Módulo 1: OSINT y esteganografía

Laura Sánchez Santiago
Carla Gómez Cabanillas

Universidad
Rey Juan Carlos

Universidad Rey Juan Carlos

Índice

OSINT

Carla Gómez Cabanillas

Universidad
Rey Juan Carlos

Introducción OSINT

- Publicaciones en redes sociales
- Compras en línea
- Uso de foros y blogs
- Búsquedas en internet
- Comentarios y reseñas

Universidad Rey Juan Carlos

Introducción OSINT

Publicaciones en redes sociales

Compras en línea

Uso de foros y blogs

Búsquedas en internet

Comentarios y reseñas

Ubicación

Gustos

Lugares que frecuentamos

Ideas, pensamientos, opiniones

Amistades

Preferencias de consumo

Dirección de envío

Hábitos diarios

Datos financieros

Webs que más utilizamos

Definición OSINT

- **O**pen **S**ource **Int**elligence
- Recopilar y analizar información pública.
- Tirando del hilo...encontraremos la flag!

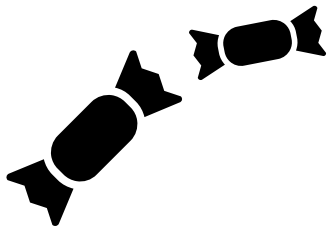
Categorías

- HUMINT
- IMINT
- GEOINT
- SIGINT

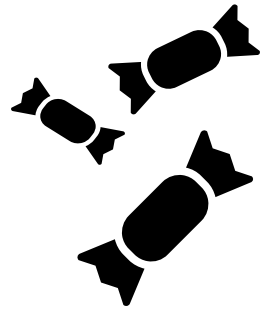
OSINT Framework

Link: OSINT Framework

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



RETO 1



¿QUIÉNES GANARÁN EL PRIMER RETO?

TRUQUITO: Prepara las herramientas vistas de OSINT Framework

Universidad Rey Juan Carlos

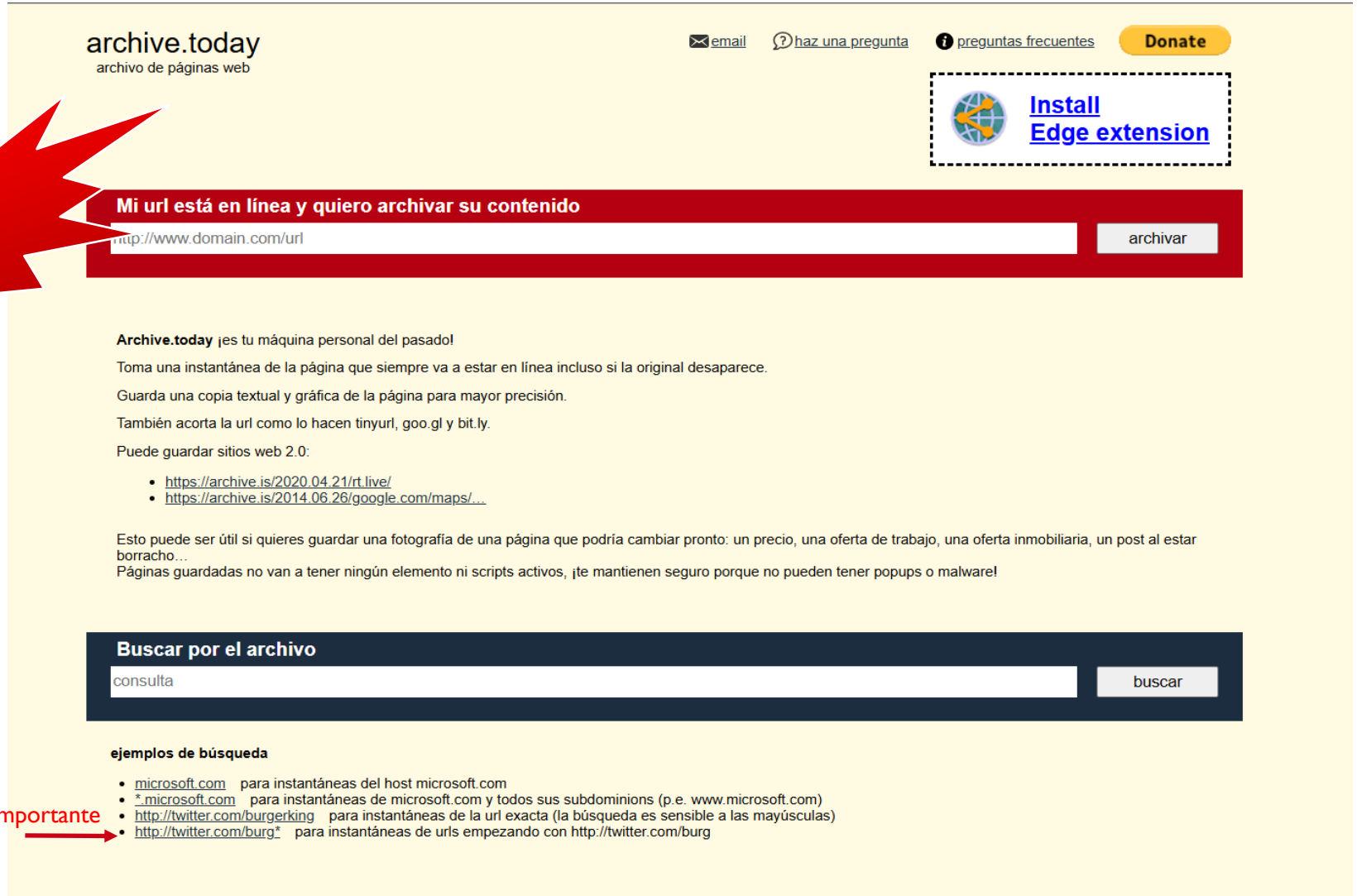
INTERNET NUNCA OLVIDA

WAYBACK MACHINE

¿¿Cómo era tu web hace x años?? → Ejemplo: Conciertos WiZink Center

INTERNET NUNCA OLVIDA

Herramienta OSINT



importante

Webpage archive

Habilidades HUMINT:

PERSEVERANCIA

PACIENCIA

OBJETIVIDAD

FLEXIBILIDAD

Cotilleo – boca a boca

Habilidades HUMINT:

