

#STICPUNTACANA

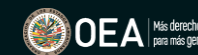
III JORNADAS STIC

CAPÍTULO REPÚBLICA DOMINICANA



Simulador de Cibervigilancia

Como familiarizarse con la cibervigilancia



Wiktor Nykiel



WiktorNykiel



WiktorNykiel_GINSEG_Inteligencia

- ✓ Padre de [ELENA, Simulador de Técnicas de Cibervigilancia](#).
- ✓ Colaborador del [Centro Criptológico Nacional](#), CCN, adscrito al Centro Nacional de Inteligencia, CNI.
- ✓ Co-fundador de la comunidad de [ciberinteligencia Ginseg](#) y del [congreso IntelCon](#).
- ✓ Ponente en diferentes congresos nacionales e internacionales.



Índice

- 01 Conceptos esenciales
- 02 Sobre Elena
- 03 Un ejemplo real: Counterfeit en comercios web
- 04 Un ejemplo de caso de investigación en Elena
- 05 Seguridad Operativa en actividades de cibervigilancia
- 06 Inteligencia de imágenes
- 07 Dorking con buscadores genéricos
- 08 Dorking con buscadores especializados
- 09 Reportando y entregando el producto

Anexos



Índice

- 01 Conceptos esenciales
- 02 Sobre Elena
- 03 Un ejemplo real: Counterfeit en comercios web
- 04 Un ejemplo de caso de investigación en Elena
- 05 Seguridad Operativa en actividades de cibervigilancia
- 06 Inteligencia de imágenes
- 07 Dorking con buscadores genéricos
- 08 Dorking con buscadores especializados
- 09 Reportando y entregando el producto
- Anexos



Qué es y qué no es la Cibervigilancia

Cibervigilancia

Definición: Monitorización de un individuo o grupo, su información y comportamiento por medio de herramientas cibernéticas, que aplicando un análisis sea capaz de ayudar en la toma de decisiones.

Que es

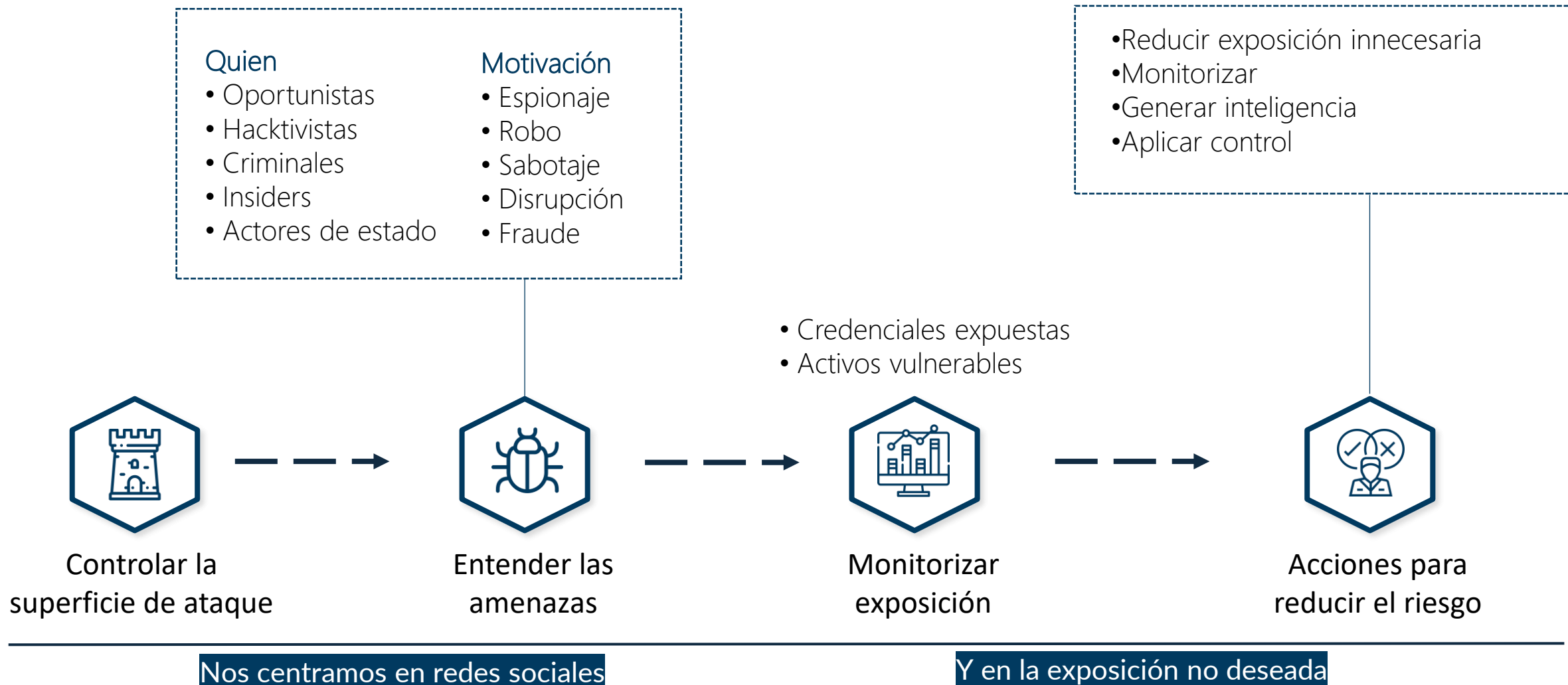
1. Nos permite **detectar posibles amenazas** asociadas hacia la **marca u objetivo**, de forma **preventiva** y con características constituyentes que permitan identificar, basados en evidencias, estas amenazas.
2. Se consigue realizando una **monitorización de amenazas**, alertando en tiempo, después de haber hecho un **análisis de los posibles impactos** que pueda tener.
3. Nos sirve para intentar **predecir posibles eventos futuros y conflictos**, además de **estudiar eventos pasados y tomar lecciones aprendidas**.
4. Las fuentes de información que usamos son principalmente **fuentes abiertas**. También se utilizan **redes sociales** para la **obtención de los datos**.

Que no es

1. **Infiltración en comunidades con identidades ficticias**, interactuando y engañando al objetivo para obtener información.
2. **Contrainteligencia**.
3. **Ataques activos en contra del objetivo**.



Objetivo de la cibervigilancia



Donde encajan estas disciplinas

Cibervigilancia



OSINT

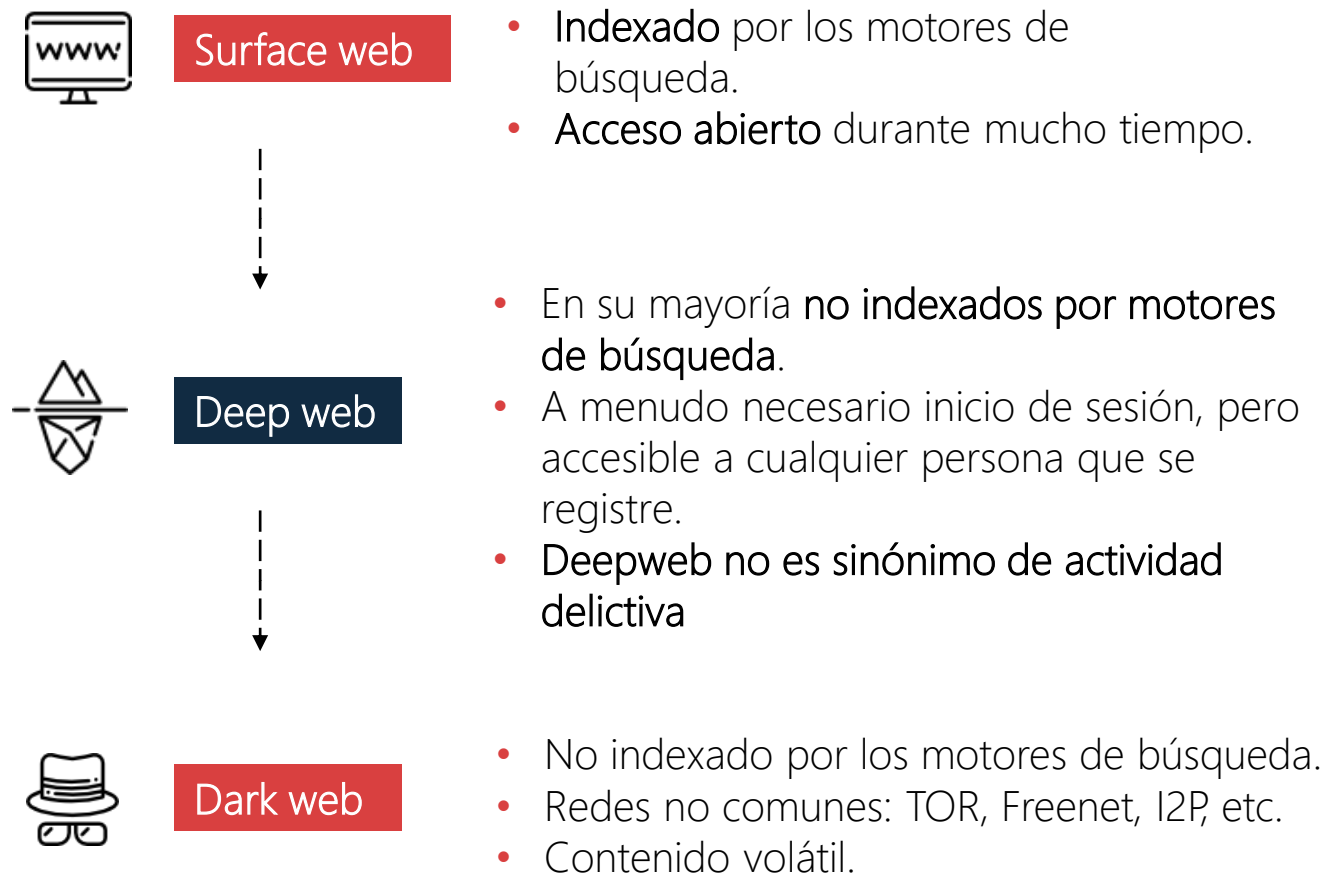


SOCMINT



Profundidad y agregación de los datos

Conceptualmente, podríamos distinguir tres:



