



# OSINT y Esteganografía

---

Julio López de Lucas y Mari Luz Charfolé Maestro

# Índice

## 1. OSINT

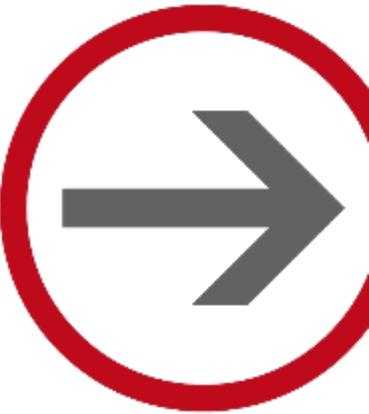
- Definición y tipos
- OSINT Framework
- Herramientas
- Leaks
- Reconocimiento
- IMINT y GEOMINT



## 2. Esteganografía

- ¿Qué es?
- Tipos
  - Texto
  - Imagen
  - Sonido
- Herramientas





# OSINT

---

Julio López de Lucas

# Definición OSINT



## Open Source Intelligence

Recopilar y analizar información  
pública

HUMINT  


GEOINT  


IMINT  


SIGINT  


# Fuentes abiertas

Redes sociales  
y blogs



Direcciones IP y  
puertos abiertos



Compras  
online



Búsquedas en  
Internet



# OSINT Framework

 [OSINT Framework](#)

Plataforma en línea que agrupa una amplia variedad de herramientas y recursos destinados a OSINT.



# Herramientas interesantes

- Sitios dónde aparece una persona:  
<https://webmii.com/?language=es>
- Cuentas de Instagram:  
<https://inflact.com/instagram-viewer/profile/>
- Números de teléfono:  
<https://whocalld.com>
- Mapa a lo largo de los años:  
<https://livingatlas.arcgis.com/wayback/#active=20337&mapCenter=-115.26176%2C36.05678%2C12&mode=explore>



# INTERNET NUNCA OLVIDA



🔗 [WAYBACK MACHINE](#)



# INTERNET NUNCA OLVIDA



Herramienta  
OSINT

archive.today  
archivo de páginas web

email haz una pregunta preguntas frecuentes Donate

Install Edge extension

Mi url está en línea y quiero archivar su contenido

http://www.domain.com/url archivar

Archive.today ¡es tu máquina personal del pasado!

Toma una instantánea de la página que siempre va a estar en línea incluso si la original desaparece.

Guarda una copia textual y gráfica de la página para mayor precisión.

También acorta la url como lo hacen tinyurl, goo.gl y bit.ly.

Puede guardar sitios web 2.0:

- <https://archive.is/2020.04.21/rt.live/>
- [https://archive.is/2014.06.26/google.com/maps/...](https://archive.is/2014.06.26/google.com/maps/)

Esto puede ser útil si quieres guardar una fotografía de una página que podría cambiar pronto: un precio, una oferta de trabajo, una oferta inmobiliaria, un post al estar borracho...

Páginas guardadas no van a tener ningún elemento ni scripts activos, ¡te mantienen seguro porque no pueden tener popups o malware!

Buscar por el archivo

consulta buscar

ejemplos de búsqueda

- [microsoft.com](#) para instantáneas del host microsoft.com
- [\\*.microsoft.com](#) para instantáneas de microsoft.com y todos sus subdominios (p.e. www.microsoft.com)
- [http://twitter.com/burgerking](#) para instantáneas de la url exacta (la búsqueda es sensible a las mayúsculas)
- [http://twitter.com/burg\\*](#) para instantáneas de urls empezando con http://twitter.com/burg

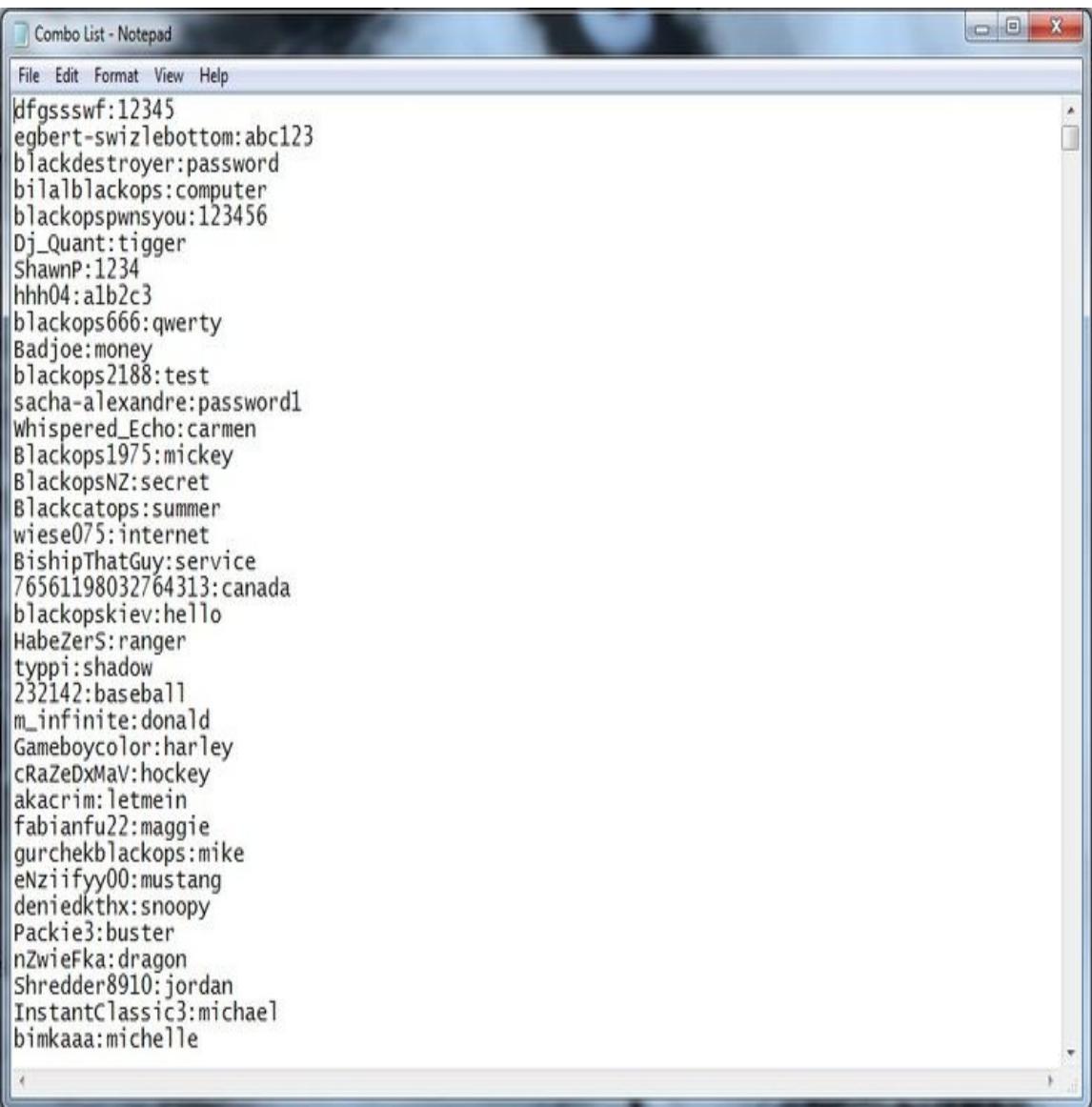
importante →

[Webpage archive](#)

