



# Curso OSINT

*Este será un curso sobre OSINT*

La **primera sección** hablará sobre tipos de buscadores web para obtención de información valiosa.

En **primer punto** se **habla de buscadores locales** de cada región como: Yandex (Rusia), Baidu (China), Google (Global), DuckDuckGo (Muy seguro respecto a política de datos)

**También** se hablará en la búsqueda inversa de imágenes ( Sobre todo usadas para la búsqueda de fake news). Yandex o Google contarán con estas tecnologías

En la **tercera sección** se hablará de buscadores tecnológicos: Shodan (Enfocado búsqueda con banners de tecnologías) ej. (apache city: Sevilla), Otros son: Zoomeye o MrLooquer.

**Finalmente buscadores de Deep Web:** Aclaración (La Deep Web: Será toda aquella información no accesible con el indexado de un buscador, por ejemplo los archivos de un aula virtual, en cambio la Dark Web ya tratará de información dañina y sensible ).  
Buscadores: Ahmia.fi, Torch, Not Evil, Grams, Candle

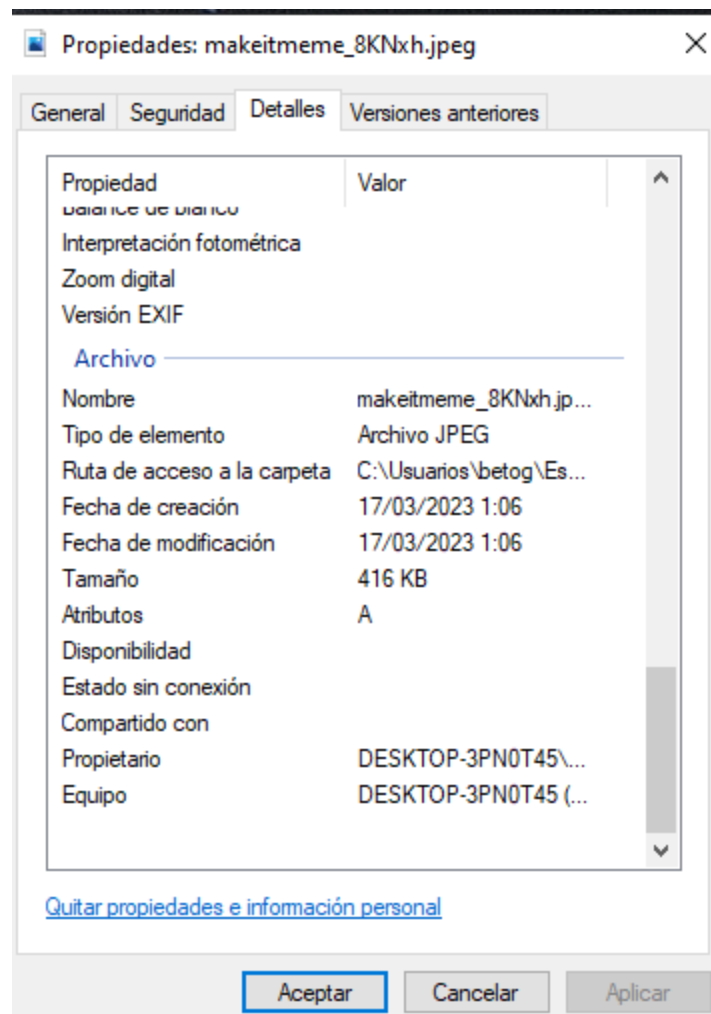
---

## Metadatos

---

Son aquellos datos que están escondidos o difícilmente accesibles

Algunos ejemplos son: conversaciones grabadas o imágenes.



