected non-whitespace character after JSON data at line 2 column 1 of the JSON data
Contenido de respuesta
b4CbAWV89nhZAbFPUuhh3tD_YB3llmV-FQA\",1],\"10
95 solicitudes 6,56 MB / 1,36 MB transferido Finalizado: 1,29 min

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. Esteganografía

¿Qué es la esteganografía?

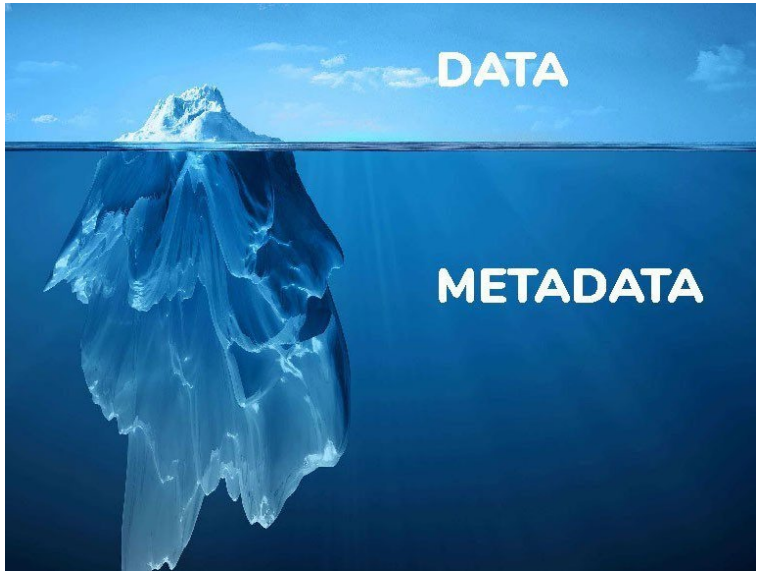
La **esteganografía** trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos dentro de otros, de modo que no se perciba su existencia.

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.

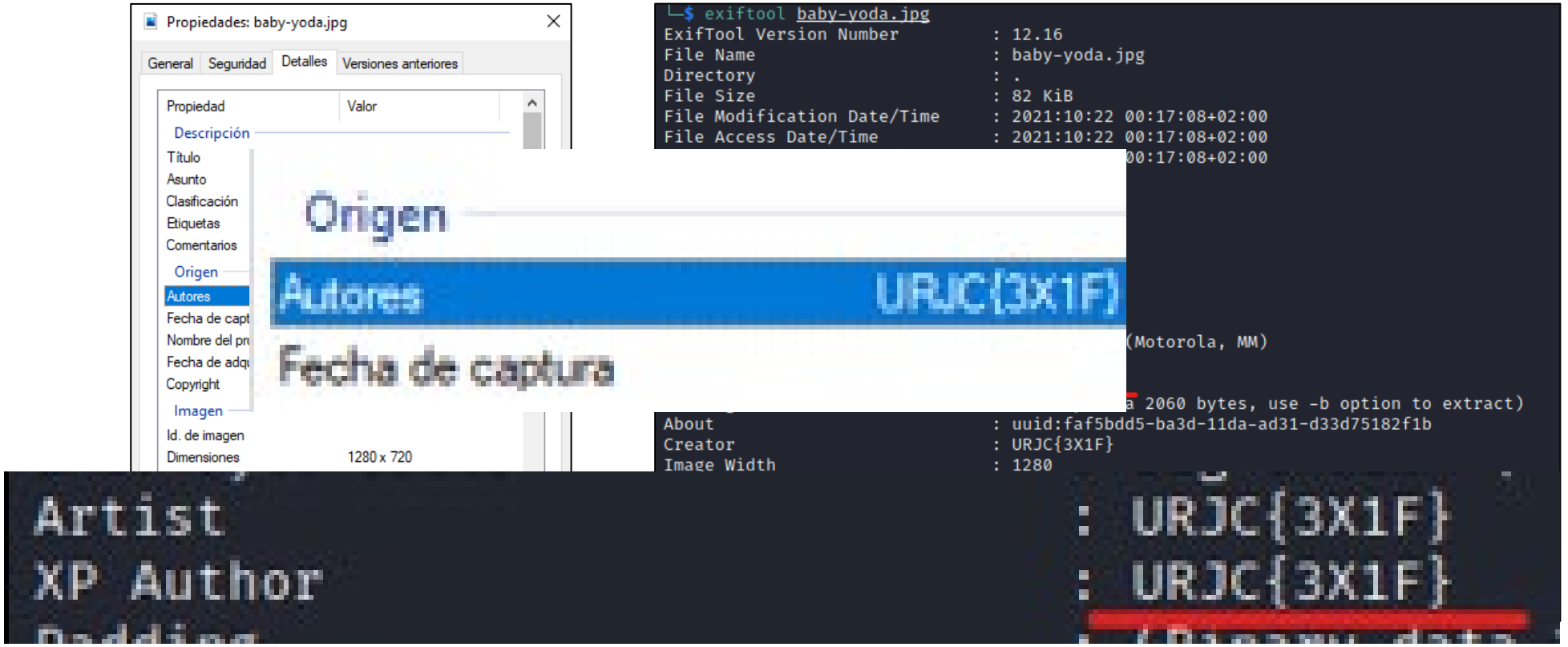


En los metadatos podremos encontrar información relevante.

