

Martin

Dalla Pozza

Presentacion trabajo practico

Recopilacion informacion

- 1.....Uso de Security Trails
- 2.....Otras herramientas
- 3.....Uso de Google Dorks
- 4.....Obtención de metadatos (FOCA)
- 5.....Uso de Shodan

1 Creacion cuenta y uso SecurityTrails

Desbloquee el Manual de Inteligencia: Su guía para la inteligencia de amenazas ciberneticas. [Consíguelo gratis →](#)

SecurityTrails
A Recorded Future Company

API de seguridad Precios Recursos ▾ Acceso [Regístrate gratis](#)

¡Sumerjase en nuestros datos!
Ofrecemos API y servicios de datos robustos para equipos de seguridad en todo el mundo.

RESPONSE 200 OK

```
1- {
  "endpoint": "/v1/history/securitytrails.com/dns/a",
  "pages": 1,
  "records": [
    {
      "first_seen": "2021-11-04",
      "last_seen": "2023-01-05",
      "organizations": [
        "Cloudflare, Inc."
      ],
      "type": "a",
      "values": [
        {
          "ip": "172.66.41.38"
        }
      ]
    }
  ]
}
```

API de SecurityTrails™
A toda velocidad, sin parar
Permite que sus aplicaciones utilicen nuestros datos actuales e históricos increíblemente rápido.
[OBTENGA SU CLAVE API >](#)

Obtenga el punto de vista de un atacante: descubra su huella digital [Solicitar acceso](#)

Regístrate - Gratis
Comience hoy mismo a monitorear sus DNS, IP y nombres de dominio para detectar amenazas y riesgos!

Nombre

Correo electrónico

Compañía

Contraseña

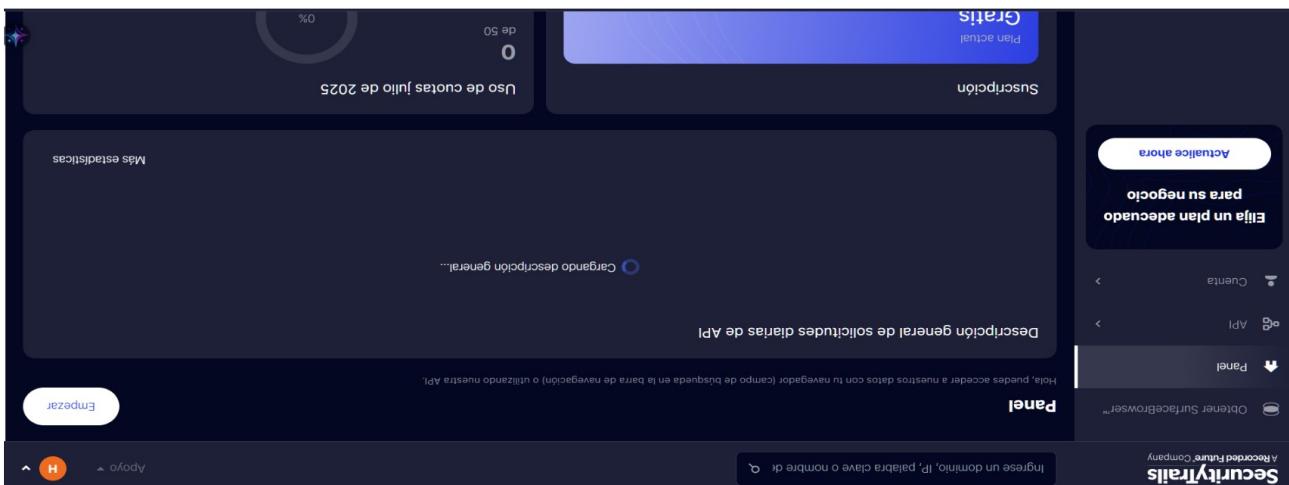
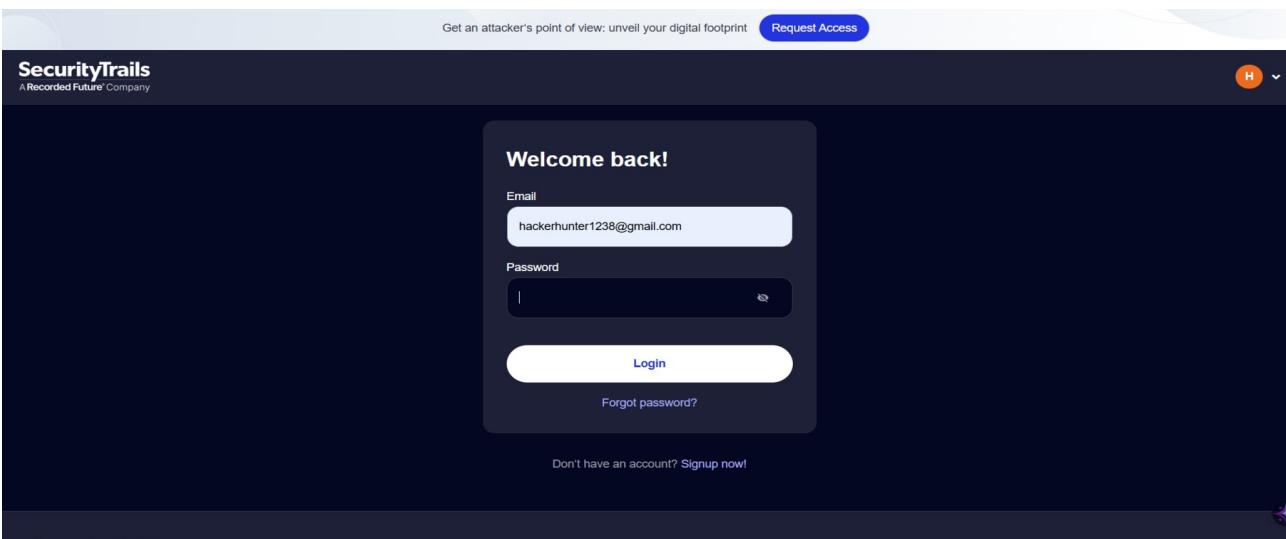
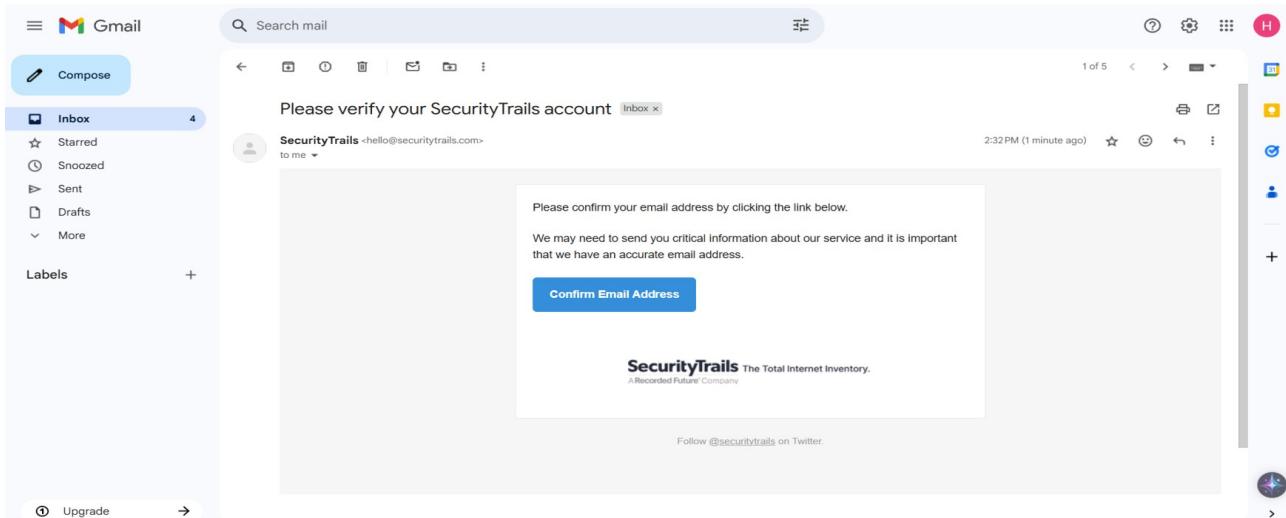
Razones para unirse gratis:

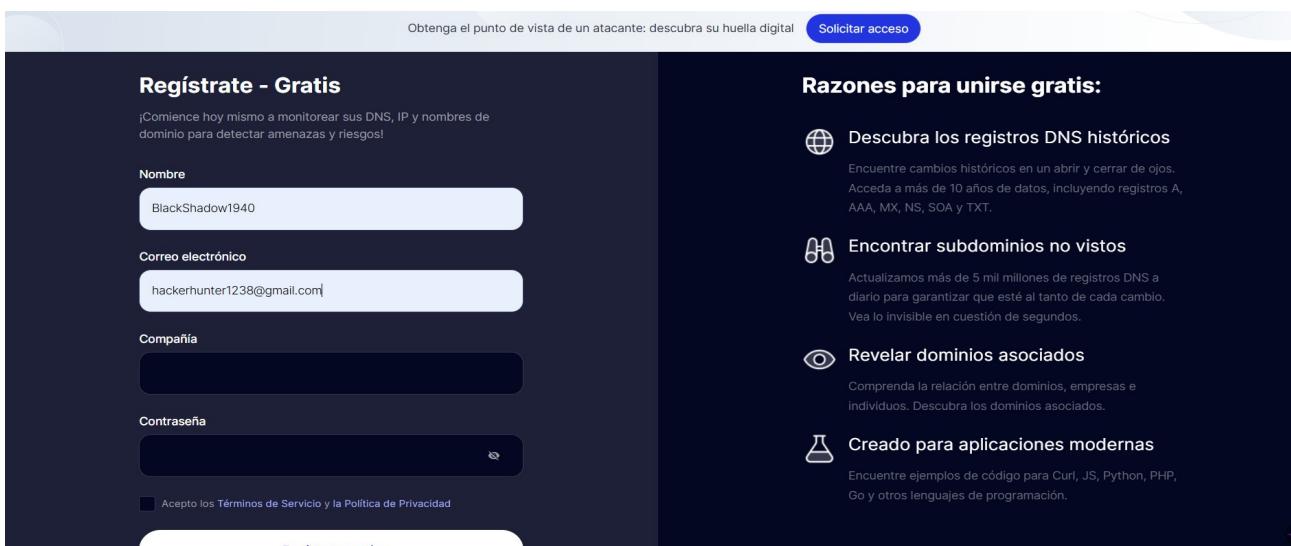
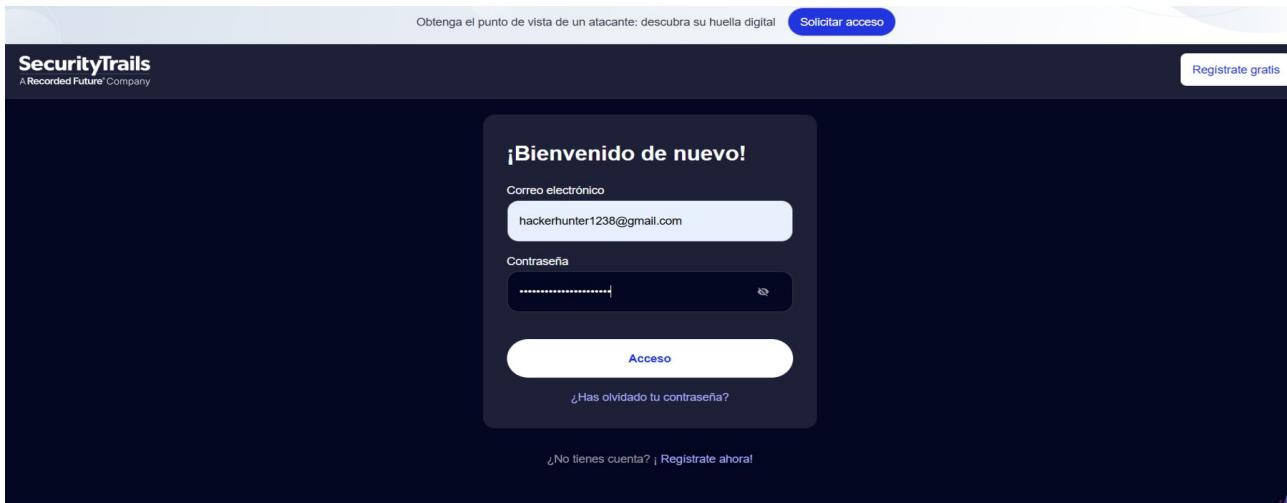
🌐 Descubra los registros DNS históricos
Encuentre cambios históricos en un abrir y cerrar de ojos. Acceda a más de 10 años de datos, incluyendo registros A, AAA, MX, NS, SOA y TXT.

🔍 Encontrar subdominios no vistos
Actualizamos más de 5 mil millones de registros DNS a diario para garantizar que esté al tanto de cada cambio. Vea lo invisible en cuestión de segundos.

🕒 Revelar dominios asociados
Comprenda la relación entre dominios, empresas e individuos. Descubra los dominios asociados.

🧪 Creado para aplicaciones modernas
Encuentre ejemplos de código para Curl, JS, Python, PHP.





En esta parte, muestra cada paso de como hace la creacion de la cuenta.

SecurityTrails ofrece:

Recopilacion y analisis de datos:

Almacena y analiza enormes cantidades de datos actuales e históricos de internet, incluyendo registros DNS (pasivos y activos), datos WHOIS, información de certificados SSL, subdominios, tecnologías de sitios web, puertos abiertos, bloques de IP, etc.