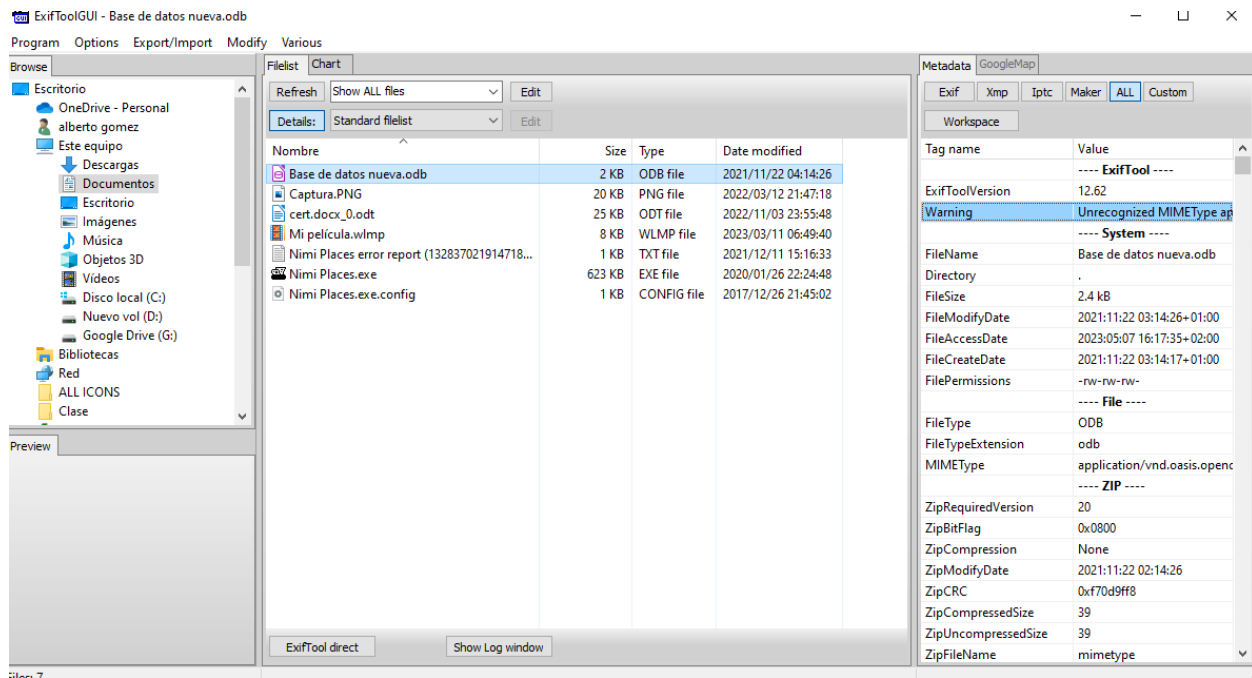
Esos son los metadatos de una imagen en Windows

## Aplicaciones para editar los metadatos

### ExifTool:

Descargaremos ExifTool.exe y su archivo GUI

Desde esta app podremos ver los datos de cualquier archivo y editarlos:



## Foca:

Estará más orientada a dominios:

Descargaremos Foca y Microsoft Sql Server para su uso:

Una vez iniciado le daremos a crear nuevo proyecto y pondremos el url del sitio web que queramos escanear

A continuación veremos un panel en el que podremos seleccionar que buscador usaremos para el análisis y los tipos de archivos que queremos, en mi caso:

Project Name - FOCA Open Source 3.4.7.1

Project Plugins Options TaskList About

Project Name Network Domains Document Analysis

**Search engines**

- ☒ Google
- ☒ Bing
- ☒ DuckDuckGo

**Extensions**

| All                                     | None                                     |
|---|--|
| <input checked="" type="checkbox"/> doc | <input checked="" type="checkbox"/> docx |
| <input checked="" type="checkbox"/> ppt | <input checked="" type="checkbox"/> pptx |
| <input checked="" type="checkbox"/> pps | <input checked="" type="checkbox"/> ppsx |
| <input checked="" type="checkbox"/> xls | <input checked="" type="checkbox"/> xlsx |
| <input checked="" type="checkbox"/> swx | <input checked="" type="checkbox"/> odt  |
| <input checked="" type="checkbox"/> odp | <input checked="" type="checkbox"/> pdf  |
| <input checked="" type="checkbox"/> ods | <input checked="" type="checkbox"/> wpd  |
| <input checked="" type="checkbox"/> odg | <input checked="" type="checkbox"/> rtf  |

Custom search Search All

| Id | Type | URL  | Download | Download Date | Size | Metadata |
|----|------|--|----------|---------------|------|----------|
| 0  | xlsx | https://www.pccomponentes.com/marketplace/wp-cont... | ✗        | -             | -    | ✗        |
| 1  | xlsx | https://www.pccomponentes.com/marketplace/wp-cont... | ✗        | -             | -    | ✗        |
| 2  | pdf  | http://www.pccomponentes.com/videos/SAT/PC_COM...    | ✗        | -             | -    | ✗        |

| Time     | Source         | Severity | Message  |
|----------|----------------|----------|--|
| 16:42:38 | MetadataSearch | medium   | BingWeb search finished successfully!! Total found result count: 0                     |
| 16:42:44 | MetadataSearch | medium   | GoogleWeb search finished successfully!! Total found result count: 0                   |
| 16:43:04 | MetadataSearch | error    | An error has occurred on DuckDuckGoWeb: Error en el servidor remoto: (403) Prohibido.. |
| 16:43:05 | MetadataSearch | medium   | BingWeb search finished successfully!! Total found result count: 0                     |
| 16:43:20 | MetadataSearch | medium   | GoogleWeb search finished successfully!! Total found result count: 3                   |

