



Módulo I: OSINT y esteganografía

Laura Sánchez Santiago
Carla Gómez Cabanillas



Universidad
Rey Juan Carlos

Índice

1. OSINT

- Introducción
- Definición y categorías
- OSINT Framework
- HUMINT
- IMINT
- GEOINT

2. Esteganografía

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



OSINT

Carla Gómez Cabanillas

Introducción OSINT

Publicaciones
en redes
sociales

Compras en
línea

Uso de foros
y blogs

Búsquedas en
internet

Comentarios
y reseñas



Introducción OSINT

Ubicación

Gustos

Publicaciones
en redes
sociales

Compras en
línea

Preferencias de consumo

Dirección de envío

Lugares que frecuentamos

Uso de foros
y blogs

Búsquedas en
internet

Hábitos diarios

Ideas, pensamientos, opiniones

Amistades

Comentarios
y reseñas

Datos financieros

Webs que más utilizamos

Definición OSINT



- **Open Source Intelligence**
- Recopilar y analizar información pública.
- Tirando del hilo...encontraremos la flag!

Categorías

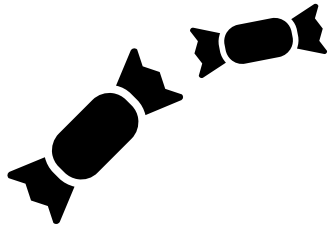
- HUMINT 
- IMINT 
- GEOINT 
- SIGINT 

OSINT Framework

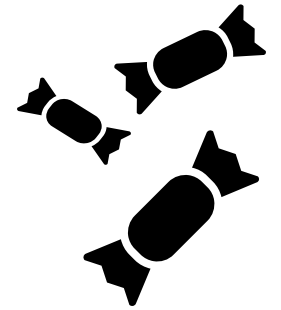
Link: [OSINT Framework](#)

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



Herramienta
OSINT

WAYBACK MACHINE

WayBack Machine

¿¿Cómo era tu web hace x años??



Ejemplo: [Conciertos WiZink Center](#)

INTERNET NUNCA OLVIDA



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

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

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



Habilidades HUMINT:

PERSEVERANCIA

OBJETIVIDAD

PACIENCIA

FLEXIBILIDAD

Cotilleo – boca a boca



Habilidades HUMINT:

PERSEVERANCIA

OBJETIVIDAD

PACIENCIA

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 (LinkedIn, TripAdvisor...)

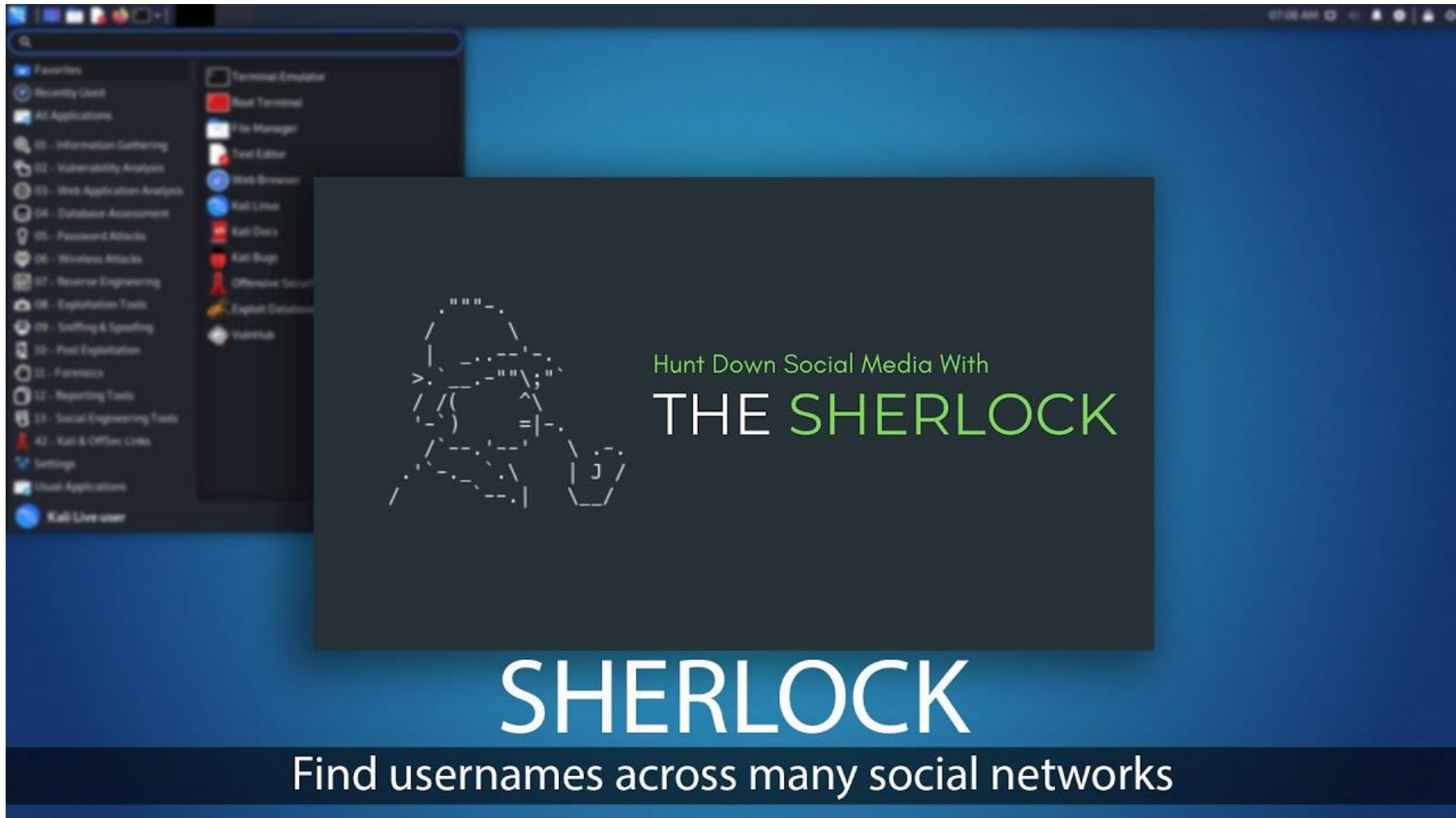
[Webmii](#)