Inteligencia de amenazas:

Permite a los equipos de seguridad, investigadores y "cazadores de amenazas" (threat hunters) detectar posibles amenazas, investigar actividades maliciosas y realizar análisis de seguridad.

Gestion de la superficie de ataque:

Ayuda a las organizaciones a comprender y reducir su "superficie de ataque", es decir, todos los puntos de entrada potenciales que un atacante podría explotar. Esto incluye identificar activos digitales olvidados o expuestos.

Protección de marca:

Facilita el monitoreo y la detección de actividades de infracción de derechos de autor y marcas registradas, como dominios fraudulentos.

Investigacion forense:

Proporciona datos cruciales para investigaciones forenses ciberneticas y para rastrear el historial de dominios e Ips.

API:

Ofrece una API robusta para que los usuarios puedan integrar los datos de SecurityTrails en sus propias aplicaciones y flujos de trabajo de seguridad.

SecurityTrails
A Recorded Future Company

google.com

Registros DNS de google.com al 26 de julio de 2025

| Un registro | | Registros AAAA |
|-------------|----------------|------------------------|
| Google LLC | 142.250.31.100 | 2607:f8b0:4004:c0b::65 |
| | 142.250.31.101 | 2607:f8b0:4004:c0b::66 |
| | 142.250.31.102 | 2607:f8b0:4004:c0b::8a |
| | 142.250.31.113 | 2607:f8b0:4004:c0b::8b |
| | 142.250.31.138 | |
| | 142.250.31.139 | |

Registros MX

Registros NS

SecurityTrails
A Recorded Future Company

google.com

subdominios de google.com

| Dominio | Rango | Proveedor de alojamiento | Proveedor de correo |
|---------------------|-------|--------------------------|---------------------|
| mapas.google.com | 12 | Google LLC | - |
| sopporte.google.com | 14 | Google LLC | - |
| play.google.com | 17 | Google LLC | - |
| plus.google.com | 18 | Google LLC | - |
| docs.google.com | 21 | Google LLC | - |
| drive.google.com | 22 | Google LLC | - |

SecurityTrails
A Recorded Future Company

google.com

Direcciones IP

| Direcciones IP | Organización | Visto por primera vez | Última vez visto | Duración vista |
|--|--------------|------------------------|-----------------------|----------------|
| 172.253.115.100 172.253.115.101 172.253.115.102 172.253.115.113 172.253.115.138 172.253.115.139 | Google LLC | 2025-07-22 (5 días) | 2025-07-25 (2 días) | 3 días |
| 142.251.179.100 142.251.179.101 142.251.179.102 142.251.179.113 142.251.179.138 142.251.179.139 | Google LLC | 19/07/2025 (8 días) | 2025-07-22 (5 días) | 3 días |
| 64.233.180.100 64.233.180.101 64.233.180.102 64.233.180.113 64.233.180.138 64.233.180.139 | Google LLC | 16/07/2025 (11 días) | 19/07/2025 (8 días) | 3 días |

En esta otra hice una busqueda de google.com
Y en ella muestra mucha informacion al respecto.

2 Otras herramientas (whois)

```
Microsoft Windows [Versión 10.0.26100.4770]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>whois google.com

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to COM.whois-servers.net...

WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:00Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-07-28T14:08:35Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
```

For more information on Whois status codes, please visit <https://icann.org/epp>

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated and high-volume to access or query the Whois database except as reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time.

```

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.

Connecting to whois.markmonitor.com...

WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2024-08-02T02:17:33+0000
Creation Date: 1997-09-15T07:00:00+0000
Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Name Server: ns1.google.com
Name Server: ns4.google.com
Name Server: ns3.google.com
Name Server: ns2.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2025-07-28T14:04:24+0000 <<<

For more information on WHOIS status codes, please visit:
https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain's Registrant or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN's Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).

```

```

Web-based WHOIS:
https://domains.markmonitor.com/whois/contact/google.com

If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.

The data in MarkMonitor's WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name's registration record. While MarkMonitor believes the data to be accurate,
the data is provided "as is" with no guarantee or warranties regarding its
accuracy.

By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
(1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
(2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain name contacts (or
its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.

Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220
--
```

La herramienta WHOIS es un protocolo que permite consultar bases de datos que almacenan información sobre los usuarios registrados o asignados de un recurso de Internet, principalmente nombres de dominio y bloques de direcciones IP. Piensa en ella como una "guía telefónica" para el internet.

La información que la herramienta WHOIS puede mostrar, aunque con ciertas variaciones debido a las políticas de privacidad (como el GDPR en Europa) y los

servicios de "privacidad de dominio" ofrecidos por los registradores, generalmente incluye:

Informacion del Registrante (Propietario del Dominio):

Nombre (o nombre de la organización)

Dirección postal

Número de teléfono

Dirección de correo electrónico

A veces, información de contacto para roles específicos como "Contacto Administrativo" y "Contacto Técnico".

Información del Dominio:

Fecha de registro del dominio.

Fecha de vencimiento del dominio.

Última fecha de actualización del registro.

Estado del dominio (por ejemplo, si está activo, en período de gracia, etc.).

Informacion del Registrador:

Nombre del registrador (la empresa a través de la cual se registró el dominio).

Información de contacto del registrador (a menudo un correo electrónico de abuso).

Servidores de Nombres (Nameservers):

Los servidores de nombres asociados con el dominio, que indican dónde se aloja el sitio web o dónde se gestionan sus registros DNS.

Para que se utiliza la herramienta WHOIS?

Verificar la propiedad de un dominio

Investigaciones de seguridad

Adquisición de dominios

Verificar la disponibilidad de un dominio

Cumplimiento legal y protección de la propiedad intelectual

Monitoreo del propio portafolio de dominios

Es importante tener en cuenta que, debido a las regulaciones de privacidad (como el GDPR), mucha de la información personal del registrante puede estar "redactada" o "oculta" por defecto, y en su lugar se mostrará información del registrador o un servicio de privacidad de dominio. Sin embargo, en ciertos casos y con una justificación legítima (por ejemplo, para cumplimiento legal), se puede solicitar acceso a la información no pública a través de canales específicos proporcionados por ICANN o los registradores.

3 Google Dorks

Los Google Dorks, también conocidos como Google Hacking, son técnicas de búsqueda avanzada que utilizan operadores o "dorks" específicos para filtrar la información en el buscador de Google y obtener resultados muy precisos. En lugar de simplemente buscar palabras clave, los Google Dorks permiten a los usuarios afinar sus consultas para encontrar tipos de información muy concretos.

Para qué sirven los Google Dorks?