## Información filtrada:

PERSEVERANCIA  
OBJETIVIDAD  
FLEXIBILIDAD  
PACIENCIA

Listas User-Pass



```
Combo List - Notepad
File Edit Format View Help
dfgssswf:12345
egbert-swizlebottom:abc123
blackdestroyer:password
bilalblackops:computer
blackopspwnsyou:123456
Dj_Quant:tigger
ShawnP:1234
hhh04:a1b2c3
blackops666:qwerty
Badjoe:money
blackops2188:test
sacha-alexandre:password1
Whispered_Echo:carmen
Blackops1975:mickey
BlackopsNZ:secret
Blackcatops:summer
wiese075:internet
BishopThatGuy:service
76561198032764313:canada
blackopskiev:hello
HabeZerS:ranger
typpi:shadow
232142:baseball
m_infinite:donald
Gameboycolor:harley
cRaZeDxMaV:hockey
akacrim:letmein
fabianfu22:maggie
gurcheblackops:mike
eNziifyy00:mustang
deniedkthx:snoopy
Packie3:buster
nZwieFka:dragon
Shredder8910:jordan
InstantClassic3:michael
bimkaaa:michelle
```

## Información filtrada:

PERSEVERANCIA  
OBJETIVIDAD  
FLEXIBILIDAD  
PACIENCIA



SABER BUSCAR

Listas User-Pass

```
Combo List - Notepad
File Edit Format View Help
dfgssswf:12345
egbert-swizlebottom:abc123
blackdestroyer:password
bilalblackops:computer
blackopspwnsyou:123456
Dj_Quant:tigger
ShawnP:1234
hhh04:a1b2c3
blackops666:qwerty
Badjoe:money
blackops2188:test
sacha-alexandre:password1
Whispered_Echo:carmen
Blackops1975:mickey
BlackopsNZ:secret
Blackcatops:summer
wiese075:internet
BishopThatGuy:service
76561198032764313:canada
blackopskiev:hello
HabeZerS:ranger
typpi:shadow
232142:baseball
m_infinite:donald
Gameboycolor:harley
cRaZeDxMaV:hockey
akacrim:letmein
fabianfu22:maggie
gurcheblackops:mike
eNziifyy00:mustang
deniedkthx:snoopy
Packie3:buster
nZwieFka:dragon
Shredder8910:jordan
InstantClassic3:michael
bimkaaa:michelle
```

# DATA LEAKS

## HERRAMIENTAS

1. Google Dorks
2. Telegram
3. Dark Web



# DATA LEAKS

# Google Dorks

Permiten añadir filtros a nuestras b usquedas, es la herramienta m as potente en el mundo del OSINT.

Principales ejemplos:[Google dork cheatsheet](#)

En Google Hacking Database hay cientos de ejemplos de b usquedas orientadas al Hacking: [Google Hacking Database \(GHDB\)](#)



# EXPLOIT DATABASE

Google Hacking Database

Show 15 ▾

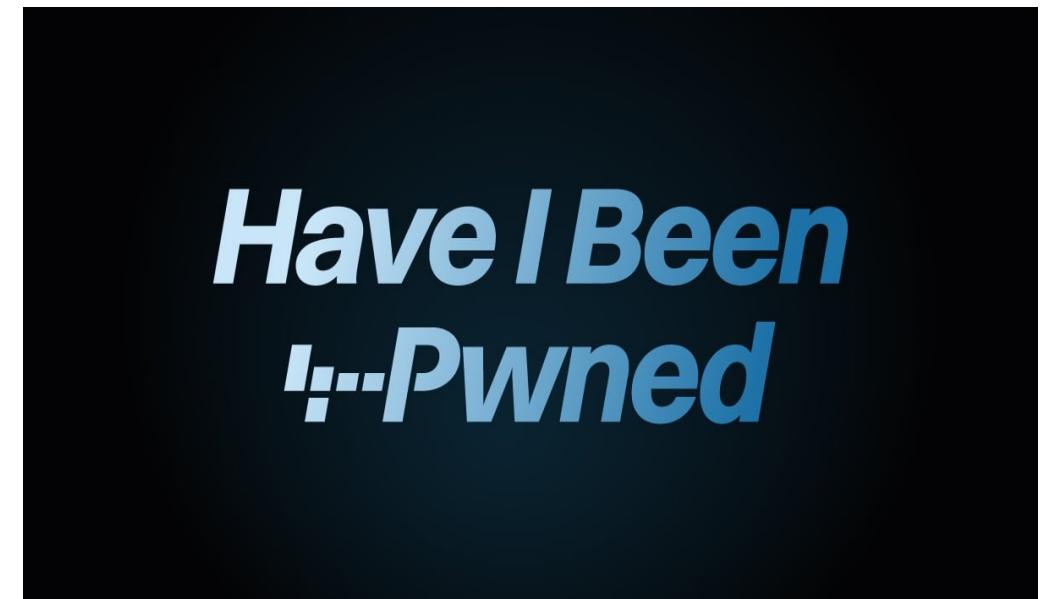
Quick Search

Date Added	Dork	Category	Author
2024-08-23	site:github.com "BEGIN OPENSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-08-23	ext:nix "BEGIN OPENSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-07-26	inurl:home.htm intitle:1766	Various Online Devices	Kishoraram
2024-07-04	intitle:"SSL Network Extender Login" -checkpoint.com	Vulnerable Servers	Everton Hydd3n
2024-07-04	intext:"siemens" & inurl:"/portal/portal.mwsl"	Vulnerable Servers	Kishoraram
2024-07-04	Google Dork Submission For GlobalProtect Portal	Vulnerable Servers	Gurudatt Choudhary
2024-07-04	inurl:"cgi-bin/koha"	Vulnerable Servers	Hilary Soita
2024-07-04	intext:"aws_access_key_id"   intext:"aws_secret_access_key" filetype:json   filetype:yaml	Files Containing Passwords	Joel Indra
2024-07-04	intext:"aws_access_key_id"   intext:"aws_secret_access_key" filetype:xml   filetype:yaml	Files Containing Passwords	Enrico Mazzoni