Fuentes

+

Agregación de datos

Online pastes

Honeynets

Trapmails

Online trackers

Referers

BBDDs antivirus

CERTs

xBLs

Spam blacklists

Safe browsing

Cybersquatting

APK Markets

TOR crawler

Hidden IRC

STIX / TAXII

IoC

Malware

Botnets / C&C

Social Media

BBDDs threat intelligence

Agregación de todas las fuentes

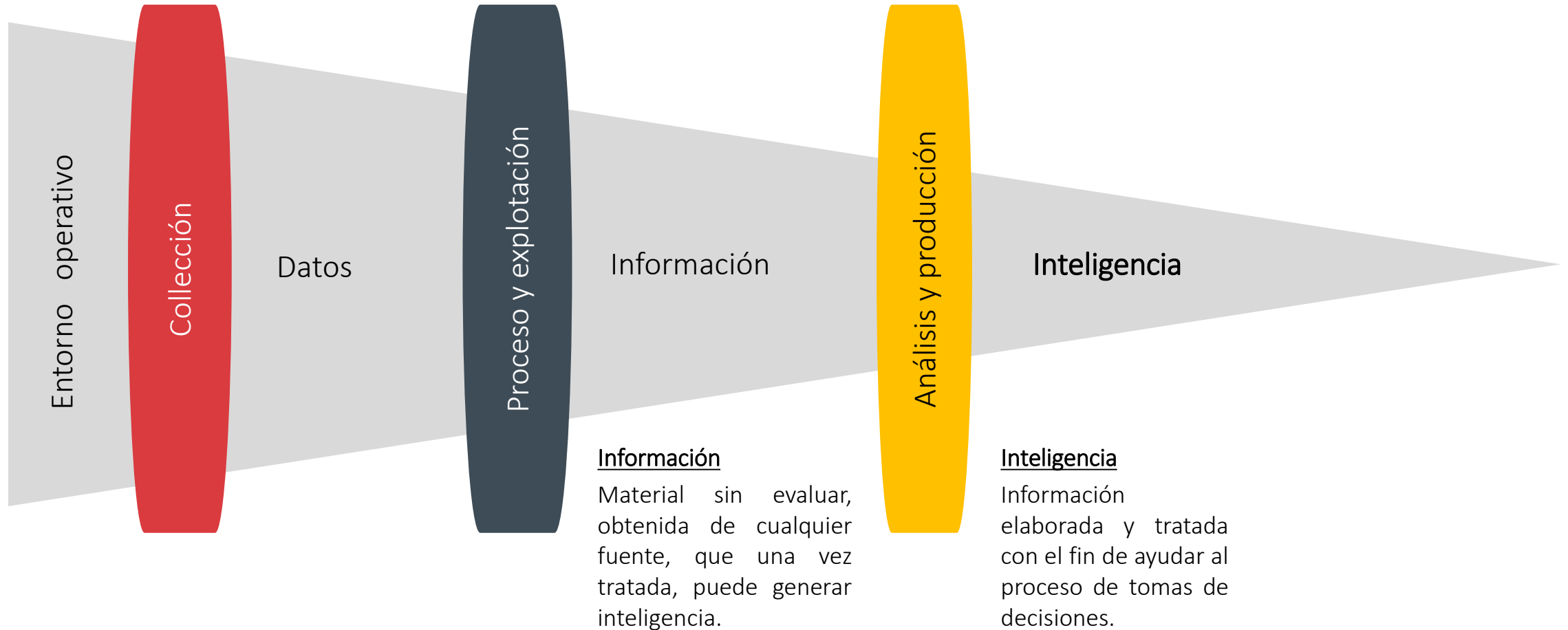
Enriquecimiento de los datos

Filtrado

Categorización

Entrega

Datos, información e inteligencia



Recolectamos y entregamos

Internet



Redes Sociales



Deep & Dark web



Descargas



Foros y comunidades



Análisis + Inteligencia

Perfiles multidisciplinares

Idiomas y Culturas

Analistas de Inteligencia / Malware / Ciberseguridad



Organización



Seguridad lógica



Seguridad física



Marketing



Recursos Humanos



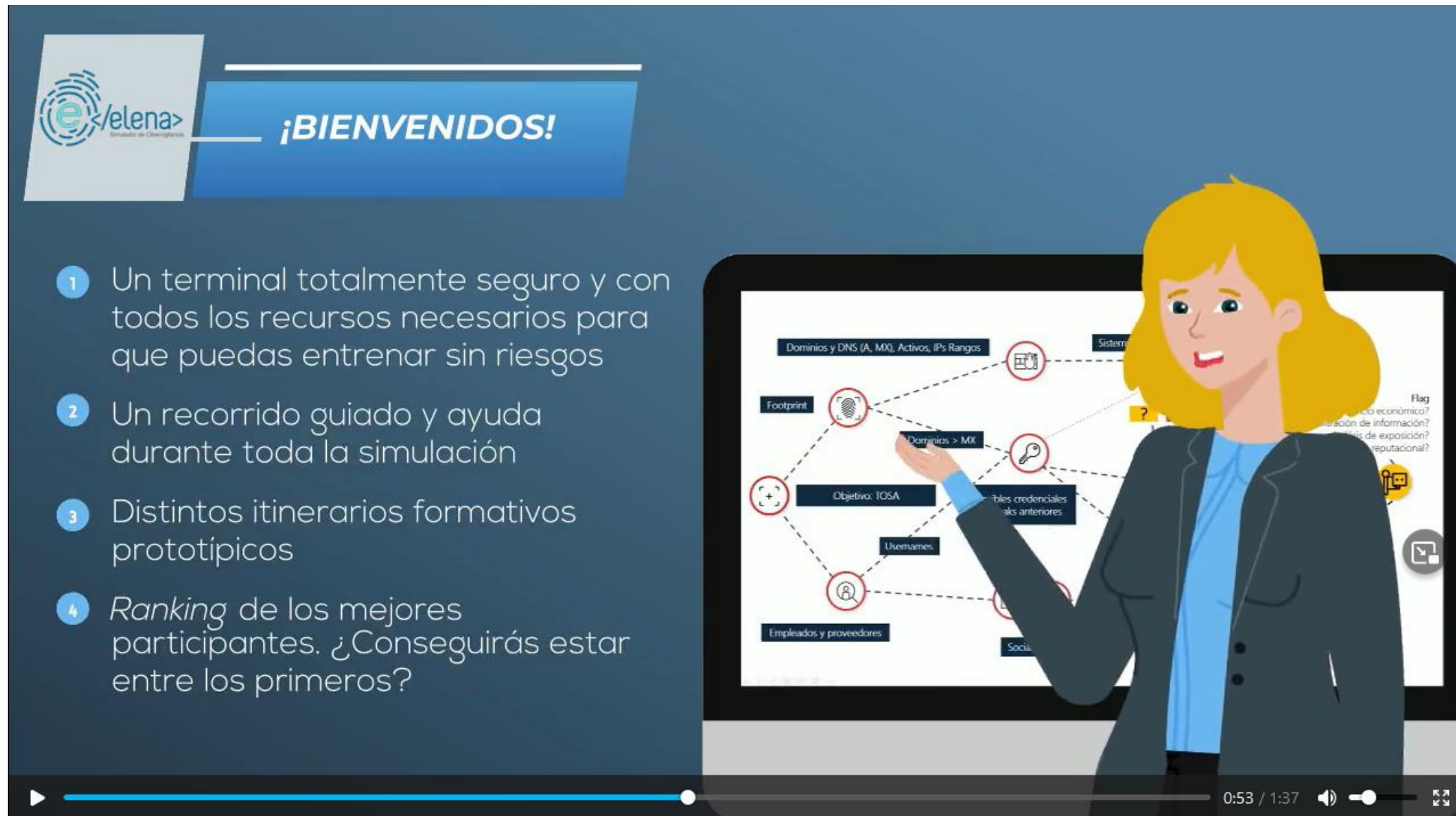
Consejo Administrativo

Índice

- 01 Conceptos esenciales
- 02 Sobre Elena
- 03 Un ejemplo real: Counterfeit en comercios web
- 04 Un ejemplo de caso de investigación en Elena
- 05 Seguridad Operativa en actividades de cibervigilancia
- 06 Inteligencia de imágenes
- 07 Dorking con buscadores genéricos
- 08 Dorking con buscadores especializados
- 09 Reportando y entregando el producto
- Anexos



Nos lo cuenta Elena en un minuto



 **¡BIENVENIDOS!**

- 1 Un terminal totalmente seguro y con todos los recursos necesarios para que puedas entrenar sin riesgos
- 2 Un recorrido guiado y ayuda durante toda la simulación
- 3 Distintos itinerarios formativos prototípicos
- 4 *Ranking* de los mejores participantes. ¿Conseguirás estar entre los primeros?

The screen displays a network diagram with nodes and connections. Nodes include: 'Dominios y DNS (A, MX), Activos, IPs Rangos', 'Footprint', 'Dominios > MX', 'Objetivo: TOSA', 'Usuarios', 'Empleados y proveedores', 'Sistema', 'Flag', '¿Análisis de información?', '¿Análisis de exposición?', '¿Análisis de reputacional?', 'Credenciales anteriores', and 'Social'. A woman with blonde hair, wearing a blue shirt and a dark blazer, is pointing at the screen.

0:53 / 1:37

<https://simulador.tecnicas-cibervigilancia.com/videos/IntroSTCElena.mp4>

Simulador Elena

Simulador creado como **herramienta de apoyo a los cursos de formación en temática de cibervigilancia**.

Para poder superar los ejercicios, es necesario aplicar las técnicas y procedimientos de recolección y tratamiento de información que permitan obtener y plasmar las correspondientes conclusiones de un caso que pretende representar de forma fehaciente las etapas una investigación de forma guiada.



<https://www.ccn-cert.cni.es/soluciones-seguridad/elena.html>

Simulador Elena



El propósito de este elemento complementario de aprendizaje es ofrecer un **entorno autocontenido que simule un escenario real** donde el analista de ciberinteligencia pueda practicar y realizar capacitaciones de cibervigilancia.

El entorno y sus itinerarios han sido creados en base a la experiencia adquirida durante la realización de numerosos cursos, los cuales han servido de base y referencia para crear esta solución.

Este simulador se ha creado 100% en España con el liderazgo del CCN-Cert – Centro Criptológico Nacional en colaboración con Ginseg Cibervigilancia Ciberinteligencia OSINT.



Recorrido asistido durante el aprendizaje



Árbol de decisiones



Aprendizaje asistido con multitude de posibles caminos

Tipos de ejercicios donde el participante tiene que tomar una serie de decisiones en función a una reciente amenaza que esta afectando a su organización. Para llevar a cabo este escenario será necesario aplicar una serie de actuaciones que contrarresten la propia amenaza, utilizando para ello diversas técnicas de cibervigilancia.

Herramientas emuladas

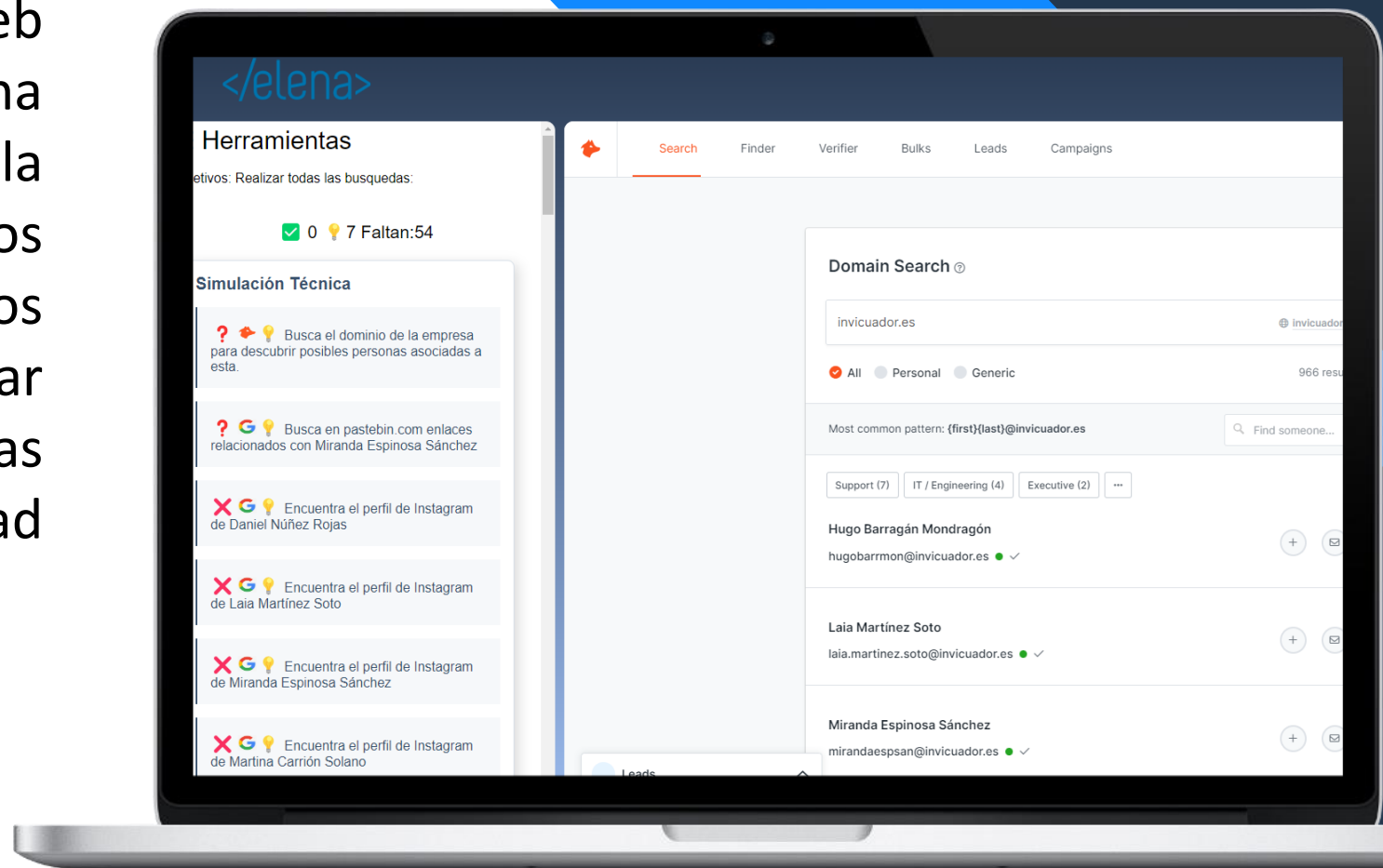
Tanto las herramientas web necesarias para realizar una investigación, como las de consola son emuladas y pobladas con datos generados para cada uno de los ejercicios, permitiendo así generar escenarios y laboratorios realistas con un seguimiento de la actividad del alumno detallada.

35+

Herramientas
Web

15+

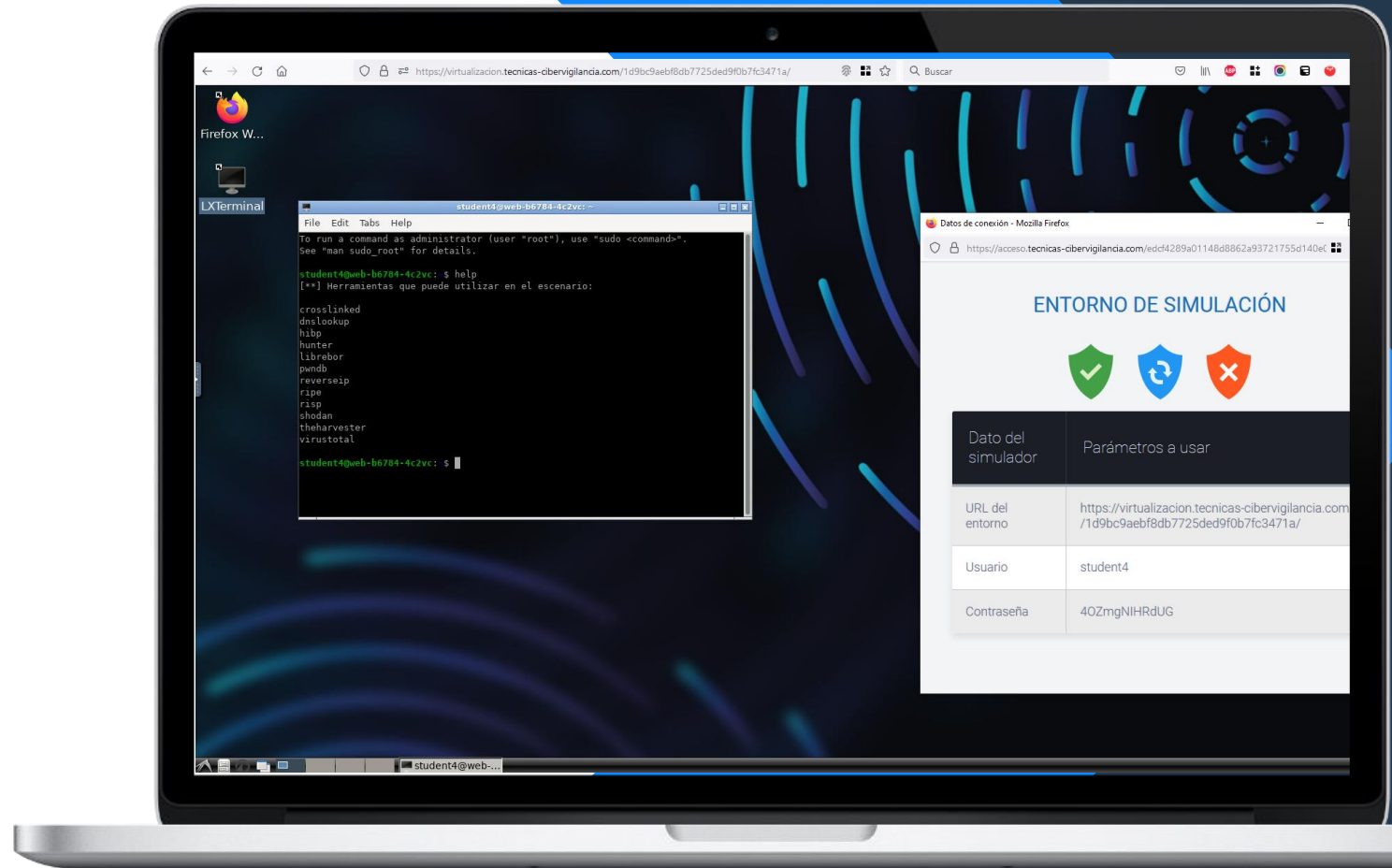
Herramientas
de terminal



Escritorios virtualizados en el navegador

Para complementar y permitir realizar al alumno ejercicios desde cualquier equipo siendo o no corporativo, con más o menos recursos y sin necesidad de instalar software adicional ni elevar privilegios, se han creado escritorios virtualizados accesibles desde el navegador.

Estos entornos permiten acceder a las herramientas y datos necesarios para practicar en un entorno seguro y autocontenido.

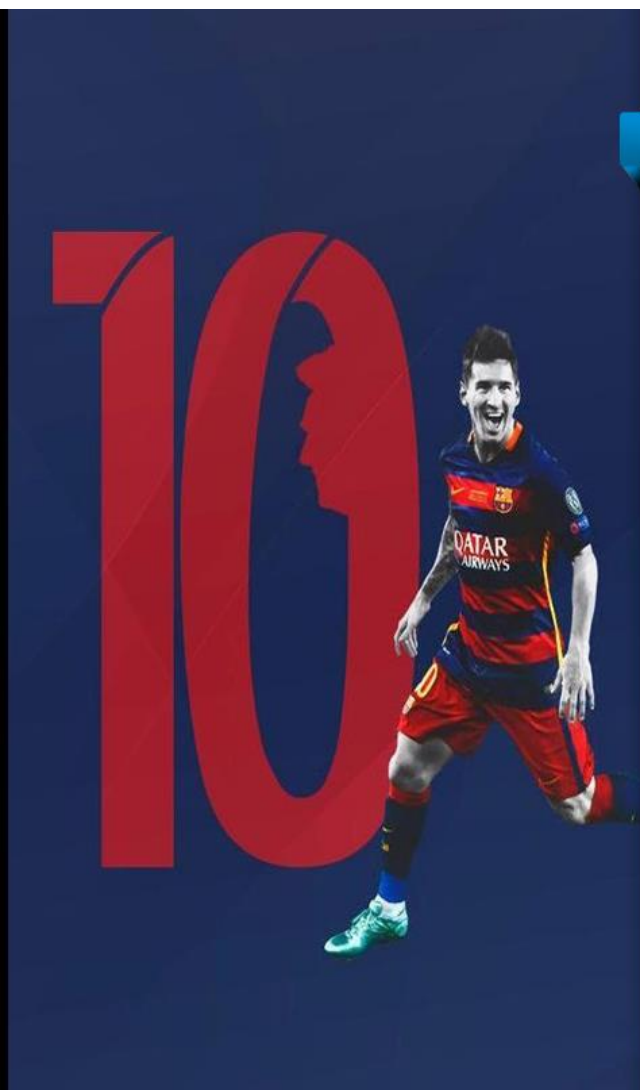


Índice

- 01 Conceptos esenciales
- 02 Sobre Elena
- 03 Un ejemplo real: Counterfeit en comercios web
- 04 Un ejemplo de caso de investigación en Elena
- 05 Seguridad Operativa en actividades de cibervigilancia
- 06 Inteligencia de imágenes
- 07 Dorking con buscadores genéricos
- 08 Dorking con buscadores especializados
- 09 Reportando y entregando el producto
- Anexos