PERSEVERANCIA

PACIENCIA

OBJETIVIDAD

FLEXIBILIDAD

INVESTIGACIÓN

Saber preguntar

Cotilleo – boca a boca

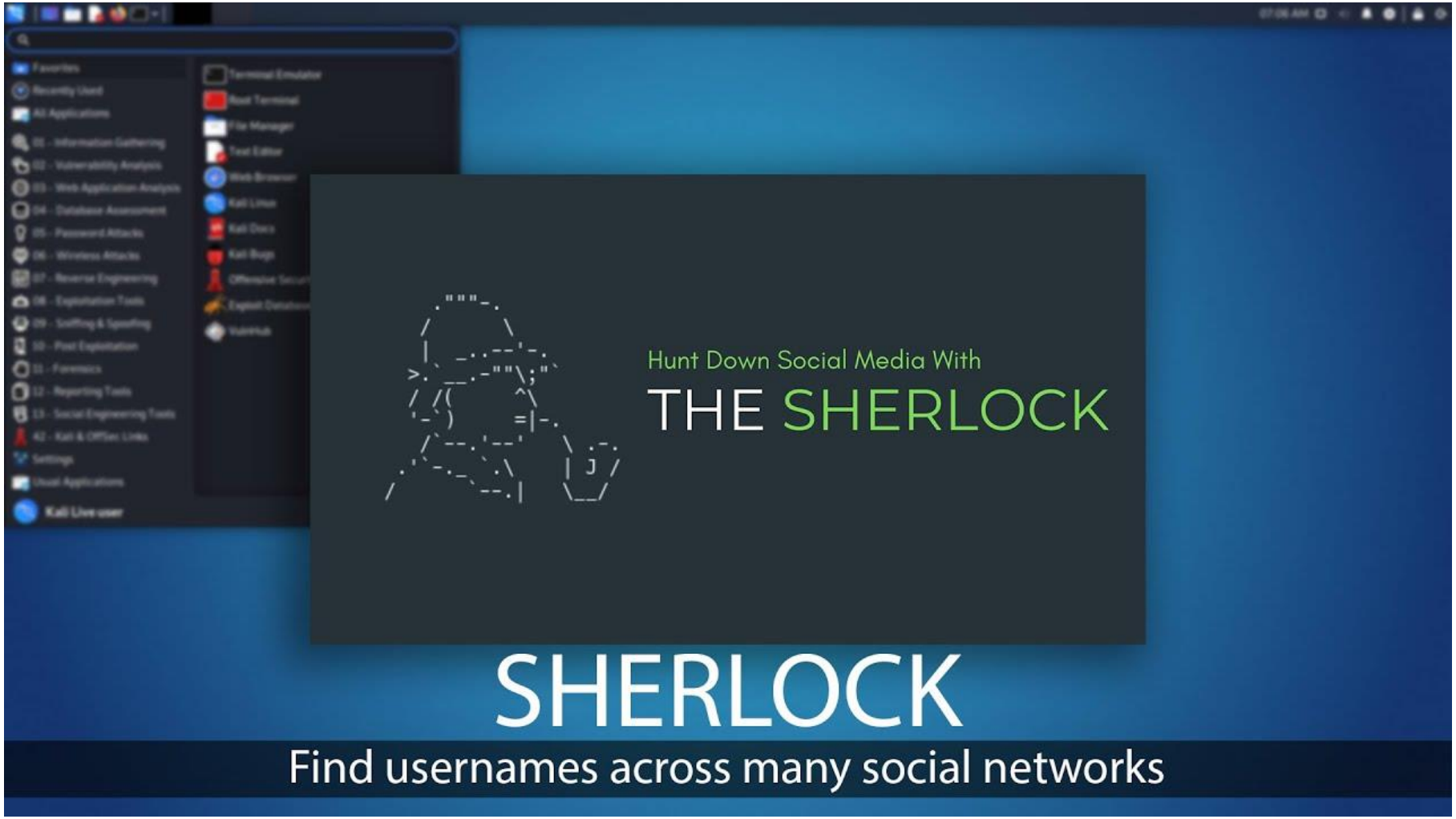
HUMINT (Human Intelligence)

¿QUÉ INFORMACIÓN PODEMOS OBTENER CON HUMINT?

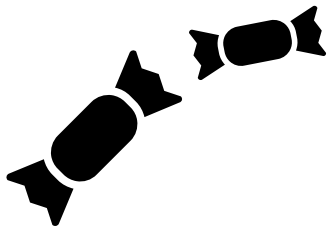
¿QUÉ PODEMOS HACER CON ELLA?

Email	• Cuentas asociadas • Saber si ha sufrido una violación de datos	Have I Been Pwned
Números de teléfono	• Cuentas asociadas en RRSS • Herramientas abiertas	
GESTOR 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	Veremos sherlock

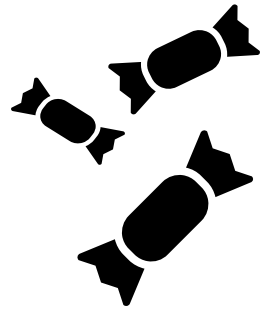
HUMINT (Human Intelligence)



Para instalar: sudo apt install sherlock



RETO 2



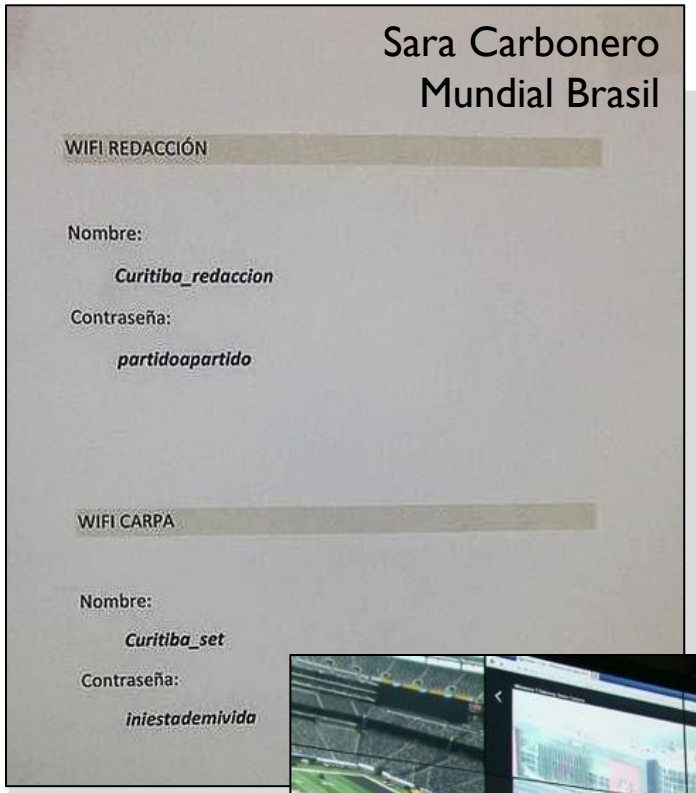
¿QUIÉNES GANARÁN EL SEGUNDO RETO?

TRUQUITO: ¡¡Prepara las herramientas que hemos visto!!

Universidad Rey Juan Carlos

Tim Cook (CEO Apple)

Centro de seguridad
Mundial Brasil



Sara Carbonero
Mundial Brasil

Centro de seguridad
SuperBowl 2020

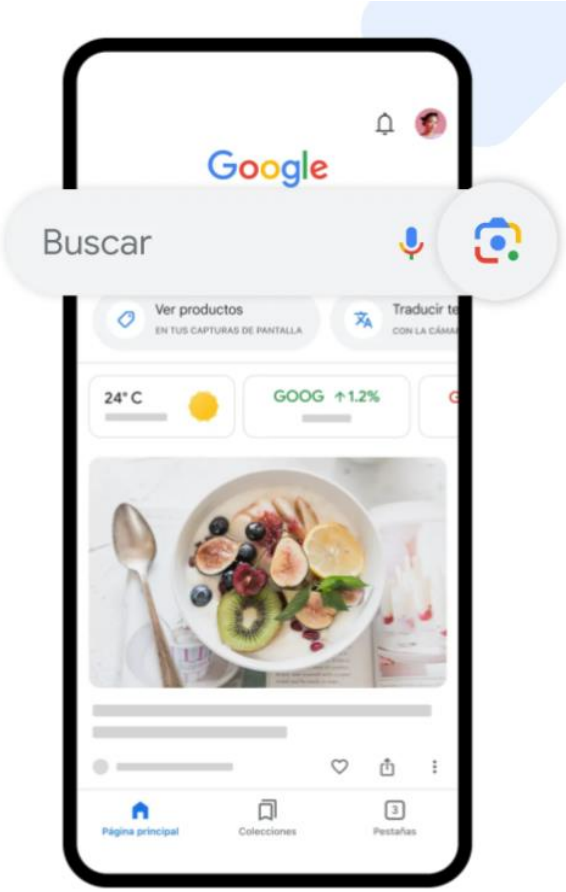
IMINT (Image Intelligence)