Nick

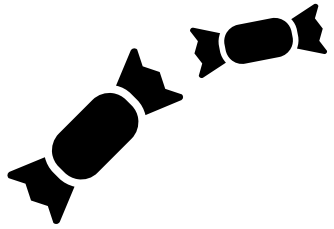
- Cuentas que se tienen con ese mismo nick

Veremos sherlock

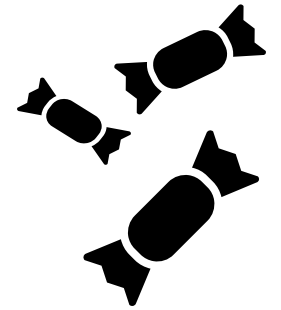
HUMINT (Human Intelligence)



Para instalar: `sudo apt install sherlock`



RETO 2



¿QUIÉNES GANARÁN EL SEGUNDO RETO?

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

Foto divulgada por CEO de Apple revela que se usa Windows para fabricar los Macbooks



Tim Cook (CEO Apple)



Centro de seguridad Mundial Brasil

Sara Carbonero
Mundial Brasil

WIFI REDACCIÓN

Nombre:
Curitiba_redaccion
Contraseña:
partidoapartido

WIFI CARPA

Nombre:
Curitiba_set
Contraseña:
iniestademivida



Centro de seguridad SuperBowl 2020

IMINT (Image Intelligence)

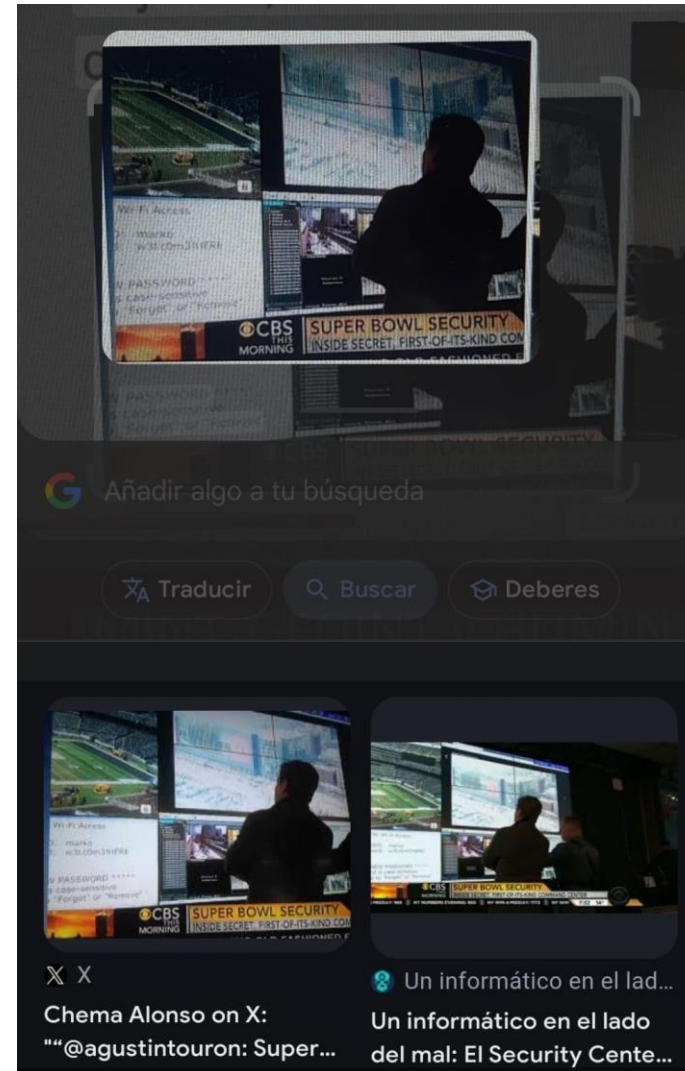
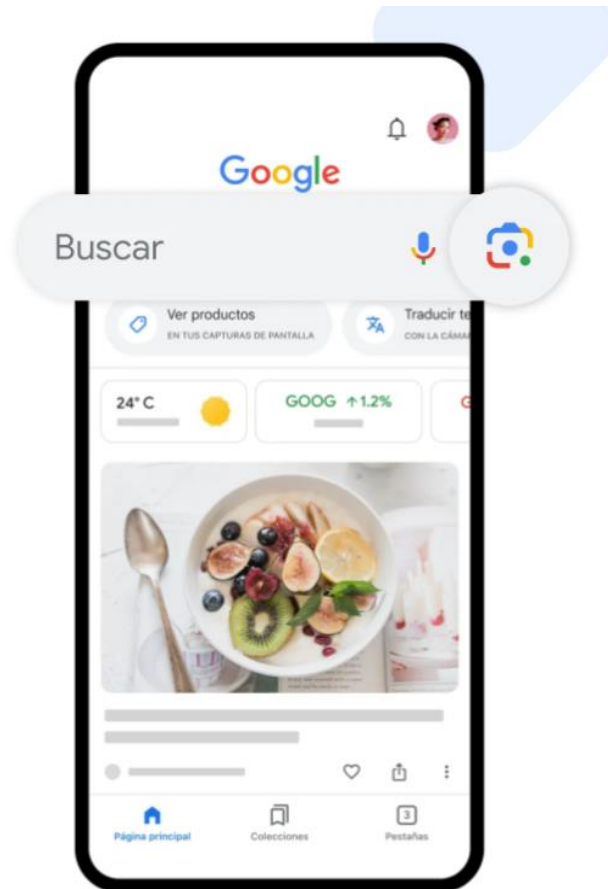
HERRAMIENTAS