Punto de partida: comercio de “oportunidad”





Buscar Search

Mi Carrito 0 Items: €0.00 View Cart checkout

Inicio Nike Mercurial Nike HyperVenom Nike Tiempo Nike Magista Nike Elastico Adidas Niños Contáctenos





Ofertas del mes en junio



Oferta Botas Adidas Predator 20.4 TF Inflight Negro Blanco
€150.00 €75.00



Oferta Botas Adidas X Ghosted.1 AG Precision To
€120.00 €60.00



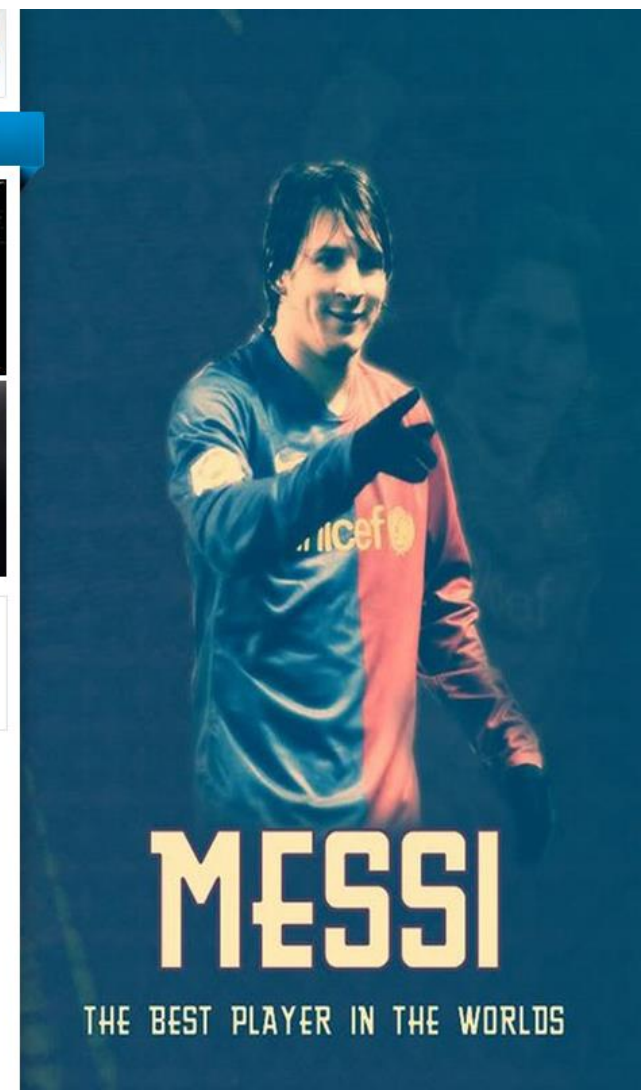
Oferta Botas Adidas X Ghosted.1 FG/AG Precision
€120.00 €60.00



Oferta Botas Adidas X Ghosted.1 TF Precision To
€150.00 €75.00



Oferta Botas Adidas X Ghosted.3 SG Precision To
€150.00 €75.00





Simulador de Cibervigilancia

Punto de partida: comercio de “oportunidad”



VENTA DE VIERNES NEGRO PRE 2018 | BIENVENIDO A LA JOYERÍA DE
PANDORA ESPAÑA TIENDA ONLINE!

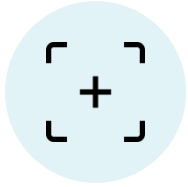
EUR  SIGN IN OR REGISTRARSE

PANDORA

INICIO Charms  Separadores Clips y Cadenas de Seguridad Conjuntos de Regalo Anillos
Pendientes Collares Pulseras Nueva Pandora Charms Jubilados y Joyerías Colecciones 



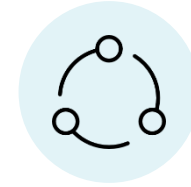
Empecemos haciendo preguntas oportunas



¿Es legítimo el comercio que estamos investigando?



¿Somos capaces de hacer una atribución?



¿Somos capaces de localizar más comercios?



¿Los sistemas son vulnerables?



¿Han dejado pistas al descubierto?



¿Localizamos información sensible?

¿Somos capaces de diferenciar la página legítima?



VENTA DE VIERNES NEGRO PRE 2018 | BIENVENIDO A LA JOYERÍA DE
PANDORA ESPAÑA TIENDA ONLINE!

EUR ▼ SIGN IN OR REGISTRARSE

PANDORA

INICIO Charms ▼ Separadores Clips y Cadenas de Seguridad Conjuntos de Regalo Anillos
Pendientes Collares Pulseras Nueva Pandora Charms Jubilados y Joyerías Colecciones ▼



¿Somos capaces de diferenciar la página legítima?

ENVÍOS GRATUITOS PARA PEDIDOS SUPERIORES A 75€

PANDORA

Búsqueda

NOVEDADES DISNEY CHARMS PULSERAS ANILLOS PENDIENTES COLLARES COLECCIONES IDEAS DE REGALO

NUEVA COLECCIÓN

Descubre un universo de joyas inspirado en cielos azules y estrellas brillantes.

¡DESCUBRIR!

2

¿Somos capaces de diferenciar la página legítima?

 www.pandorabaratitas.es

PANDORA

Hola, se puede [Iniciar Sesión](#) [O](#) [Crear Una Cuenta](#)

Moneda: **Euro**

Buscar



 Cesta
0 artículo(s) -€0.00

[Inicio](#)

[Pandora Especial Momento](#)

[PANDORA Shine](#)

[Regalos](#)

[Encantos](#)

[Pulseras](#)

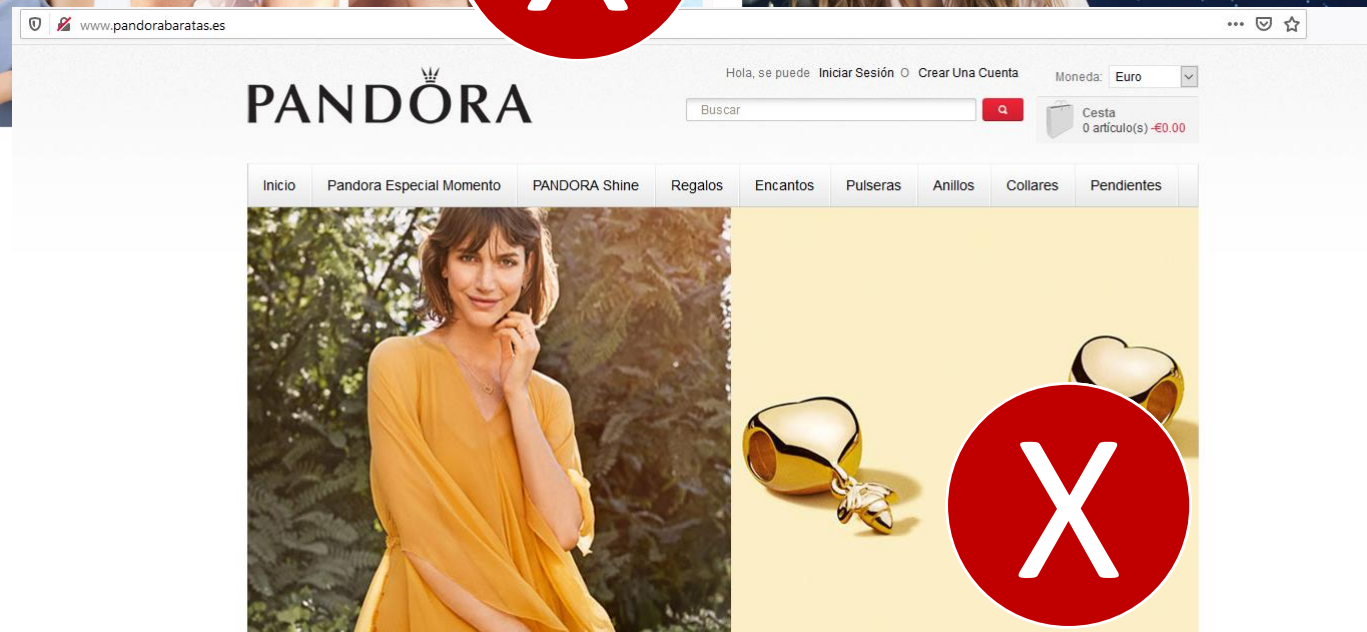
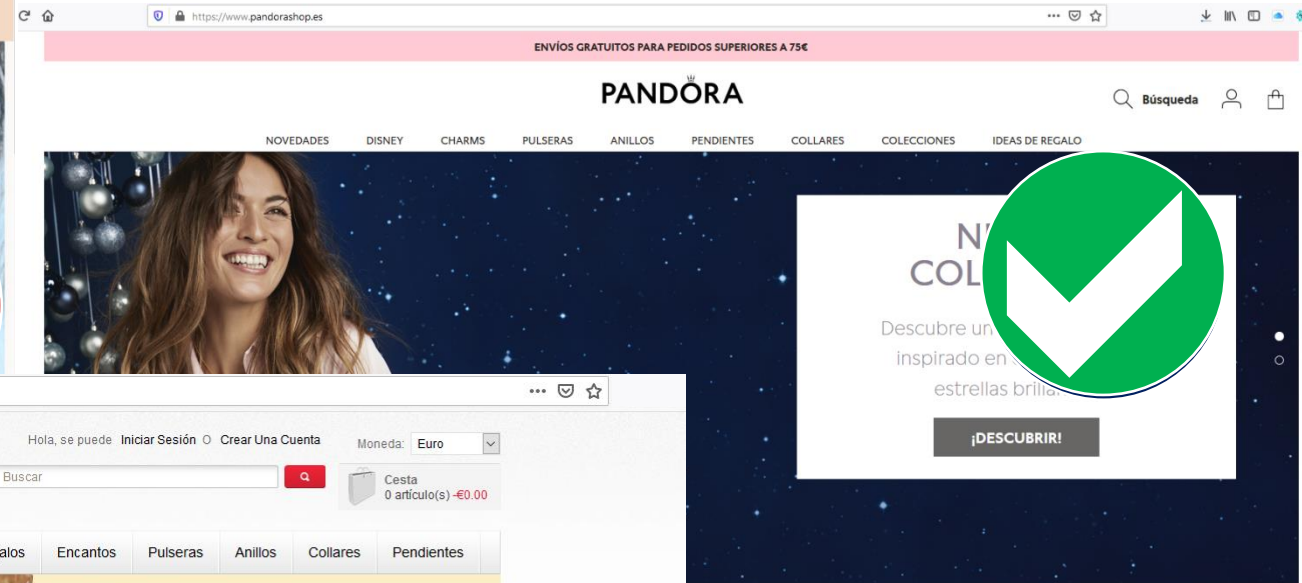
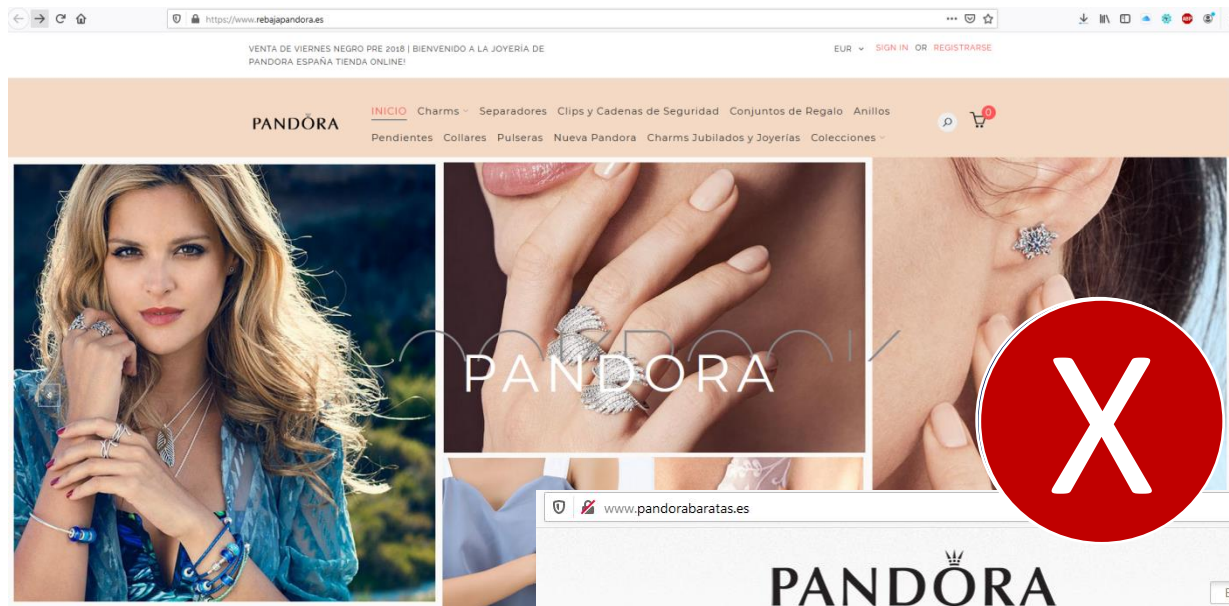
[Anillos](#)

[Collares](#)

[Pendientes](#)



¿Somos capaces de diferenciar la página legítima?



Investigando

[A simple vista]

- URLs y Certificado (sin https)
- Idioma y traducciones
- Precio excesivamente bajo
- Pago (sin https)
- Envío (desde China?)

[OSINT]

- Whois
- NS Look up (A, MX, ...)
- Ubicación geográfica
- Otras fuentes
- Tirando del hilo

PANDORA

Hola, se puede [Iniciar Sesión](#) [Crear Una Cuenta](#) Moneda: **Euro**

Buscar 

Cesta
0 artículo(s) -€0.00

[Inicio](#) [Pandora Especial Momento](#) [PANDORA Shine](#) [Regalos](#) **[Encantos](#)** [Pulseras](#) [Anillos](#) [Collares](#) [Pendientes](#)

[Inicio](#) > [Propos De Nous](#)

Productos

- ▢ Pandora Especial Momento
- ▢ PANDORA Shine
- ▢ Regalos
- ▢ Encantos
- ▢ Pulseras
- ▢ Anillos
- ▢ Collares
- ▢ Pendientes
- ▢ Pandora Abalorios

Novedades [todos]



[Comprar PANDORA SHINE REFLEXIONS ACORTAR DE](#)

Propos De Nous

Sobre Nosotros

pandorabaratass, PANDORA especialista en línea

Nuestra fórmula para el éxito es en realidad bastante simple. Nuestro personal le proporcionará el mejor servicio posible y siempre están dispuestos a hacer un esfuerzo adicional para nuestros clientes. Tratamos de proporcionar tanta información como sea posible en nuestro sitio web, pandorabaratass.es más de una tienda en línea, sino un recurso valioso tanta información como sea posible para educar a nuestros consumidores.

La satisfacción de nuestros clientes

Debido a los requerimientos de nuestros clientes están en el centro de nuestras preocupaciones, nuestro servicio de atención al cliente está disponible para contestar todas sus preguntas. Nuestro servicio post-venta se compromete a responder dentro de las 48 horas posteriores a su solicitud.

un galardonado

Nuestro deseo es desarrollar una relación privilegiada con nuestros clientes y hemos decidido premiar a todos nuestros clientes. Nuestro programa permite que todos puedan beneficiarse de diferentes descuentos.

Realmente valoramos a nuestros clientes y gracias por tomarse el

Investigando

[A simple vista]

- URLs y Certificado (sin https)
- Idioma y traducciones
- Precio excesivamente bajo
- Pago (sin https)
- Envío (desde China?)