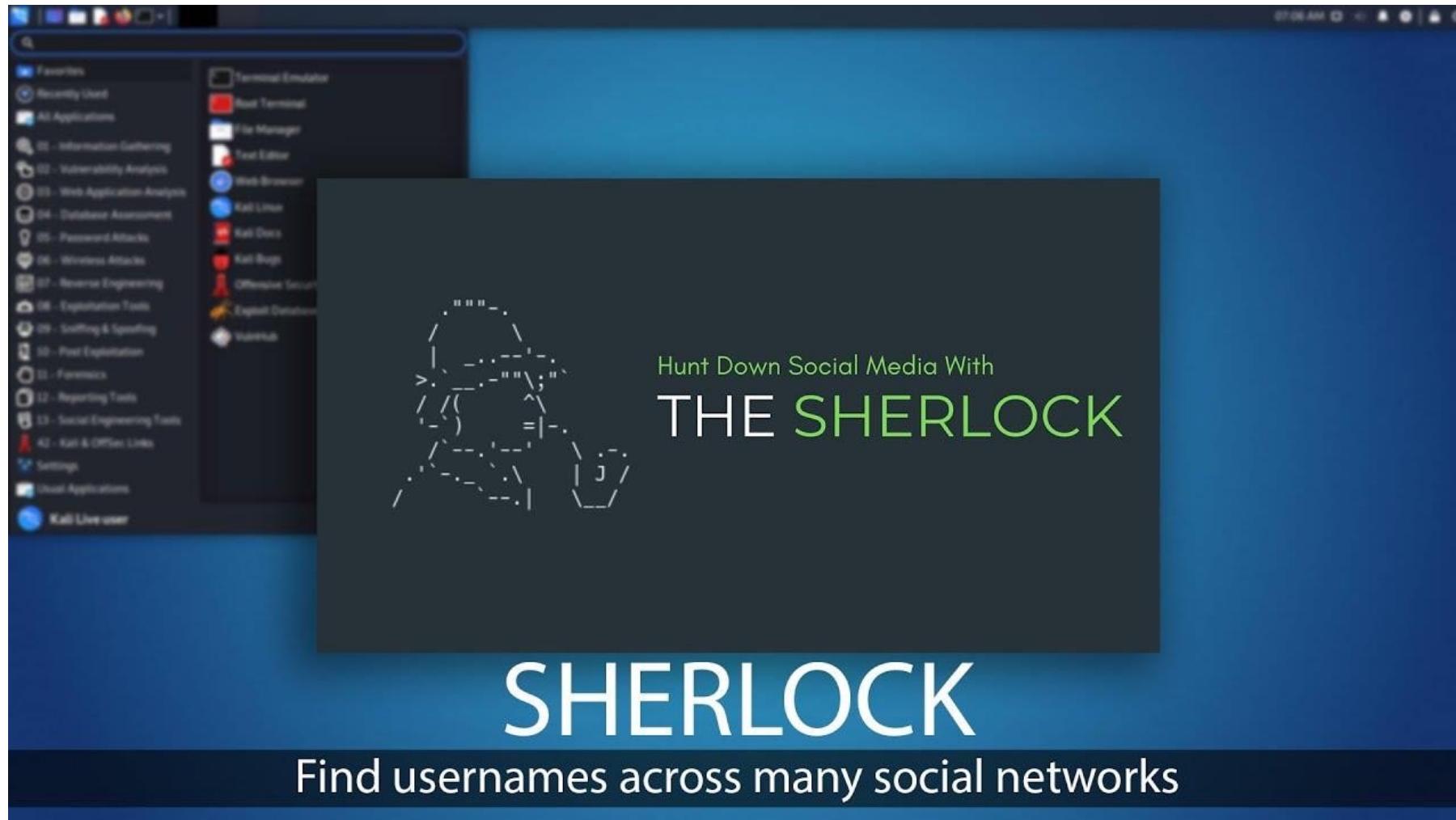
# DATA LEAKS

Otras Herramientas:

[\\_IntelligenceX](#)



# HUMINT (Human Intelligence)



Para instalar: sudo apt install sherlock

# DATA LEAKS

## ¿QUÉ INFORMACIÓN PODEMOS OBTENER CON LAS FILTRACIONES?

Email

- Cuentas asociadas
- Saber si ha sufrido una violación de datos

[Have I Been Pwned](#)

Números de teléfono

- Cuentas asociadas en RRSS
- Herramientas abiertas

Contraseñas

- Hash de contraseñas
- Saber si es segura

[Password Check | Kaspersky](#)

Nombre

- Redes donde utiliza el nombre real (LinkedIn, TripAdvisor...)

[Webmii](#)

Nick

- Cuentas que se tienen con ese mismo nick

[sherlock](#)