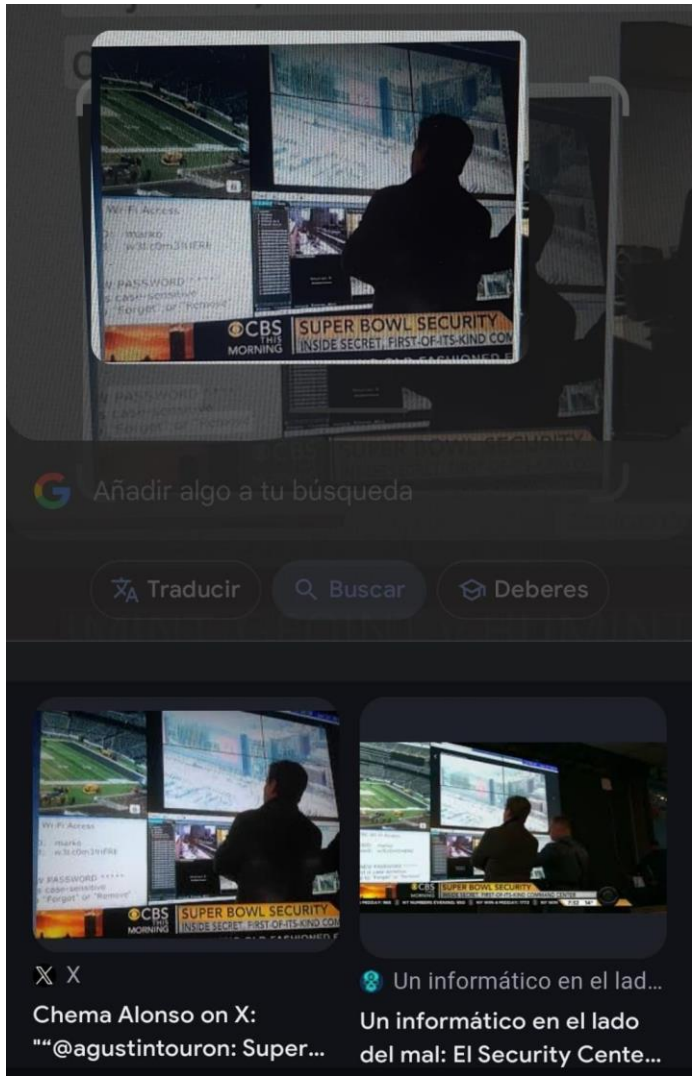
HERRAMIENTAS

1. Google Lens
2. Tin Eye
3. Yandex

IMINT (Image Intelligence)

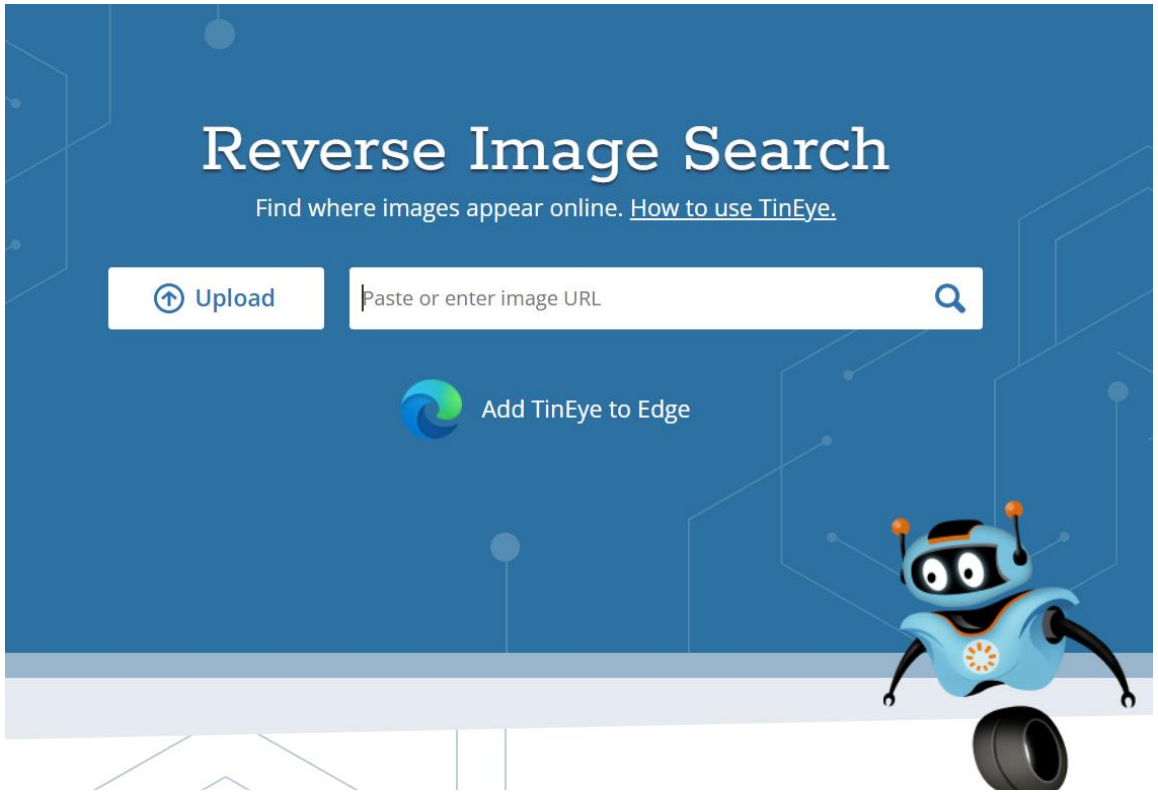
1. Google Lens





IMINT (Image Intelligence)

2. Tin Eye

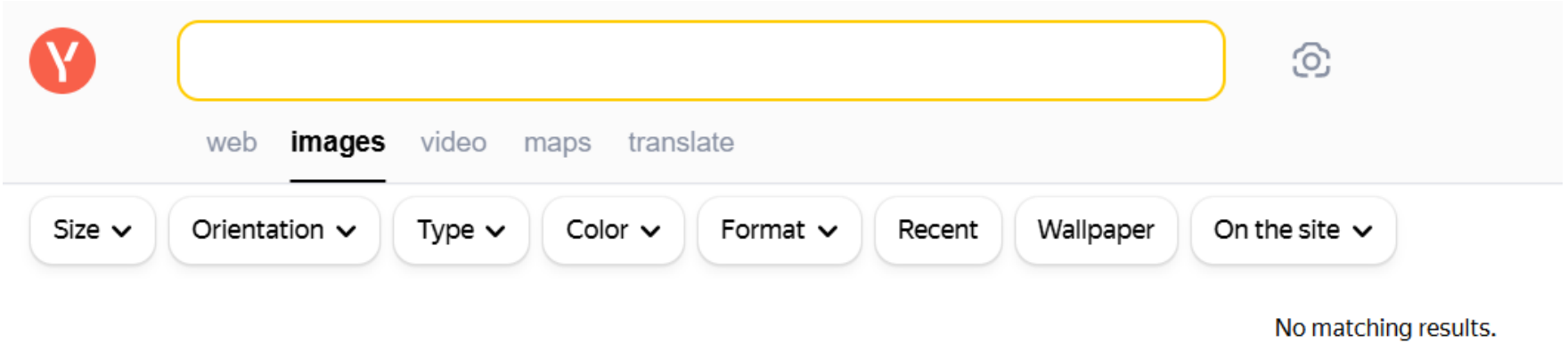


PARA ENCONTRAR:

- 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)

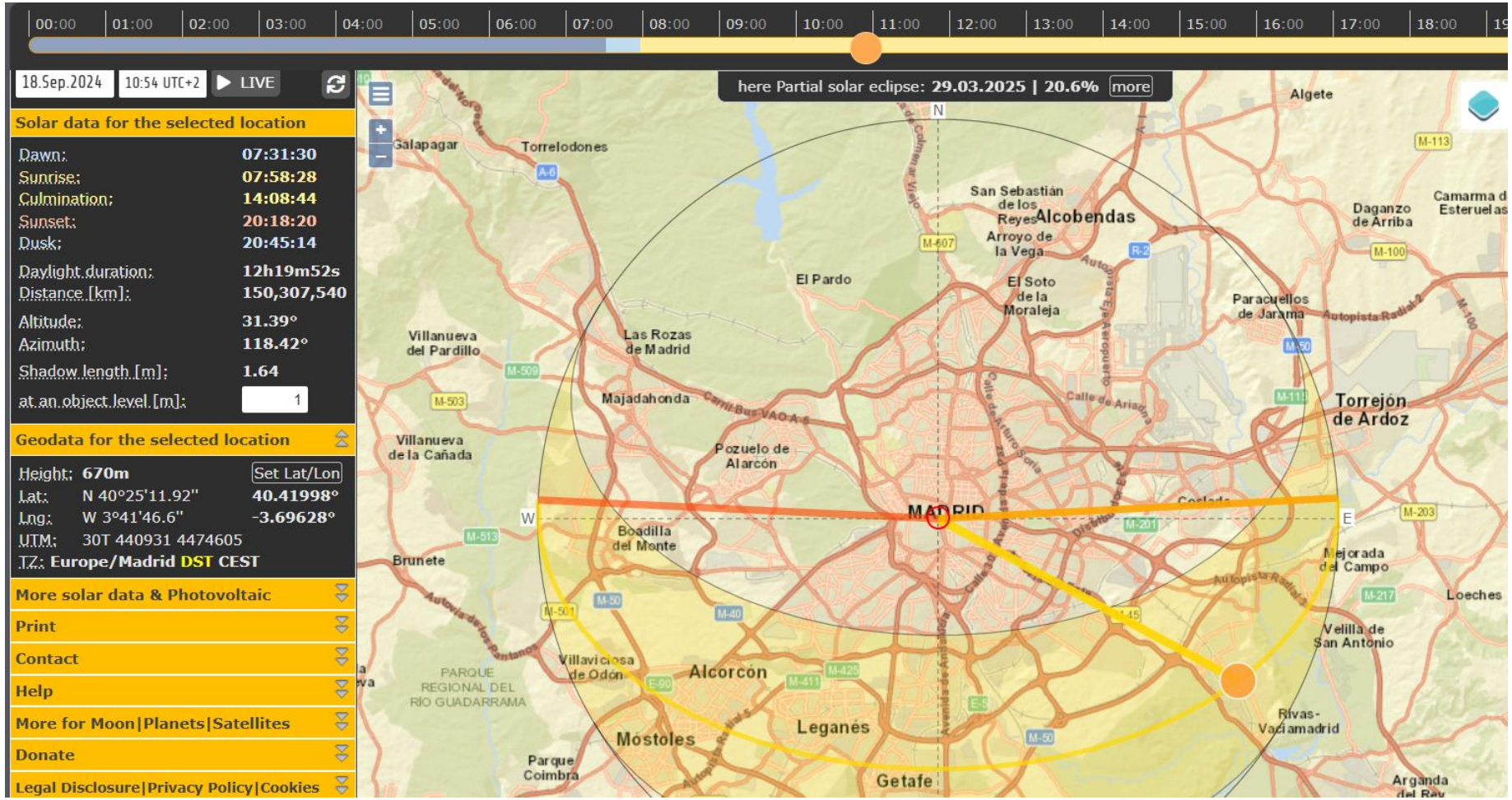
3. Yandex



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...

IMINT (Image Intelligence)



SunCalc

IMINT (Image Intelligence)