[OSINT]

- Whois
- NS Look up (A, MX, ...)
- Ubicación geográfica
- Otras fuentes
- Tirando del hilo

PANDORA

Hola, se puede [Iniciar Sesión](#) [Crear Una Cuenta](#) Moneda: **Euro**

Buscar 

Cesta
0 artículo(s) -€0.00

[Inicio](#) [Pandora Especial Momento](#) [PANDORA Shine](#) [Regalos](#) [Encantos](#) [Pulseras](#) [Anillos](#) [Collares](#) [Pendientes](#)

[Inicio](#) > [Página 3](#)

Productos

- ▢ Pandora Especial Momento
- ▢ PANDORA Shine
- ▢ Regalos
- ▢ Encantos
- ▢ Pulseras
- ▢ Anillos
- ▢ Collares
- ▢ Pendientes
- ▢ Pandora Abalorios

Novedades [todos]



Página 3

1. ¿Es mi pedido en su camino hacia mí?
Cuando su pedido ha sido enviado, usted recibirá un correo electrónico de confirmación con el número de seguimiento. Haga clic en el vínculo para ubicar el paquete. Tenga en cuenta que usted no será capaz de realizar un seguimiento de su pedido hasta el día después de recibir la información de seguimiento.

2. ¿Cómo puedo realizar un seguimiento de mi pedido?
Cuando usted realiza un pedido y se envía, recibirá un correo electrónico con el número de seguimiento. Utilice el número de seguimiento para localizar su paquete ya sea en el sitio o sitio web de seguimiento EMSExpress. Tenga en cuenta que usted no será capaz de realizar un seguimiento de su pedido hasta el día después de recibir la información de seguimiento.

3. ¿Dónde se entrega?
Sí, enviamos sus mercancías en todo el mundo a través del servicio postal, que por lo general toma alrededor de una semana para entregar lo que se ha aprobado la solicitud.

4. ¿Cuál es el volumen de suministro?
La livraison standard coûte €8 et sera livré dans les 12-15 jours ouvrables, à condition que le paiement est reçu avant 14 heures le jour où la commande est passée. S'il vous plaît noter la livraison gratuite ne sont pas disponibles lors d'une promotion. Toutes mes excuses pour toute déception.

Pedidos de más de € 69 califican para la entrega libre estándar.
Debe introducir un código en la caja. **GRATIS** El envío estándar será aplicado automáticamente cuando pasas € 69 ó más. Tenga en cuenta que esta oferta no se aplica a los códigos postales, no podemos entregar a.

5. Lo entrega urgente?
Entrega de correo cuesta 15 € y su pedido se entregará el siguiente día laborable 3, siempre que el pago se recibe 14 horas antes del día de la realización del pedido.
Ejemplos:

Investigando

[A simple vista]

- URLs y Certificado (sin https)
- Idioma y traducciones
- Precio excesivamente bajo
- Pago (sin https)
- Envío (desde China?)

[OSINT]

- Whois
- NS Look up (A, MX, ...)
- Ubicación geográfica
- Otras fuentes
- Tirando del hilo

www.pandorabaratitas.es/shopping_cart.html

Hola, se puede [Iniciar Sesión](#) [Crear Una Cuenta](#) Moneda: Euro

Buscar

Cesta 1 artículo(s) -€10.00

[Inicio](#) [Pandora Especial Momento](#) [PANDORA Shine](#) [Regalos](#) **[Encantos](#)** [Pulseras](#) [Anillos](#) [Collares](#) [Pendientes](#)

[Inicio](#) > Carro de Compra [\[Ayuda \(?\)\]](#)

Su carro de compra contiene:

Total de Artículos: 1 Peso: 150lbs Cantidad: €10.00

Cant.	Artículo	Precio	Total
1	 Comprar AZUL RIPPLES ENCANTO	€10.00	€10.00

Subtotal: €10.00

[Continuar comprando](#) [Actualice el pedido](#)

Los clientes que regresan [Login/Registrar](#)

dirección De Envío

Nombre: *

Apellidos: *

E-mail: *

Teléfono: *

Dirección: *

Localidad: *

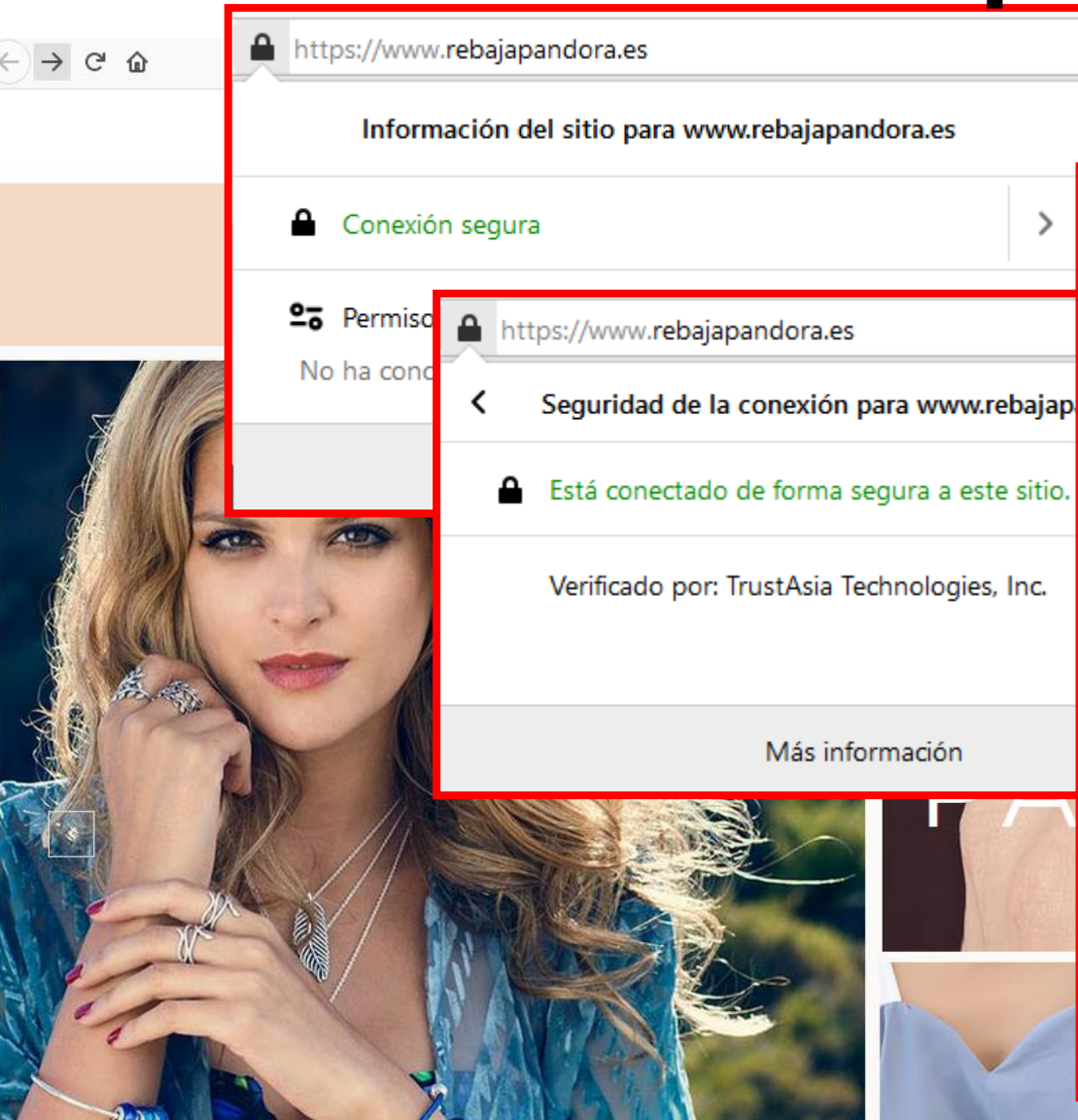
Provincia: *

Método De Envío

☐ DHL :Plazo de entrega: 3-7 días  €15.00
(La Compañía no asume los derechos de aduana, por supuesto, la posibilidad de carga arancelaria es del 5%, Las tarifas de las aduanas:15-30 Euro, en caso de desacuerdo, por favor elegir otras formas de envío) Envío a

☒ China Post :Plazo de entrega: 20-25 días  €8.90
(El tiempo de transporte es muy largo, pero el coste de envío más barato, y las costumbres no cobrará ninguna tarifa) Envío a

Certificados sospechosos



Alternativas para localizar más webs

9d89048d5a9c80de88101d0d0c766b1363bc37c689764c923f5ae0b5e



Q Certificates

5406a289d89048d5a9c80de88101d0d0c766b1363bc37c689764c923f5ae0b5e

C



Certificate Trust CT ZLint PEM

Raw Data Explore

Basic Information

Subject DN CN=rebajapandora.es

Issuer DN C=CN, O=TrustAsia Technologies, Inc., OU=Domain Validated SSL, CN=TrustAsia TLS RSA CA

Serial 20822975852889255748620273115233613284

Validity 2019-07-27 00:00:00 to 2020-07-26 12:00:00 (365 days, 12:00:00)

Names rebajapandora.es
www.rebajapandora.es

Fingerprint

SHA-256 5406a289d89048d5a9c80de88101d0d0c766b1363bc37c689764c923f5ae0b5e

SHA-1 f893040a0efb7eaf04d0d211cb789a993504f5bf

MD5 71b5ebba2ce3b23c689bf128a34721f4

Public Key

Browser Trust

Apple Browser Trusted

Microsoft Browser Trusted

Mozilla NSS Browser Trusted

Key Usage and Constraints

Key Usage Digital Signature, Key Encipherment

Ext. Key Usage Client Auth, Server Auth

Alternativas para localizar más webs

%29+and+parent_spki_subject_fingerprint%3A+96c647304bad78a67abc93bbb49856473c1c08e22f108605d4c5cec568bea94e



Q Certificates

(nike) and parent_spki_subject_fingerprint: 96c647304bad78a67abc93bbb49856473c1c08e22f108605d4c5cec568bea94e

C

[Results](#) [Report](#) [Docs](#)

Quick Filters

For all fields, see [Data Definitions](#)

Tag:

- 30 CT
- 30 DV
- 30 Google CT
- 30 Leaf
- 23 Currently Trusted

[More](#)

Issuer:

- 30 TrustAsia Technologies, Inc.

Certificates

Page: 1/2 Results: 30 Time: 926ms Query Plan: [expanded](#)

CN=cheap-nike-free.com

TrustAsia TLS RSA CA
 2019-10-09 – 2020-10-08
 cheap-nike-free.com, www.cheap-nike-free.com
 parent_spki_subject_fingerprint: 96c647304bad78a67abc93bbb49856473c1c08e22f108605d4c5cec568bea94e

CN=cheap-nike-free.com

TrustAsia TLS RSA CA
 2019-10-09 – 2020-10-08
 cheap-nike-free.com, www.cheap-nike-free.com
 parent_spki_subject_fingerprint: 96c647304bad78a67abc93bbb49856473c1c08e22f108605d4c5cec568bea94e

CN=nike-star-shoes.com

TrustAsia TLS RSA CA
 2019-10-09 – 2020-10-08

Investigando

[A simple vista]

- URLs y Certificado (sin https)
- Idioma y traducciones
- Precio excesivamente bajo
- Pago (sin https)
- Envío (desde China?)

[OSINT]

- Whois
- NS Look up (A, MX, ...)
- Ubicación geográfica
- Otras fuentes
- Tirando del hilo

Whois Record for Pandorabarat.es

Domain Profile

Registrar Status	taken
Name Servers	AIDA.NS.CLOUDFLARE.COM CHIP.NS.CLOUDFLARE.COM
Tech Contact	—
IP Address	104.28.4.230 - 551 other
IP Location	 - Texas - Dallas - Carrollton
ASN	 AS13335 CLOUDFLARENET
Hosting History	2 changes on 3 unique

Website

Website Title	Pandora Joyas
Server Type	cloudflare
Response Code	200
Terms	460 (Unique: 204, L
Images	14 (Alt tags missing
Links	155 (Internal: 142,

Whois Record (last updated on 2019-11-07)

% NOTE: The registry for this domain name does not have any whois records (whois records) in the standard format. This information represents the most likely status of the domain based on the information provided by the Internet's domain

domain: pandorabarat.es
status: taken
nameserver: aida.ns.cloudflare.com
nameserver: chip.ns.cloudflare.com

% For more information, please visit <http://www.nic.es/>



Español | Català | Euskera | Galego | English



Síguenos en:



Buscar...



INICIO

BUSCA Y REGISTRA
TU DOMINIO

AGENTES
REGISTRADORES

TODO LO QUE
NECESITAS SABER

GESTIONA TU
DOMINIO

ACTUALIDAD Y
NOTICIAS

SOBRE
NOSOTROS



Información de Dominio

Volver

Los datos de contacto de este dominio están ocultos. Si desea comunicarse con el Titular y el PCA pulse [aquí](#)

DATOS DEL TITULAR

Nombre del Dominio **pandorabarat.es**
Estado **Activado**
Identificador **E44409-ESNIC-F5**
Titular **eric walter**
Fecha de Alta **28-10-2016**
Fecha de Caducidad **28-10-2020**
Agente Registrador **REGISTRAR.EU**

PERSONA DE CONTACTO ADMINISTRATIVO

Identificador **12D3F26-ESNIC-F5**
Nombre **Matthias Gerber**

PERSONA DE CONTACTO TECNICO

Identificador **12D3F26-ESNIC-F5**
Nombre **Matthias Gerber**

SERVIDORES DNS

Nombre Servidor
chip.ns.cloudflare.com
aida.ns.cloudflare.com

IP



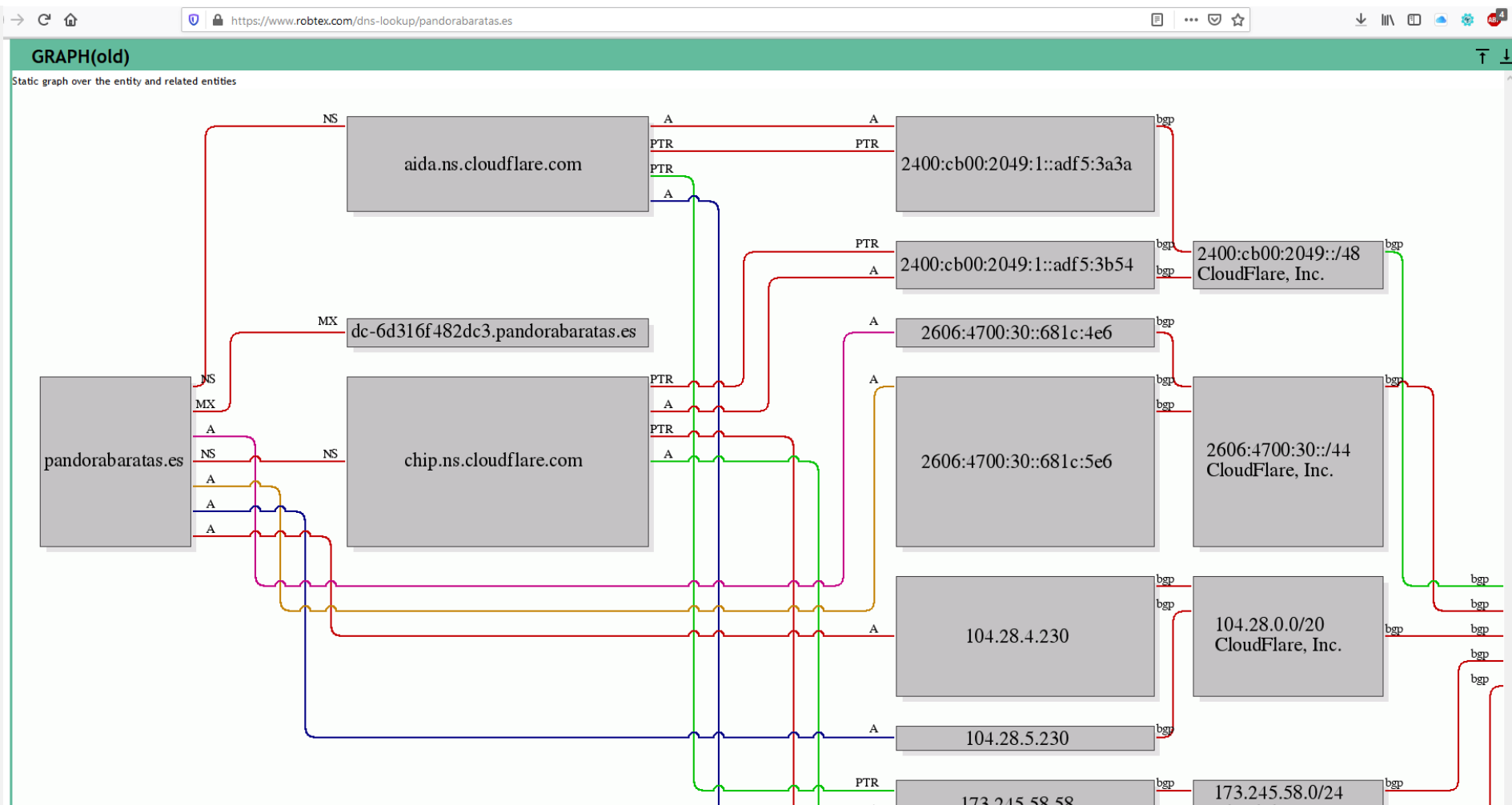
Investigando

[A simple vista]

- URLs y Certificado (sin https)
- Idioma y traducciones
- Precio excesivamente bajo
- Pago (sin https)
- Envío (desde China?)