Settings Deactivate AutoScroll Clear Save log to File

All searchers have finished

umbrete\_8\_-12.pdf  
Valencina.pdf  
VICEPRESIDENTE-2.pdf  
vicepresidente.pdf  
votoporcorreo.pdf  
\_Consejeros2017\_2.pdf  
\_Juridica2017.pdf  
\_Pe%C3%B1as2017.pdf  
\_Vicepresidente2017\_2.pdf  
xlsx (2)  
Creacion\_producto.xlsx  
Plantilla-descuentos.xlsx

Metadata Summary

- Users (37)
- Folders (39)**
- Printers (0)
- Software (62)
- Emails (8)
- Operating Systems (0)
- Passwords (0)
- Servers (0)
- Malware Summary (DIARIO)

| Attribute | Value   |
|-----------|---|
| Path      | https://twitter.com/RealBetisFundacion/status/                        |
| Path      | https://loscordonesdorados.com/                                       |
| Path      | w:\   |
| Path      | http://www.pdf-tools.com/   |
| Path      | https://twitter.com/EscuelaBetis/status/                              |
| Path      | https://twitter.com/RBetisFundacion/status/1274643221524762628/photo/ |
| Path      | https://youtu.be/   |
| Path      | O:\   |
| Path      | https://accionistas.realbetisbalompie.es/                             |
| Path      | https://realbetisbalompie.es/   |
| Path      | http://solidaridadverdiblanca.org/                                    |
| Path      | https://solidaridadverdiblanca.org/                                   |
| Path      | https://twitter.com/RealBetisBasket/status/                           |
| Path      | P:\   |
| Path      | http://www.realbetisbalompie.es/                                      |
| Path      | http://www.escuelafbetis.org/   |
| Path      | http://www.waingunga.com/   |
| Path      | https://www.soziabie.es/  |