Fotoforense

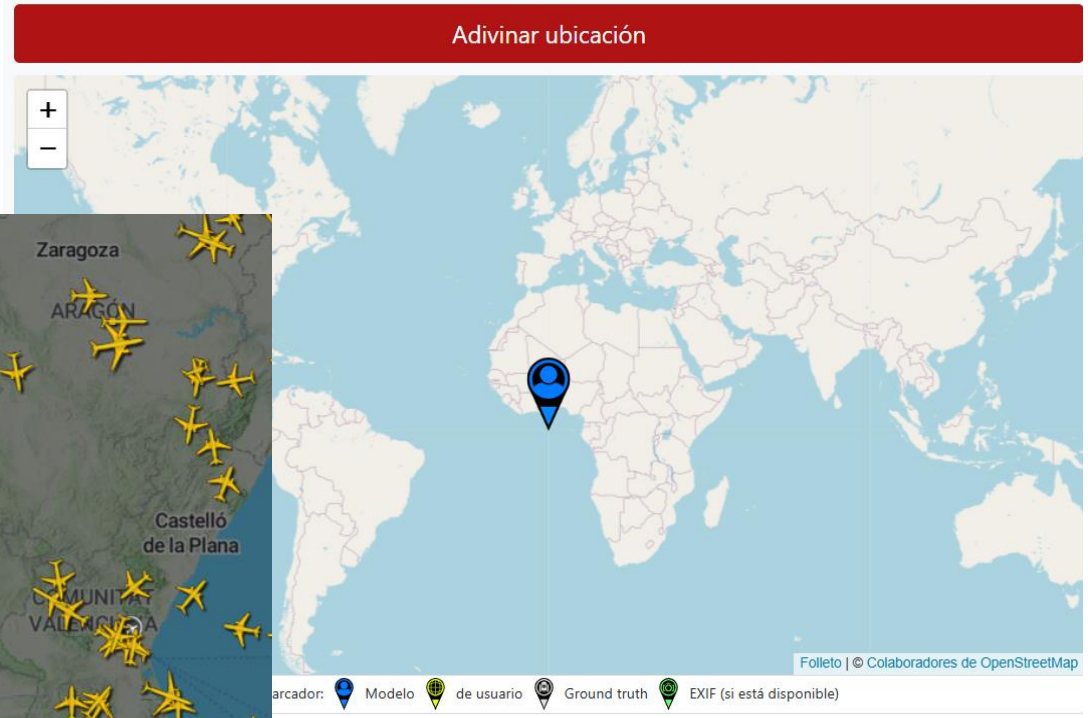
Analizar manifestaciones

Controlar el tráfico

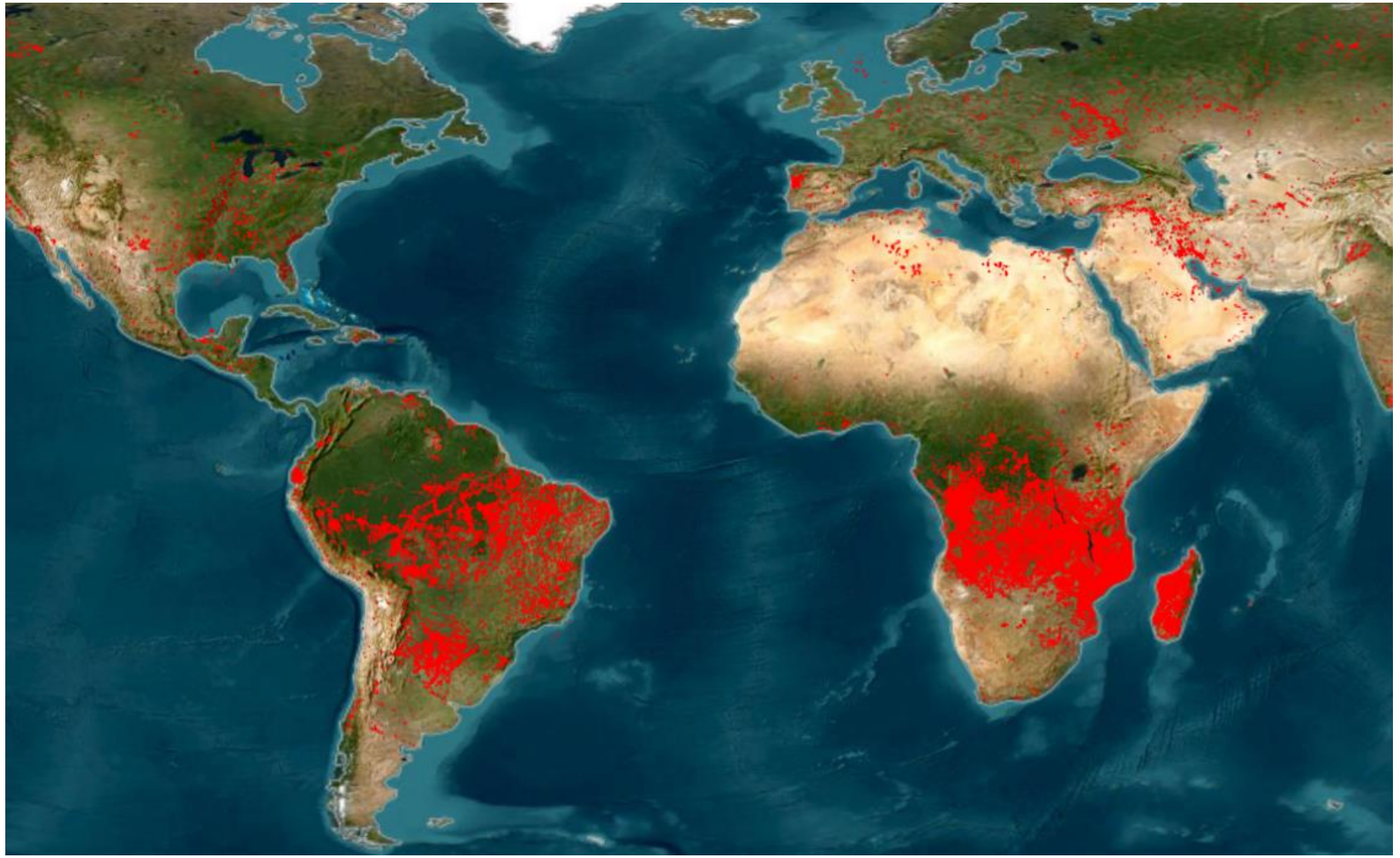
• • •

GEOINT (Geospatial Intelligence)

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



GEOINT (Geospatial Intelligence)



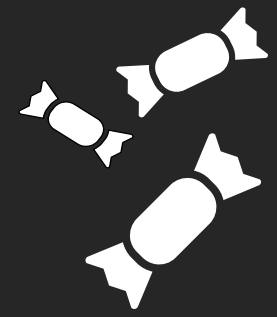
La NASA | LANA | EMPRESAS

Herramientas OSINT

- OSINT Framework: OSINT Framework
- Wayback Machine: WAYBACK MACHINE
- Archive.is: Webpage archive
- Have I been pwned: Have I Been Pwned
- Password checker: Password Check | Kaspersky
- Webmii: Webmii
- Google Lens: Google Lens
- Tin Eye: Tin Eye
- Yandex: Yandex
- Suncalc: SunCalc
- Foto Forensics: Fotoforense
- Geoestimation TIB: Estimación de geolocalización (tib.eu)
- Radar box: AirNav RadarBox
- Modaps (incendios) NASA: La NASA | LANA | EMPRESAS

CTF 1

OSINT



Universidad
Rey Juan Carlos

Esteganografía

Laura Sánchez Santiago

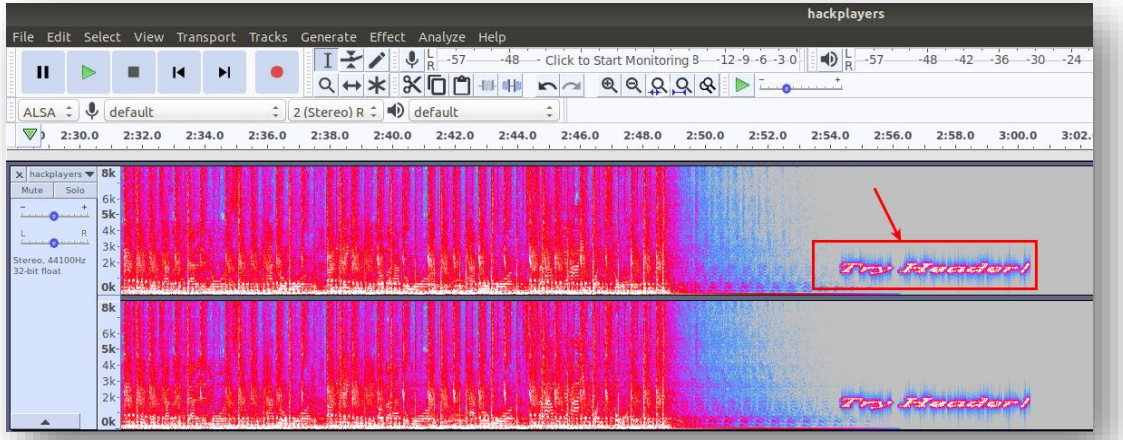
Universidad
Rey Juan Carlos

Universidad Rey Juan Carlos

¿Qué es?

Ocultar información dentro de otro mensaje u objeto físico para evitar su detección

```
[/tmp/steg]-$ time stegseek --seed GIFTS.jpg -
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found (possible) seed: "45ff2f96"
        Plain size: 47.0 Byte(s) (compressed)
        Encryption Algorithm: none
        Encryption Mode:      cbc
[i] Original filename: "flag.txt".
[i] Extracting to stdout.

X-MAS{l00k$_l!k3_y0u_l1k3_b0sE64}

real    0m13,612s
user    1m48,268s
sys     0m0,032s
[/tmp/steg]-$
```




```
Terminal                                                    ⌥⌘1

(17:50) dmulholl ~/dev
 >> ./hexdump -n 128 hexdump.c
    0 | 23 69 6E 63  6C 75 64 65  20 22 61 72  67 73 2E 68 | #include "args.h
   10 | 22 0A 23 69  6E 63 6C 75  64 65 20 3C  73 74 64 69 | ".#include <stdi
   20 | 6F 2E 68 3E  0A 23 69 6E  63 6C 75 64  65 20 3C 73 | o.h>.#include <s
   30 | 74 64 6C 69  62 2E 68 3E  0A 23 69 6E  63 6C 75 64 | tdlib.h>.#includ
   40 | 65 20 3C 73  74 64 62 6F  6F 6C 2E 68  3E 0A 23 69 | e <stdbool.h>.#i
   50 | 6E 63 6C 75  64 65 20 3C  73 74 64 69  6E 74 2E 68 | nclude <stdint.h
   60 | 3E 0A 0A 0A  63 68 61 72  2A 20 68 65  6C 70 74 65 | >...char* helpte
   70 | 78 74 20 3D  0A 20 20 20  20 22 55 73  61 67 65 3A | xt =.    "Usage:

(--:--) dmulholl ~/dev
 >>
```