[OSINT]

- Whois
- NS Look up (A, MX, ...)
- Ubicación geográfica
- Otras fuentes
- Tirando del hilo



<https://www.robtext.com/dns-lookup/pandorabarat.es>

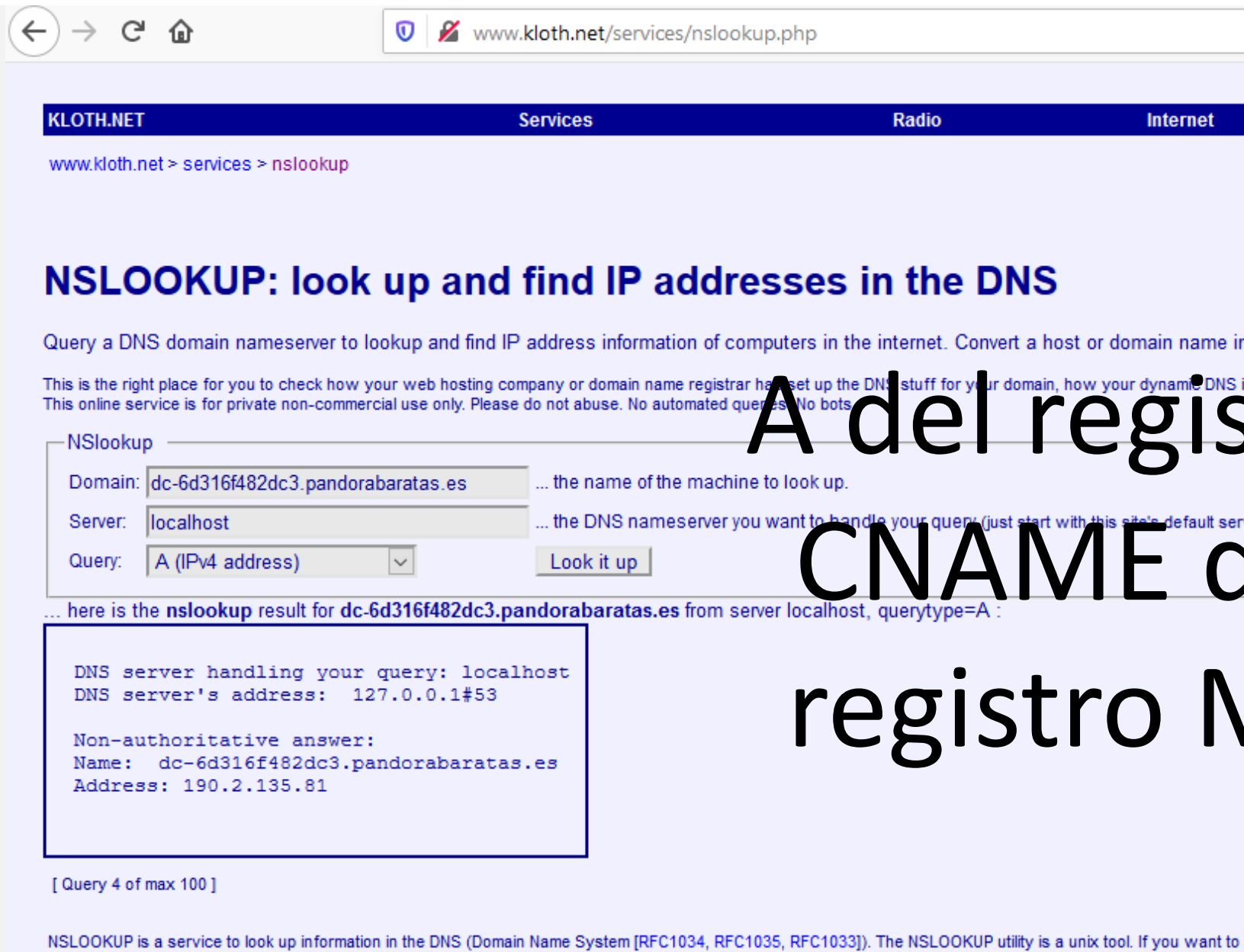
Investigando

[A simple vista]

- URLs y Certificado (sin https)
- Idioma y traducciones
- Precio excesivamente bajo
- Pago (sin https)
- Envío (desde China?)

[OSINT]

- Whois
- NS Look up (A, MX, ...)
- Ubicación geográfica
- Otras fuentes
- Tirando del hilo



The screenshot shows a web browser window with the address bar displaying `www.kloth.net/services/nslookup.php`. The page has a dark blue header with the text "KLOTH.NET" and navigation links for "Services", "Radio", and "Internet". Below the header, the breadcrumb path `www.kloth.net > services > nslookup` is shown. The main heading is "NSLOOKUP: look up and find IP addresses in the DNS". A descriptive paragraph explains the service's purpose: "Query a DNS domain nameserver to lookup and find IP address information of computers in the internet. Convert a host or domain name in... This is the right place for you to check how your web hosting company or domain name registrar has set up the DNS stuff for your domain, how your dynamic DNS is... This online service is for private non-commercial use only. Please do not abuse. No automated queries. No bots." The "NSlookup" form contains three input fields: "Domain:" with the value `dc-6d316f482dc3.pandorabaratatas.es`, "Server:" with the value `localhost`, and "Query:" with a dropdown menu set to "A (IPv4 address)". A "Look it up" button is to the right of the query field. Below the form, a text line reads "... here is the nslookup result for dc-6d316f482dc3.pandorabaratatas.es from server localhost, querytype=A :". A blue-bordered box contains the following text: "DNS server handling your query: localhost", "DNS server's address: 127.0.0.1#53", "Non-authoritative answer:", "Name: dc-6d316f482dc3.pandorabaratatas.es", and "Address: 190.2.135.81". At the bottom of the page, it says "[Query 4 of max 100]" and a footer note states "NSLOOKUP is a service to look up information in the DNS (Domain Name System [RFC1034, RFC1035, RFC1033]). The NSLOOKUP utility is a unix tool. If you want to k".

A del registro
CNAME del
registro MX

Investigando

[A simple vista]

- URLs y Certificado (sin https)
- Idioma y traducciones
- Precio excesivamente bajo
- Pago (sin https)
- Envío (desde China?)

[OSINT]

- Whois
- NS Look up (A, MX, ...)
- Ubicación geográfica
- Otras fuentes
- Tirando del hilo

https://hackertarget.com/reverse-ip-lookup/

HACKER TARGET

SCANNERS TOOLS RESEARCH SERV

Reverse IP Lookup

Perform a **reverse IP lookup** to find all **A records** associated with an IP address. The results can pinpoint virtual hosts being served from a v expand the attack surface when identifying vulnerabilities on a server.

dc-6d316f482dc3.pandorabaratatas.es

FIND DNS A RECORDS FROM IP

```
dc-0012c36ee44d.pandoranecklacesale.com
dc-0019bc39b240.pandoraofertas2019.es
dc-001a9db5165e.squadrenba.com
dc-009aca8206bd.nikenbastore.es
dc-00cd7cf585e1.maillotnba2018pascher.fr
```

<https://api.hackertarget.com/reverseiplookup/?q=190.2.135.81>

Busqueda inversa a partir de la IP



dc-00039b79da0b.replicasdecamisetas2019.com	dc-6fac9537e5c3.chaussuredefootnikepascher.fr
dc-0012c36ee44d.pandoranecklacesale.com	dc-6fb6833a0de5.nbaitaliastore.it
dc-00155ed46740.camisetasfutbolthai2019.com	dc-70295c5e178e.itscarpedacalcio.it
dc-0019bc39b240.pandoraofertas2019.es	dc-706985f62cd8.complementospulserapandora.com
dc-001a9db5165e.squadrenba.com	dc-70707c1dde4e.nouveaumagliettapolo.it
dc-00873c41a0ff.nikecramponpascher.fr	dc-7081874f1b3a.tuttocalcio2021.it
dc-009aca8206bd.nikenbastore.es	dc-70d9e66d4305.magliecalcioshop2019.it
dc-00cd7cf585e1.maillotnba2018pascher.fr	dc-70eafc7403f2.chaussurerunningasics.fr
dc-00e70277d155.magliettapoloralphlauren.it	dc-71056f90c393.silverbraceletssale.com
dc-01211779c3d3.2018chaussuredefoot.fr	dc-713e9beedf8a.zapatillasdedeportes.es
dc-0136a395fafb.nbasquadre.it	dc-7189164e5ee0.pandorapulsera.es
dc-0141683368bf.canottenbashop.it	dc-7201fbb7d059.pandoracuir.fr
dc-0164832a3c13.pandoraheartcharm.com	dc-72219451f19a.camisetareplicas.es
dc-01893ebddcc5.equiperestonnes.com	
dc-01bb388d6570.camisetasbaratas2020.es	
dc-02083ef05aa9.tiendasdefutbolonline2020.com	
dc-0276d9c3f375.cramponnikepascher.fr	
dc-02af13eecefd.equipacionesbarata2020.es	
dc-02c909045338.maillotnbapascher2019.fr	
dc-0375e0820d02.magliacalcio2019.it	
dc-03a7c92c3c51.tiendasdefutbolonline2020.com	
dc-03afacdff683.pandorasmckenbilligt.se	
dc-03d4fa13fb7c.pandoraswedishcharms.se	

Usando Google dorks

Google search results for "https://www.google.com/search?source=hp&ei=jA3FXe2pLKSGjLs" showing results for Nike backpacks on imanews.es.

imanews.es / Nike

Envío gratis en pedidos superiores a 59 €

Posición

Resultados: 20

Image	Product Name	Price
	NIKE SPORTSWEAR MOCHILA BLACK	19,75 €
	NIKE SPORTSWEAR HERITAGE LABEL - MOCHILA OUTDOOR GREEN/MINERAL	17,63 €
	NIKE SPORTSWEAR HERITAGE - MOCHILA OBSIDIAN/BLACK	21,17 €
	NIKE SPORTSWEAR MOCHILA TEAM ORANGE/BLACK	21,19 € 31,77 €
	NIKE SB MOCHILA DESERT	35,33 € 77,70 €
	NIKE SPORTSWEAR AF-1 BACKPACK - MOCHILA GUNSMOKE/THUNDER GREY	28,26 € 56,50 €

Usando Google dorks

Ofertas de 2018 - Preci...

blox.es

didasonline.es/#

EUR SIGN IN REGISTRARSE

Inicio Adidas ZX Flux Adidas Stan Smith Adidas Gazelle Adidas Superstar Adidas EQT Adidas NMD Adidas Yeezy Boost Adidas Ultra Boost

EQT CUSHION ADV
ADIDAS ORIGINALS

NUEVOS PRODUCTOS

Finalizar Compra Acceder

tienda... **Buscar**

€0.00
0 items

AIR JORDAN BAG: (0)

to Nike Online Outlet Store

Simulador de Ciberseguridad

Usando Google dorks

blox.es

futbolreplicas2019.es

Ofertas de 2019 - Dracis Barata

comprazapatillasoutlet.es



Currency: euro - EUR Welcome to Nike Online Outlet Store

Mi cuenta | Mi carrito | Finalizar Compra | Acceder

Buscar en toda la tienda... **Buscar**

INICIO SPORTS NIKE AIR MAX NIKE FREE TRAINING NIKE LUNAR NIKE SB NIKELAB HUARACHE AIR JORDAN **BAG: (0)**

KISS MY AIRS. KISS MY AIRS. KISS MY AIRS. BOOT UP

Michael Jordan

MJ 23

MICHAEL JORDAN



Usando Google dorks

Ofertas de 2018 - Precio Barato x

joyasbaratas2020

blox.es

INICIO Adidas Nike AJ Under Armour Puma Sneakers

Wish list (0) €0.00 0 items

Porsche Design Sport X Adidas Bounce S4 Leather Zapatillas - Hombre - Gunmet/Black B34167
146,41€ 58,01 €

Balenciaga Triple S Trainer Zapatillas De Running - Unisexo - Gris/Rojo-Azul
124,31€ 53,40 €

Classic Vans Sk8-Hi Trainers - Unisexo - Armada
93,00€ 41,43 €

UA Curry 2.5 Journey To Excellence Pack Sun Wukong Zapatillas De Baloncesto - Hombre - Negro 1288403-750
132,60€ 53,40 €

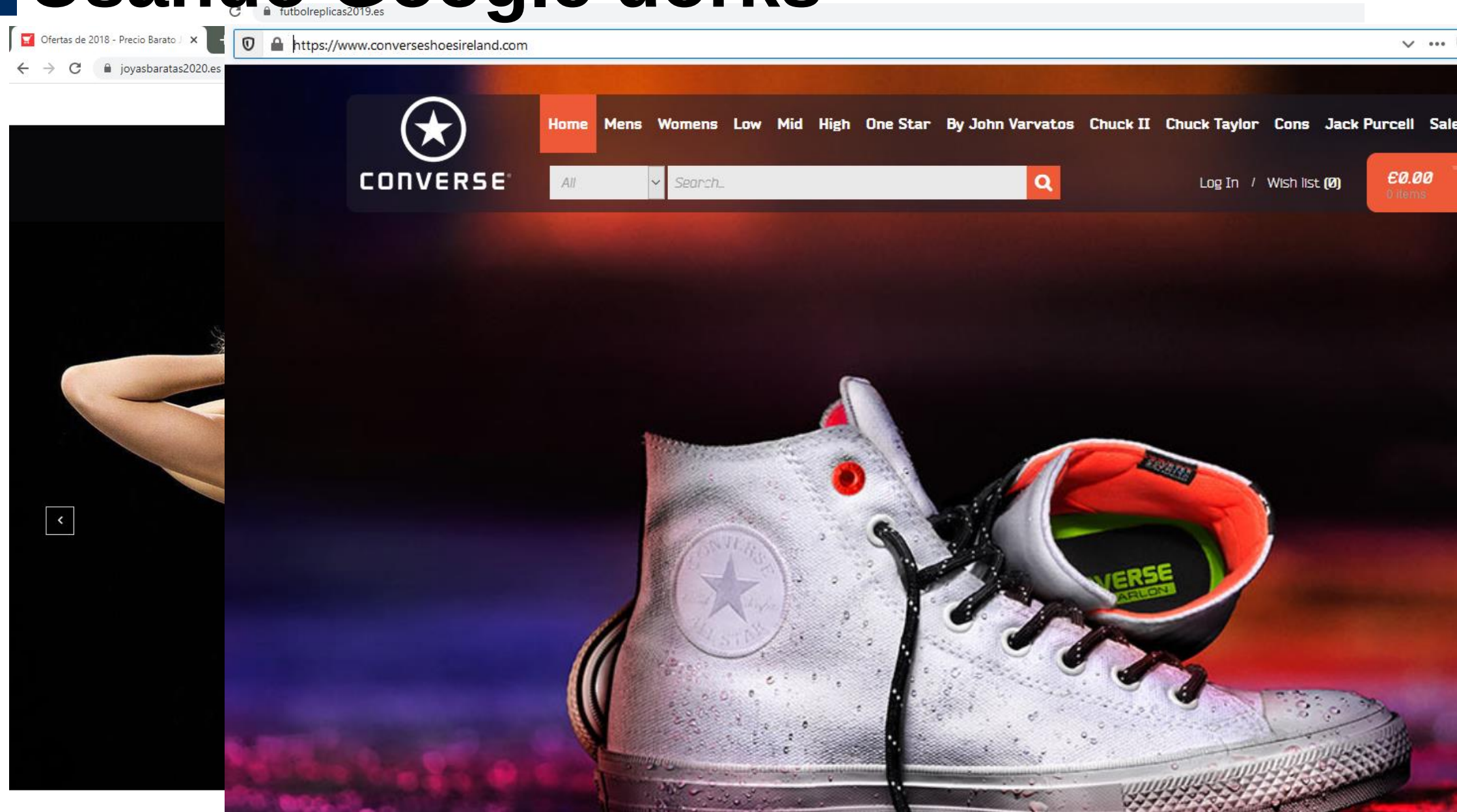
SPLY-350

Asics Gel-Lyte III

Adidas Originals

Adidas Originals

Usando Google dorks



Investigando

[A simple vista]

- URLs y Certificado (sin https)
- Idioma y traducciones
- Precio excesivamente bajo
- Pago (sin https)
- Envío (desde China?)