Principalmente, los Google Dorks se utilizan para:

Investigación y análisis de seguridad (Hacking Etico / Pentesting):

Identificación de vulnerabilidades

Reconocimiento (OSINT)

Optimización para Motores de Búsqueda (SEO):

Análisis de la competencia

Auditoría de un sitio web

Investigación general y búsqueda de información específica

Ejemplos de Google Dorks y su función:

Si quiero buscar algún archivo PDF en YouTube
site:youtube.com "filetype:pdf"

Me saldrán archivos en PDF

También archivos xls o doc

Puedo buscar cosas relacionadas con mi Instagram

site:instagram "dallapozza1978"

Lo mismo con Tik Tok

site:Tik Tok "dallapozza1978"

Ejemplos de Google Dorks y su función:

"palabra o frase exacta": Busca la frase exacta entre comillas.

Ejemplo: "credenciales de usuario"

site:dominio.com: Restringe la búsqueda a un dominio específico.

Ejemplo: site:ejemplo.com "información confidencial"

filetype:pdf: Busca archivos de un tipo específico (PDF, DOCX, TXT, PPT, etc.).

Ejemplo: filetype:pdf "política de seguridad"

intitle:"texto en el título": Busca páginas que contengan un texto específico en el título.

Ejemplo: intitle:"index of /admin" (puede revelar directorios de administración expuestos)

inurl:"texto en la URL": Busca páginas que contengan un texto específico en la URL

La pagina Exploit Database sirve para los siguientes propósitos clave:

Educacion y aprendizaje en ciberseguridad

Investigacion de vulnerabilidades

Pruebas de penetracion (Pentesting)

Mantenimiento y mejora de la seguridad

Desarrollo de herramientas de seguridad

Analisis forense y respuesta a incidentes

Exploit Database es un lugar de conocimiento practico sobre exploits que beneficia a toda la comunidad de ciberseguridad, desde quienes aprenden hasta quienes defienden sistemas, promoviendo la comprensión y la mejora de la seguridad informática.

Google Dorks y Exploits Database es lo mismo?

No son lo mismo, aunque están relacionados y a menudo se usan en conjunto en el ambito de la ciberseguridad.

Relación entre ambos

Google Dorks pueden ser el primer paso en un proceso de reconocimiento y explotación:

Un atacante o pentester podría usar Google Dorks para descubrir un sistema vulnerable (por ejemplo, un servidor web con una versión específica de un software que se sabe que tiene fallos).

Una vez identificada la posible vulnerabilidad, podrían ir a Exploit Database para buscar si existe un exploit conocido y público para esa versión específica del software y esa vulnerabilidad. Si encuentran un exploit, podrían intentar usarlo (en un entorno legal y ético, con permiso) para confirmar la vulnerabilidad y demostrar el impacto potencial.

En resumen:

Google Dorks te ayudan a encontrar información expuesta y sistemas potencialmente vulnerables en la vastedad de internet.

Exploit Database te proporciona el código o las instrucciones para aprovechar una vulnerabilidad una vez que ha sido identificada.

Son herramientas diferentes, pero complementarias, en el arsenal de cualquier profesional de la ciberseguridad.

4 Obtención de metadatos (FOCA)

FOCA es una herramienta informatica que se utiliza para la obtencion de Metadatos.

Para que sirve?

Permite extraer información oculta de diversos tipos de archivos (como documentos de Microsoft Office, PDF, imágenes, etc.). Esta información puede incluir nombres de usuarios, rutas de archivos, versiones de software, fechas de creación y modificación, e incluso la ubicación geográfica donde se tomó una foto.

Usos:

Se utiliza para auditorias de seguridad, investigaciones forenses digitales y para identificar posibles vulnerabilidades en sistemas o sitios web, ayudando a las organizaciones a protegerse de fugas de información.

A continuación voy a mostrar unas capturas de pantalla, para ver el potencial de esta herramienta.

Project Name - FOCA Open Source 3.4.7.1

Project Plugins Options TaskList About

Project Name

- Network
 - Clients (0)
 - Servers (0)
 - Unknown Servers
- Domains
- Document Analysis
 - Files (0/0)
 - Metadata Summary
 - Users (1)
 - Folders (0)
 - Printers (0)
 - Software (0)
 - Emails (0)
 - Operating Systems (0)
 - Passwords (0)
 - Servers (0)
- Malware Summary (DIARIO)

Foca
OPENSOURCE

Search engines: Google, Bing, DuckDuckGo

Extensions: doc, docx, swx, odp, ppt, ptx, odt, pdf, pps, ppss, ods, wpd, xls, xlsx, odg, rtf

Custom search

| ID | Type | URL | Download | Download Date | Size | Metadata E... | Malware An... | Modified Date |
|----|------|-----|----------|---------------|------|---------------|---------------|---------------|
| | | | | | | | | |

Time Source Severity Message

Settings Deactivate AutoScroll Clear Save log to File

Metadata analysis completed

Project Name - FOCA Open Source 3.4.7.1

Project Plugins Options TaskList About

Project Name

- Network
 - Clients (0)
 - Servers (0)
 - Unknown Servers
- Domains
- Document Analysis
 - Files (3/3)
 - Metadata Summary
 - Users (1)
 - Folders (0)
 - Printers (0)
 - Software (0)
 - Emails (0)
 - Operating Systems (0)
 - Passwords (0)
 - Servers (0)
- Malware Summary (DIARIO)

Foca
OPENSOURCE

Search engines: Google, Bing, DuckDuckGo

Extensions: doc, docx, swx, odp, ppt, ptx, odt, pdf, pps, ppss, ods, wpd, xls, xlsx, odg, rtf

Custom search

| ID | Type | URL | Download | Download Date | Size | Metadata E... | Malware An... | Modified Date |
|----|------|---|----------|---------------------|---------|---------------|---------------|---------------------|
| 0 | jpg | C:\Archivos Martin\Fotos Metadatos\Img4.jpg | * | 07/30/2025 15:00:04 | 4.88 MB | x | x | 07/30/2025 15:00:04 |
| 1 | jpg | C:\Archivos Martin\Fotos Metadatos\Img5.jpg | * | 07/30/2025 15:00:04 | 3.19 MB | x | x | 07/30/2025 15:00:04 |
| 2 | jpg | C:\Archivos Martin\Fotos Metadatos\Img6.jpg | * | 07/30/2025 15:00:04 | 4.18 MB | x | x | 07/30/2025 15:00:04 |