Universidad Rey Juan Carlos

Tipos

```
[/tmp/steg]~$
```

Texto

- Ocultar información en archivos de texto

- Herramientas:
  Binwalk
  Stegseek
  Strings

```
STRINGS(1)                  GNU Development Tools                  STRINGS(1)

NAME
       strings - print the strings of printable characters in files.

SYNOPSIS
       strings [-afovV] [-min-len]
               [-n min-len] [--bytes=min-len]
               [-t radix] [--radix=radix]
               [-e encoding] [--encoding=encoding]
               [-] [--all] [--print-file-name]
               [-T bfdname] [--target=bfdname]
               [--help] [--version] file
```

Binwalk

```
┌──(kali㉿kali)-[~/Downloads/reto]
└─$ binwalk -D ".*" PurpleThing.jpeg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 780 x 720, 8-bit/color RGBA, non-interlaced
41            0x29            Zlib compressed data, best compression
153493        0x25795         PNG image, 802 x 118, 8-bit/color RGBA, non-interlaced


┌──(kali㉿kali)-[~/Downloads/reto]
└─$ tree
.
├── PurpleThing.jpeg
└── _PurpleThing.jpeg.extracted
    ├── 0
    ├── 25795
    ├── 29
    └── 29-0

2 directories, 5 files
```