[OSINT]

- Whois
- NS Look up (A, MX, ...)
- Ubicación geográfica
- Otras fuentes
- Tirando del hilo

en.utrace.de/?query=dc-6d316f482dc3.pandorabaratatas.es

utrace*

IP address or domain:

dc-6d316f482dc3.pandorabaratatas.es

Search

[English | Deutsch]

The domainname "dc-6d316f482dc3.pandorabaratatas.es" is located in the following region:



Curacao, la isla de colores
lavanguardia.com



5 espectaculares playas en Curacao - National Ge...
ngenespanol.com



Curacao, un paraíso de 30 playas
eluniversal.com.mx



Qué hacer y ver en Curacao | Playas de Curaz...
aviatur.com



Curacao es un destino paradisíaco en el Caribe...
elcomercio.com



Qué hacer y ver en Curacao | Playa...
aviatur.com



Foto de Renaissance Curacao Resort &...
tripadvisor.com.mx



CURACAO (Willemstad) - Super guía para prep...
cruceadictio.com



Curacao, un paraíso de 30 playas
eluniversal.com.mx



Curacao, la isla de colores
lavanguardia.com

¿Es posible hacer una atribución?

Browser tabs: 登陆到 Webmin, i7.RU - Регистрация доменов, X, .es Información de Dominio

Address bar: No es seguro | 190.2.135.81:10000

**Webmin**

您必须输入账号和密码以登录服务器
190.2.135.81

 用户名

 密码

☐ 记住我

 登录



Marcas involucradas que presentan acciones legales

Case: 1:22-cv-02323 Document #: 1 Filed: 05/04/22 Page 5 of 17 PageID #:5

1,525,782		For: hosiery, footwear, t-shirts, sweat shirts, tank tops, pajamas, sport shirts, belts, nightshirts, stocking caps, warm-up or jogging suits, jackets, bibs, head bands and wrist bands in class 025. For: entertainment services, namely, organizing and conducting basketball exhibitions in class 041.
1,715,549		For: jewelry; namely, wrist watches, pins, earrings, necklaces, rings, cuff links and belt buckles in class 014.
1,966,924		For: clothing, namely hosiery, footwear, t-shirts, sweat shirts, sweatpants, pants, tank tops, jerseys, shorts, pajamas, sport shirts, rugby shirts, sweaters, belts, ties, nightshirts, hats, warm-up suits, jackets, parkas, coats, cloth bibs, head bands, wrist bands, aprons, boxer shorts, slacks, caps, ear muffs, and gloves in class 025.
2,157,039		For: clothing, namely, hosiery, footwear, sweat shirts, sweatpants, pants, tank tops, jersey, shorts, pajamas, sport shirts, rugby shirts, sweaters, belts, ties, nightshirts, warm-up suits, parkas, coats, cloth bibs, head bands and wrist bands in class 025.
2,079,493		For: clothing, namely, hosiery, footwear, sweat shirts, sweatpants, pants, tank tops, jerseys, shorts, pajamas, sport shirts, rugby shirts, sweaters, belts, ties, nightshirts, warm-up suits, parkas, coats, cloth bibs, head bands and wrist bands in class 025.
5,237,767		For: Jewelry; costume jewelry; beaded jewelry; rubber or silicon wristbands in the nature of a bracelet, beaded necklaces; beads for use in the manufacture of jewelry; earrings, necklaces, rings, bracelets, cuff links, pendants, charms for collar jewelry and bracelets; clocks; watches; watch bands and watch straps, watch cases, watch fobs; jewelry boxes, tie clips; medallions; non-monetary coins of

Case: 1:22-cv-02323 Document #: 1 Filed: 05/04/22 Page 6 of 17 PageID #:6

		precious metal; precious metals; key chains of precious metal; key chains as jewelry; figures and figurines of precious metal; trophies of precious metals in class 014.
--	--	--

The above U.S. registrations for the NBA Trademarks are valid, subsisting, in full force and effect, and many are incontestable pursuant to 15 U.S.C. § 1065. The registrations for the NBA Trademarks constitute *prima facie* evidence of their validity and of NBAP's exclusive right to use the NBA Trademarks pursuant to 15 U.S.C. § 1057(b). True and correct copies of the Federal Trademark Registrations for the above NBA Trademarks are attached hereto as Exhibit 1.

8. The NBA brand of professional basketball and NBA Trademarks are widely known to and enormously popular with both sports fans and the general public. NBAP has promoted and advertised the NBA, the NBA Teams and NBA Trademarks extensively for many years. NBA Trademarks are among the most renowned and immediately recognizable marks in professional sports today. As a result of substantial advertising, promotion and media attention, and NBAP's extensive licensing and sponsorship program for a wide variety of goods and services, NBA Trademarks have acquired secondary meaning and represent significant goodwill of great value to NBAP, the NBA and the NBA Teams.

9. Hundreds of millions of fans have attended NBA games and related events, enjoyed television and radio broadcasts of NBA games and related events, and purchased merchandise bearing NBA Trademarks to identify with their favorite NBA Teams. Millions visit <NBA.com>, the official NBA website, as well as the official websites of the individual NBA Teams, which prominently display, and in many cases are accessed by domain names containing,

Fuente: <http://gbcinternetenforcement.net/21-5521/>

Comercios counterfight de falsificaciones

NBA Properties, Inc. v. The Partnerships and Unincorporated Associations Identified on Schedule "A"
- Case No. 22-cv-2323

Schedule A

Defendant Online Marketplaces		
No	URL	Name / Seller Alias
1	augjewelry.en.alibaba.com	Quanzhou Aug Jewelry Trading Co., Ltd
2	caoshi.en.alibaba.com	Yiwu Cao Shi Electronic Commerce Co., Ltd
3	cnsportgear.en.alibaba.com	Shishi Zaojiu Garment Business Firm
4	commodity2008.en.alibaba.com	Yiwu Ebey Commodity Factory
5	cy2018.en.alibaba.com	Yiwu Chenyao E-Commerce Firm
6	fscraft.en.alibaba.com	Yiwu Fanshu E-Commerce Firm
7	huahang01.en.alibaba.com	Yiwu Huahang Import And Export Co., Ltd.
8	linghu2021.en.alibaba.com	Yiwu Linghu Trading Co., Ltd
9	lvjewelry.en.alibaba.com	Zhangpu Duxun Town Gutong Apparel Shop
10	pjjewelry.en.alibaba.com	Yiwu Pengjin Jewelry Co., Ltd.
11	salinca.en.alibaba.com	Yiwu Salinca Import And Export Co., Ltd.
12	selabrity.en.alibaba.com	Haifeng Selabrity Jewelry Co., Ltd.
13	xhanmiao.en.alibaba.com	Yiwu Hanmiao Trading Co., Ltd.
14	xinsiding.en.alibaba.com	Shenzhen Xinsiding Technology Co., Ltd.
15	yiwumiaoyi.en.alibaba.com	Yiwu Miaoyi Jewelry Factory
16	yiwuweikang.en.alibaba.com	Yiwu Wei Kang Medical Instruments Co., Ltd
17	aliexpress.com/store/2944259	The Lord of championship Rings Store
18	aliexpress.com/store/3755016	VERFANS Store
19	aliexpress.com/store/5367142	OATHBIRD-DIY Store
20	aliexpress.com/store/5722101	Miqiao boutique a Store
21	aliexpress.com/store/5876249	Shop5876249 Store
22	aliexpress.com/store/910568419	Stephen Mattei Trading Store
23	aliexpress.com/store/911114258	YANGTAI COLLECTON Store
24	aliexpress.com/store/911765020	no name store Store
25	aliexpress.com/store/911783287	Alina ornament Store
26	aliexpress.com/store/911798884	China Lafayette Store
27	aliexpress.com/store/912020380	Cullinan Store
28	aliexpress.com/store/912164467	xiaomingtongxue Store
29	aliexpress.com/store/912258387	Shion Sportswear Store
30	aliexpress.com/store/912341668	Championship ring Store
31	aliexpress.com/store/5879640	Shop5879640 Store
32	aliexpress.com/store/910341067	Saalort Official Store
33	amazon.com/sp?seller=A10VZCL1YCGHBH	The Huge Fan

Case: 1:22-cv-02323 Document #: 31 *SEALED* Filed: 05/11/22 Page 13 of 15 PageID #:2713

110	ebay.com/usr/shjd-86	shjd-86
111	ebay.com/usr/tpu4_10	tpu4_10
112	ebay.com/usr/wdiao92	wdiao92
113	ebay.com/usr/weifenmaoyig	weifenmaoyig
114	ebay.com/usr/xiaosarensheg10-9	xiaosarensheg10-9
115	ebay.com/usr/yalwa42	yalwa42
116	ebay.com/usr/zhangq_80	zhangq_80
117	ebay.com/usr/zmi8-71	zmi8-71
118	ebay.com/usr/giganxxc	giganxxc
119	wish.com/merchant/5d416e0d0ff7f9662fe1b665	yilingchen
120	wish.com/merchant/5e705ae87e53210bc0bec102	Pippadfgdgsrffgsfvdsv
121	wish.com/merchant/607bb1fea659d579a25a2f4a	binlinbu
122	wish.com/merchant/60b7b64a936d5f3bdf68ee8a	AntipordaMaria
123	jerseyoutfits.ecrater.com	jerseyoutfits.ecrater.com
124	bestjerseys.ru	bestjerseys.ru
125	esaltuning.com	esaltuning.com
126	Foxapparels.com	Foxapparels.com
127	Funnyds.com	Funnyds.com
128	htysportsgood.com	htysportsgood.com
129	jerseysfamily.com	jerseysfamily.com
130	jerseysoccer.online	jerseysoccer.online
131	kobesjersey.com	kobesjersey.com
132	lewanoshop.com	lewanoshop.com
133	minejerseys.ru	minejerseys.ru
134	nbacamisetas.top	nbacamisetas.top
135	nbaclothesstore.com	nbaclothesstore.com -2
136	nbafanjersey.org	nbafanjersey.org
137	nbasalejersey.net	nbasalejersey.net
138	nbasalejersey.org	nbasalejersey.org
139	nbastoresingapore.com	nbastoresingapore.com
140	prudentsport.store	prudentsport.store
141	ringofchamp.com	ringofchamp.com
142	soccerdealshop.cn	soccerdealshop.cn

Defendant Domain Names		
No	URL	Name / Seller Alias
143	nbaapparel2022.com	nbaapparel2022.com

13

Case: 1:22-cv-02323 Document #: 31 *SEALED* Filed: 05/11/22 Page 14 of 15 PageID #:2714

144	nbabestvest.com	nbabestvest.com
145	nbajerseysales2022.com	nbajerseysales2022.com
146	nbajerseyss.com	nbajerseyss.com
147	nbaonlinemall.com	nbaonlinemall.com
148	nbaretrojersey.com	nbaretrojersey.com
149	aaduyr.top	aaduyr.top
150	aafcad.xyz	aafcad.xyz
151	aafdor.xyz	aafdor.xyz
152	aafzpb.best	aafzpb.best
153	aahaop.best	aahaop.best
154	aahjnt.xyz	aahjnt.xyz
155	aahwop.best	aahwop.best
156	aajqou.best	aajqou.best
157	aakfrt.xyz	aakfrt.xyz
158	aakgot.shop	aakgot.shop
159	aapdop.best	aapdop.best
160	aapfkp.best	aapfkp.best
161	aaqest.shop	aaqest.shop
162	aaqhop.shop	aaqhop.shop
163	aarkuh.shop	aarkuh.shop
164	aarsmt.xyz	aarsmt.xyz
165	aataub.best	aataub.best
166	aatbwu.best	aatbwu.best
167	aatwop.best	aatwop.best
168	aatxqw.best	aatxqw.best
169	aatyou.best	aatyou.best
170	aatznp.best	aatznp.best
171	aazjcb.shop	aazjcb.shop
172	aazsgy.shop	aazsgy.shop
173	basketballjerseys2022.com	basketballjerseys2022.com
174	basketballshorts2022.com	basketballshorts2022.com
175	bbdert.best	bbdert.best
176	bbjdet.top	bbjdet.top
177	bbjhyt.top	bbjhyt.top
178	bbjnz.shop	bbjnz.shop
179	bbjwab.best	bbjwab.best
180	bbjxot.best	bbjxot.best
181	bbpzw.best	bbpzw.best
182	bbtpbj.best	bbtpbj.best
183	bbtgyc.best	bbtgyc.best
184	bbtucw.best	bbtucw.best
185	bbtvop.best	bbtvop.best

14

Índice

- 01 Conceptos esenciales
- 02 Sobre Elena
- 03 Un ejemplo real: Counterfeit en comercios web
- 04 Un ejemplo de caso de investigación en Elena
- 05 Seguridad Operativa en actividades de cibervigilancia
- 06 Inteligencia de imágenes
- 07 Dorking con buscadores genéricos
- 08 Dorking con buscadores especializados
- 09 Reportando y entregando el producto
- Anexos



Los personajes



Julio

Julio Sánchez
CEO de Tiendas Online S.A.

Se que han comprometido nuestra empresa, pero no se ni quién ni por qué querrían hacerlo. Quiero estado y una solución urgente.

He encargado a Diego la investigación del incidente. Como acaba de llegar a la compañía, se coordinará junto con el equipo de Cyber Warriors para averiguar lo sucedido.

Elena Olimpia
Equipo de seguridad de TOSA

Me han notificado que nos han podido comprometer, pero no tengo más que un Tweet que hace alusión al ataque. Se está haciendo revuelo en más medios, parece una amenaza real y lo he escalado.



Elena



Diego Pérez
CISO de Tiendas Online S.A

Acabo de incorporarme a la empresa en el mejor momento, el anterior director de seguridad ha muerto de un infarto.