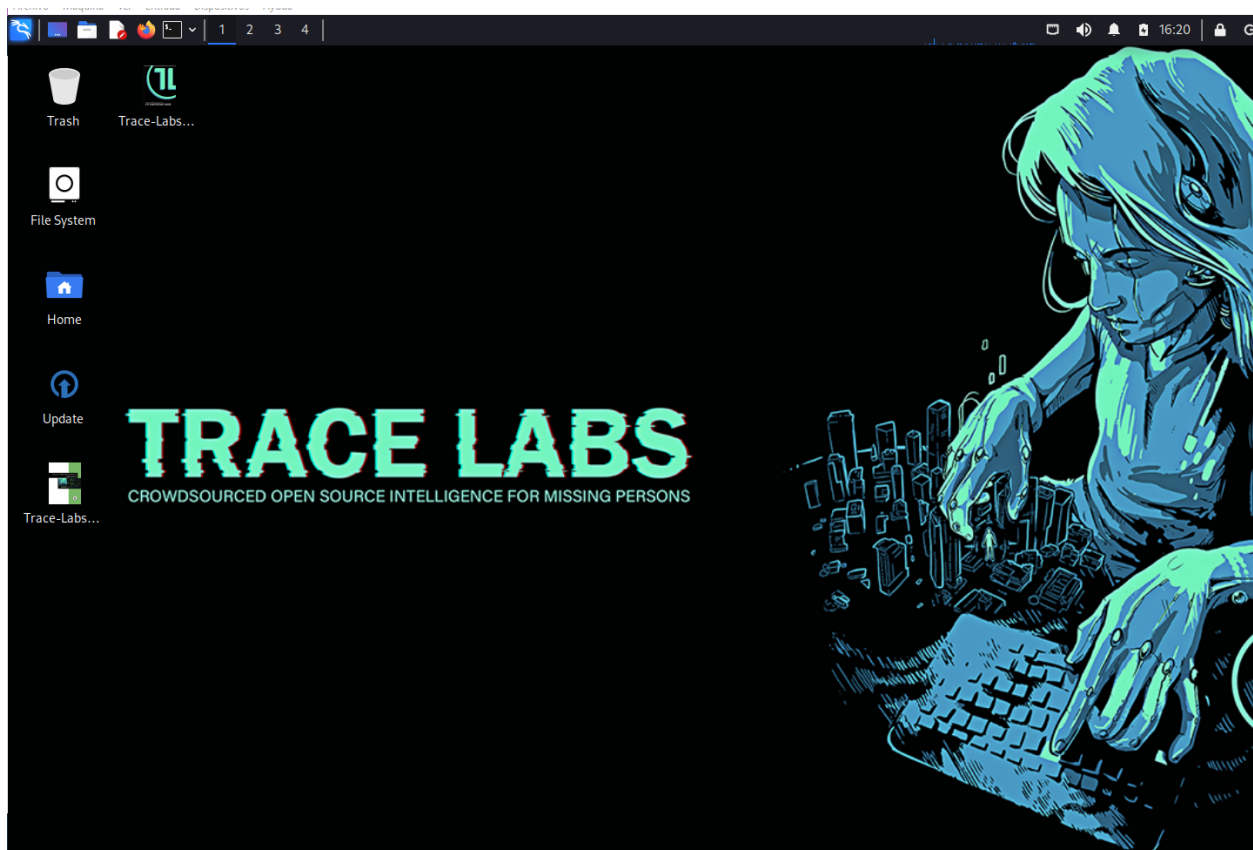
# Herramientas OSINT

# OSR-Framwork

Serán usadas desde VirtualBox

En este caso instalaremos TL OSINT VM SO

Este tendrá como user y contraseña default user: osint,  
password: osint



Lanzaremos los siguientes comandos para instalar las dependencias:

```
Actualización:  
$ sudo apt-get update  
$ sudo apt-get upgrade  
Instalación de notepadqq:  
$ sudo add-apt-repository ppa:notepadqq-team/notepadqq  
$ sudo apt-get update  
$ sudo apt-get install notepadqq  
Actualización pip:  
$ sudo pip install --upgrade pip
```

```
Instalación de OpenOffice Calc:  
$ sudo apt-get install libreoffice-calc
```

También descargaremos osrframework desde su repositorio y lo meteremos en la carpeta de la máquina virtual

## Ver cuentas de un usuario en webs

```
sudo usufy.py -p all -n "ejemplo"
```

```
+-----+-----+
-+      | https://www.virustotal.com/en/user/ejemplo | ejemplo | Virustotal
-+      | |
+-----+-----+
-+      | https://ejemplo.soup.io | ejemplo | Soup
-+      | |
+-----+-----+
-+      | https://www.wattpad.com/user/ejemplo | ejemplo | wattpad
-+      | |
+-----+-----+
-+      | http://ca.wikipedia.org/wiki/Usuari:ejemplo | ejemplo | Wikipedia_ca
-+      | |
+-----+-----+
-+      | http://community.wikia.com/wiki/User:ejemplo | ejemplo | Wikia
-+      | |
+-----+-----+
-+      | http://www.v7n.com/forums/members/ejemplo.html | ejemplo | V7n
-+      | |
+-----+-----+
-+      | http://ar.wikipedia.org/wiki/user:ejemplo | ejemplo | Wikipedia_ar
-+      | |
+-----+-----+
-+      | http://es.wikipedia.org/wiki/Usuario:ejemplo | ejemplo | Wikipedia_es
-+      | |
+-----+-----+
```

## Ver si móvil es spam

```
sudo phonefy.py -n 981980683
```

```

2023-05-11 15:14:54.551463      Results obtained:

/usr/lib/python3/dist-packages/pyexcel/deprecated.py:208: UserWarning: Deprecated usage since v0.2.1! Explicit import is no longer required. pyexcel.ext.text is auto imported.
  warnings.warn(
Objects recovered (2023-5-11_15h14m).:
+-----+-----+
| com.i3visio.URI | com.i3visio.Platform |
+-----+-----+
| http://www.infotelefonica.es/981980683 | Infotelefonica |
+-----+-----+
| http://www.listaspam.com/busca.php?Telefono=981980683 | Listaspam |
+-----+-----+

```

## Ver si dominio está ocupado

```
sudo domainfy.py -n openwebinars
```

```

/usr/lib/python3/dist-packages/pyexcel/deprecated.py:208: UserWarning: Deprecated usage since v0.2.1! Explicit import is no longer required. pyexcel.ext.text is auto imported.
  warnings.warn(
Objects recovered (2023-5-11_15h17m).:
+-----+-----+
| com.i3visio.Domain | com.i3visio.IPv4 |
+-----+-----+
| openwebinars.net | 198.199.125.132 |
+-----+-----+
| openwebinars.com | 34.197.121.219 |
+-----+-----+

