OSINT y Esteganografía

Julio López de Lucas y Mari Luz Charfolé Maestro

Universidad
Rey Juan Carlos

Universidad Rey Juan Carlos

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

Universidad
Rey Juan Carlos

Definición OSINT

Open Source Intelligence

Recopilar y analizar información pública

HUMINT

IMINT

GEOINT

SIGINT

Universidad Rey Juan Carlos

Fuentes abiertas

Redes sociales y blogs

Direcciones IP y puertos abiertos

Datos filtrados

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

Universidad Rey Juan Carlos

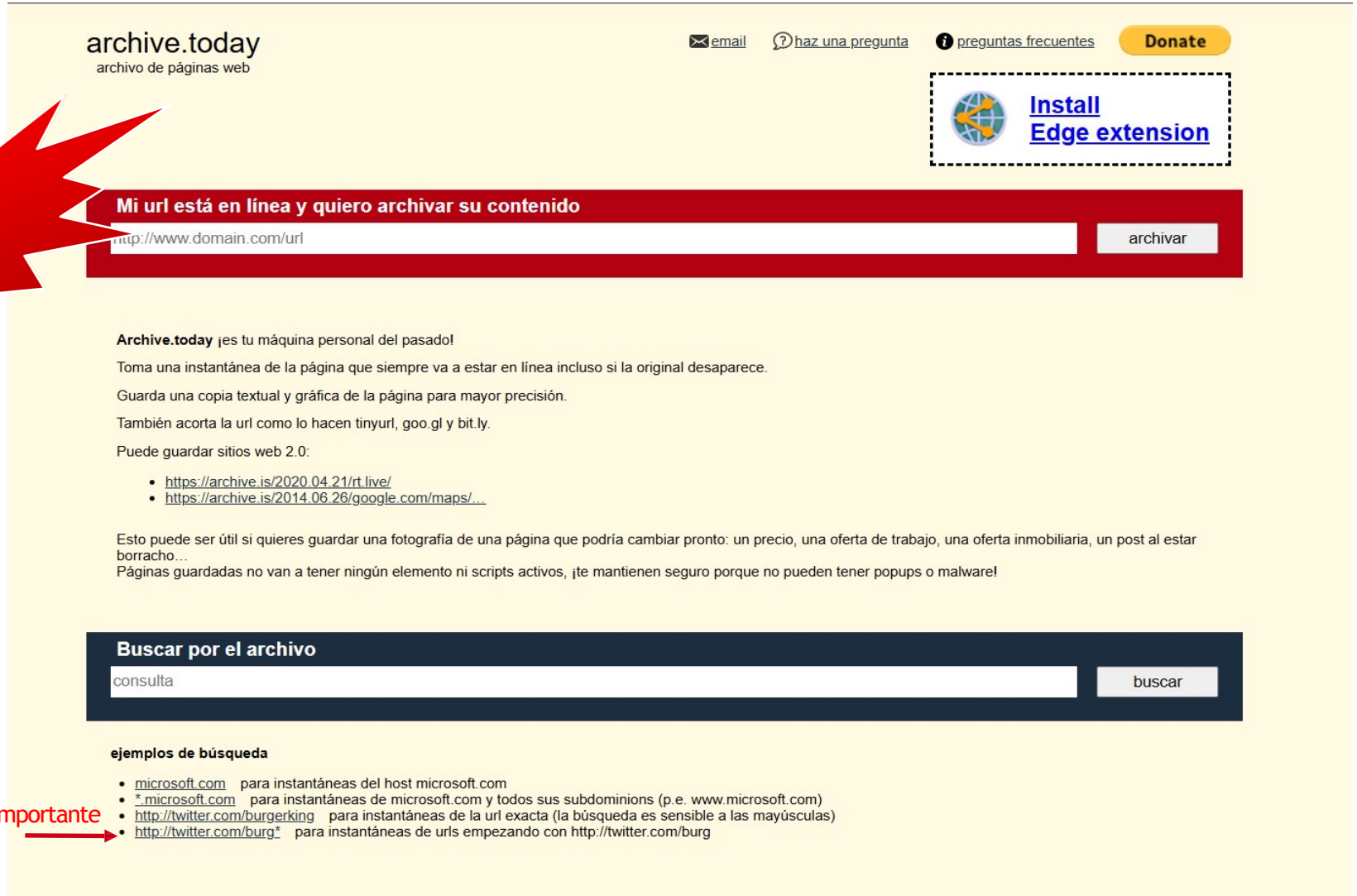
INTERNET NUNCA OLVIDA

Herramienta OSINT

🔗 WAYBACK MACHINE

INTERNET NUNCA OLVIDA

Herramienta OSINT



importante

Webpage archive

DATA LEAKS

Información filtrada:

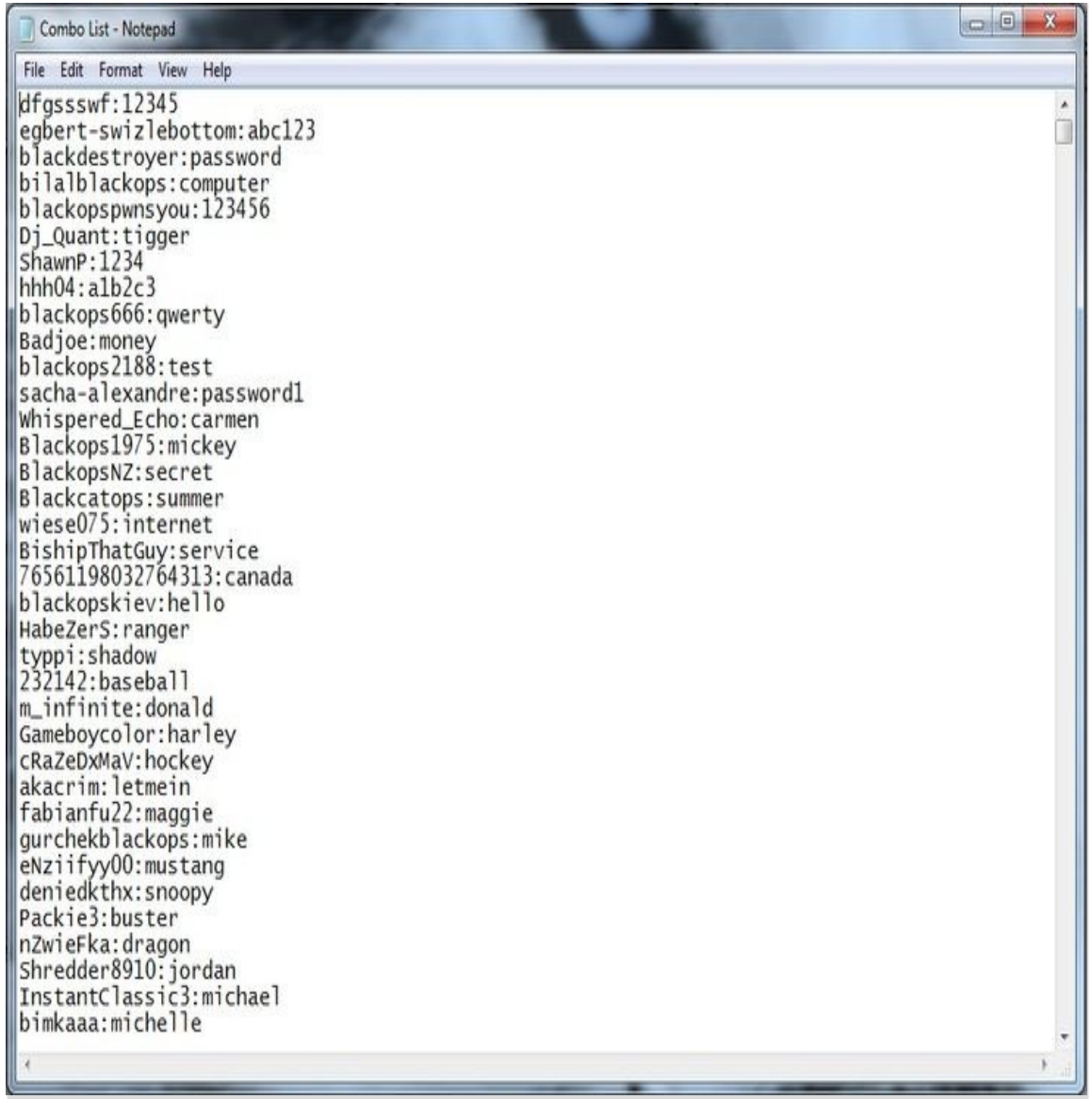
PERSEVERANCIA

PACIENCIA

OBJETIVIDAD

FLEXIBILIDAD

Listas User-Pass



Información filtrada:

PERSEVERANCIA

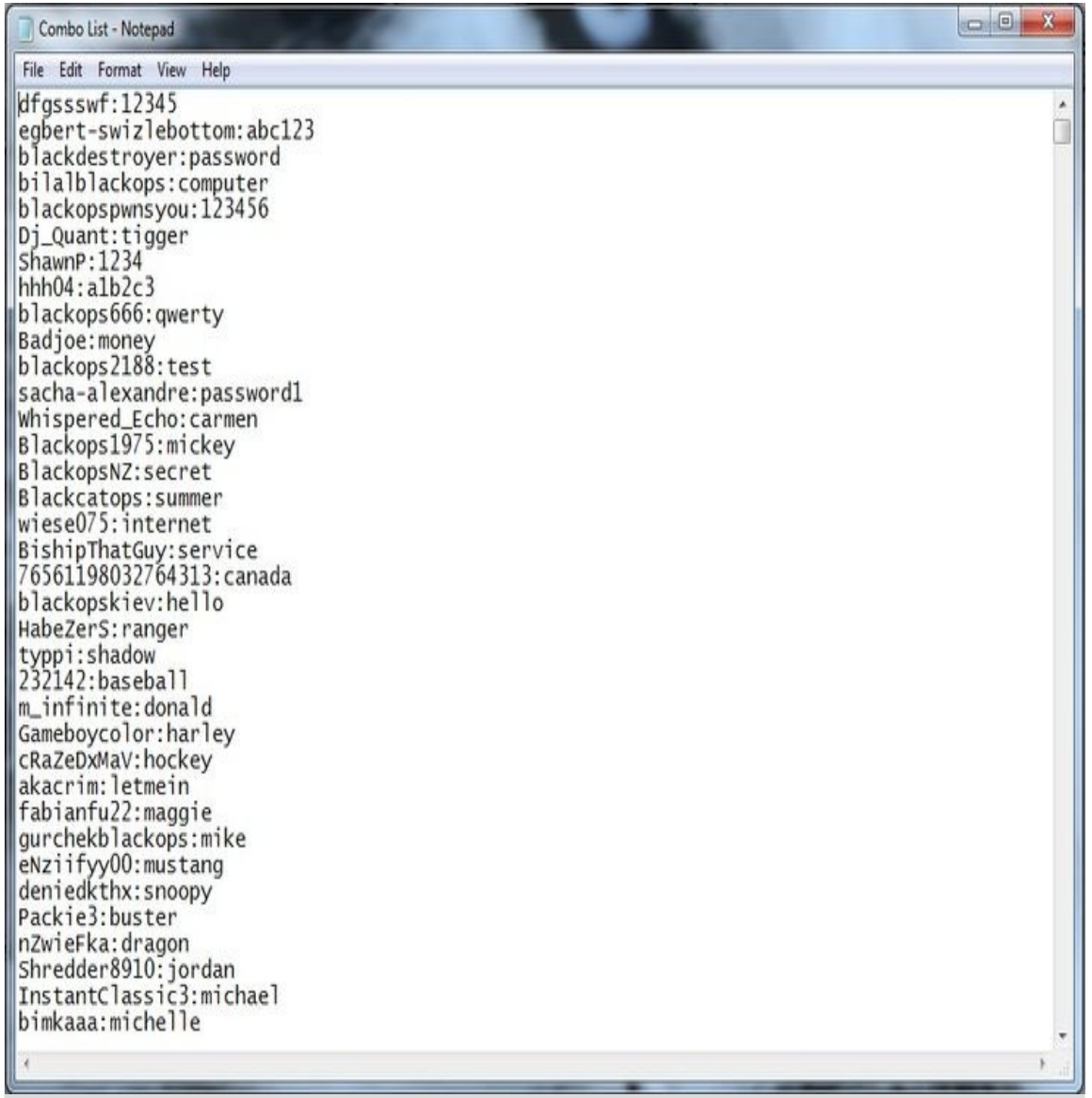
PACIENCIA

OBJETIVIDAD

FLEXIBILIDAD

SABER BUSCAR

Listas User-Pass



Universidad Rey Juan Carlos

DATA LEAKS

HERRAMIENTAS

1. Google Dorks
2. Telegram
3. Dark Web

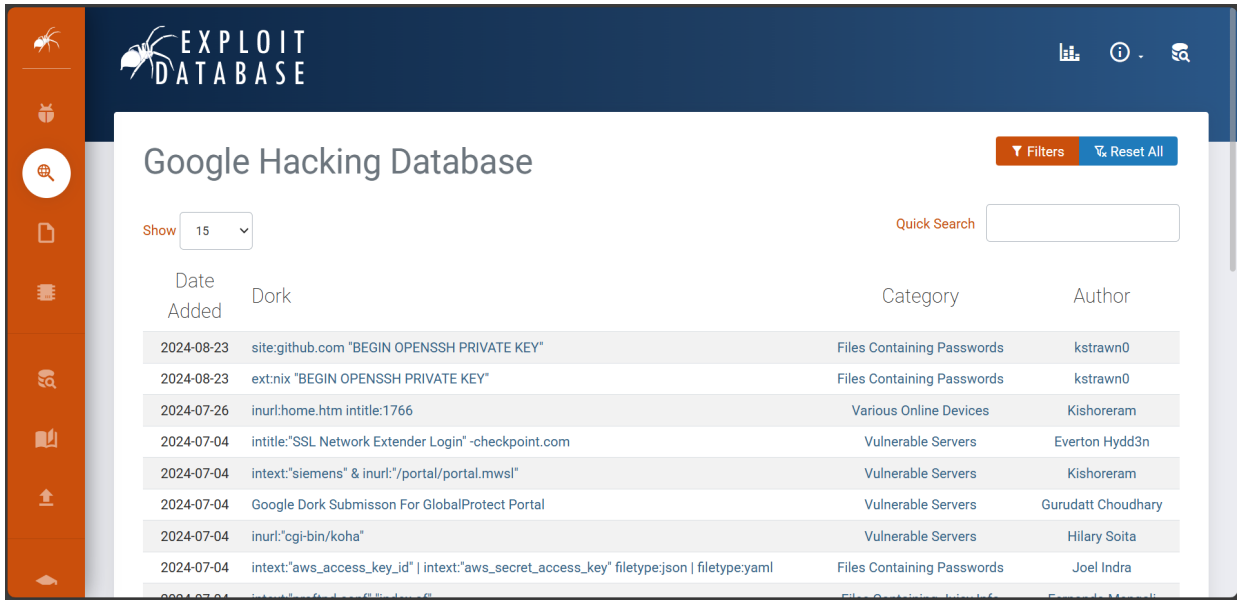
DATA LEAKS

Google Dorks

Permiten añadir filtros a nuestras búsquedas, es la herramienta más potente en el mundo del OSINT.

Principales ejemplos:[Google dork cheatsheet]

En Google Hacking Database hay cientos de ejemplos de búsquedas orientadas al Hacking: [Google Hacking Database (GHDB)]



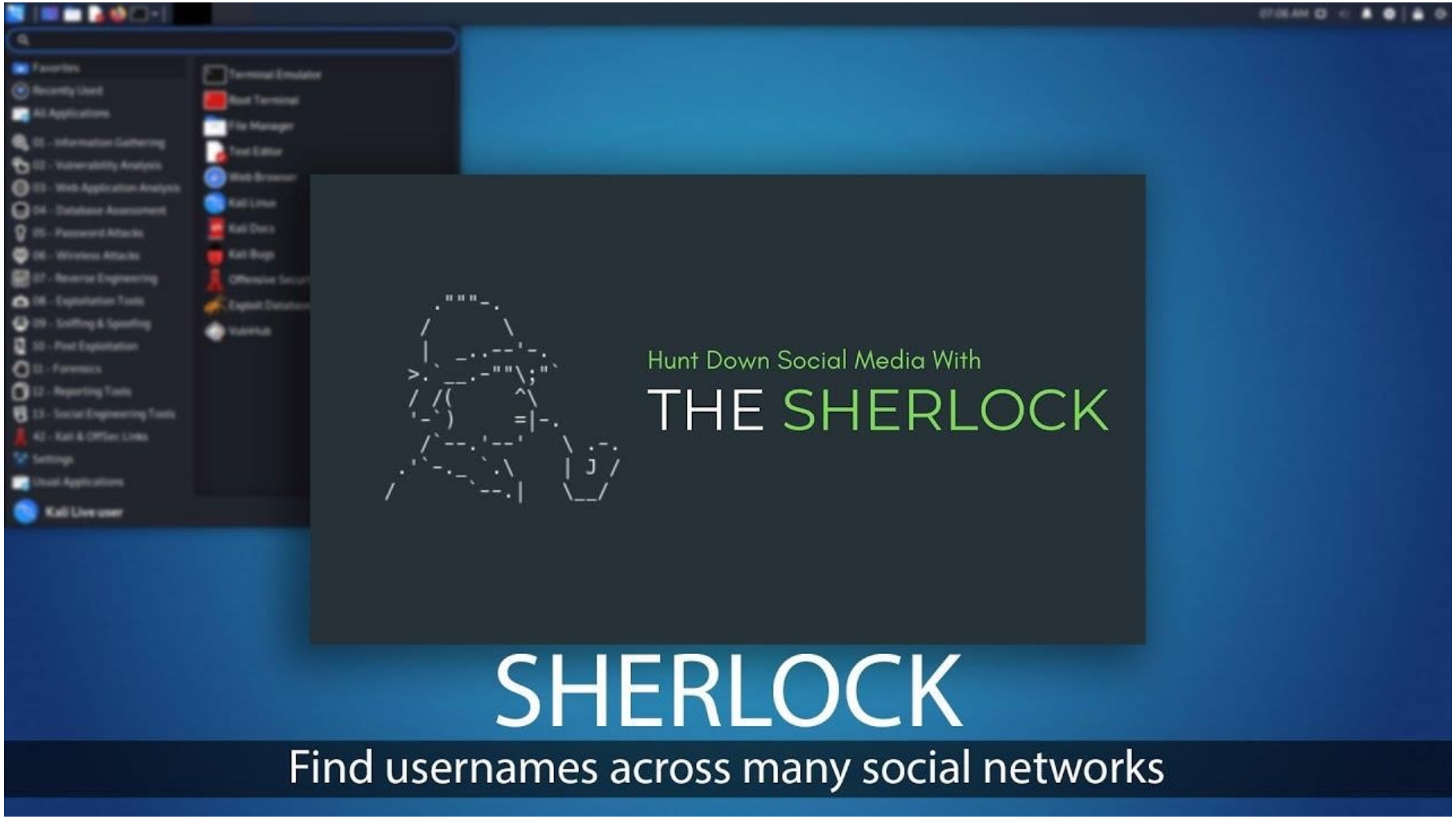
Universidad Rey Juan Carlos

DATA LEAKS

Otras Herramientas:

IntelligenceX

HUMINT (Human Intelligence)