Necesito identificar los activos de la compañía y descubrir por dónde han podido atacarnos cuanto antes. Este ataque esta teniendo mucha repercusión.

CCN Warrior
Investigadores de inteligencia

Equipo designado que descubrirá lo que ha pasado y aportará un breve resumen al CISO, el cual a su vez lo transmitirá al CEO.

Los datos de partida son escasos, ¿el nombre de la empresa? ¡Vaya! Nos espera un gran trabajo por delante, el mismo que ya han hecho nuestros atacantes.



Diego



CCN-Warrior

El guión

Diego, me han llegado noticias de que nos han comprometido
¿Cómo de grave es el asunto?



Julio

Julio, parece haber evidencias después de una primera aproximación, de que nuestras **tiendas online están comprometidas** y no sabemos si ha sido por un posible **correo de phishing** qué parece haber recibido tu secretaria Anabel.



Diego

Me preocupa el correo por los datos sensibles de la empresa que hayan podido obtener los atacantes, pero sobre todo la seguridad y datos personales de nuestros clientes. Por favor, mantenme informado.

El guión

Hola CCN-Warrior, me han llegado referencias de que sois los mejores en este tipo de investigaciones. Nos han comprometido y no sabemos ni por dónde han podido acceder, ni si están patrocinados por algún gobierno o son universitarios curiosos. Nuestro presidente esta muy preocupado, ¿nos podéis ayudar?



Diego

Diego, tenemos el equipo perfecto para darte solución a este problema. **¿Qué datos tenemos de partida?**



CCN-Warrior

Acabo de incorporarme a la empresa y solo os puedo proporcionar el **nombre, Tiendas Online S.A.** Buscad posibilidades emulando a los atacantes reales para encontrar la información exfiltrada y los puntos débiles que han podido ser explotados.

Nos ponemos a ello, no son muchos datos la verdad, pero usaremos la ciberinteligencia para llegar al fondo de la cuestión. ¿Disponemos de alguna pista más?

También ha llegado a mis oídos que se están vendiendo productos a mitad de precio en tiendas alternativas, que parecen ser pagados con puntos de fidelización de TOSA que han podido ser sustraídos a los clientes.

Adicionalmente, hay claras sospechas de un correo de phishing abierto por Anabel, la secretaria del presidente.

Punto de partida

1

Qué tenemos

- Nombre de una de las empresas del grupo.
- Indicios de puntos de fidelización sustraídos.
- Comercios online con nuestros productos a mitad de precio.
- Indicios de correo de phishing abierto por una empleada.

2

Qué buscamos

- Resto de empresas del grupo para conocer su exposición.
- Sus dominios asociados, direcciones IP, servidores de correo para reducir la superficie de búsqueda de credenciales, etc.
- Activos a nombre de la empresa, servidores, rangos de red, etc.
- Tiendas que estén suplantando nuestra marca y vendiendo productos para blanquear puntos de fidelidad.
- Credenciales y datos confidenciales expuestos.
- Otros datos que puedan ser de interés para un atacante.

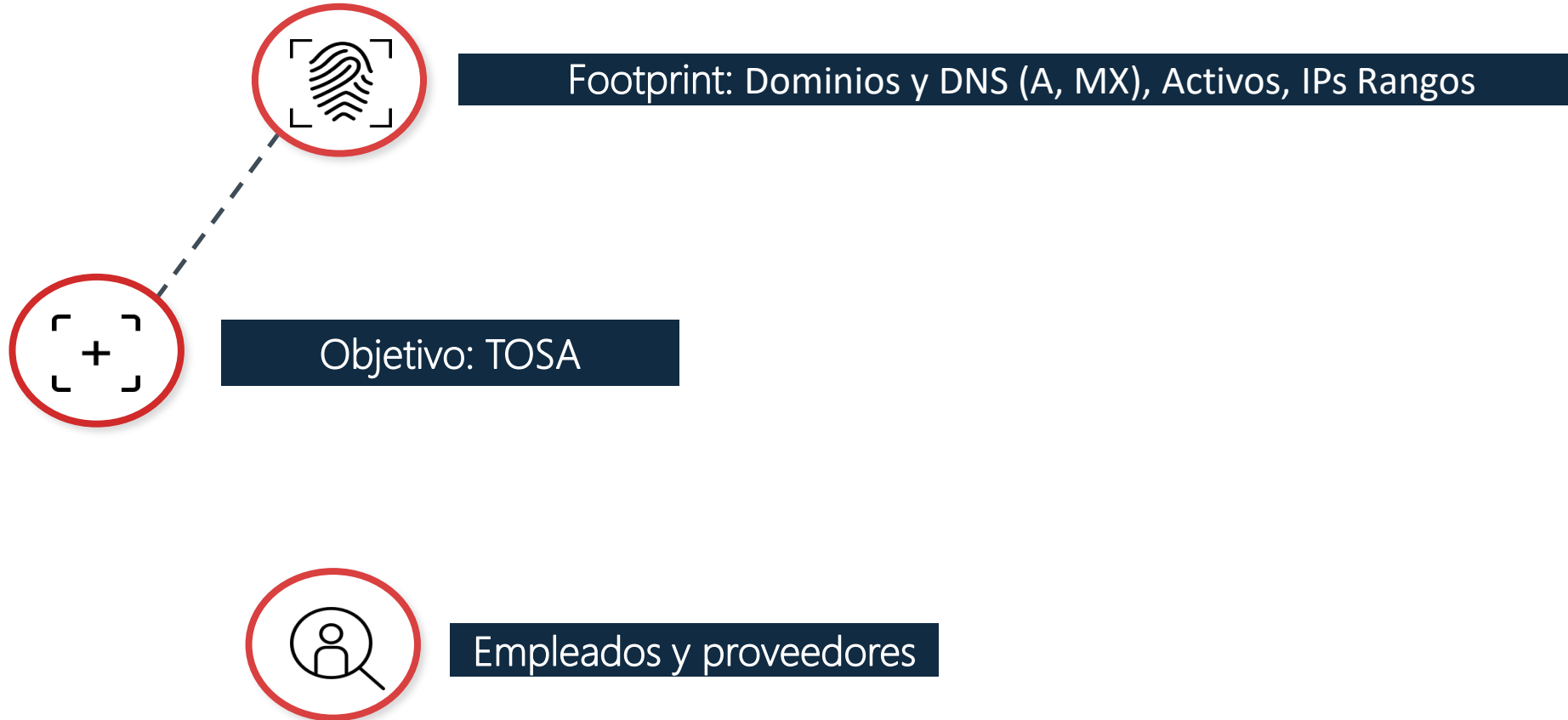
3

Qué necesitamos

- Documentar nuestros hallazgos. Informar adecuadamente de los descubrimientos al interlocutor adecuado.

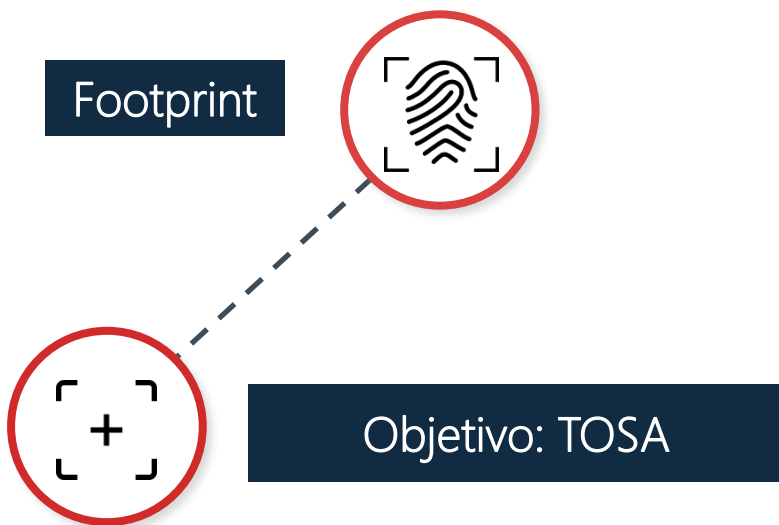


¿Por donde empezamos a investigar?



Explorando el objetivo con OSINT

Dominios y DNS (A, MX), Activos, IPs Rangos



Localizando fuentes de datos



Se observa una imagen con el mapa mundi de los diferentes órganos de gestión de direcciones de internet como son RIPE, ARIN, LACNIC, APNIC, AFRINIC y descargas de datos de diferentes fuentes

Repositorio de datos: RIPE

<https://ftp.ripe.net/ripe/dbase/>

Index of /ripe/dbase

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
RIPE.CURRENTSERIAL	20-Jan-2017 00:00	8	
ripe.db.gz	20-Jan-2017 01:20	336M	
split/	20-Jan-2017 00:00	-	

<https://ftp.ripe.net/ripe/dbase/split/>

Index of /ripe/dbase/split

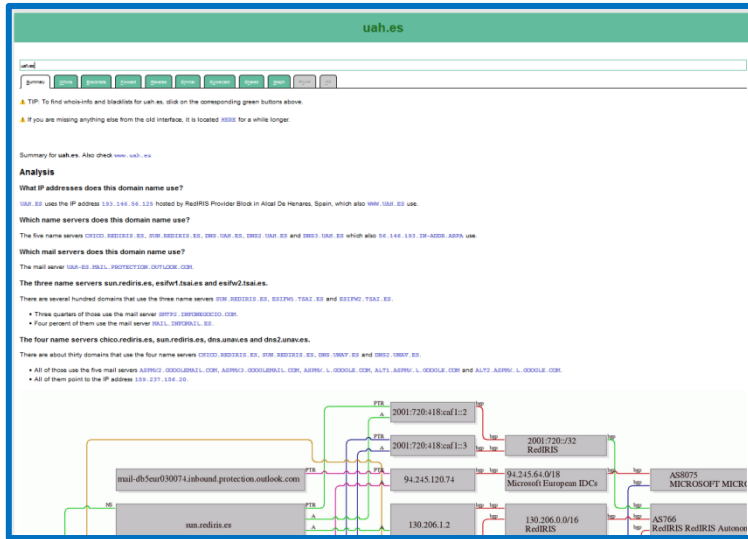
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
ripe.db.as-block.gz	20-Jan-2017 01:20	9.4K	
ripe.db.as-set.gz	20-Jan-2017 01:20	2.0M	
ripe.db.aut-num.gz	20-Jan-2017 01:20	7.5M	
ripe.db.domain.gz	20-Jan-2017 01:20	10M	

Contenido de archivo parcial **ripe.db.inetnum.gz**

```
root@prometheus002:~/taller_ciberseg# cat ripe.db.inetnum
#
# The contents of this file are subject to
# RIPE Database Terms and Conditions
#
# http://www.ripe.net/db/support/db-terms-conditions.pdf
#
inetnum:      80.16.151.184 - 80.16.151.191
netname:      NETECONOMY-MG41731
descr:        TELECOM ITALIA LAB SPA
country:      IT
admin-c:      DUMY-RIPE
tech-c:       DUMY-RIPE
status:       ASSIGNED PA
notify:       neteconomy.rete@telecomitalia.it
mnt-by:       INTERB-MNT
created:      1970-01-01T00:00:00Z
last-modified: 2001-09-21T22:08:01Z
source:       RIPE
remarks:      *****
remarks:      * THIS OBJECT IS MODIFIED
remarks:      * Please note that all data that is generally regarded as personal
remarks:      * data has been removed from this object.
remarks:      * To view the original object, please query the RIPE Database at:
remarks:      * http://www.ripe.net/whois
remarks:      *****
```

Se presentan los listados de directorio de RIPE con los datos agregados o por separado así como una captura del fichero principal de RIPE.

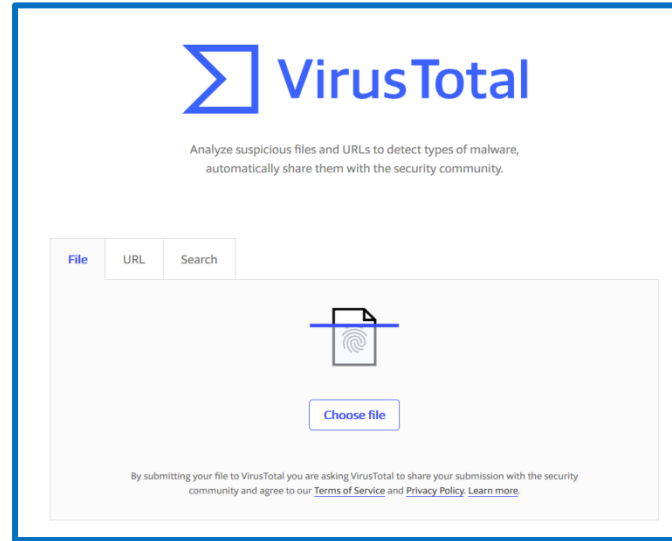
Escogiendo las herramientas adecuadas



robtex.com

Herramienta pasiva que proporciona información relacionada con direcciones IP, dominios, subdominios, DNS, servidores de correo y blacklist.

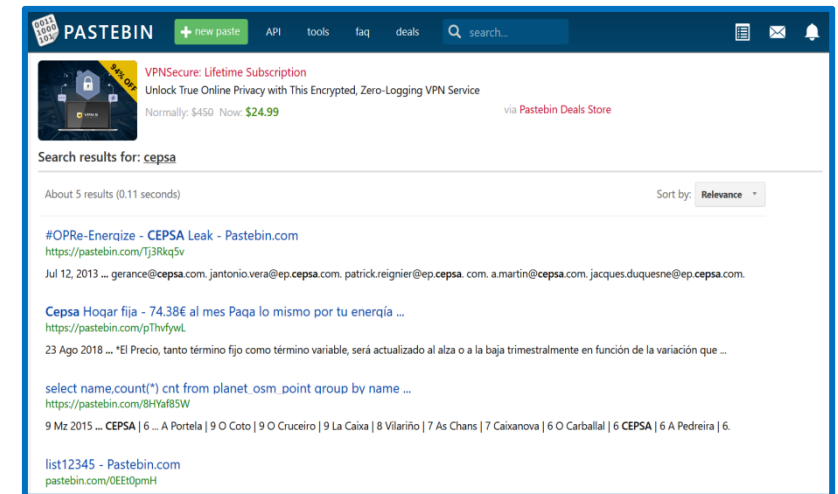
Input Dominio, IP, Rango IP o ASN



virustotal.com

Permite analizar ficheros, URLs, dominios, IP o Hashes para descubrir presencia Malware.