1. Google Lens
2. Tin Eye
3. Yandex

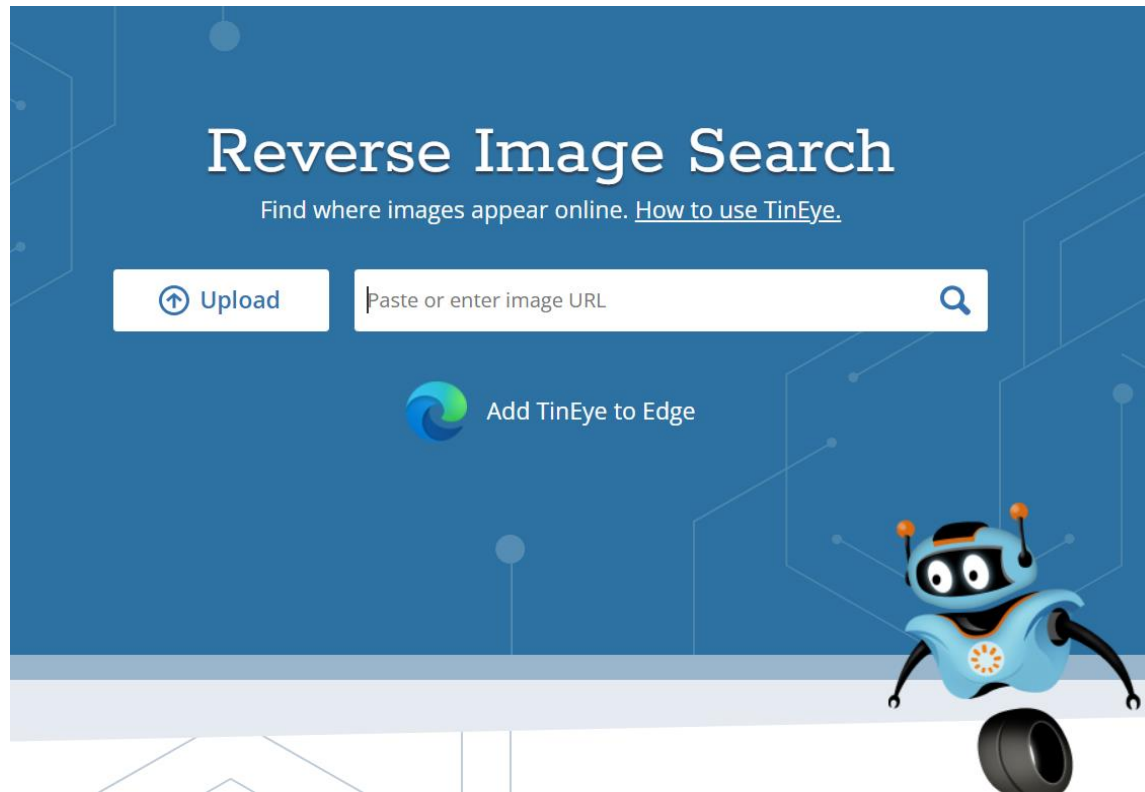


IMINT (Image Intelligence)

1. Google Lens



2. Tin Eye

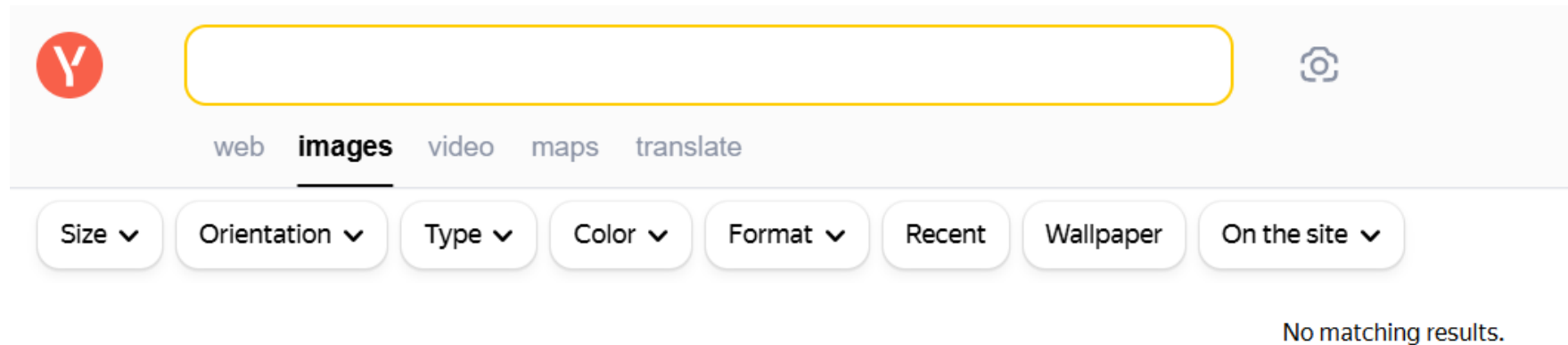


PARA ENCONTRAR:

- 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)

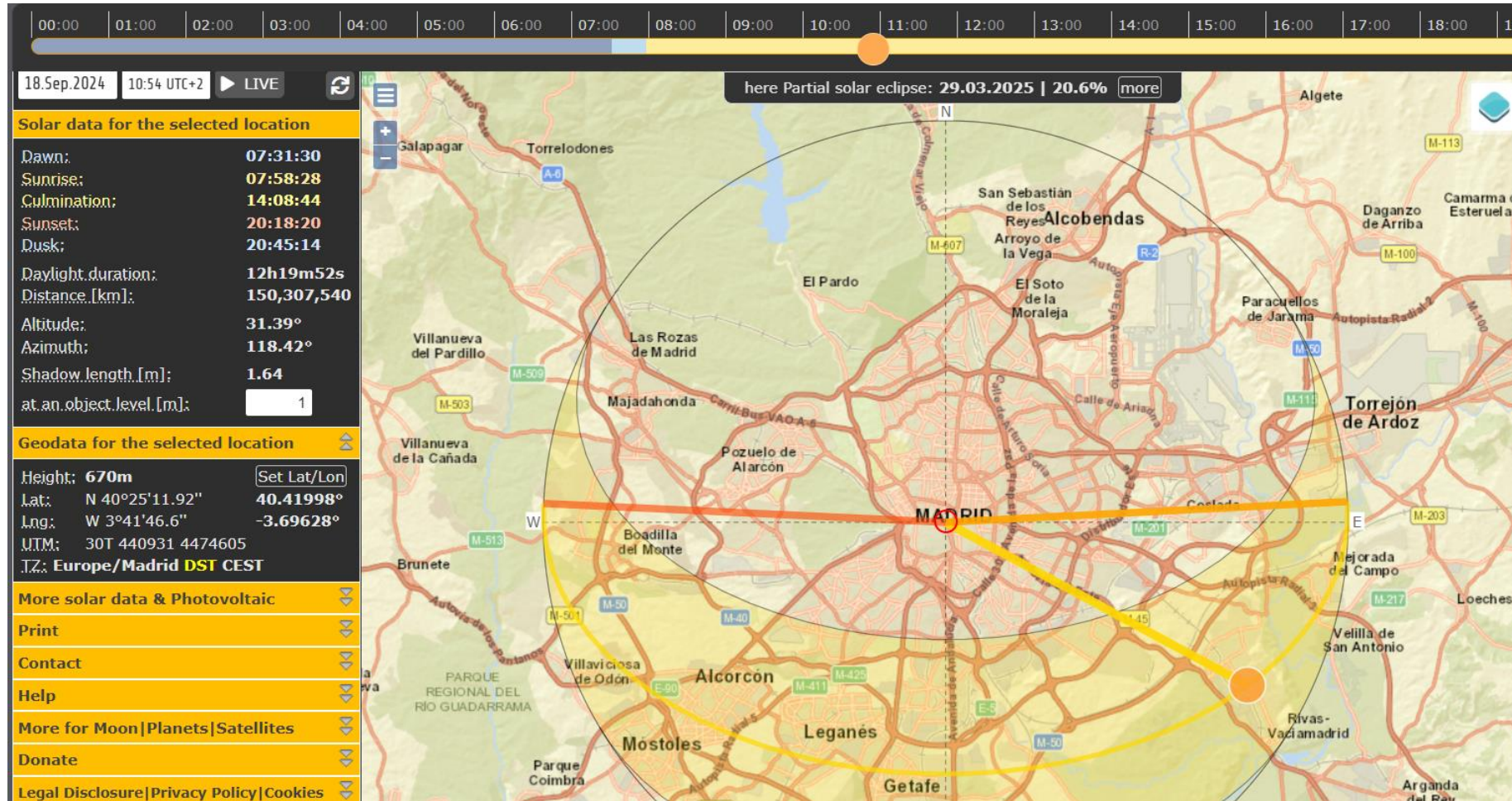
3. Yandex



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)



IMINT (Image Intelligence)



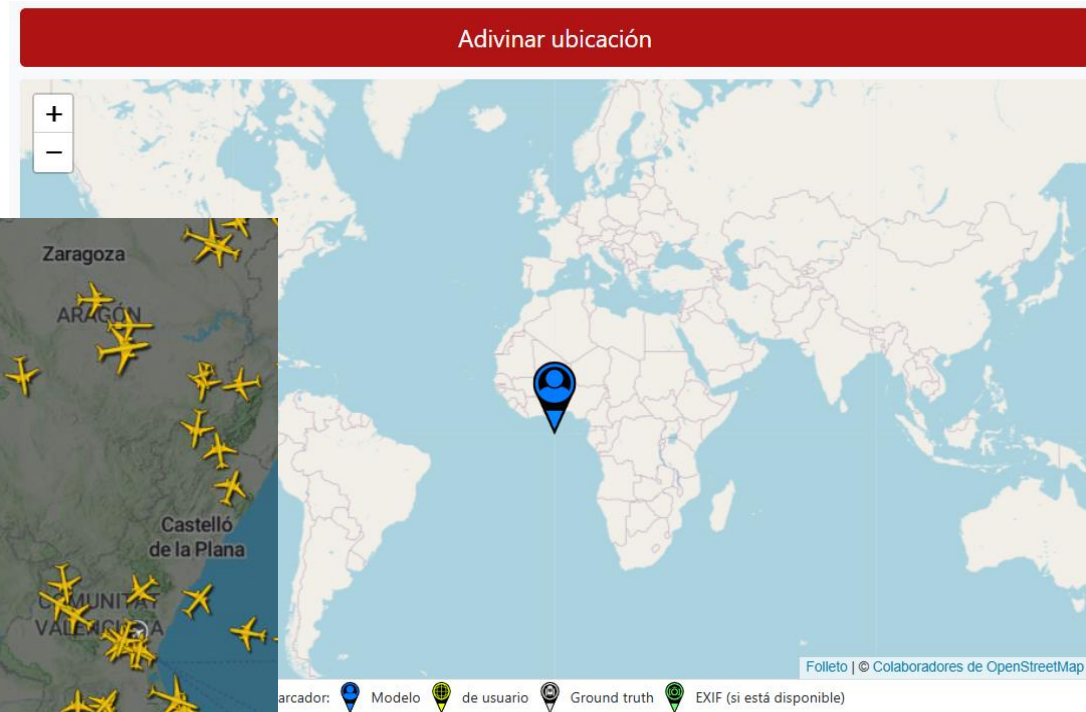
Envíe un archivo **imagen** para análisis forense