```

- Todos los logs se guardarán en profiles.csv

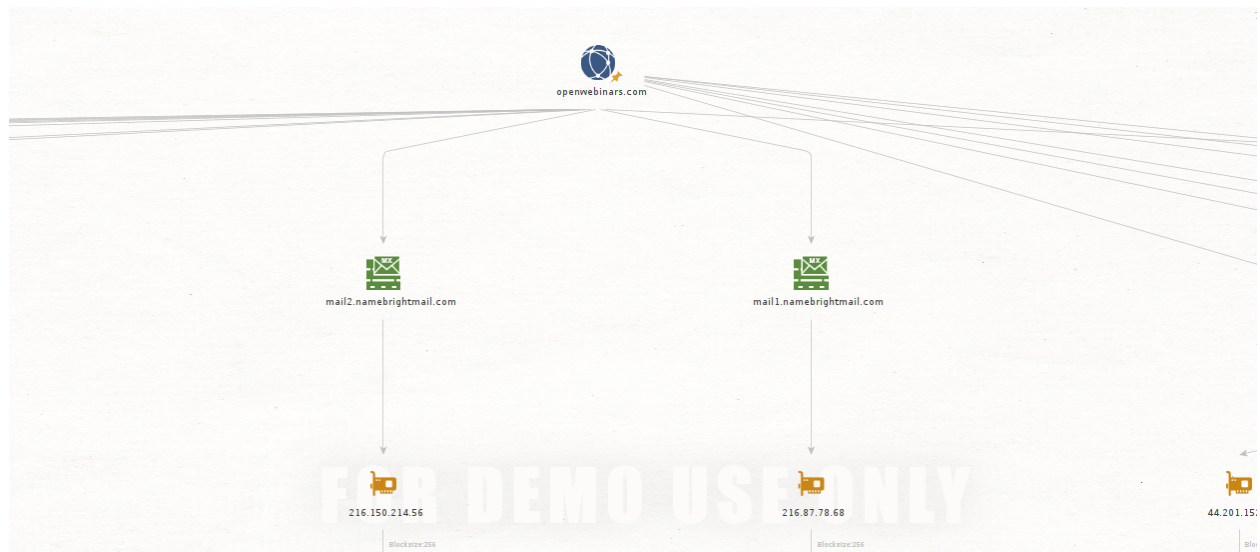
## Maltego

Descarga Maltego Deb

Lo extraes en una carpeta y son el comando sudo

ejecutaremos maltego que estará en usr/bin

Usando click derecho en el Dominio que creemos podremos ejecutar todas las consultas que queramos.



Tiene numerosas funciones, solo tendrás que instalar las distintas aplicaciones.

## Repositorios OSINT

- [inteltechniques.com](https://inteltechniques.com)