## Información de las Máquinas:

Direcciones IP

Geolocalización

Puertos abiertos

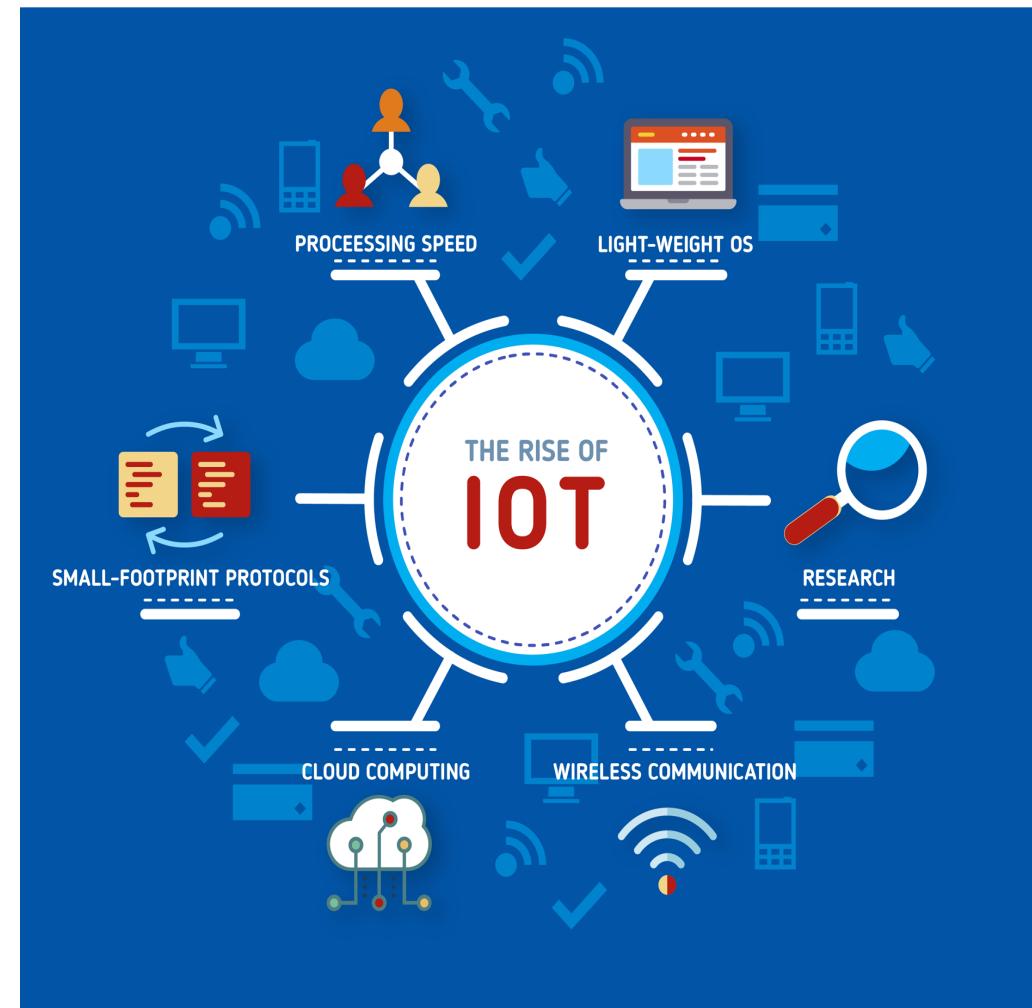
Respuestas a peticiones

DNS

Versiones

Vulnerabilidades asociadas

Internet of things



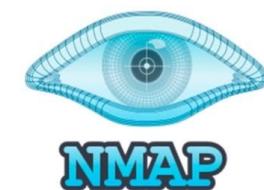
# Reconocimiento

# HERRAMIENTAS

1. Shodan
  2. Recon-ng
  3. Nmap



# SHODAN



# Reconocimiento

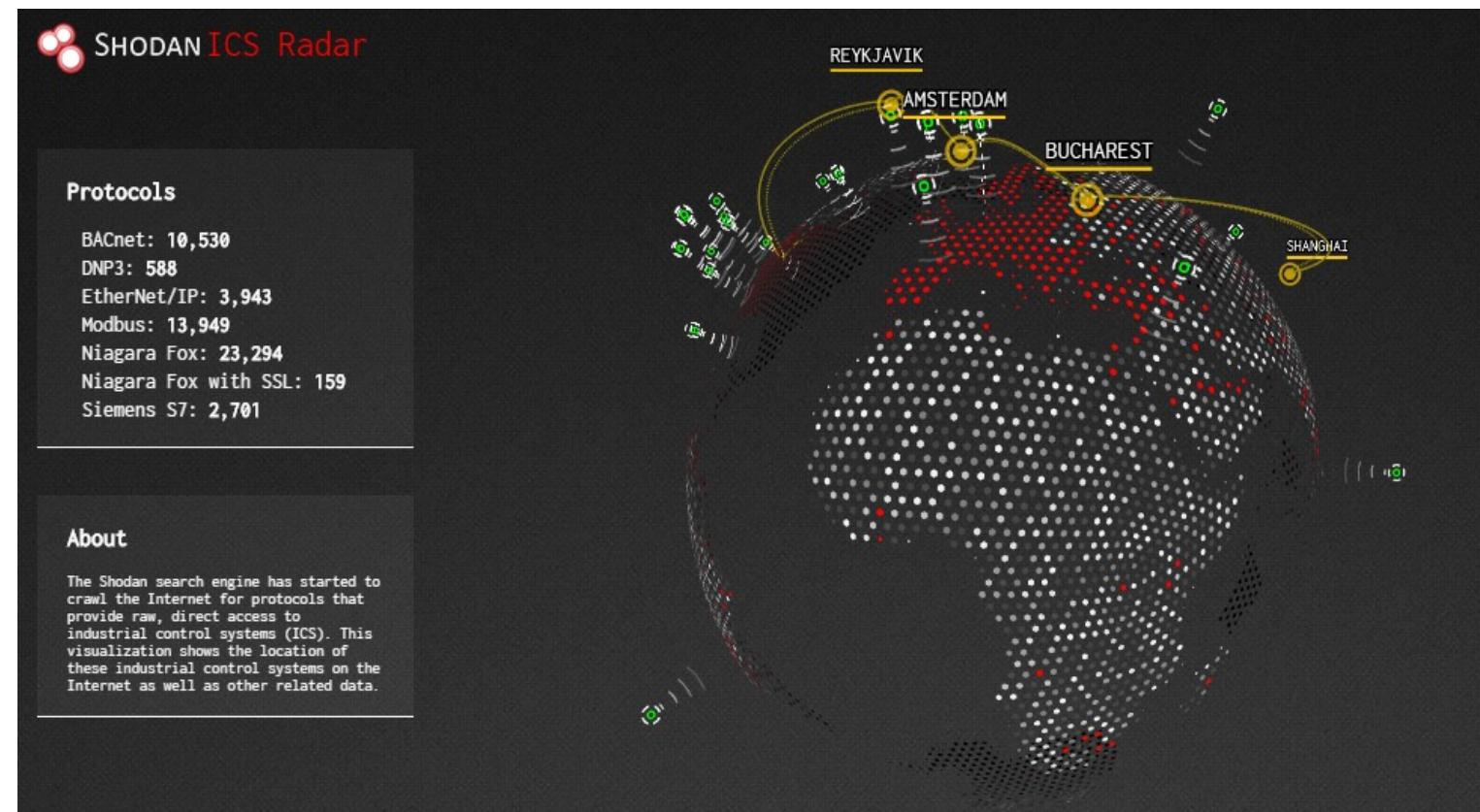
## Shodan

Es un buscador de internet de las cosas (IOT): [Shodan Search Engine](#)

Tiene sus propios dorks para afinar las búsquedas: [Shodan Cheat Sheet](#)

Hay otras herramientas muy parecidas y de gran calidad como Censys

Puedes pedirles una cuenta premium por ser estudiante escribiendo a [academic@shodan.io](mailto:academic@shodan.io)





Centro de seguridad  
Mundial Brasil



Sara Carbonero  
Mundial Brasil

WIFI REDACCIÓN

Nombre: *Curitiba\_redaccion*  
Contraseña: *partidoapartido*

WIFI CARPA

Nombre: *Curitiba\_set*  
Contraseña: *iniestadademivida*

Centro de seguridad  
SuperBowl 2020

# IMINT (Image Intelligence)

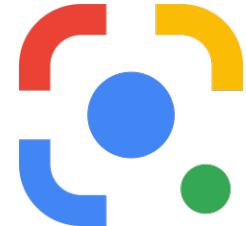
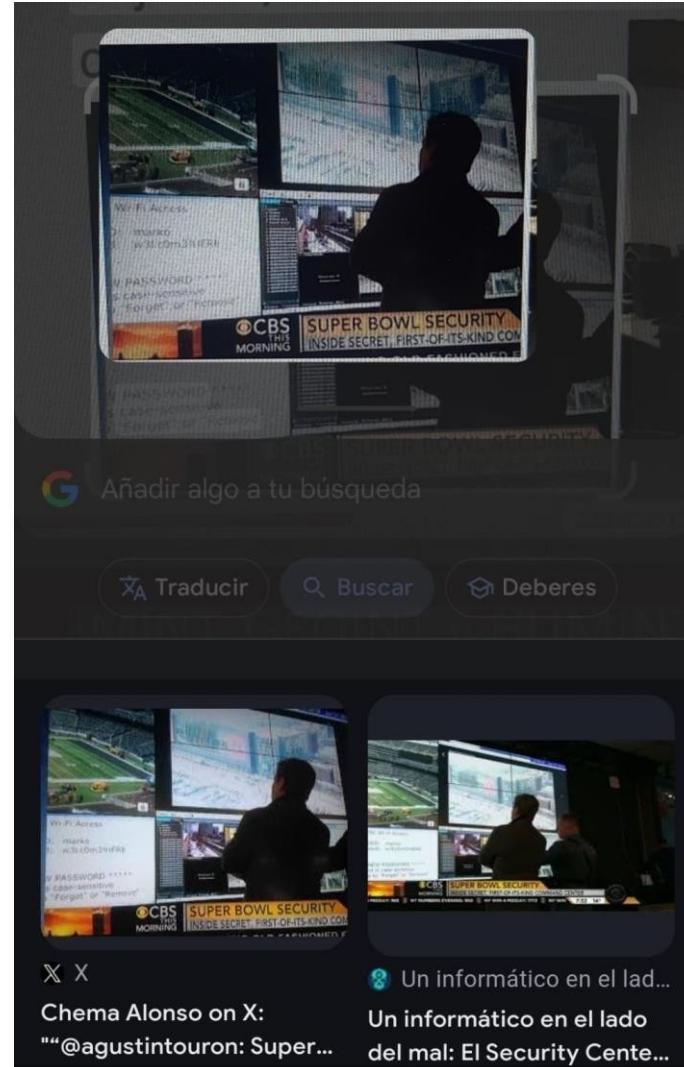
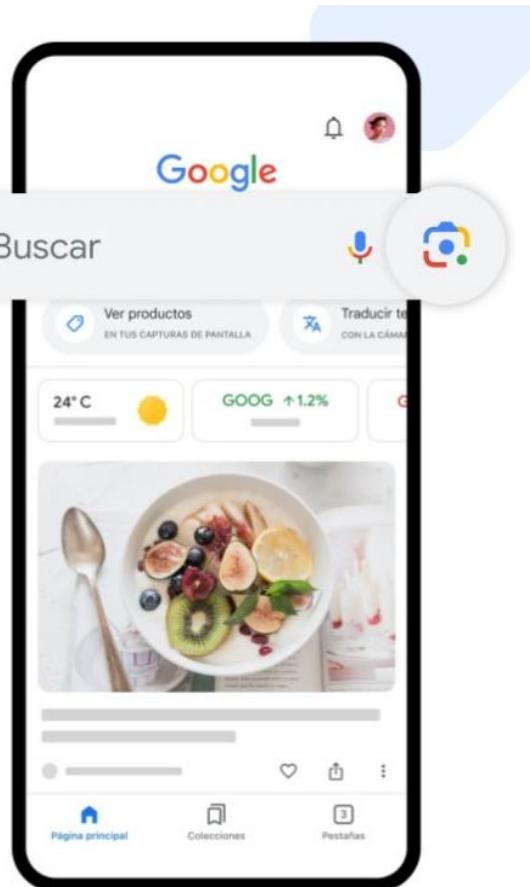
## HERRAMIENTAS