Para instalar: sudo apt install sherlock

DATA LEAKS

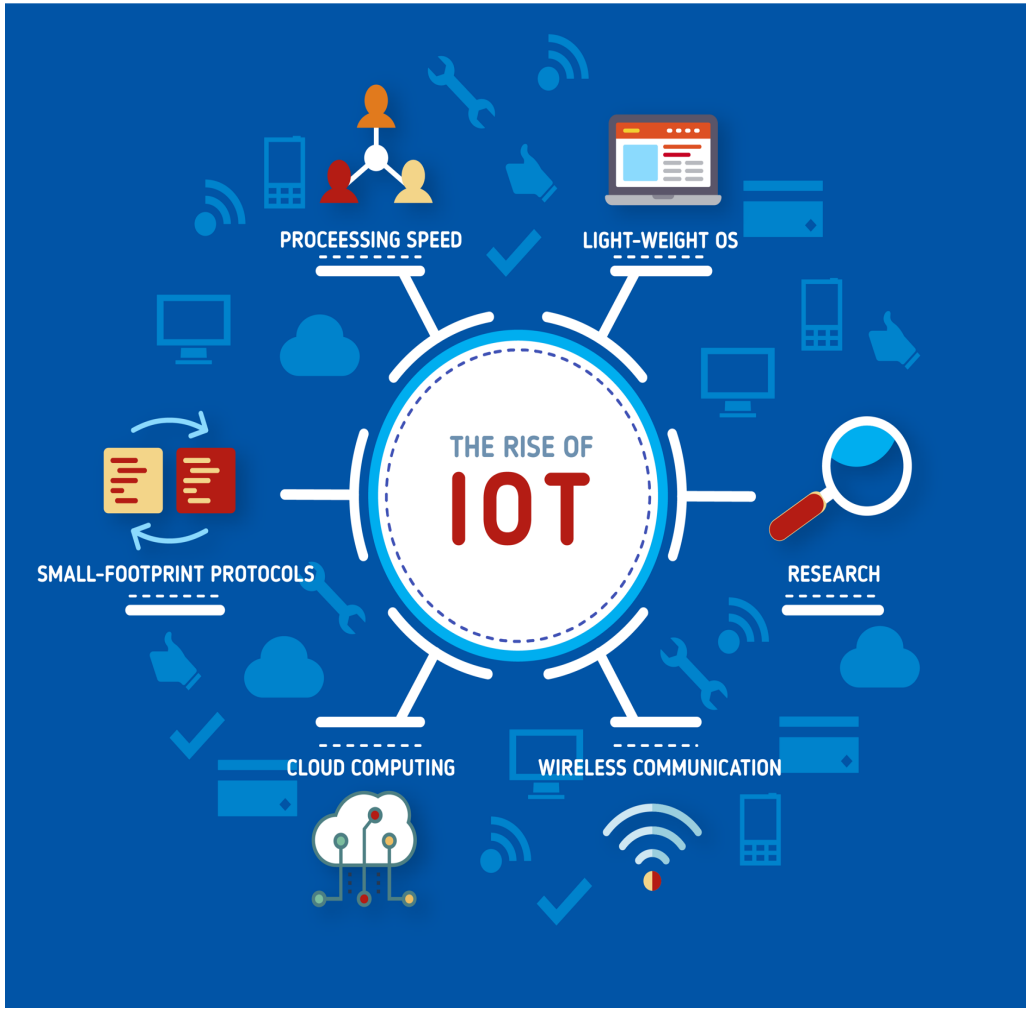
¿QUÉ INFORMACIÓN PODEMOS OBTENER CON LAS FILTRACIONES?

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 (Linkedln, 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