1. Esteganografía

Exiftool

Herramienta utilizada para extraer los metadatos de los archivos.



https://exiftool.org/

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 seghide.


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"
```

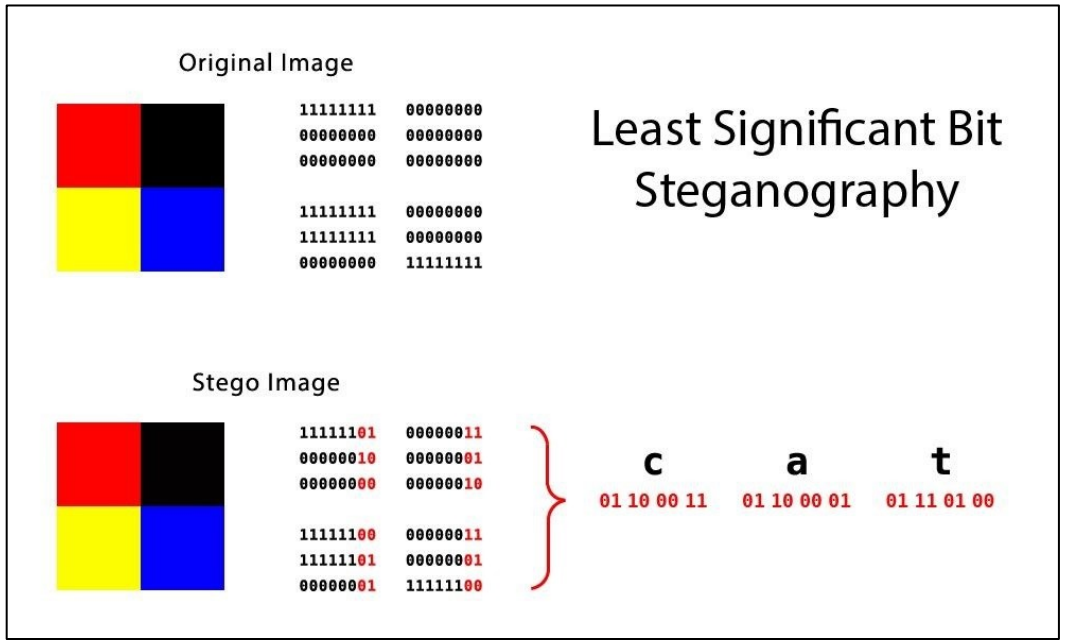
Técnicas y herramientas comunes

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.

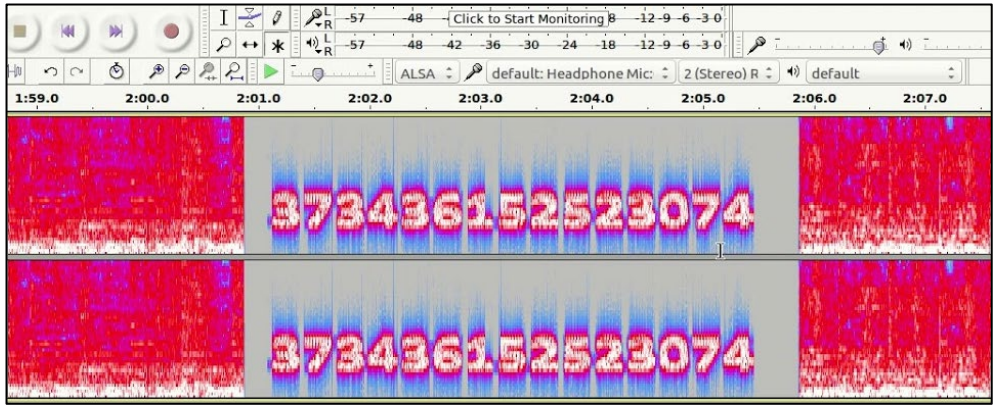
https://pypi.org/project/stego-lsb/



1. Esteganografía

Archivos de audio/vídeo

Suele ser interesante ver el **espectograma** 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

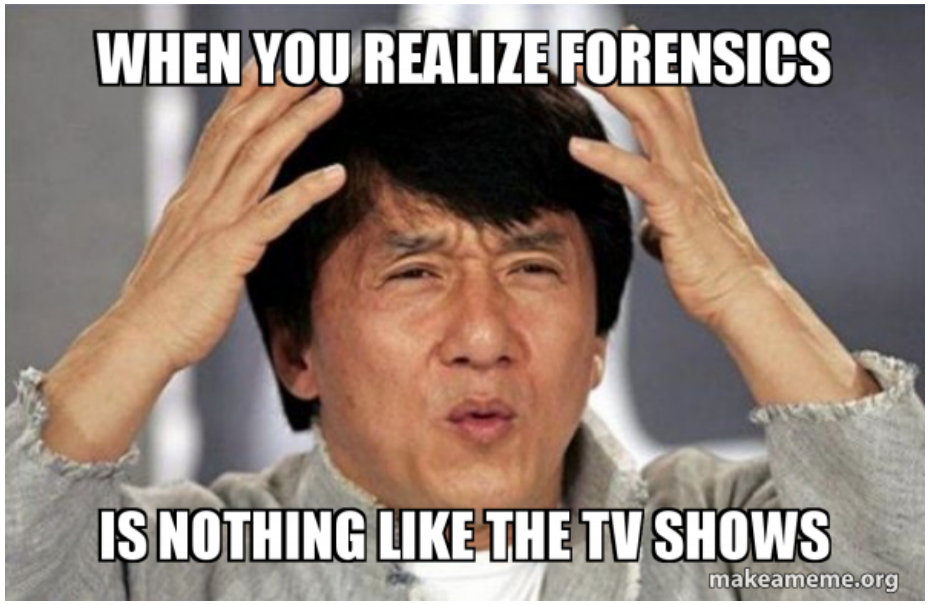
Tool	Description	How to use
file	Check out what kind of file you have	`file stego.jpg`
exiftool	Check out metadata of media files	`exiftool stego.jpg`
binwalk	Check out if other files are embedded/appended	`binwalk stego.jpg`
strings	Check out if there are interesting readable characters in the file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

III. Forense

¿Qué es el análisis forense?

La ciencia forense digital es una ciencia forense en la que los expertos estudian los dispositivos informáticos para ayudar a resolver los delitos.

Conjunto de técnicas destinadas a extraer información valiosa de discos, sin alterar el estado de estos mismos



III. Forense - Magic Bytes

Primeros bytes de un fichero, utilizados por los sistemas Linux para identificar el **formato del mismo**