1. Google Lens
2. Tin Eye
3. Yandex



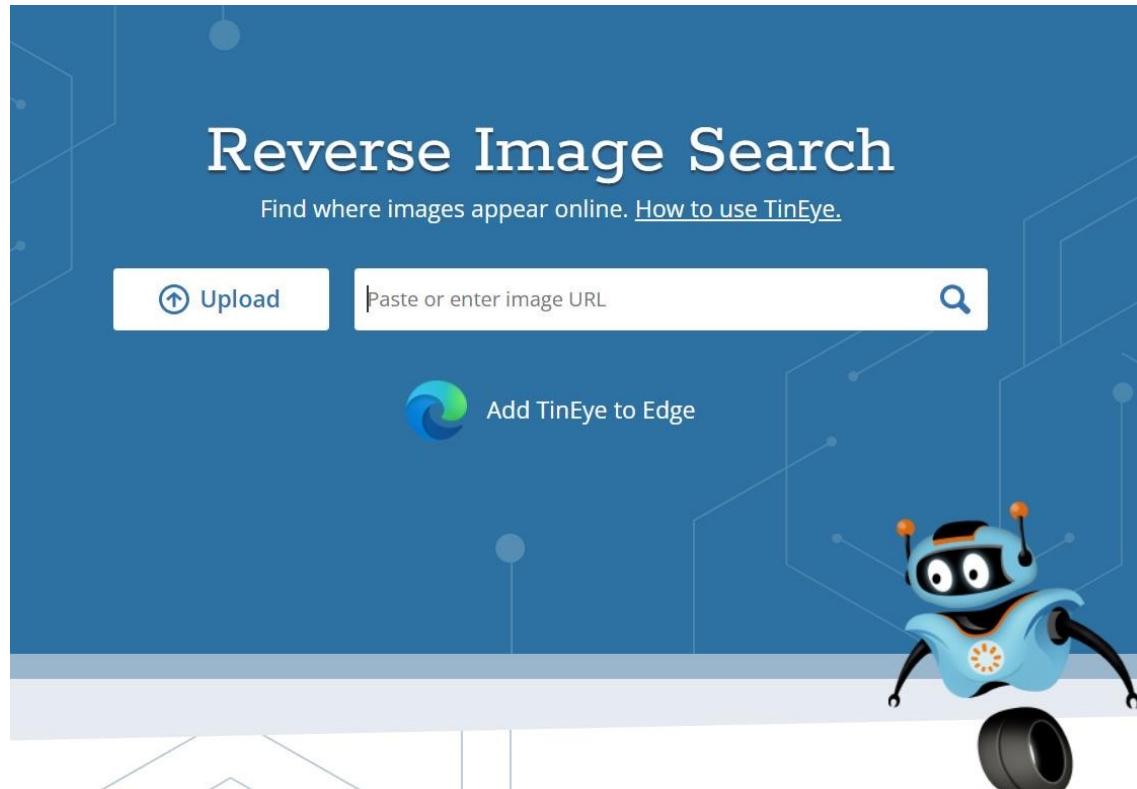
# IMINT (Image Intelligence)

## 1. Google Lens



# IMINT (Image Intelligence)

## 2. Tin Eye

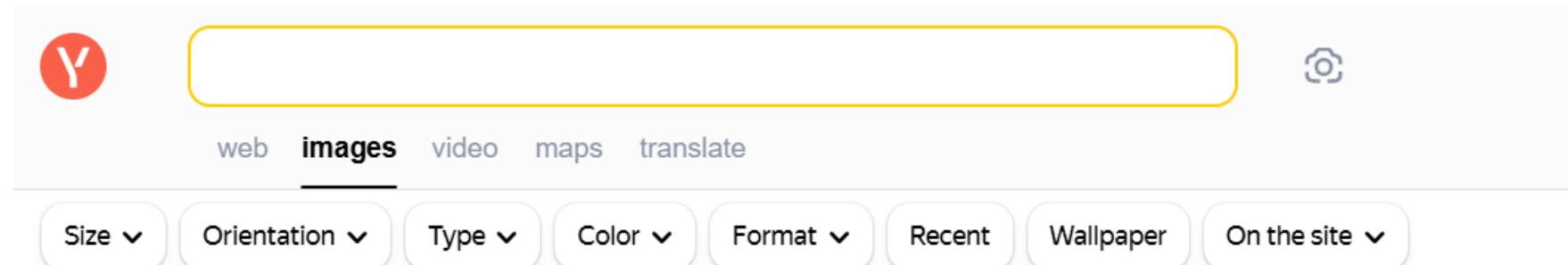


### PARA ENCONTRAR:

- imágenes de mayor calidad
- páginas que utilicen la misma imagen
- versiones editadas de la misma imagen
- si la foto es de quien dice ser
- el origen de una foto..