https://github.com/ReFirmLabs/binwalk

Detecta y extrae archivos que se encuentran ocultos dentro de otros

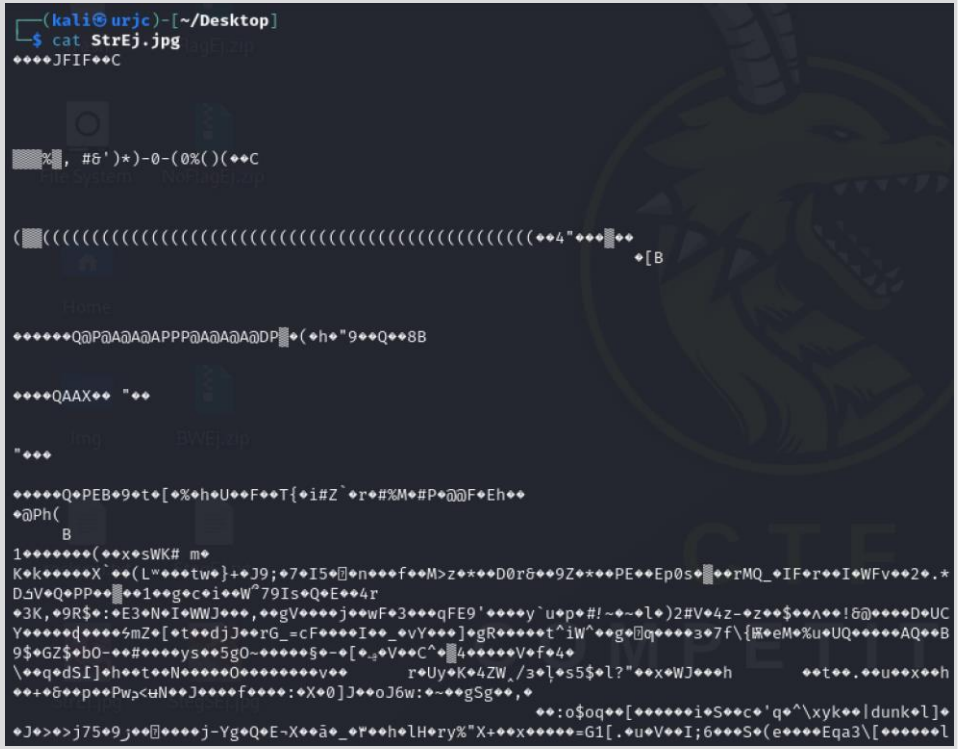
Stegseek

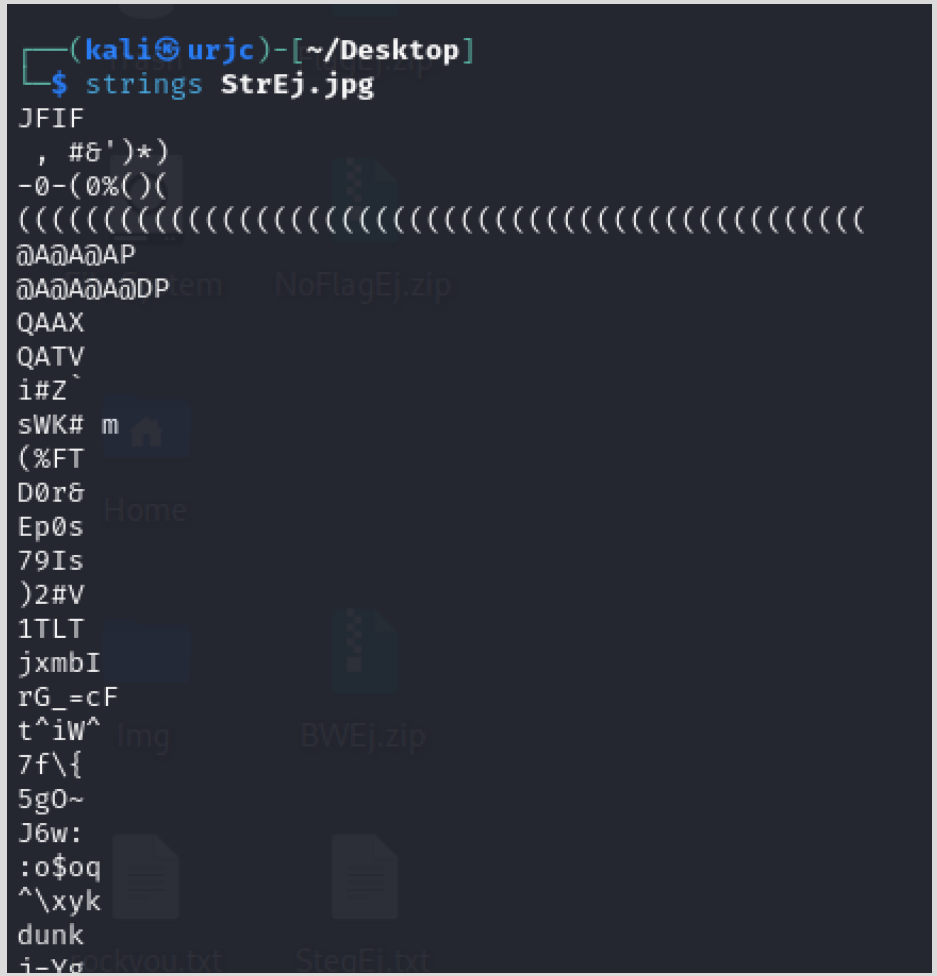
```
┌──(kali㉿kali)-[~/Downloads/reto]
└─$ stegseek --crack -sf th-2669789895.jpeg -wl /usr/share/wordlists/rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[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 la herramienta steghide en imágenes .jpg

https://github.com/RickdeJager/stegseek

Strings





Imprime las secuencias legibles de un archivo

https://github.com/glowyphp/strings

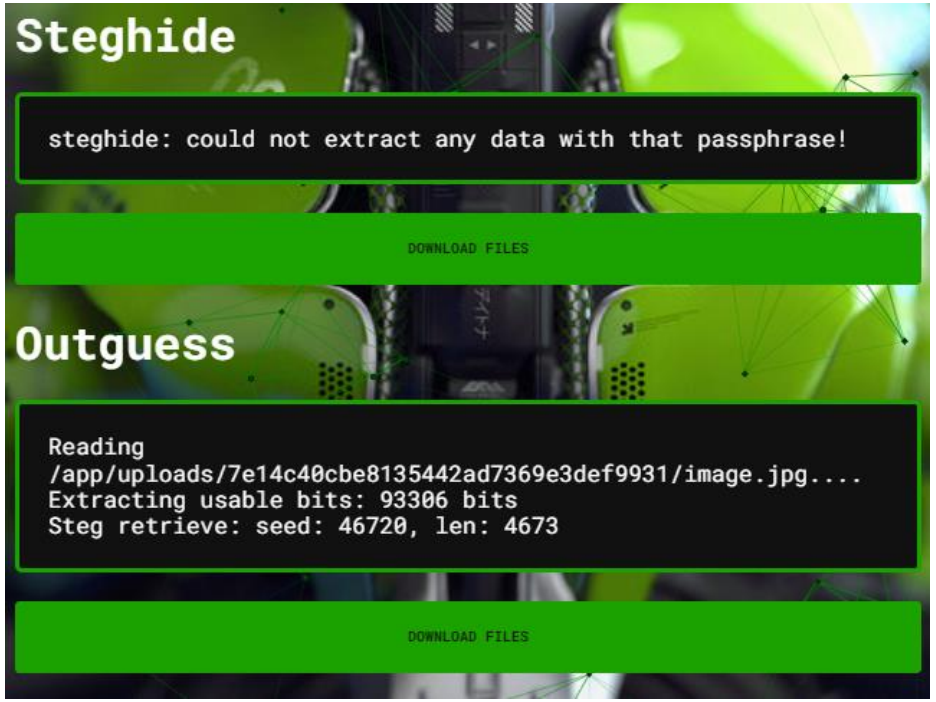
Tipos

Imagen

- Herramientas:
  Fotoforensics (online)
  Aperisolve (online)
  Steghide

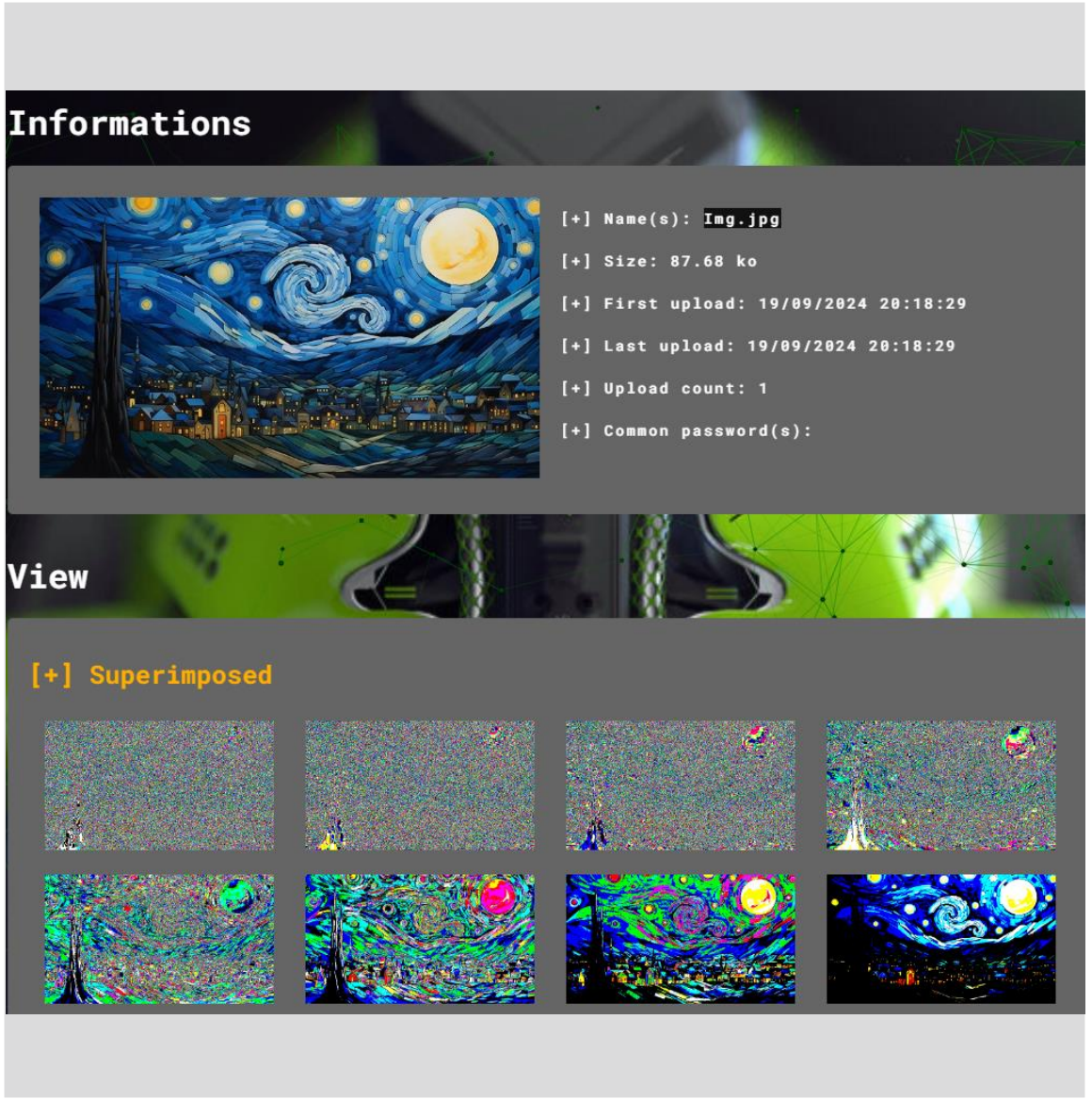
- Ocultar información en archivos de imagen

Aperisolve



Plataforma online que realiza análisis de capas en imágenes además de examinarlas en profundidad

https://www.aperisolve.com/



Universidad Rey Juan Carlos

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
```

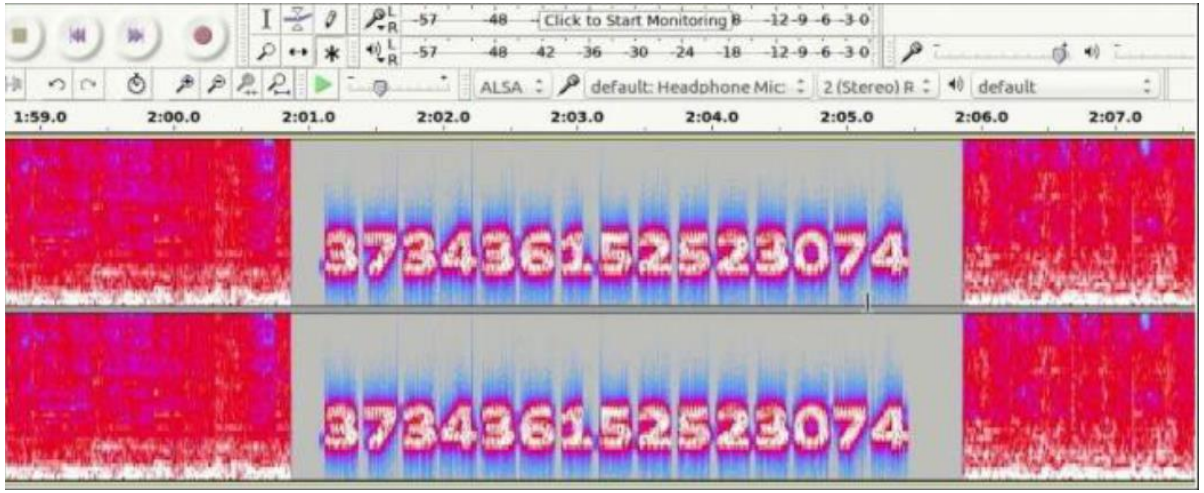
Nos permite ocultar archivos dentro de una imagen .jpg utilizando una contraseña