# INTELTECHNIQUES

By Michael Bazzell

Training

Services

Res

## Tools

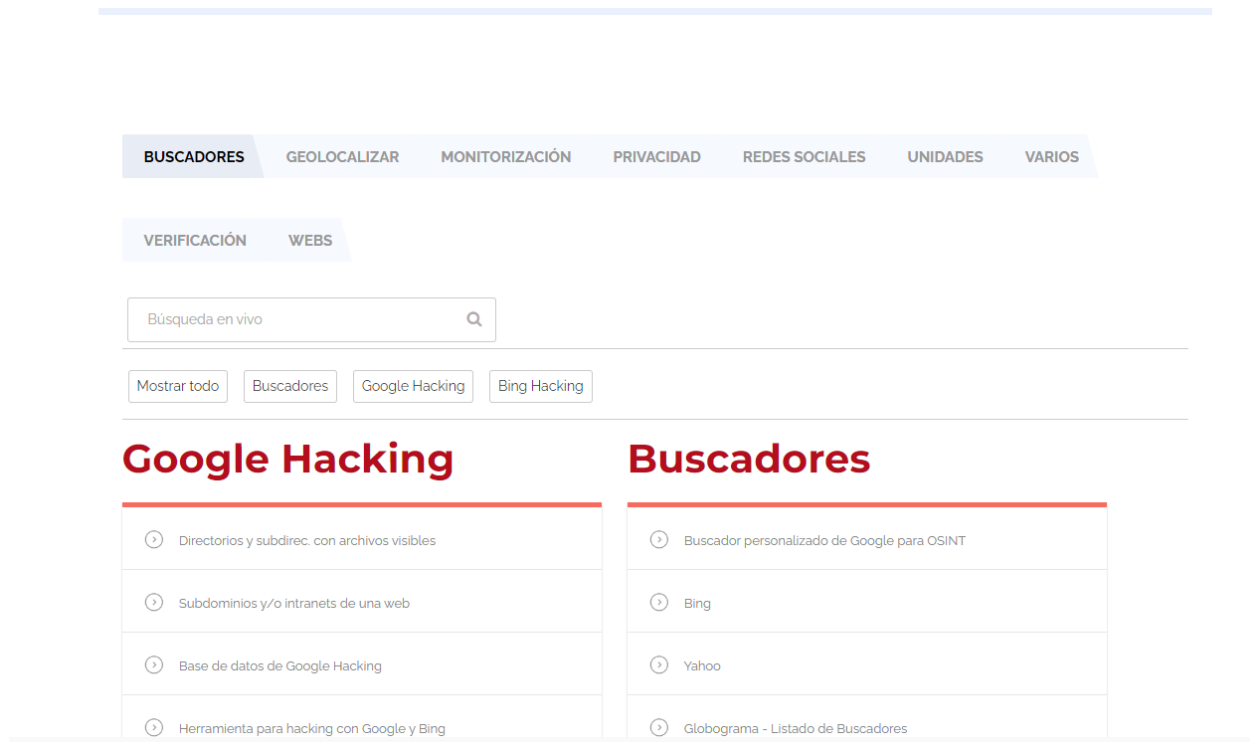
- 🔍 [Search Engines](#)
- 🔍 [Facebook](#)
- 🔍 [Twitter](#)
- 🔍 [Instagram](#)
- 🔍 [LinkedIn](#)
- 🔍 [Communities](#)
- 🔍 [Email Addresses](#)
- 🔍 [Usernames](#)
- 🔍 [Names](#)
- 🔍 [Addresses](#)
- 🔍 [Telephone Numbers](#)
- 🔍 [Maps](#)
- 🔍 [Documents](#)
- 🔍 [Pastes](#)
- 🔍 [Images](#)
- 🔍 [Videos](#)
- 🔍 [Domains](#)
- 🔍 [IP Addresses](#)
- 🔍 [Business & Government](#)
- 🔍 [Vehicles](#)
- 🔍 [Virtual Currencies](#)
- 🔍 [Breaches & Leaks](#)
- 🔍 [Live Audio Streams](#)
- 🔍 [Live Video Streams](#)
- 🔍 [APIs](#)

## Intel

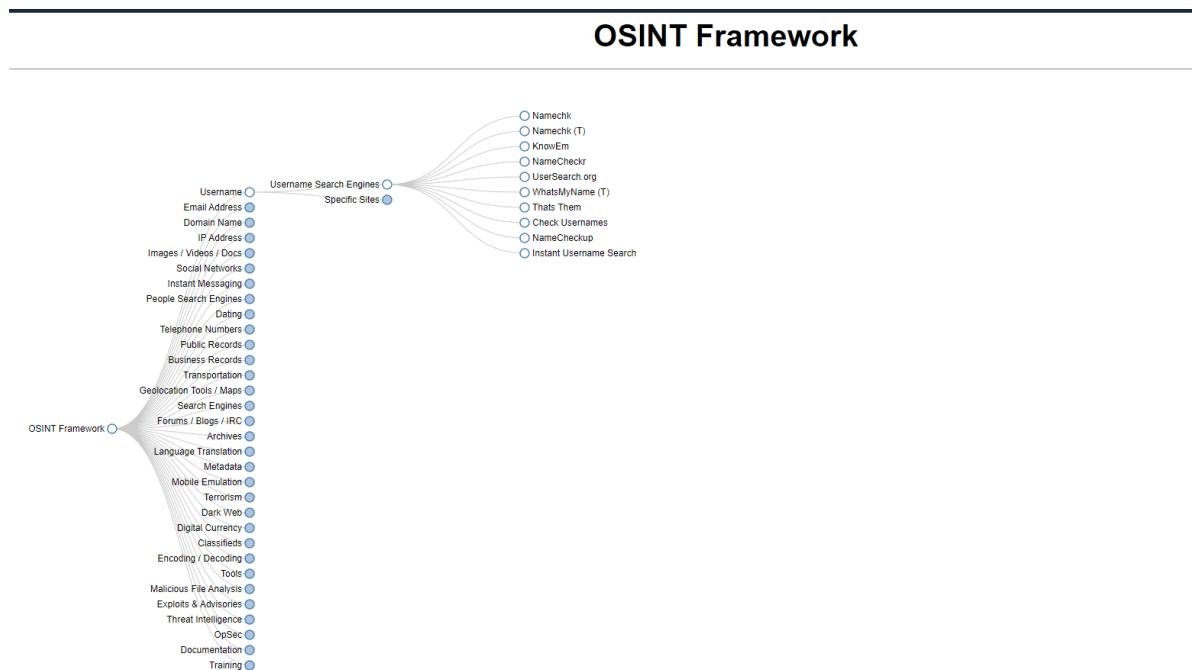
Updat

These  
[online](#)  
book.