URL de la imagen:

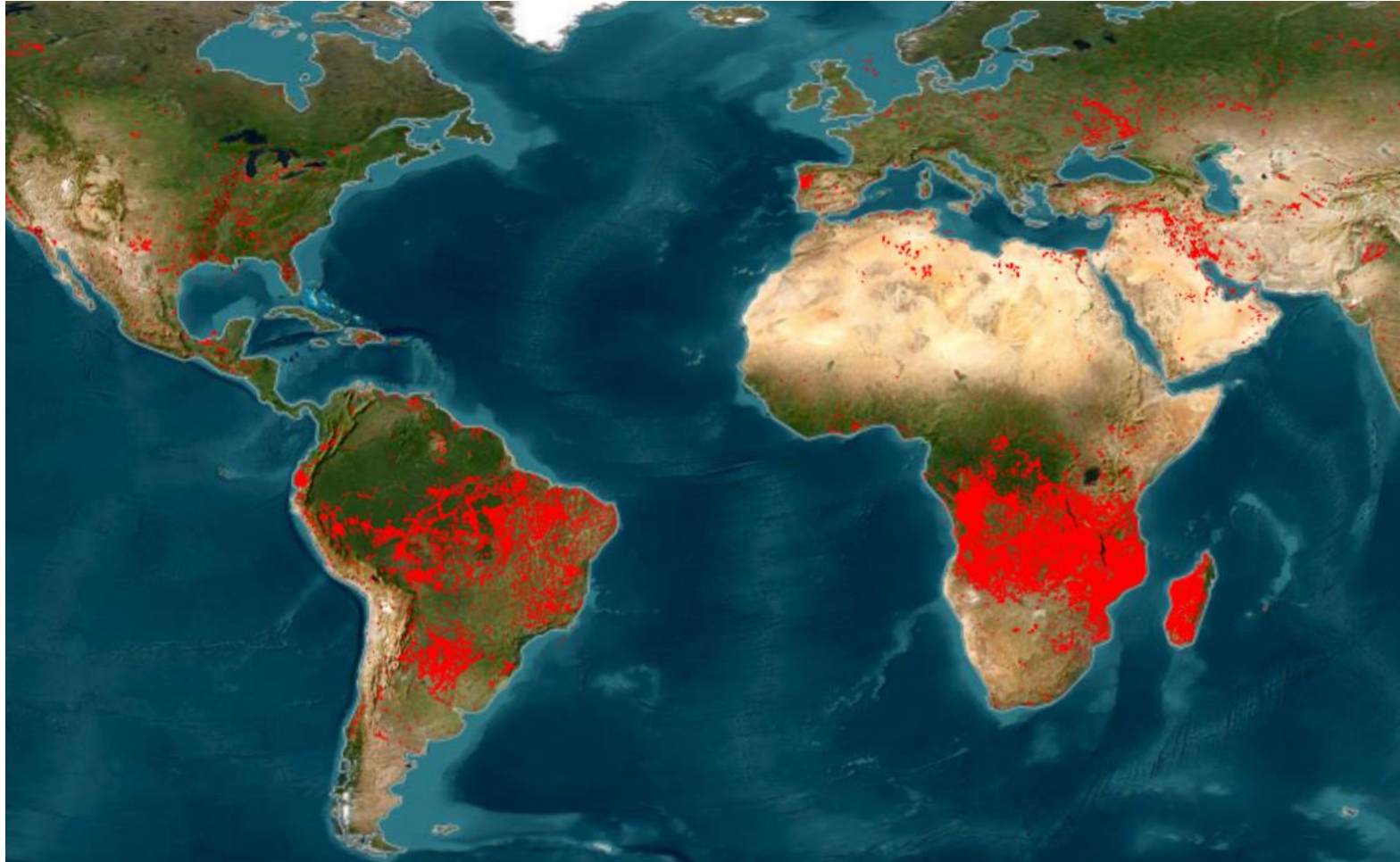
Subir archivo: No se ha seleccionado ningún archivo

GEOINT (Geospatial Intelligence)

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



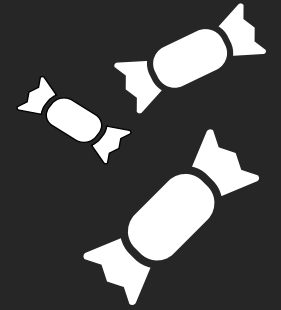
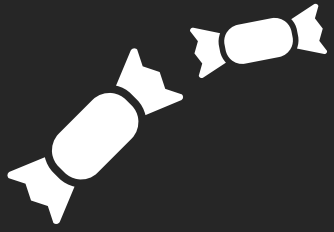
GEOINT (Geospatial Intelligence)