```
~/Desktop hexdump imagen.png| head
0000000 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52
0000010 00 00 03 ac 00 00 01 08 08 06 00 00 00 5b 29 79
0000020 95 00 00 0c 6c 69 43 43 50 49 43 43 20 50 72 6f
0000030 66 69 6c 65 00 00 48 89 95 57 07 5c 93 47 1b bf
```

89 50 4E 47 0D 0A 1A 0A	%PNGCRLFSUBLF	0	png

Hexdump / binwalk

Universidad Rey Juan Carlos

III. Forense - ¿Seguro que es el archivo que parece?

```
❯ binwalk kali.rar

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 3840 x 2160, 8-bit/color RGBA, non-interlaced
75            0x4B            Zlib compressed data, default compression

❯ file kali.rar
kali.rar: PNG image data, 3840 x 2160, 8-bit/color RGBA, non-interlaced
```

```
❯ exiftool kali.rar
ExifTool Version Number         : 12.30
File Name                       : kali.rar
Directory                       : .
File Size                       : 604 KiB
File Modification Date/Time     : 2021:09:27 21:13:59+02:00
File Access Date/Time           : 2021:09:27 21:14:22+02:00
File Inode Change Date/Time     : 2021:09:27 21:14:16+02:00
File Permissions                : -rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 3840
Image Height                    : 2160
```

Universidad Rey Juan Carlos

III. Forense - Strings

Strings es una herramienta que nos permite mostrar caracteres imprimibles que contienen los ficheros.

```
~/Desktop/retos/MagicNumber  strings retoMagicNumber.png
bfff
[-f&
^r[zA|
J8xK\
[KW_7[w
/w[_
;HzJp
!X[:HYIVV][
_][%HY^VZZ[
. 5C
}k[_./Ui
```

Strings

III. Forense – Retos Cortitos

Vamos a hacer 3 ejercicios rápidos que utilizan las herramientas que hemos comentado.

Strange Photo	Forensics
Everything is not what it seems	Forensics
AAAHHHHHHHH	Forensics

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㉿ETSIICTF)-[~/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, Win2008
R2SP1x64_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"

Universidad Rey Juan Carlos

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	sppsvc.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

Ismael Gómez, Alejandro Bermejo, Inés Martín y Sergio Pérez

Universidad
Rey Juan Carlos