- <https://ciberpatrulla.com/links/>



- [osintframework.com](https://osintframework.com)





## Herramientas rastreo IP y WHOIS

<https://whois.domaintools.com/>

[Home](#) > [Whois Lookup](#) > [OpenWebinars.com](#)

### Whois Record for OpenWebinars.com

#### — Domain Profile

|                    |   |
|--------------------|---|
| Registrant         | Redacted for GDPR privacy   |
| Registrant Country | ES  |
| Registrar          | Domainwards.com LLC<br>IANA ID: 1540<br>URL: <a href="http://www.NameBright.com">http://www.NameBright.com</a><br>Whois Server: <a href="http://whois.NameBright.com">whois.NameBright.com</a><br><a href="mailto:abuse@namebright.com">abuse@namebright.com</a><br>(p) +1.7204960020   |
| Registrar Status   | clientTransferProhibited  |
| Dates              | 3,110 days old<br>Created on 2014-11-04<br>Expires on 2023-11-04<br>Updated on 2020-09-16   |
| Name Servers       | NS1.NAMEBRIGHTDNS.COM (has 4,706,154 domains)<br>NS2.NAMEBRIGHTDNS.COM (has 4,706,154 domains)  |
| Tech Contact       | Redacted for GDPR privacy<br>Redacted for GDPR privacy,<br>Redacted for GDPR privacy, Redacted for GDPR privacy, Redacted for GDPR privacy,<br>Redacted for GDPR privacy<br><a href="mailto:openwebinars.com@namebrightprivacy.com">openwebinars.com@namebrightprivacy.com</a><br>(p) Redacted for GDPR privacy (f) Redacted for GDPR privacy |
| IP Address         | 34.197.121.219 - 261,457 other sites hosted on this server  |
| IP Location        |  - Virginia - Ashburn - Amazon Technologies Inc.   |
| ASN                |  AS14618 AMAZON-AES, US (registered Nov 04, 2005)  |
| Domain Status      | Registered And No Website   |
| IP History         | 102 changes on 102 unique IP addresses over 17 years  |
| Registrar History  | 3 registrars with 3 drops   |
| Hosting History    | 10 changes on 7 unique name servers over 17 years   |

<https://mxtoolbox.com/>

SuperTool Beta7

openwebinars.com MX Lookup

mx:openwebinars.com Find Problems Solve Email Delivery Problems

**EMAILS BOUNCING?** MxToolbox has your email delivery solutions

| Pref | Hostname                 | IP Address   | TTL     |                           |
|------|--------------------------|--|---------|---------------------------|
| 10   | mail1.namebrightmail.com | 216.87.78.68<br>Flacental Colorado Corp. (AS13849)   | 180 min | Blacklist Check SMTP Test |
| 10   | mail2.namebrightmail.com | 216.150.214.56<br>Flacental Colorado Corp. (AS13849) | 180 min | Blacklist Check SMTP Test |

|   | Test                     | Result                                 |
|---|--------------------------|--|
| ✓ | DMARC Record Published   | DMARC Record found                     |
| ✓ | DMARC Policy Not Enabled | DMARC Quarantine/Reject policy enabled |
| ✓ | DNS Record Published     | DNS Record found                       |

dns lookup dns check dmARC lookup spf lookup dns propagation

Reported by ns2.namebrightdns.com on 5/11/2023 at 2:46:21 PM (UTC -5), just for you

Transcript

# Monitoreo de OSINT

En este caso usaremos:

tweetdeck.twitter.com

Alberto @Alberto82218066

Twitter

Agregar columna

Paneles de columnas

Personal

**Agregar columna**

Buscar en Twitter

Q #osint

Buscar \*#osint\*

CiberInteligencia Cibervigilancia OSI... @gIntelSeg

OSINT Latam Group @OSINTLatamGroup

BrigadaOsint @BrigadaOsint

Maria Gilda Carballo @SraOSINT

OSINTomático @OSINTomatic

Manuel E. Persia @osintvznla

Agregar columna

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

 **@openwebinars** OpenWebinars

8,453 tweets 1,698 following 7,509 followers 310 listed


Joined Twitter on August 26, 2013 as user #1,701,186,788

Somos la plataforma líder de #eLearning IT en español. Ofrecemos el mayor catálogo de cursos de #programación y #sistemas para #empresas y profesionales 🚀