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](#)

OSINT

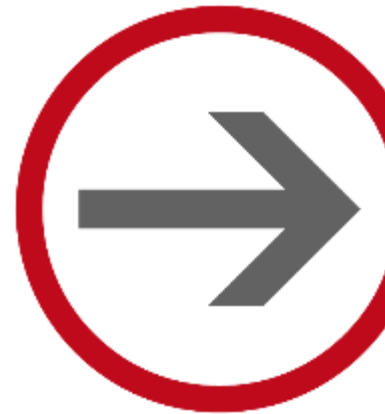


CTF 1

OSINT



Universidad
Rey Juan Carlos

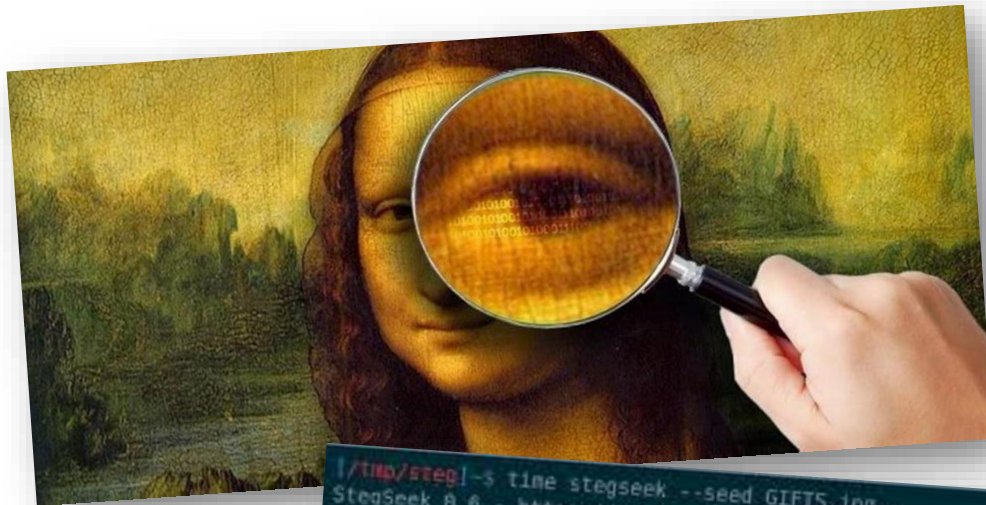


Esteganografía

Laura Sánchez Santiago

¿Qué es?

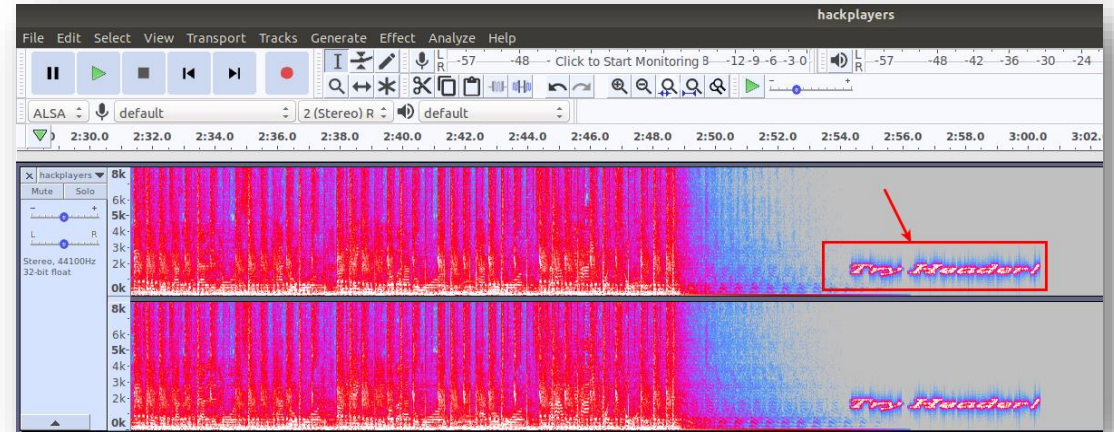
Ocultar información dentro de otro mensaje u objeto físico para evitar su detección



```

/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{100k$_1!k3_y0u_1!k3_b0sE64}

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



```

Terminal
(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
>>
  
```

Texto

- Ocultar información en archivos de texto

30

- 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
```

```
(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
```

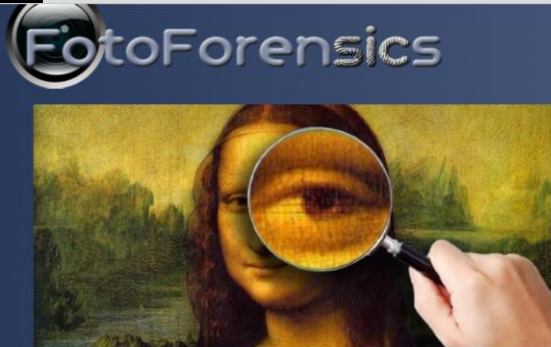
Realiza un ataque de diccionario para encontrar la contraseña de la herramienta steghide en imágenes .jpg