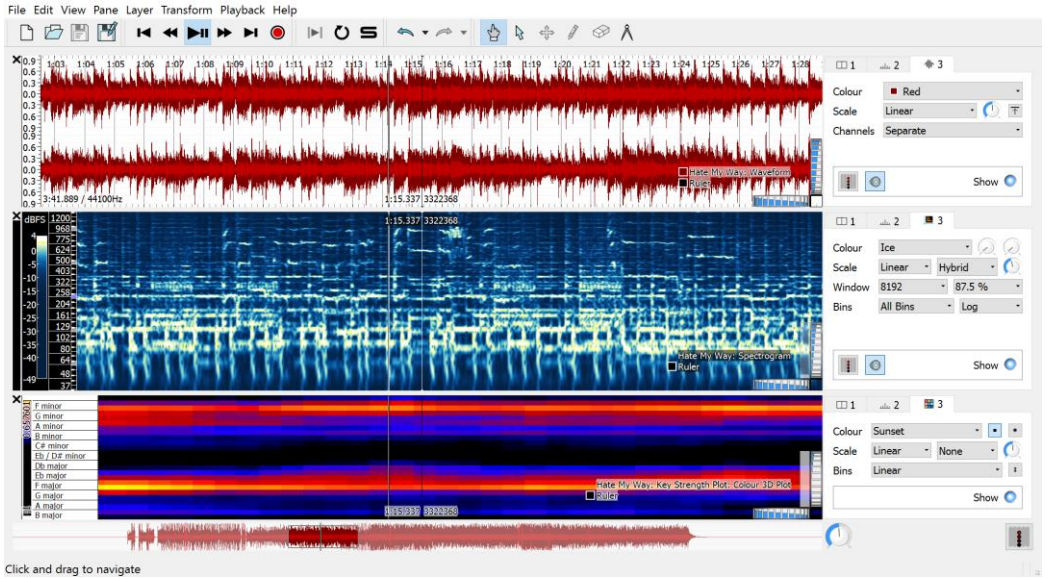
https://steghide.sourceforge.net/

Tipos

Audio

- Herramientas:
  Audacity
  Sonic Visualizer

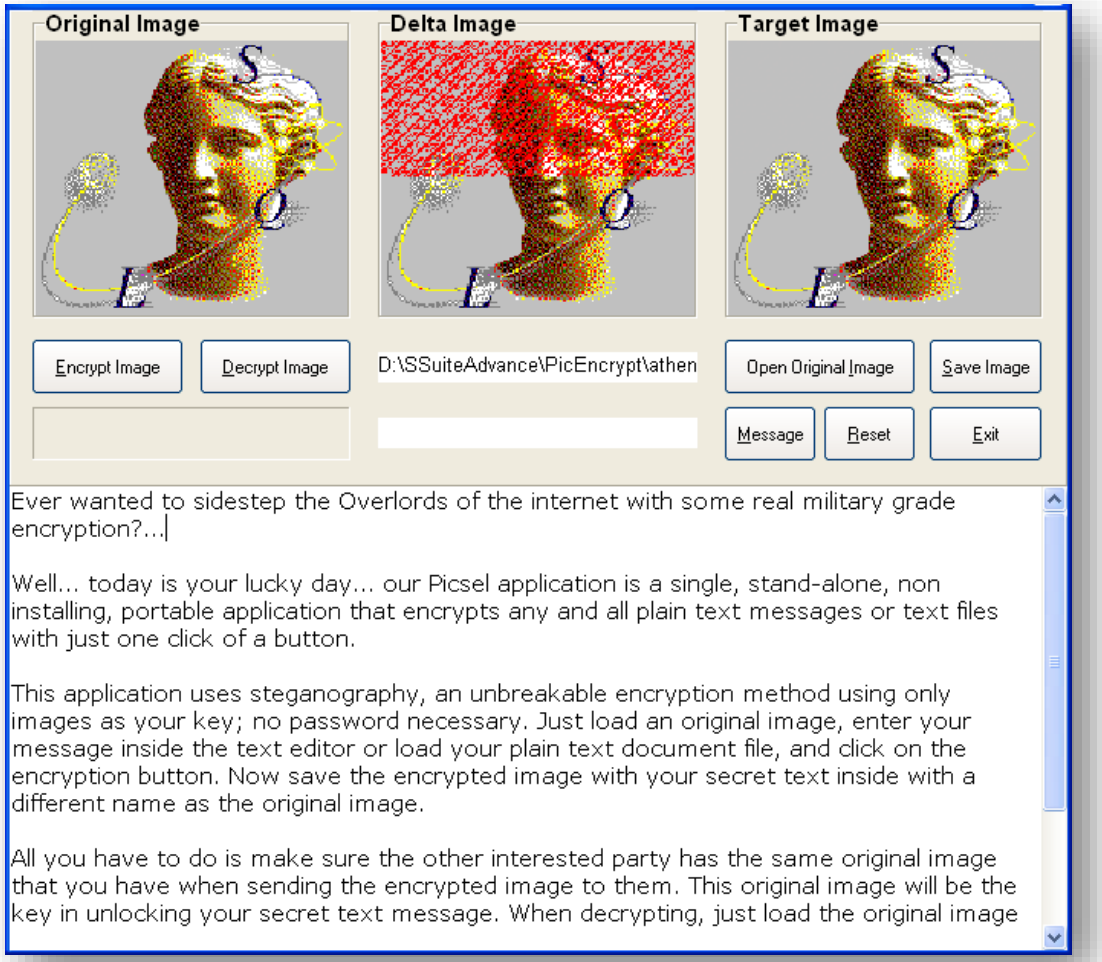




- Ocultar información en archivos de audio

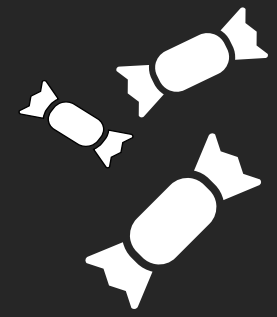
Herramientas esteganografía

- Foto Forensics: https://fotoforensics.com/
- Aperisolve: https://www.aperisolve.com/
- Exiftool (instalada en la OVA): https://exiftool.org/
- Steghide (instalada en la OVA): http://steghide.sourceforge.net/
- Stego-LSB: https://pypi.org/project/stego-lsb/
- Stegseek (instalada en la OVA): https://github.com/RickdeJager/stegseek
- Strings (instalada en la OVA): https://linux.die.net/man/1/strings
- Audacity: https://audacity.es/
- Sonic Visualizer: https://www.sonicvisualiser.org/
- Spectrum Analyzer: https://academo.org/demos/spectrum-analyzer/
- Binwalk (instalada en la OVA): https://github.com/ReFirmLabs/binwalk
- Hexdump (instalada en la OVA): https://man7.org/linux/man-pages/man1/hexdump.1.html



CTF 2

ESTEGANOGRAFÍA



Universidad
Rey Juan Carlos