Time Source Severity Message

Settings Deactivate AutoScroll Clear Save log to File

Metadata analysis completed

Project Name - FOCA Open Source 3.4.7.1

Project Plugins Options TaskList About

Custom search

| ID | Type | URL | Download | Download Date | Size | Metadata E... | Malware An... | Modified Date |
|----|------|---|----------|---------------------|---------|---------------|---------------|---------------------|
| 0 | jpg | C:\Archivos Martin\Fotos Metadatos\Img4.jpg | . | 07/30/2025 15:01:43 | 4.88 MB | x | x | 07/30/2025 15:01:43 |
| 1 | jpg | C:\Archivos Martin\Fotos Metadatos\Img5.jpg | . | 07/30/2025 15:01:43 | 3.19 MB | x | x | 07/30/2025 15:01:43 |
| 2 | jpg | C:\Archivos Martin\Fotos Metadatos\Img6.jpg | . | 07/30/2025 15:01:43 | 4.18 MB | x | x | 07/30/2025 15:01:43 |

Time Source Severity Message

All documents were analyzed

Extract All Metadata

Save log to File

Extract All Metadata

Analyze All Metadata

Analyze All Malware

Delete All

Add file

Add folder

Add URLs from file

Link(s)

Las proximas capturas son de la imagen 4

Project Name - FOCA Open Source 3.4.7.1

Project Plugins Options TaskList About

Custom search

| ID | Type | URL | Download | Download Date | Size | Metadata E... | Malware An... | Modified Date |
|----|------|---|----------|---------------------|---------|---------------|---------------|---------------------|
| 0 | jpg | C:\Archivos Martin\Fotos Metadatos\Img4.jpg | . | 07/30/2025 15:01:43 | 4.88 MB | • | x | 07/28/2025 10:00:54 |
| 1 | jpg | C:\Archivos Martin\Fotos Metadatos\Img5.jpg | . | 07/30/2025 15:01:43 | 3.19 MB | • | x | 07/28/2025 10:01:20 |
| 2 | jpg | C:\Archivos Martin\Fotos Metadatos\Img6.jpg | . | 07/30/2025 15:01:43 | 4.18 MB | • | x | 07/28/2025 10:01:44 |

Project Name - FOCA Open Source 3.4.7.1

Project Plugins Options TaskList About

Project Name

- Network
 - Clients (0)
 - Servers (0)
 - Unknown Servers
- Domains
- Document Analysis
 - Files (3/3)
 - Img4.jpg
 - Img4.jpg
 - Img5.jpg
 - EXIF
- Metadata Summary

Attribute Value

| | |
|------------------------|---------------------------|
| Exif IFD0 | |
| Image Width | 4032 pixels |
| Image Height | 3072 pixels |
| Copyright | Copyright: Spreadium 2011 |
| Resolution Unit | Inch |
| Image Description | Exif_JPEG_420 |
| Make | CUBOT |
| Model | NOTE 50 |
| Software | Software Version v1.1.0 |
| Date/Time | 2025-07-28 10:00:54 |
| YCbCr Positioning | Center of pixel array |
| X Resolution | 72 dots per inch |
| Y Resolution | 72 dots per inch |
| Artist | Artist-freed |
| <hr/> | |
| Exif SubIFD | |
| ISO Speed Ratings | 50 |
| Exposure Program | Shutter priority |
| Unique Image ID | IMAGE 2025-07-28 10:00:54 |
| F-Number | f/1.8 |
| Exposure Time | 1000/318471 sec |
| Sub-Sec Time Digitized | 20 |
| Time Zone Digitized | +02:00 |
| Sub-Sec Time Original | 100 |
| Time Zone Original | +02:00 |
| Sub-Sec Time | 10 |

Project Name - FOCA Open Source 3.4.7.1

Project Plugins Options TaskList About

Project Name

- Network
 - Clients (0)
 - Servers (0)
 - Unknown Servers
- Domains
- Document Analysis
 - Files (3/3)
 - Img4.jpg
 - Img4.jpg
 - Img5.jpg
 - EXIF
- Metadata Summary

Attribute Value

| | |
|------------------|---|
| <hr/> | |
| File Information | |
| URL | C:\Archivos Martin\Fotos Metadatos\Img4.jpg |
| Local path | C:\Archivos Martin\Fotos Metadatos\Img4.jpg |
| Download | Yes |
| Analyzed | Yes |
| Download date | 30/07/2025 15:01:43 |
| Size | 4.88 MB |
| <hr/> | |
| Users | |
| UserName | Artist-freed |
| <hr/> | |
| Dates | |
| Creation date | 28/07/2025 10:00:54 |
| <hr/> | |
| Other Metadata | |
| Camera Model | NOTE 50 |

Project Name - FOCA Open Source 3.4.7.1

Project Plugins Options TaskList About

Project Name

- Network
 - Clients (0)
 - Servers (0)
 - Unknown Servers
- Domains
- Document Analysis
 - Files (3/3)
 - Img4.jpg
 - Img4.jpg
 - Img5.jpg
 - Img5.jpg
- Metadata Summary

| Attribute | Value |
|--------------------------|---------------------------|
| Exif SubIFD | |
| ISO Speed Ratings | 50 |
| Exposure Program | Shutter priority |
| Unique Image ID | IMAGE 2025.07.28 10:00:54 |
| F-Number | f/1.8 |
| Exposure Time | 1000/318471 sec |
| Sub-Sec Time Digitized | 20 |
| Time Zone Digitized | +02:00 |
| Sub-Sec Time Original | 100 |
| Time Zone Original | +02:00 |
| Sub-Sec Time | 10 |
| Time Zone | +02:00 |
| Focal Length | 4,1 mm |
| Flash | Flash did not fire |
| White Balance | Tungsten (Incandescent) |
| Scene Capture Type | Standard |
| Max Aperture Value | f/2.6 |
| Date/Time Digitized | 2025.07.28 10:00:54 |
| Exif Image Height | 3072 pixels |
| White Balance Mode | Auto white balance |
| Date/Time Original | 2025.07.28 10:00:54 |
| Exif Image Width | 4032 pixels |
| Exposure Mode | Auto exposure |
| Aperture Value | f/1.9 |
| Components Configuration | YCbCr |

Project Name - FOCA Open Source 3.4.7.1

Project Plugins Options TaskList About

Project Name

- Network
 - Clients (0)
 - Servers (0)
 - Unknown Servers
- Domains
- Document Analysis
 - Files (3/3)
 - Img4.jpg
 - Img4.jpg
 - Img5.jpg
 - Img5.jpg
- Metadata Summary

| Attribute | Value |
|--------------------------|----------------------------|
| Exif Image Width | 4032 pixels |
| Exposure Mode | Auto exposure |
| Aperture Value | f/1.9 |
| Components Configuration | YCbCr |
| Color Space | sRGB |
| Exif Version | 2.20 |
| FlashPix Version | 1.00 |
| File Source | Digital Still Camera (DSC) |

Thumbnail

Picture

En las imágenes se puede apreciar todos los datos relacionado con la foto:

Descripcion de la imagen
Marca y modelo del movil
Hora y fecha
Zona horaria
Y muchos datos mas.....