[openwebinars.net](https://openwebinars.net) España

4.42 followers/following ⓘ 41 listed/1,000 followers ⓘ




[Open in Twitter](#)

 **Pinned Tweet**

@openwebinars has not pinned a tweet to their Twitter profile


 **Following** [Download & Print](#)  

lifespan) for pets 🐾 and people.

 **Andrea Clavijo**   **@AndreaClavijoR\_**


588 tweets 367 following 179 followers 1 listed 9:28 PM - 1 Dec 2009 Madrid

Software Developer at @DatamaranAI. En nuevas aventuras... 🌟 Vue, Python, React...

 **Marta Prieto** **@marta\_prieto\_**



423 tweets 646 following 458 followers 5 listed 10:00 PM - 25 Nov 2012

Front-End Web Developer || dogs lover 🐶 || No fear just Change 🌈 || #womenintech #frontend #adalaber #tech

 **maria\_shecodes** **@MShecodes**


71 tweets 210 following 73 followers 2 listed 9:10 PM - 1 Jan 2019 Spain

React Native Developer at @z1digitalstudio

 **Pepe Robles**  **@NavisCode**

11,040 tweets 692 following 53,232 followers 1,151 listed 8:12 PM - 11 Jun 2020


Formación → <https://l.co/WWm0qbund1> MD Abiertos

 **Alena Nikolaeva** **@alenanik11**




6,466 tweets 622 following 6,984 followers 75 listed 2:12 PM - 6 Jan 2019 All views

expressed are my own

a11y Engineer • Product Designer 💎 Copilot @GitHub • designed at @xata build things at @Typeform @trivago @hazostudio Raised in es IAAP member

 **Carlos Azaustre** **@carlosazaustre**

43,331 tweets 859 following 68,735 followers 1,328 listed 1:34 PM - 7 May 2007 Madrid, Spain

 **Followers** [Download & Print](#)  

## ▼ Servicio de alertas

<https://www.google.com/alerts>

Cada vez que aparezca el dato que ponemos nos mandará un aviso al gmail

# Alertas

Supervisa la Web para encontrar nuevos contenidos interesantes

🔍 España

×

Frecuencia

Cuando se produzca

Fuentes

Automático

Idioma

español

Región

Todas las regiones

Cantidad

Solo los mejores resultados

Enviar a

betogomezabrente@gmail.com

Crear alerta

Ocultar opciones ▲


## Vista previa de alerta

NOTICIAS

La sequía avanza con fuerza en **España** y drena una reserva de agua - CNN en Español

CNN en Español

**España** está siendo afectada por una gran sequía, producto de las altas temperaturas y la escasez pluvial. Esto se empieza a hacer muy notorio en ...



## Anonimato Digital

- Usar cuentas y teléfonos solor usados para esa ocasión
- Tener documento excel con todos los datos obtenidos
- Crear identidad ficticia: FakeNameGenerator
- Email: ProtonMail



### Modesto Sarabia Badillo

C/ Amoladera, 61  
28770 Colmenar Viejo

Curious what **Modesto** means? [Click here to find out!](#)

**Geo coordinates** 40.642367, -3.713543

#### PHONE

**Phone** 768 565 487

**Country code** 34

#### BIRTHDAY

**Birthday** November 27, 1957

**Age** 65 years old

**Tropical zodiac** Sagittarius

#### ONLINE

**Email Address** ModestoSarabiaBadillo@jourrapide.com

*This is a real email address. [Click here to activate it!](#)*

**Username** Actomithat1957

**Password** thei4Ielie

**Website** BayRates.es

**Browser user agent** Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_4)  
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1  
Safari/605.1.15

#### FINANCE

**Visa** 4556 0507 4325 7086

**Expires** 10/2026

**CVV2** 645

Logged in users can view full social security numbers and can save their fake names to use later.



## Enmascarar identidad

- Usar máquina virtual
- Tener en un usb un SO Light (Tails) y que use Tor
- Usar una VPN
- Usar eGarante para respaldo judicial
- KeePass guardar todas las contraseñas y guardarlas