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


```
(Luv@kali)~$ steghide --help
steghide version 0.5.1

the first argument must be one of the following:
embed, --embed      embed data
extract, --extract  extract data
info, --info        display information about a cover- or stego-file
info <filename>    display information about <filename>
encinfo, --encinfo display a list of supported encryption algorithms
version, --version  display version information
license, --license  display steghide's license
help, --help        display this usage information

embedding options:
-ef, --embedfile <filename> select file to be embedded
-ef <filename> embed the file <filename>
-cf, --coverfile <filename> select cover-file
-cf <filename> embed into the file <filename>
-p, --passphrase <passphrase> specify passphrase
-p <passphrase> use <passphrase> to embed data
-sf, --stegofile <filename> select stego file
-sf <filename> write result to <filename> instead of cover-file
-e, --encryption <e> select encryption parameters
-e <a>[<m>][<n>][<c>] specify an encryption algorithm and/or mode
-e none do not encrypt data before embedding
-z, --compress <level> compress data before embedding (default)
-z <level> using level <level> (1 best speed... 9 best compress)
-Z, --dontcompress do not compress data before embedding
-k, --nochecksum do not embed crc32 checksum of embedded data
-N, --dontembedname do not embed the name of the embedded file
-f, --force
```



Property	Value
Filename	1-dMZnyTaL4-F9UfH1HbUH5g.jpeg
Filetime	2021-01-09 03:34:14 GMT
File Type	image/jpeg
Dimensions	1280x600
Color Channels	3
Unique Colors	162157
File Size	113,037 bytes
MD5	a08a223e992e4764ee59823d6eb5aaed
SHA1	601e12e7a8094b05e11ef0eb1cada18cbaa7cfc4
SHA256	e51863d0e6e7d03913cc4caa58587cf7db2c7563fd877816048e0385cc3458b5
First Analyzed	2024-09-14 12:07:32 GMT



Imagen

- Herramientas:
Fotoforensics (online)
Aperisolve (online)
Steghide
- Ocultar información en archivos de imagen

Steghide

```
steghide: could not extract any data with that passphrase!
```

DOWNLOAD FILES

Outguess

```
Reading
/app/uploads/7e14c40cbe8135442ad7369e3def9931/image.jpg...
Extracting usable bits: 93306 bits
Steg retrieve: seed: 46720, len: 4673
```

DOWNLOAD FILES

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

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

Informations



[+] Name(s): `Img.jpg`

[+] Size: 87.68 ko

[+] First upload: 19/09/2024 20:18:29

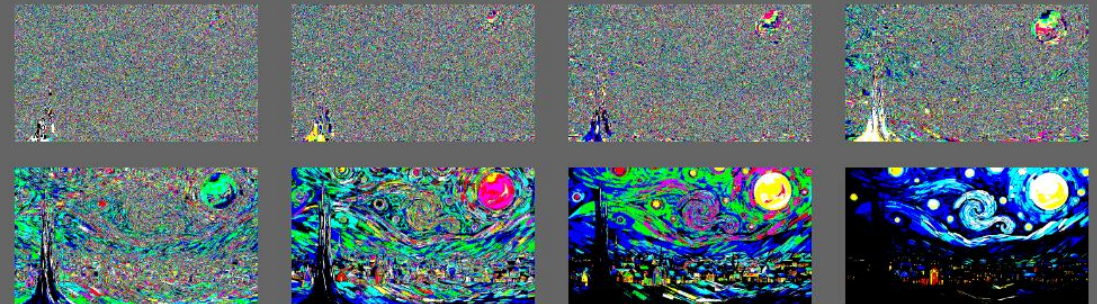
[+] Last upload: 19/09/2024 20:18:29

[+] Upload count: 1

[+] Common password(s):

View

[+] Superimposed



Steghide

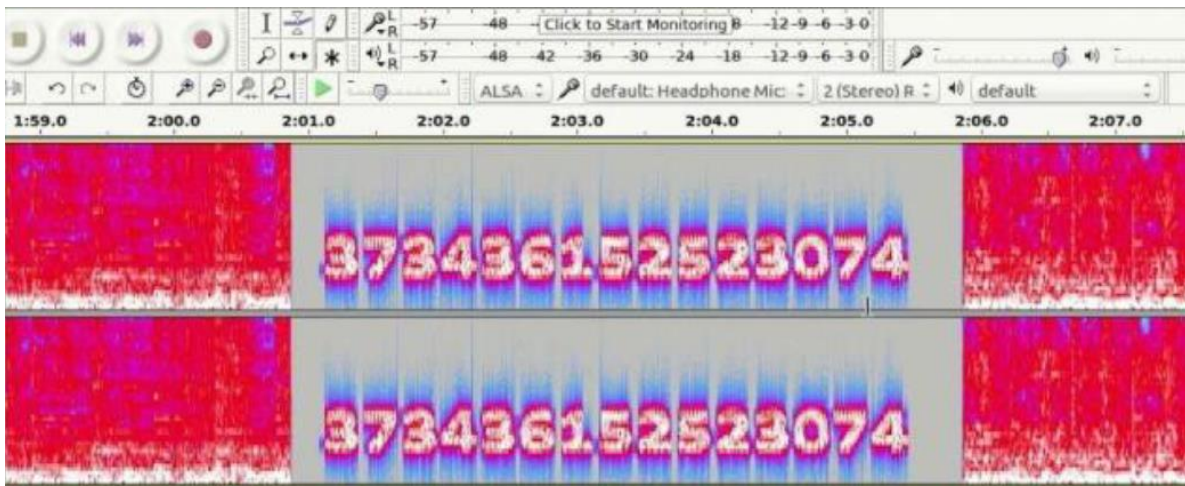
```
(kali㉿kali) - [~/Downloads/reto]
└─$ ls
texto.txt  th-2669789895.jpeg

(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
```