5 Uso de Shodan

The screenshot shows the Shodan search interface with the following details:

- TOTAL RESULTS:** 72
- TOP COUNTRIES:** United States (20), Germany (18), Spain (6), France (3), Portugal (3)
- TOP PORTS:** 443 (18), 8081 (15)
- Search Query:** 8081
- Result 1 (99.192.184.83):** Mophost, United States, Miami. IP: 99.192.184.83. Last seen: 2025-07-30T01:34:05.475041. Status: Access Granted. View Report, Browse Images, View on Map, Advanced Search.
- Result 2 (109.247.84.184):** Lyse Tele AS, Norway, Egersund. IP: 109.247.84.184. Last seen: 2025-07-30T01:30:49.029158. Status: Access Granted. View Report, Browse Images, View on Map, Advanced Search.

Spain 8

France 3

Portugal 3

More...

TOP PORTS

| Port | Count |
|----------------|-------|
| 443 | 18 |
| 8081 | 15 |
| 21 | 6 |
| 9000 | 6 |
| 80 | 3 |
| More... | |

TOP ORGANIZATIONS

| Organization | Count |
|--------------------------|-------|
| Mojohost | 13 |
| Deutsche Telekom AG | 10 |
| Digi Spain Telecom | 2 |
| Host Europe GmbH | 2 |
| myNET Internet Solutions | 2 |
| More... | |

TOP PRODUCTS

| Product | Count |
|--------------|-------|
| Apache httpd | 16 |
| nginx | 6 |
| PPTP | 3 |

109.247.84.184

184.109.247.84 customer.lyse.net
Lyse Tele AS
Norway, Egersund

HTTP/1.0 200 OK
Content-type: text/html
Connection: close
Server: MPG-Streamer/0.2
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
Pragma: no-cache
Expires: Mon, 3 Jan 2000 12:34:56 GMT
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www...

2025-07-30T01:30:49.029158

SHODAN Explore Downloads Pricing webcams country:"US" Account

TOTAL RESULTS 21

TOP CITIES

| City | Count |
|----------------|-------|
| Miami | 13 |
| Detroit | 2 |
| Lindenhurst | 1 |
| New York City | 1 |
| North Madison | 1 |
| More... | |

TOP PORTS

| Port | Count |
|------|-------|
| 443 | 15 |
| 8081 | 4 |
| 9000 | 1 |

TOP ORGANIZATIONS

| Organization | Count |
|-----------------------|-------|
| Mojohost | 15 |
| Cogent Communications | 1 |

99.192.184.83

Mojohost
United States, Miami

HTTP/1.1 200 OK
Date: Wed, 30 Jul 2025 01:34:05 GMT
Server: Apache
Accept-Ranges: bytes
Vary: Accept-Encoding,User-Agent
Cache-Control: max-age=60, private, proxy-revalidate
Transfer-Encoding: chunked
Content-type: text/html

fa
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional/...

2025-07-30T01:34:05.475041

64.59.87.48

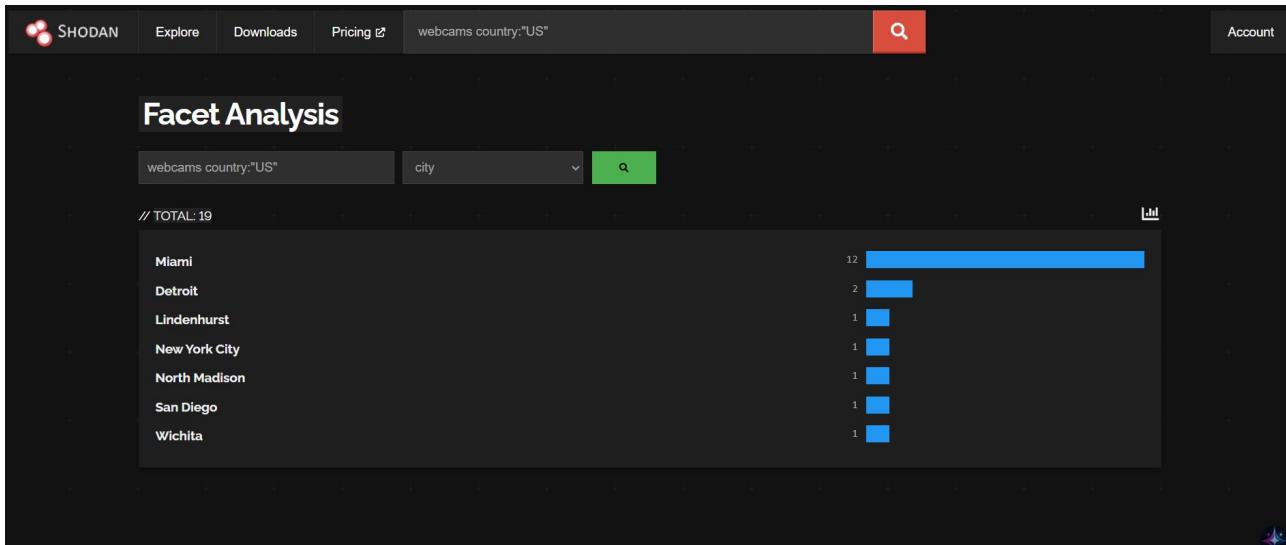
Mojohost
United States, Miami

HTTP/1.1 200 OK
Date: Tue, 29 Jul 2025 19:06:16 GMT
Server: Apache
Accept-Ranges: bytes
Vary: Accept-Encoding,User-Agent
Cache-Control: max-age=60, private, proxy-revalidate
Transfer-Encoding: chunked
Content-type: text/html