NMAP

Reconocimiento

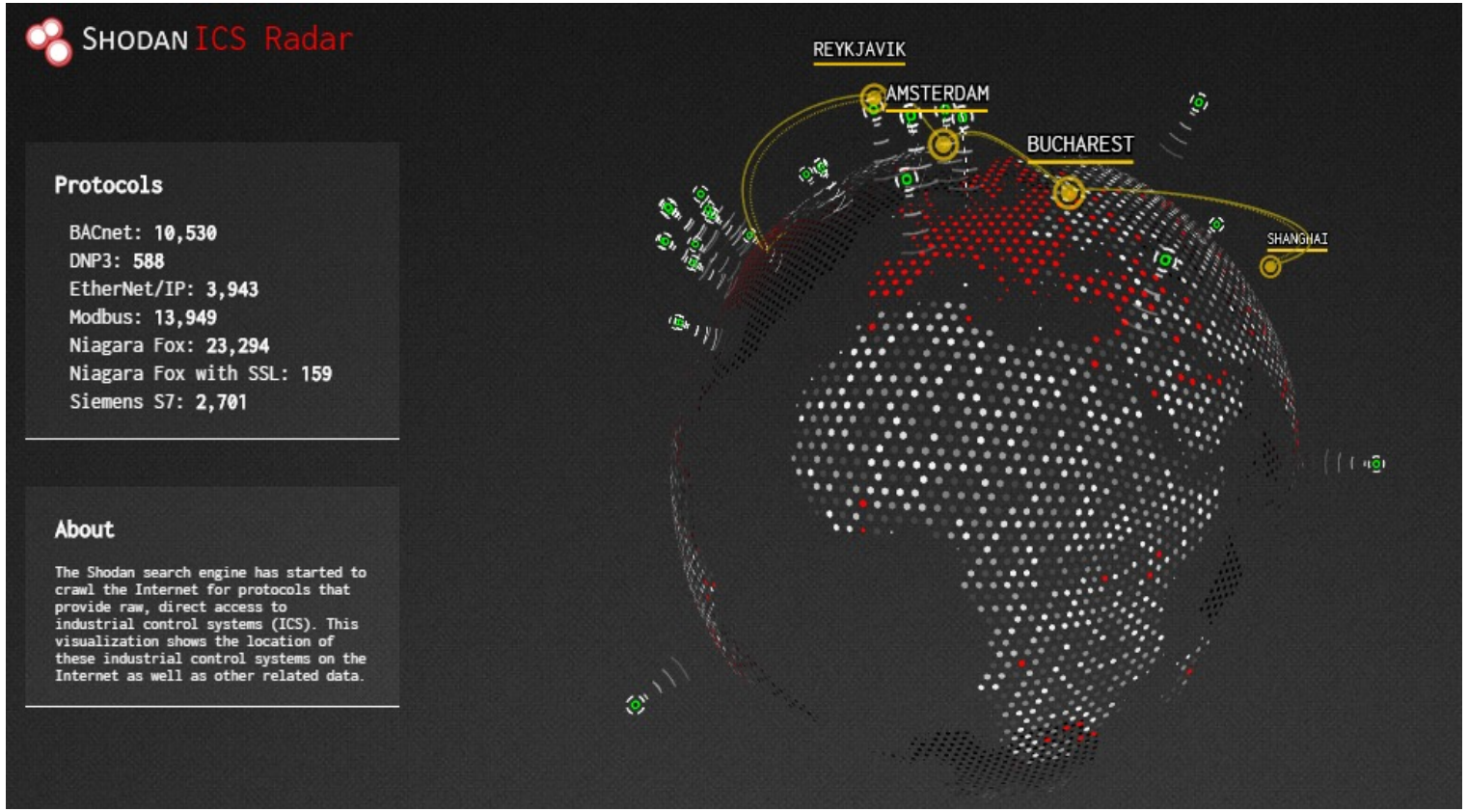
Shodan

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

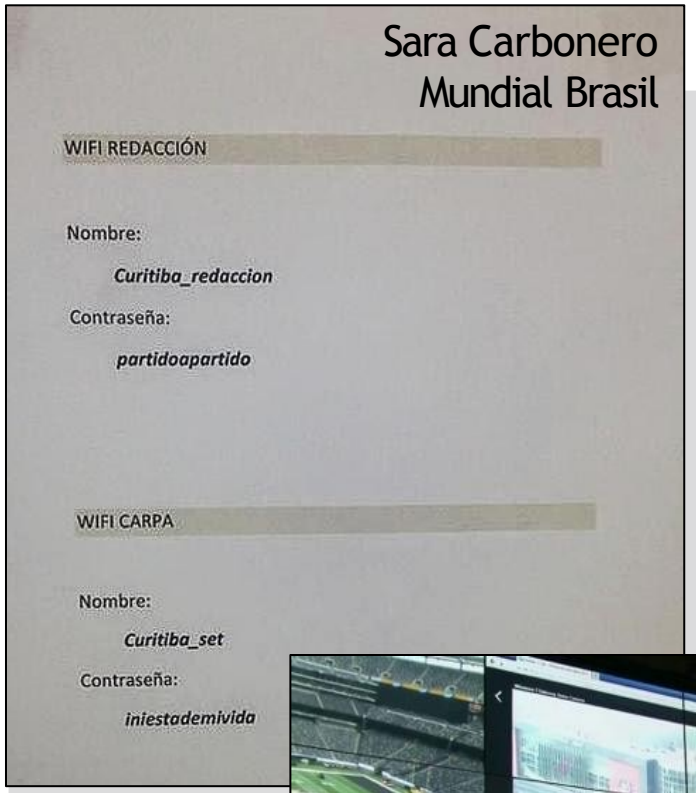
Puedes pedirles una cuenta premium por ser estudiante escribiendo a academic@shodan.io



IMINT (Image Intelligence)

Tim Cook (CEO Apple)

Centro de seguridad
Mundial Brasil



Centro de seguridad
SuperBowl 2020

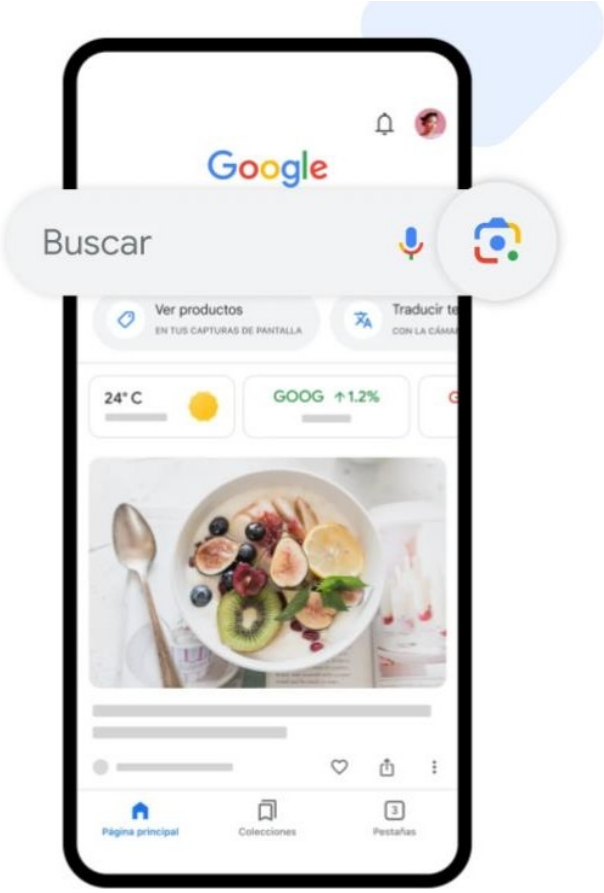
IMINT (Image Intelligence)

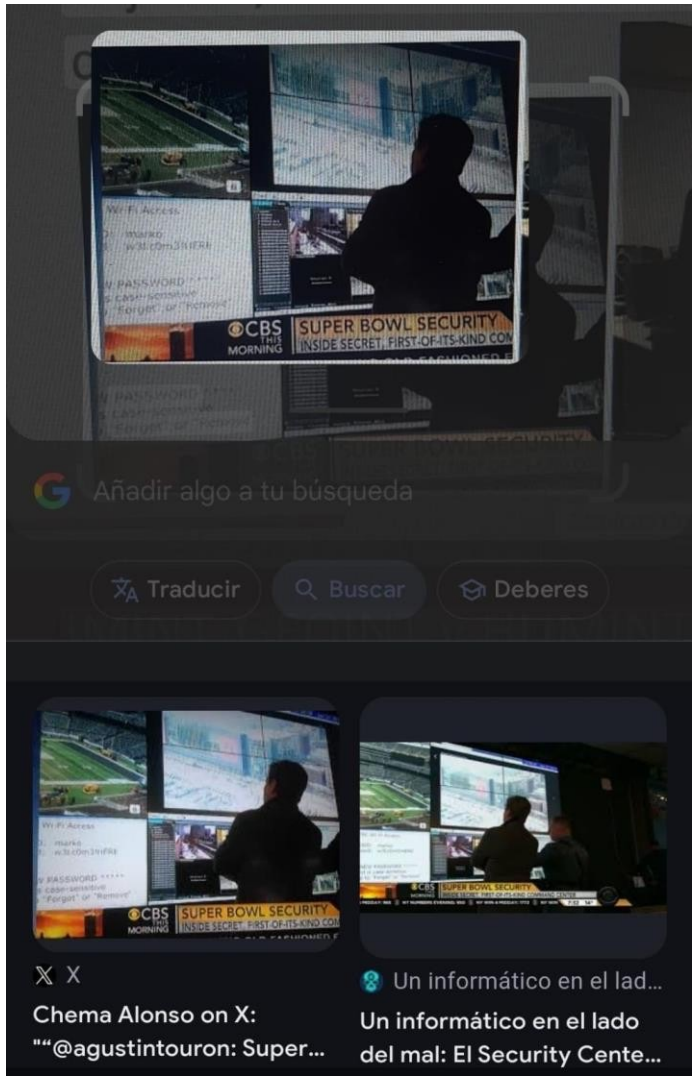
HERRAMIENTAS

1. Google Lens
2. Tin Eye
3. Yandex

IMINT (Image Intelligence)