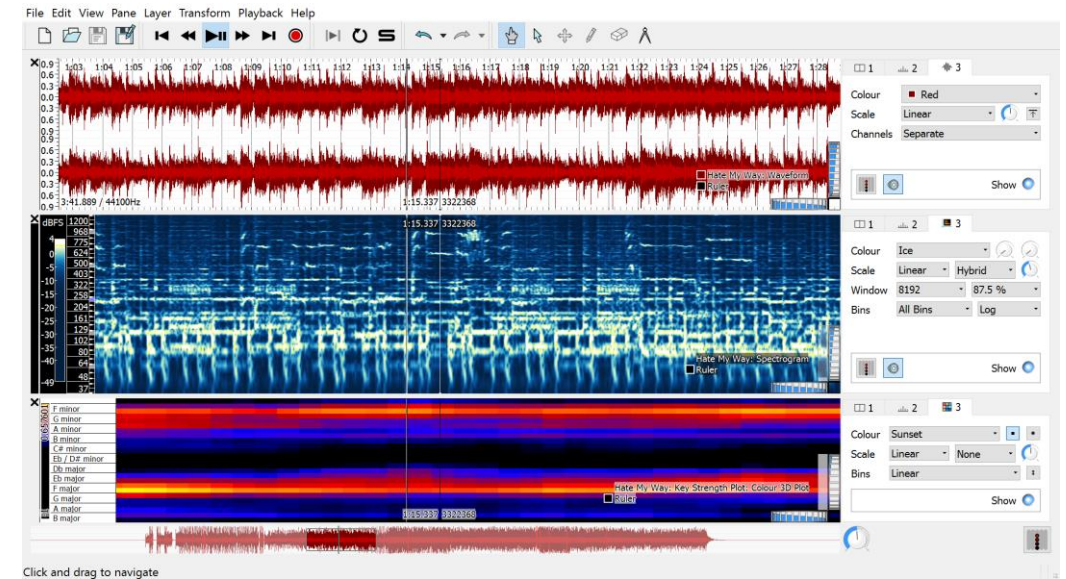
Nos permite ocultar archivos dentro de una imagen .jpg utilizando una contraseña

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

- Herramientas:
Audacity
Sonic Visualizer



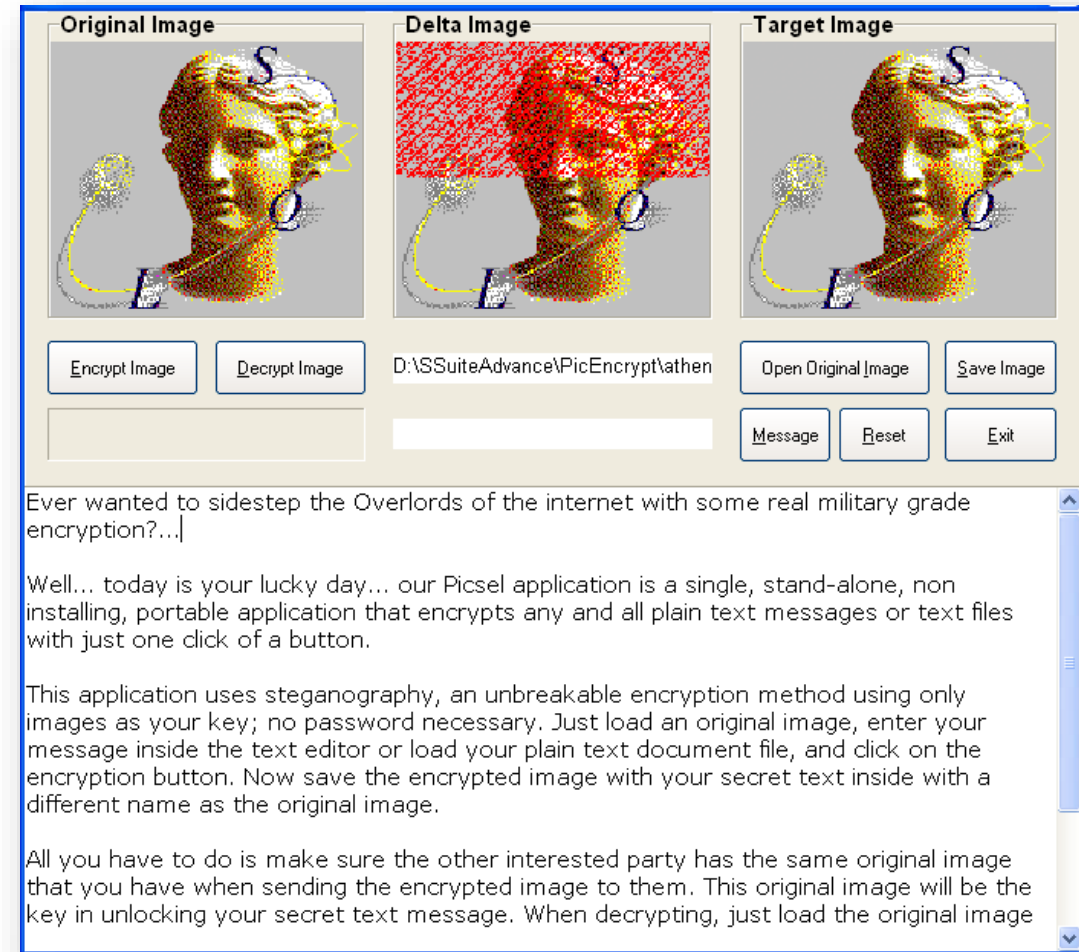
Audio



- 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