# IMINT (Image Intelligence)

## 3. Yandex



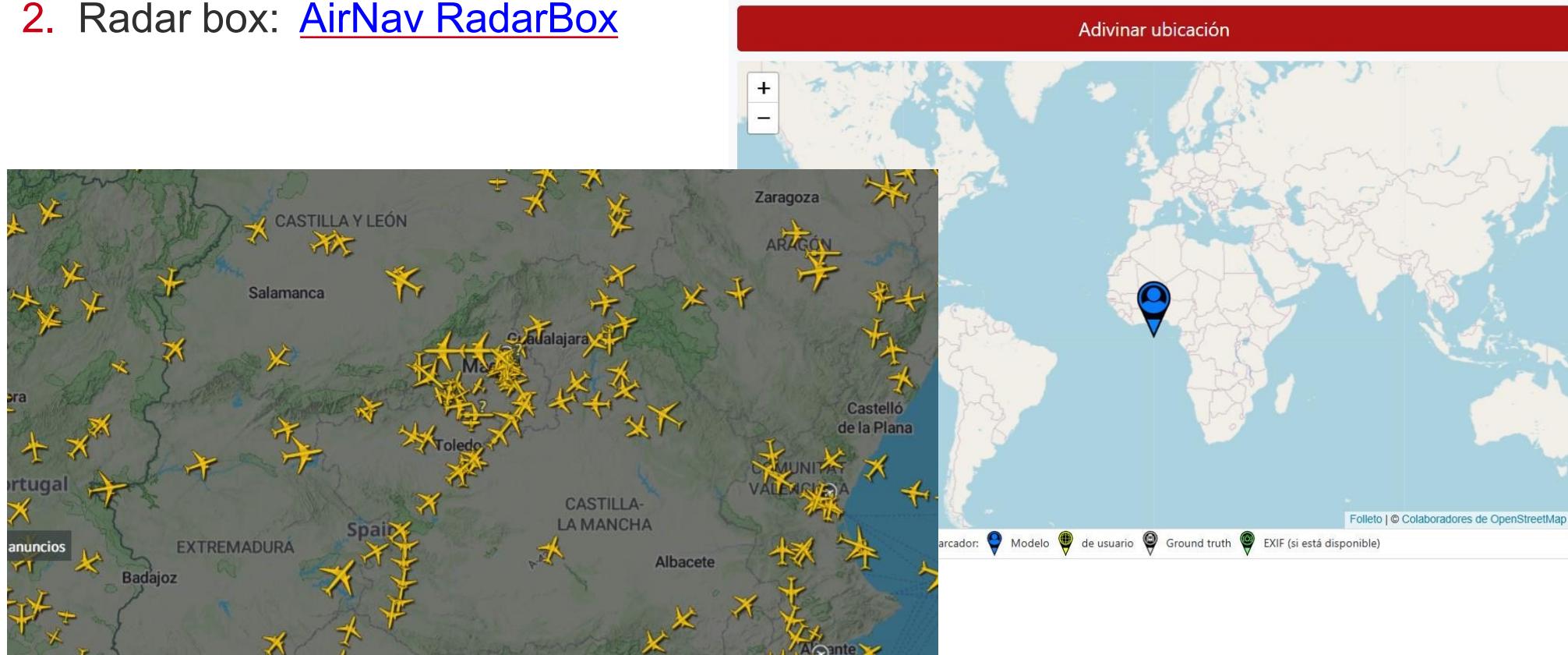
20

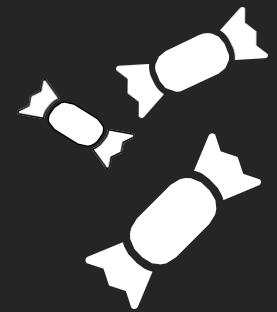
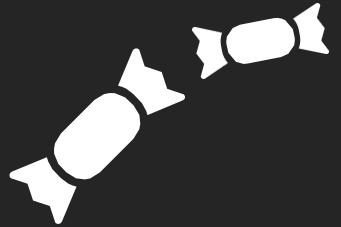
ES UN MOTOR DE BÚSQUEDA QUE PERMITE:

- Encontrar imágenes a través de palabras clave
- Averiguar el origen de una foto en concreto
- Tener más información sobre la fotografía...

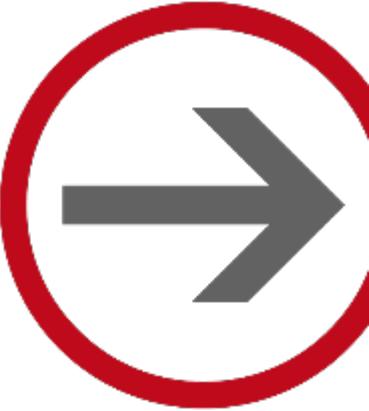
# GEOINT (Geospatial Intelligence)