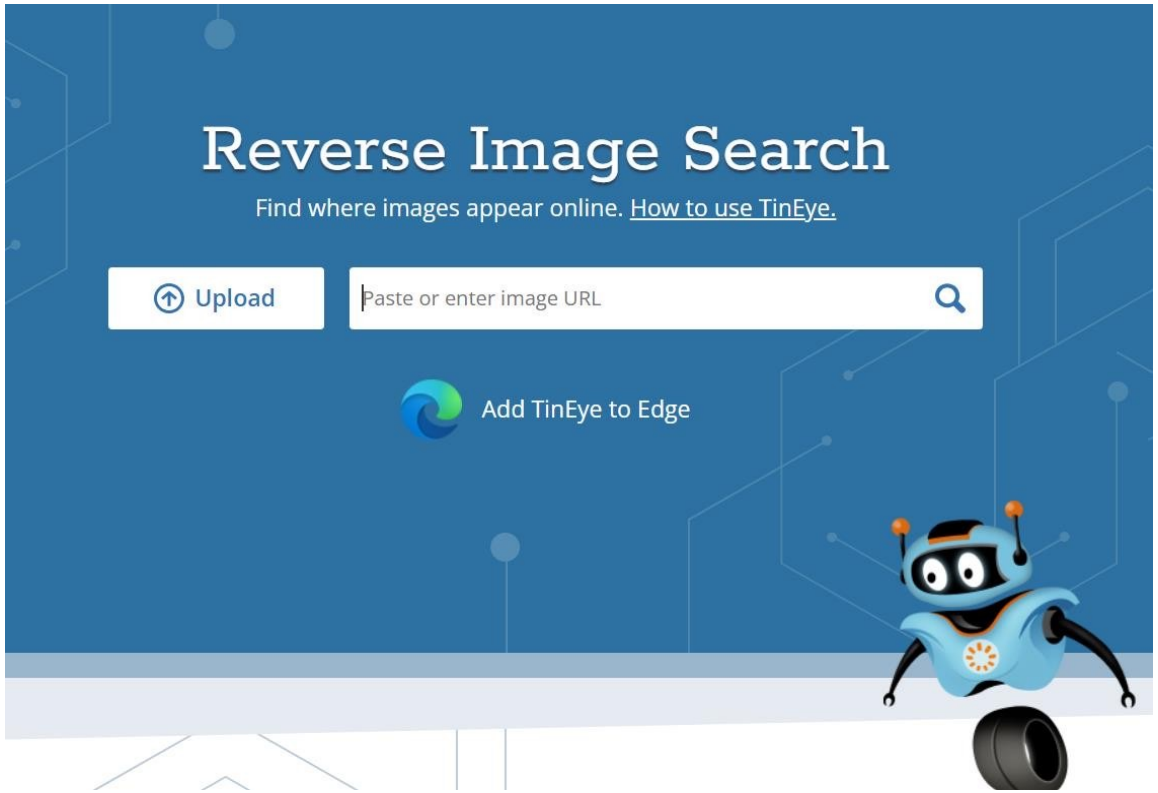
1. Google Lens





IMINT (Image Intelligence)

2. Tin Eye

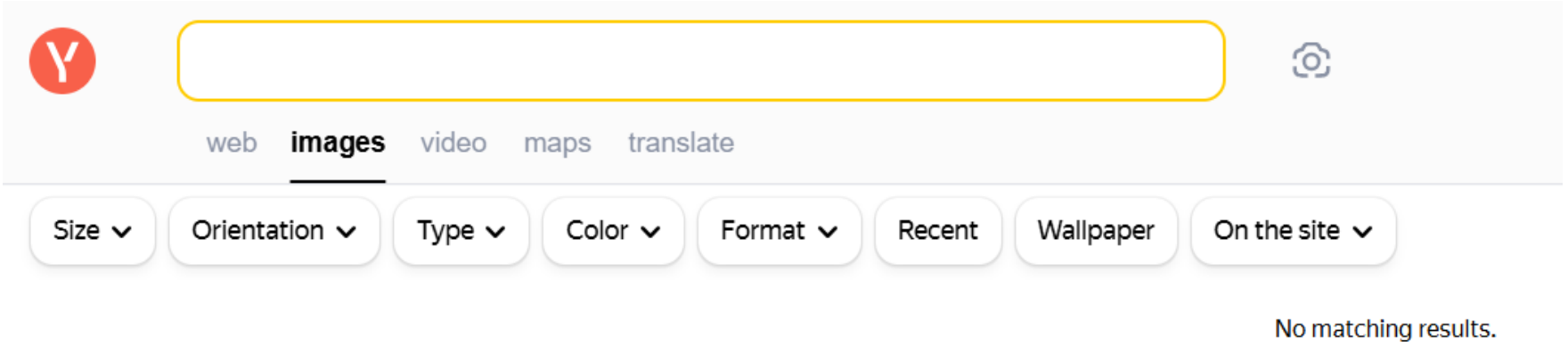


PARA ENCONTRAR:

- 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

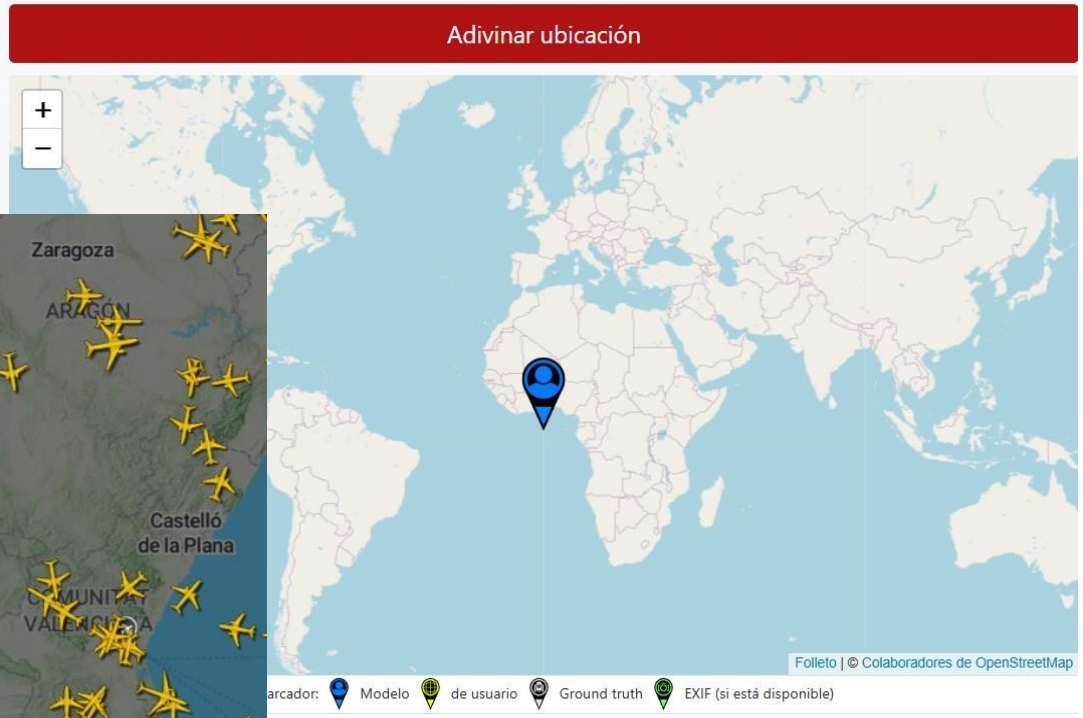


ES UN MOTOR DE BÚSQUEDA QUE PERMITE:

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

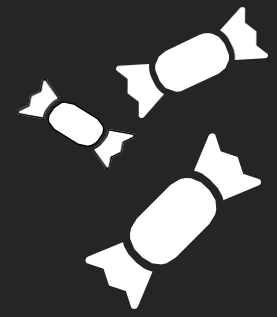
GEOINT (Geospatial Intelligence)

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



RETOS

OSINT



Preparar todas las herramientas!!

Universidad
Rey Juan Carlos

Esteganografía

Mari Luz Charfolé Maestro

Universidad
Rey Juan Carlos

Esteganografía

Ocultar información dentro de otros mensajes o medios físicos

TEXTO

AUDIO

IMÁGENES

METADATOS

Universidad Rey Juan Carlos

Comando file

```
┌──(kali㉿kali)-[~/Downloads]
└─$ file garden.jpg
garden.jpg: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72×72, segment length 16, baseline, precision 8, 2
999×2249, components 3
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ 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

Universidad Rey Juan Carlos

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
```

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

Universidad Rey Juan Carlos

Tipos: ocultar información en archivos de texto

Strings

```
┌──(kali㉿kali)-[~/Downloads]
└─$ strings garden.jpg
JFIF
XICC_PROFILE
HLino
mntrRGB XYZ
acspMSFT
IEC sRGB
-HP
cprt
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
```

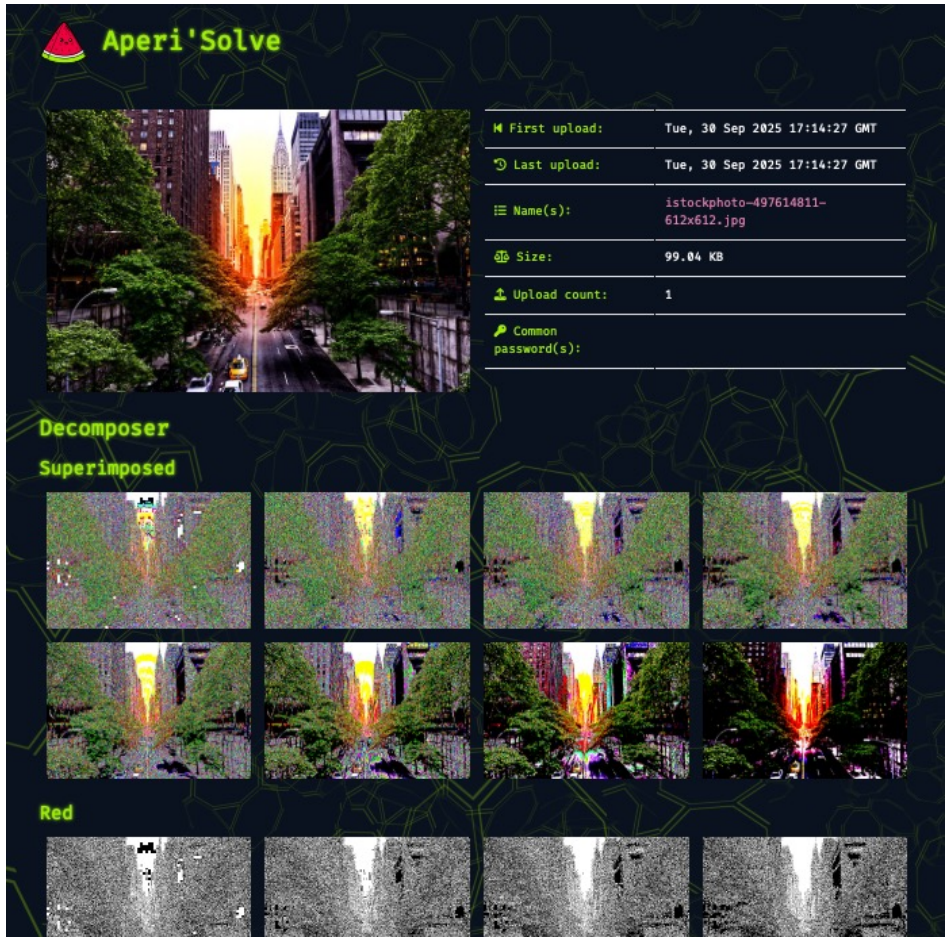
```
┌──(kali㉿kali)-[~/Downloads]
└─$ strings garden.jpg | grep picoCTF
Here is a flag "picoCTF{[redacted]}"
```