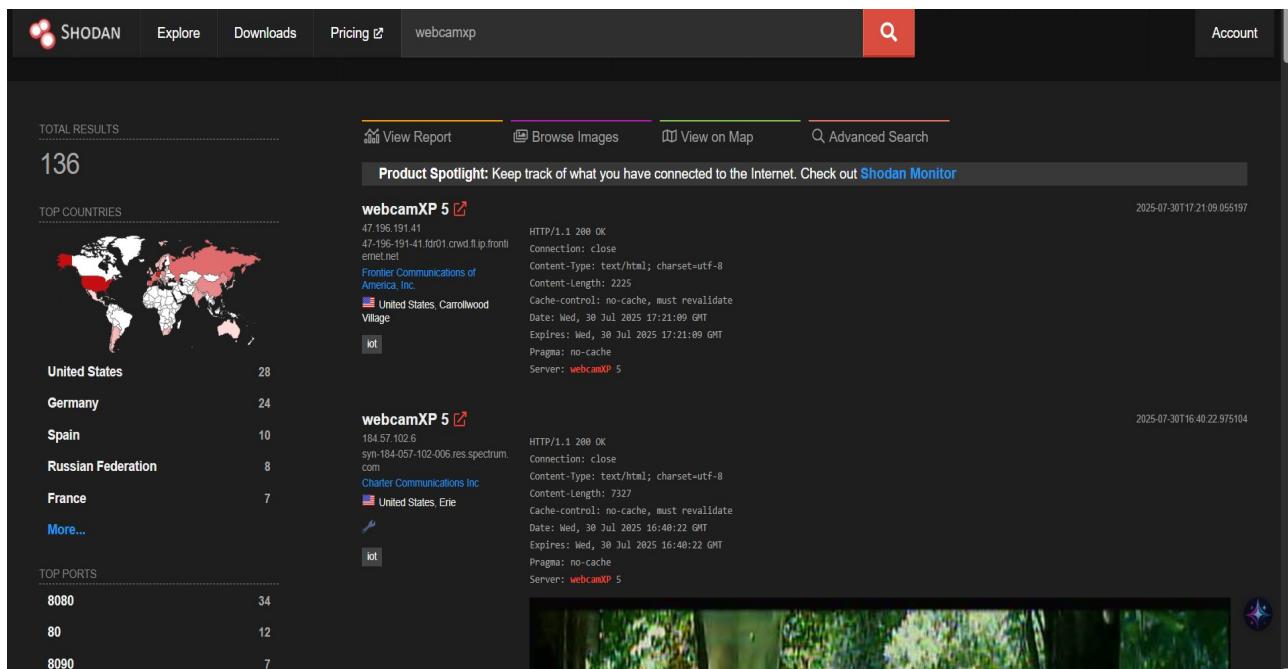
fa

2025-07-29T19:06:16.282447

En estas primeras imágenes, puse en el buscador “webcams” y me muestra a nivel internacional y luego en USA. Estas están todas con vulnerabilidades.



Aca se puede ver como filtrar por ciudades.



Germany 24

Spain 10

Russian Federation 8

France 7

More...

TOP PORTS

| | |
|------|----|
| 8080 | 34 |
| 80 | 12 |
| 8090 | 7 |
| 6080 | 6 |
| 7777 | 4 |

More...

TOP ORGANIZATIONS

| | |
|-----------------------------------|----|
| Charter Communications Inc | 10 |
| Deutsche Telekom AG | 8 |
| 1&1 Telecom GmbH | 6 |
| Telefonica de Espana SAU | 6 |
| CHINANET Sichuan province network | 5 |

More...

TOP PRODUCTS

| | |
|------------|----|
| webcamXP 5 | 83 |
|------------|----|

webcamXP 5

164.97.102.6
syn-184-057-102-006.res.spectrum.com
Charter Communications Inc
United States, Erie

HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 7327
Cache-control: no-cache, must revalidate
Date: Wed, 30 Jul 2025 16:40:22 GMT
Expires: Wed, 30 Jul 2025 16:40:22 GMT
Pragma: no-cache
Server: webcamXP 5

2025-07-30T16:40:22.975104

WEBCAMXP 5

WEBCAMS AND IP CAMERAS SERVER FOR WINDOWS

Home Multi view Smartphone Gallery Administration Not logged in

Source 1 JavaScript

Live View

Pan, Tilt & Zoom

Shodan | Maps | Images | Monitor | Developer | More... | Account

184.57.102.6

SHODAN Explore Downloads Pricing Search

Regular View Raw Data Timeline

// TAGS: iot open-dir self-signed

// LAST SEEN: 2025-07-30

General Information

Hostnames: syn-184-057-102-006.res.spectrum.com

Domains: spectrum.com

Country: United States

City: Erie

Organization: Charter Communications Inc

ISP: Charter Communications Inc

ASN: AS10796

Open Ports

21 80 443 5400 5432 5800 6500 6565 8800 9090 9550

// 21 / TCP 652854496 | 2025-07-29T21:32:15.040Z

```

220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (tim.kosse@mx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
530 Login or password incorrect!
214-The following commands are recognized:
USER PASS QUIT CMD PWD PORT PASV TYPE
LIST REST CWD RETR STOR SIZE DELE RMD
MKD RNFR RMD ABOR SYST NOOP APPE NLST
MDTM XPMDF XCUP XWD XRD NOP EPSV EPRT
AUTH ADAT PBSZ PROT FEAT MODE OPTS HELP
ALLO MLST MLSO SITE PGSM STRU CLNT MFTM
HASH
214 Have a nice day.

```

El filtro "webcamxp" busca dispositivos que se ejecutan con este software. Es muy popular para sistemas de vigilancia y webcams, que permite la transmisión de video en vivo a través de Internet.

SHODAN Explore Downloads Pricing org:orange Account

TOTAL RESULTS: 2,391,836

TOP COUNTRIES:

| Country | Count |
|----------------|-----------|
| France | 1,132,540 |
| Poland | 297,456 |
| Romania | 221,513 |
| Spain | 140,651 |
| United Kingdom | 132,580 |

More...

TOP PORTS:

| Port | Count |
|-------|---------|
| 7547 | 123,151 |
| 50995 | 117,795 |
| 443 | 117,561 |