1. Geoestimation TIB: [Estimación de geolocalización \(tib.eu\)](#)
2. Radar box: [AirNav RadarBox](#)





Universidad  
Rey Juan Carlos

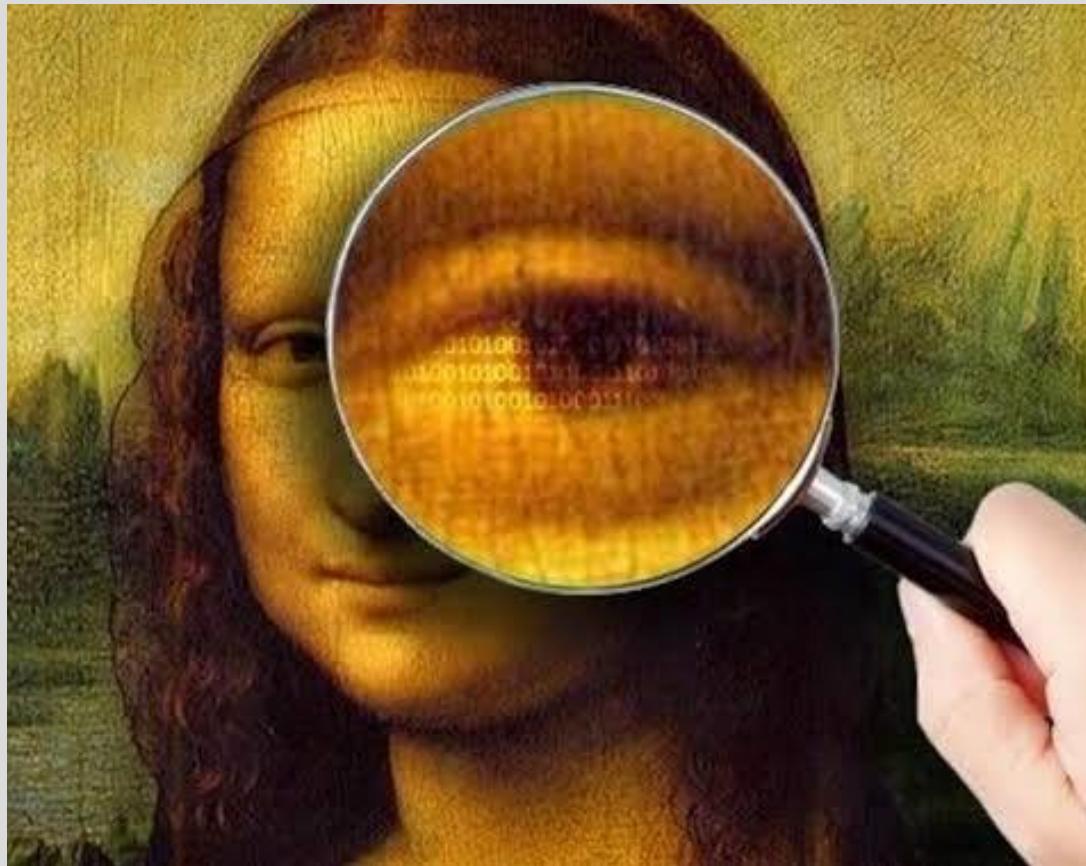


# Esteganografía

---

Mari Luz Charfolé Maestro

# Esteganografía



**Ocultar** información  
dentro de otros mensajes  
o medios físicos

6

TEXTO 

AUDIO 

IMÁGENES 

METADATOS



# Comando file



```
(kali㉿kali)-[~/Downloads]
$ file garden.jpg
garden.jpg: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 2
999x2249, components 3
```

```
(kali㉿kali)-[~/Downloads] X
$ file flag2of2-final.pdf
flag2of2-final.pdf: PNG image data, 50 x 50, 8-bit/color RGBA, non-interlaced
```

```
(kali㉿kali)-[~/Downloads]
$ exiftool flag2of2-final.pdf
ExifTool Version Number      : 12.76
File Name                   : flag2of2-final.pdf
Directory                   : .
File Size                   : 3.4 kB
File Modification Date/Time : 2024:02:07 18:50:37+01:00
File Access Date/Time       : 2025:09:30 17:47:16+02:00
File Inode Change Date/Time: 2025:09:30 17:57:03+02:00
File Permissions            : -rw-rw-r--
File Type                   : PNG
File Type Extension         : png
MIME Type                   : image/png
Image Width                 : 50
Image Height                : 50
Bit Depth                   : 8
Color Type                  : RGB with Alpha
```

# Tipos: ocultar información en archivos de texto

## Binwalk

```
(kali㉿kali)-[~/Downloads]$ binwalk flag2of2-final.pdf
/usr/lib/python3/dist-packages/binwalk/core/magic.py:431: SyntaxWarning: invalid escape sequence '\.'
  self.period = re.compile("\.\.")

DECIMAL      HEXADECIMAL      DESCRIPTION
---          ---          ---
0            0x0              PNG image, 50 x 50, 8-bit/color RGBA, non-interlaced
914           0x392             PDF document, version: "1.4"
1149          0x47D             Zlib compressed data, default compression

(kali㉿kali)-[~/Downloads]$ binwalk -e flag2of2-final.pdf
/usr/lib/python3/dist-packages/binwalk/core/magic.py:431: SyntaxWarning: invalid escape sequence '\.'
  self.period = re.compile("\.\.")

DECIMAL      HEXADECIMAL      DESCRIPTION
---          ---          ---
0            0x0              PNG image, 50 x 50, 8-bit/color RGBA, non-interlaced
914           0x392             PDF document, version: "1.4"
1149          0x47D             Zlib compressed data, default compression

(kali㉿kali)-[~/Downloads]$ cd _flag2of2-final.pdf-0.extracted
(kali㉿kali)-[~/Downloads/_flag2of2-final.pdf-0.extracted]$ ls -la
total 16
drwxrwxr-x  2 kali kali 4096 Sep 30 18:12 .
drwxr-xr-x 12 kali kali 4096 Sep 30 18:50 ..
-rw-rw-r--  1 kali kali   109 Sep 30 18:12 47D
-rw-rw-r--  1 kali kali  2213 Sep 30 18:12 47D.zlib
```

Archivos que contiene

Archivos que contiene + extraerlos

Detecta y extrae archivos que se encuentran ocultos dentro de otros

# Tipos: ocultar información en archivos de texto

## Stegseek

```
└─(kali㉿kali)-[~/Downloads/reto]
$ stegseek --crack -sf th-2669789895.jpeg -wl /usr/share/wordlists/rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "1234"
[i] Extracting to "th-2669789895.jpeg.out".

└─(kali㉿kali)-[~/Downloads/reto]
$ ls
th-2669789895.jpeg  th-2669789895.jpeg.out
```

30

Realiza un ataque de diccionario para encontrar la contraseña de un archivo.jpg modificado/protegido con steghide

# Tipos: ocultar información en archivos de texto

## Strings

```
(kali㉿kali)-[~/Downloads]$ strings garden.jpg
JFIF
XICC_PROFILE
HLino
mntrRGB XYZ
acspMSFT
IEC sRGB
-HP
cppt
3desc
lwtpt
bkpt
rXYZ
gXYZ
bXYZ
dmnd
pdmdd
vued
view
$lumi
meas
$tech
rTRC
gTRC
bTRC
text
Copyright (c) 1998 Hewlett-Packard Company
desc
sRGB IEC61966-2.1
```

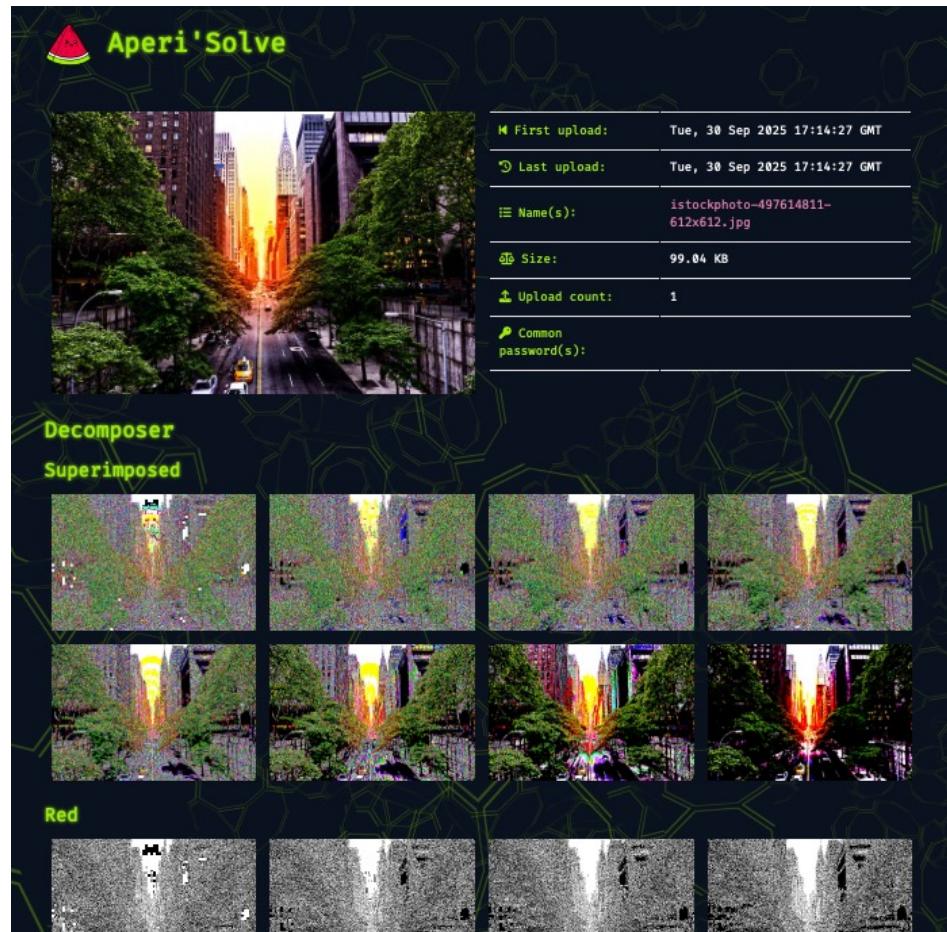
```
(kali㉿kali)-[~/Downloads]$ strings garden.jpg | grep picoCTF
Here is a flag "picoCTF{ }
```