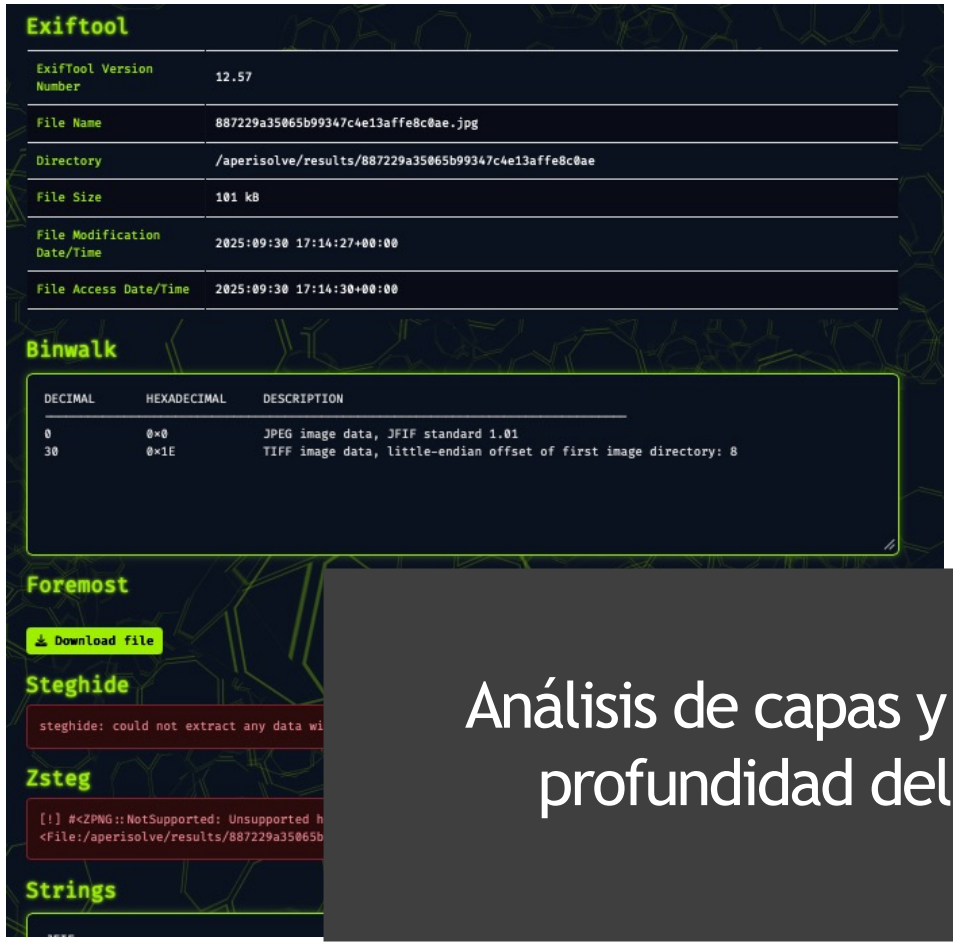
Extrae y muestra secuencias imprimibles de caracteres que aparecen dentro de un fichero

Tipos: ocultar información en imágenes

Aperisolve (y Fotoforensics)

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





Análisis de capas y análisis en profundidad del archivo

Universidad Rey Juan Carlos

Tipos: ocultar información en imágenes

Steghide

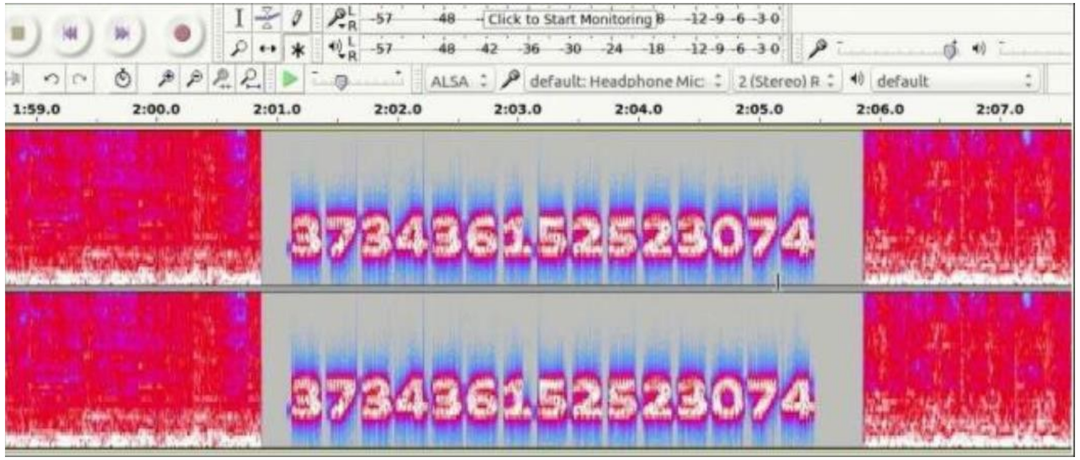
Para extraer:

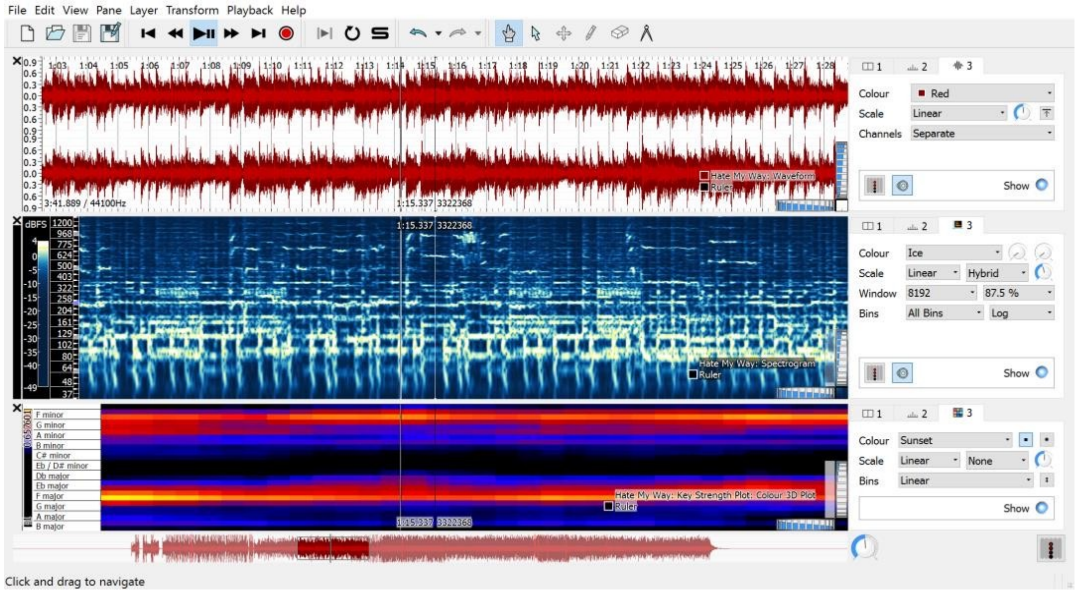
extract -sf nombre_archive_portador

Permite ocultar información dentro de otros archivos

Tipos: ocultar información en archivos de audio

Audacity y Sonic Visualizer

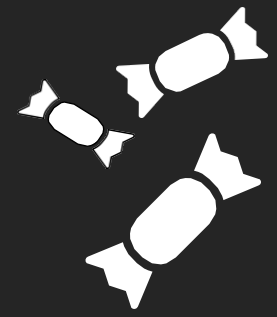




Resumen herramientas

- 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