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

92.84.45.48 Romania, Sălătău Gheorghe

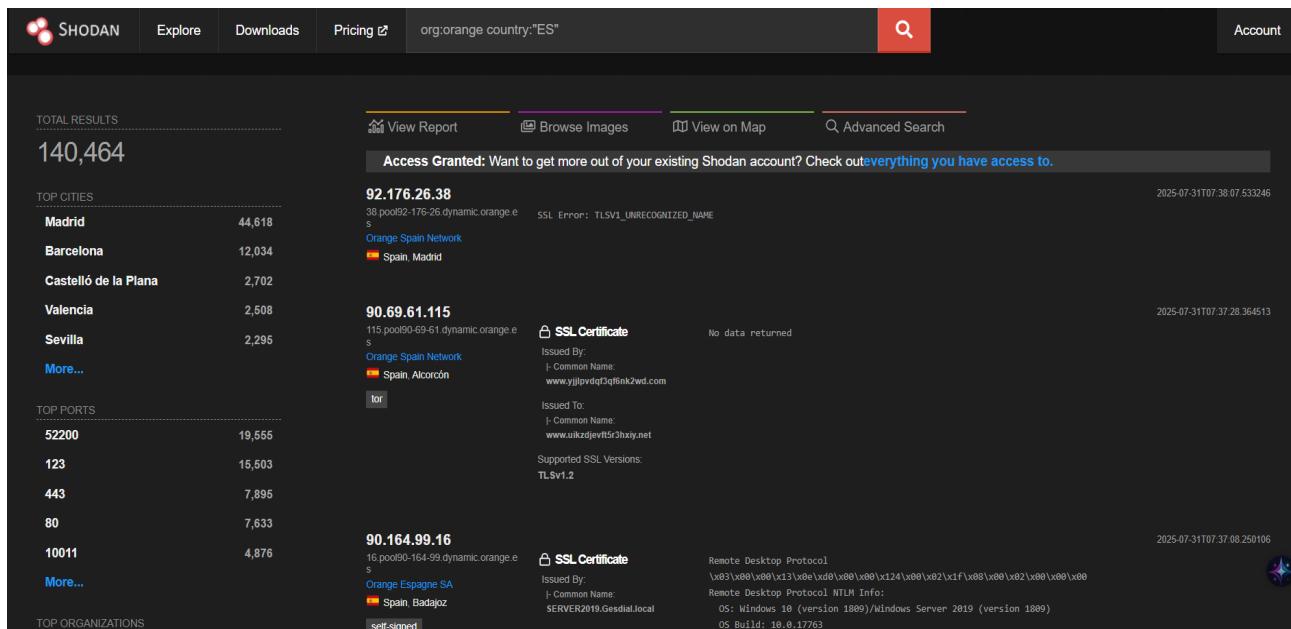
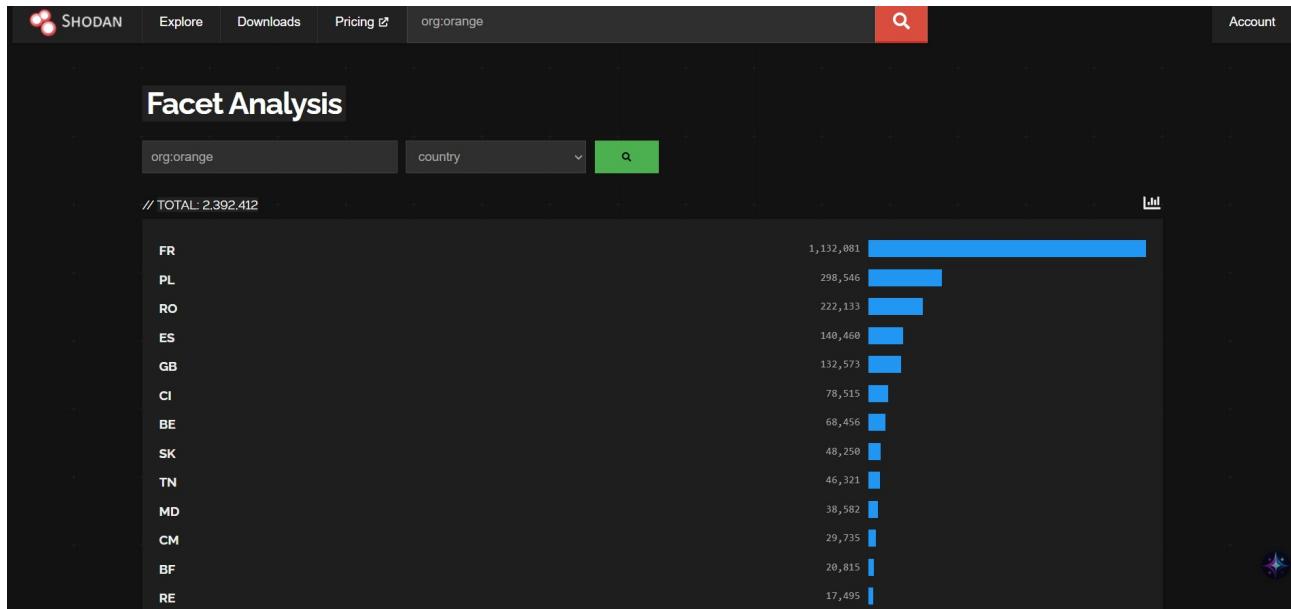
HTTP/1.1 200 OK
Content-type: text/html
Content-Length: 340
Connection: close

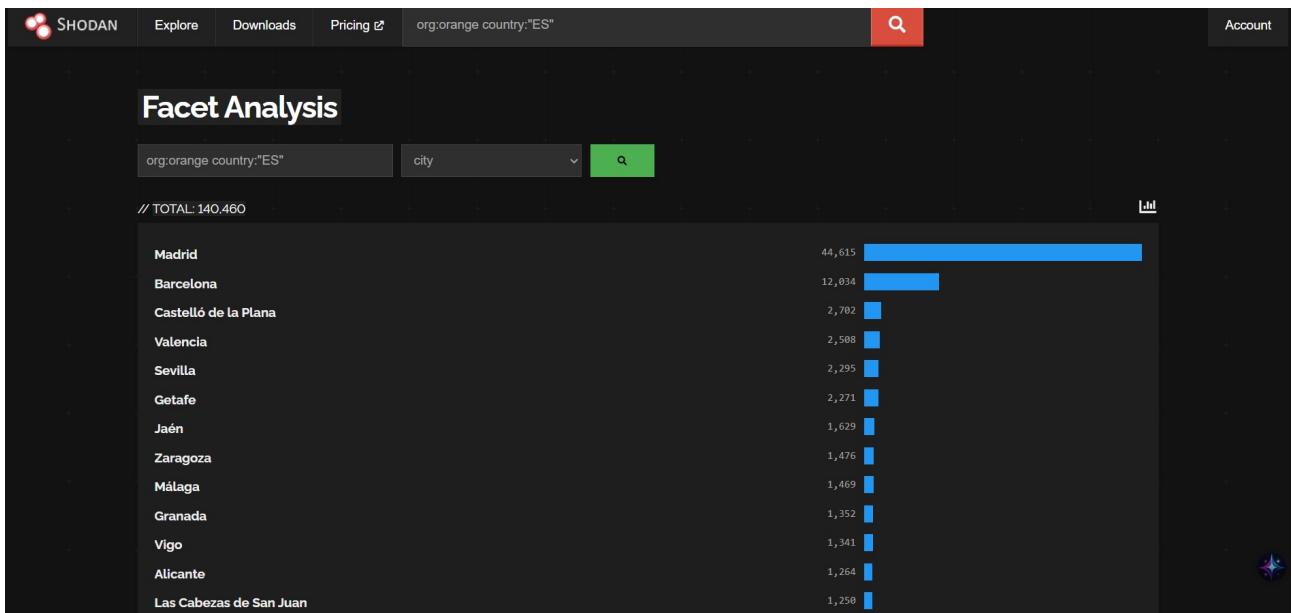
195.22.234.24 static.195.22.234.24.mdd.net Moldova, Republic of, Chisinau

SNMP:
Versions:
3
EngineID Format: mac
Engine Boots: 57
EngineID Data: 50:f7:22:0d:14:88
Enterprise: 9
Engine Time: 528 days, 9:19:47
Enterprise Name: ciscoSystems

109.98.52.255 Orange Romania S.A. Romania, Bucharest

NTP
protocolversion: 3
stratum: 4
leap: 0
precision: -10
rootdelay: 0.04833984375
rootdisp: 0.002763671875





Y por ultimo vamos a ver el filtro que se puede buscar por empresa. En este caso Orange. Y luego se puede hacer en la busqueda, cosas mas especificas, como pais y ciudad.