Extrae y muestra secuencias imprimibles de caracteres que aparecen dentro de un fichero

# Tipos: ocultar información en imágenes

## Aperisolve (y Fotoforensics)

 <https://www.aperisolve.fr/>  
 <https://fotoforensics.com>



The Aperisolve interface displays the following information for the image:

- First upload:** Tue, 30 Sep 2025 17:14:27 GMT
- Last upload:** Tue, 30 Sep 2025 17:14:27 GMT
- Name(s):** istockphoto-497614811-612x612.jpg
- Size:** 99.04 KB
- Upload count:** 1
- Common password(s):** (empty)

Below the main image, there are three sections of thumbnail previews:

- Decomposer Superimposed:** Shows the original image with various semi-transparent overlays.
- Red:** Shows the image with a red overlay.



The Foremost interface displays the following file metadata:

ExifTool Version Number	12.57
File Name	887229a35065b99347c4e13affe8c0ae.jpg
Directory	/aperisolve/results/887229a35065b99347c4e13affe8c0ae
File Size	101 kB
File Modification Date/Time	2025:09:30 17:14:27+00:00
File Access Date/Time	2025:09:30 17:14:30+00:00

The Binwalk section shows the file structure:

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

The Steghide section shows an error message:

```
steghide: could not extract any data wi
```

The Zsteg section shows an error message:

```
[!] #<ZPNG::NotSupported: Unsupported h <file:/aperisolve/results/887229a35065b
```

The Strings section shows the following output:

```
ESTEGO
```

Análisis de capas y análisis en profundidad del archivo

# Tipos: ocultar información en imágenes

## Steghide

```
(kali㉿kali)-[~/Downloads/reto]
$ ls
texto.txt  th-2669789895.jpeg

(kali㉿kali)-[~/Downloads/reto]
$ steghide embed -ef texto.txt -cf th-2669789895.jpeg -N
Enter passphrase:
Re-Enter passphrase:
embedding "texto.txt" in "th-2669789895.jpeg"... done
```

Para extraer:

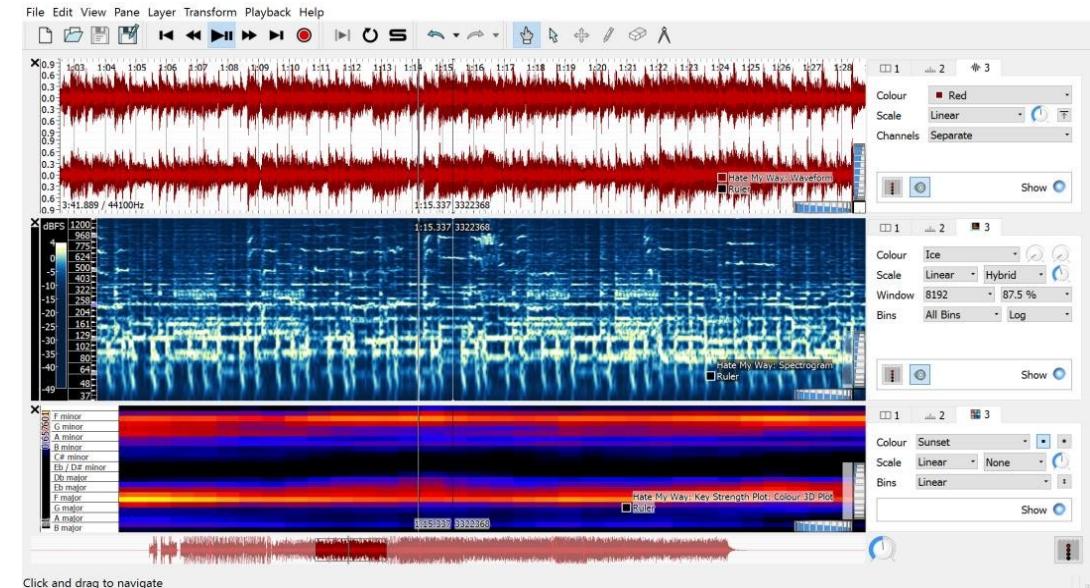
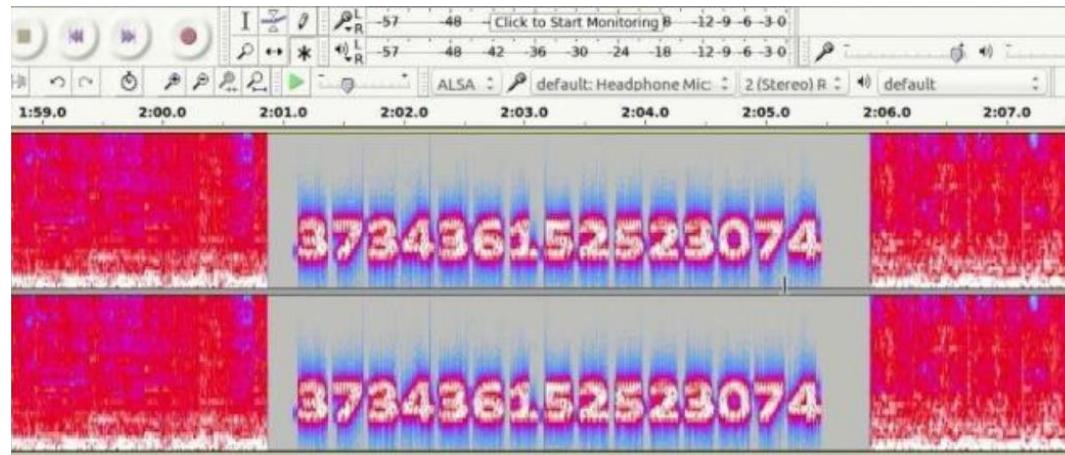
```
extract -sf nombre_archive_portador
```

30

Permite ocultar información dentro  
de otros archivos

# Tipos: ocultar información en archivos de audio

## Audacity y Sonic Visualizer



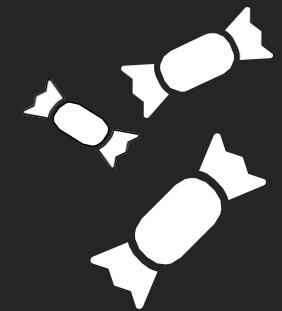
# Resumen herramientas

- Foto Forensics: <https://fotoforensics.com>
- Aperisolve: <https://www.aperisolve.fr/>
- Exiftool: <https://exiftool.org/>
- Steghide: <http://steghide.sourceforge.net/>
- Stegseek: <https://github.com/RickdeJager/stegseek>
- Strings: <https://linux.die.net/man/1/strings>
- Audacity: <https://audacity.es/>
- Sonic Visualizer: <https://www.sonicvisualiser.org/>
- Binwalk: <https://github.com/ReFirmLabs/binwalk>





# RETOS ESTEGANOGRAFÍA



Preparar todas las herramientas!!



Universidad  
Rey Juan Carlos