Input URL, Dominio, IP, Hash, Fichero

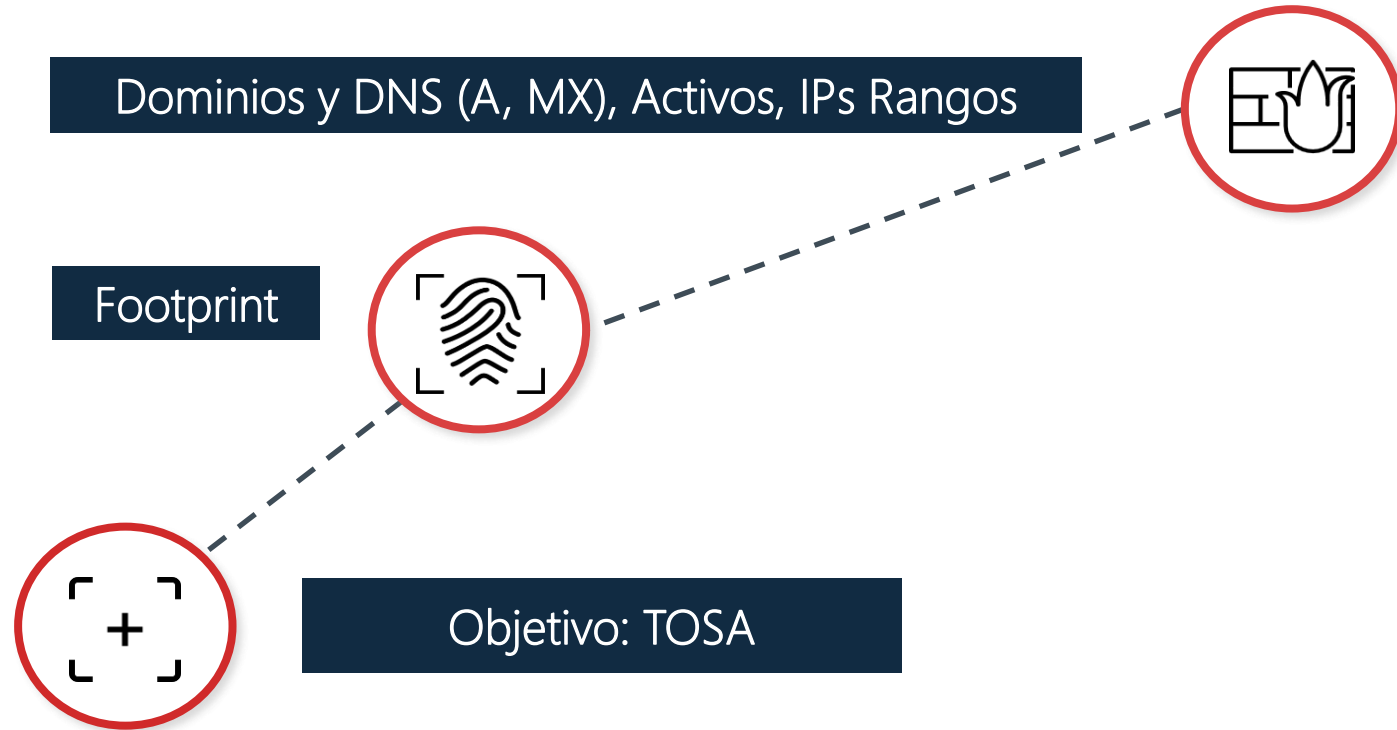


pastebin.com

Permite buscar fugas de Información publicadas.

pastebin.com/search?q=XXXXX

Explorando nuestro objetivo





Comenzando la investigación web

1

Qué tenemos

- Pagina web o dominio.

2

Qué buscamos

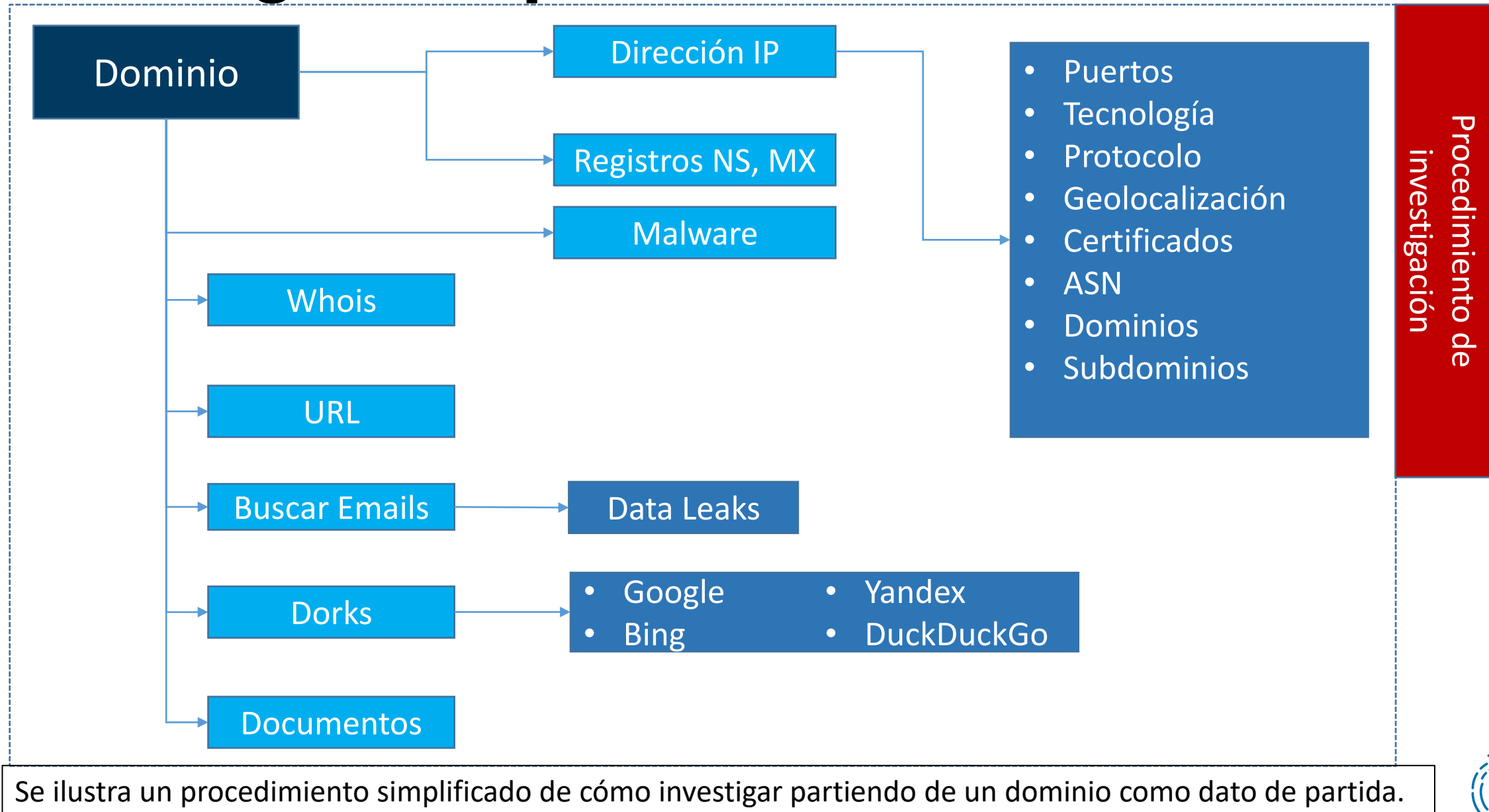
- Dirección IP a la que apunta el dominio e información asociada a la IP como tecnología que hay detrás, protocolo usado, geolocalización, certificados, ASN, subdominios y otros dominios disponibles.
- Registros DNS (NS, MX) y URLs
- Muestras de malware asociados al dominio, si las hubiera.
- Documentos públicos asociados al dominio.
- Credenciales, datos confidenciales expuestos y otros datos que puedan ser de interés para un atacante.
- Evidencias a modo de históricos de la web en el tiempo.

3

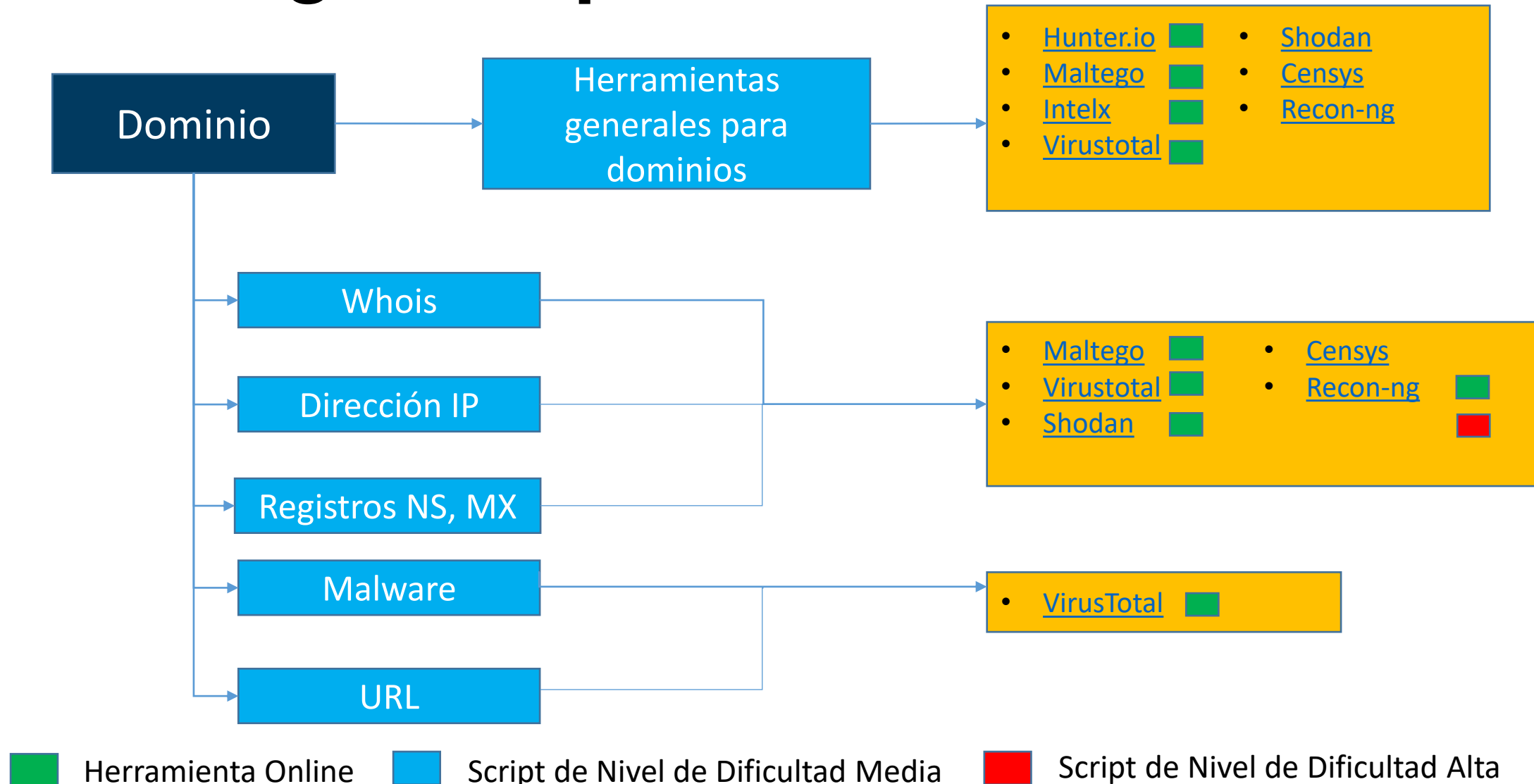
Qué necesitamos

- Establecer las herramientas que podemos usar, tanto de pago como open source.
- Crear herramientas adicionales si las herramientas disponibles no se adaptan a nuestras necesidades.
- Usar la metodología y ciclo de inteligencia para coleccionar y analizar los datos.
- Documentar nuestros hallazgos y generar información de valor relacional.

Investigación partiendo de un dominio

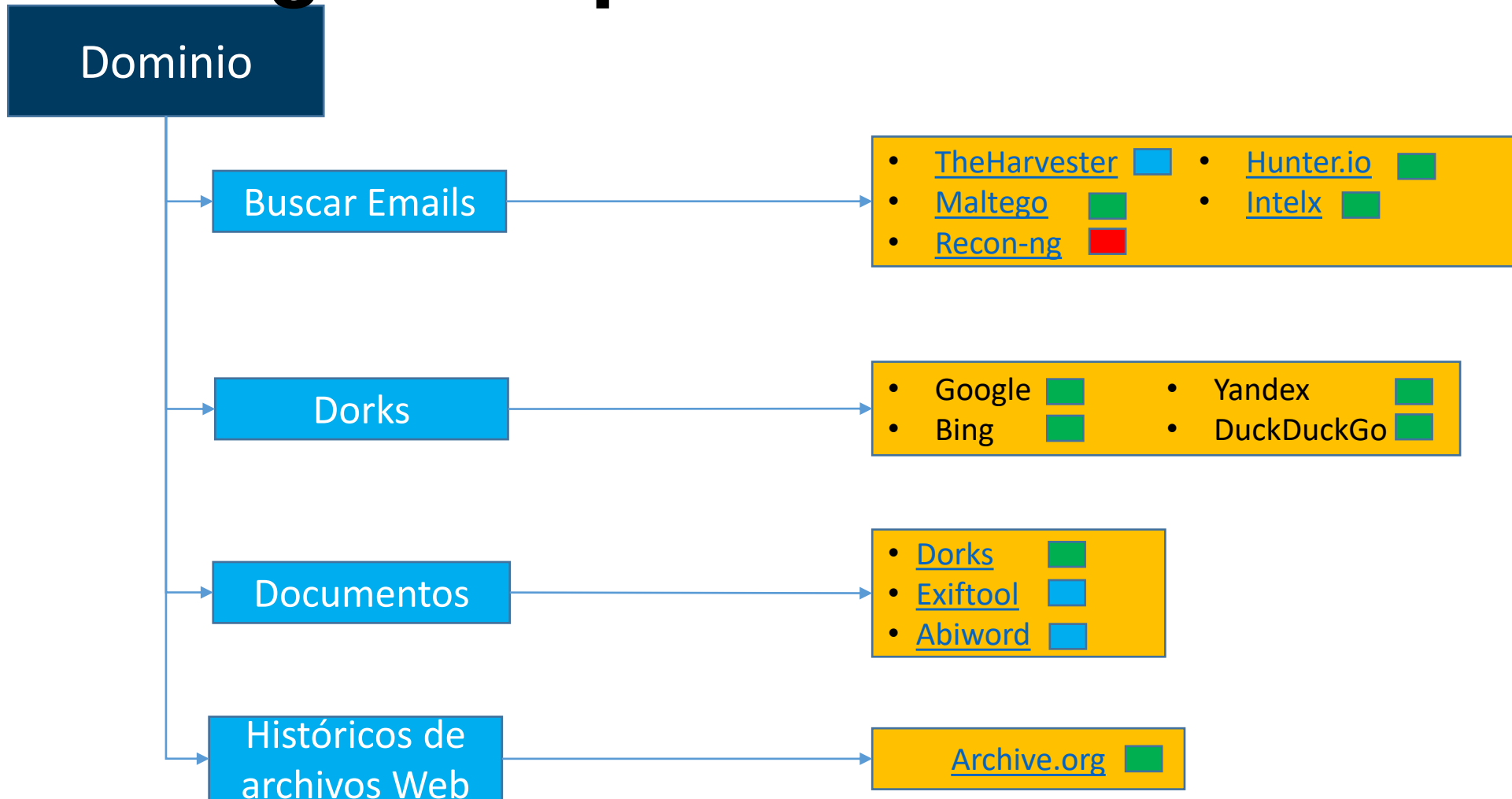


Investigación partiendo de un dominio



Se ilustra un procedimiento simplificado de cómo investigar partiendo de un dominio como dato de partida.

Investigación partiendo de un dominio



Herramienta Online Script de Nivel de Dificultad Media Script de Nivel de Dificultad Alta

Se ilustra un procedimiento simplificado de cómo investigar partiendo de un dominio como dato de partida.

Herramienta: SpiderFoot HX

The screenshot displays the SpiderFoot HX web interface. At the top, there's a navigation bar with icons for Scan, Investigate, Monitor, and Configure, along with a 'System' dropdown. Below this, the target 'BadGuys, Inc.' is shown with a 'FINISHED' status, 32348 elements, 138 correlations, and a duration of 9:05:37. A toolbar includes buttons for Overview, Correlations, Browse by..., Visualise..., Scan Settings, and Logs, along with a search bar. The main table lists data sources with columns for Risky, Unique, Total, and % of Data.

◆ Data Source	◆ Risky	◆ Unique	◆ Total	◆ % of Data
Target Website	2	8546	16569	51%
DNS	150	2073	4203	13%
Whois	0	504	2033	6%
Ahmia	1425	1502	1512	5%
CommonCrawl	0	343	960	3%
RIPE	0	624	1102	3%
Social Media	0	897	914	3%
Github	0	483	517	2%
SHODAN	53	255	505	2%
VirusTotal	47	105	496	2%

Input:

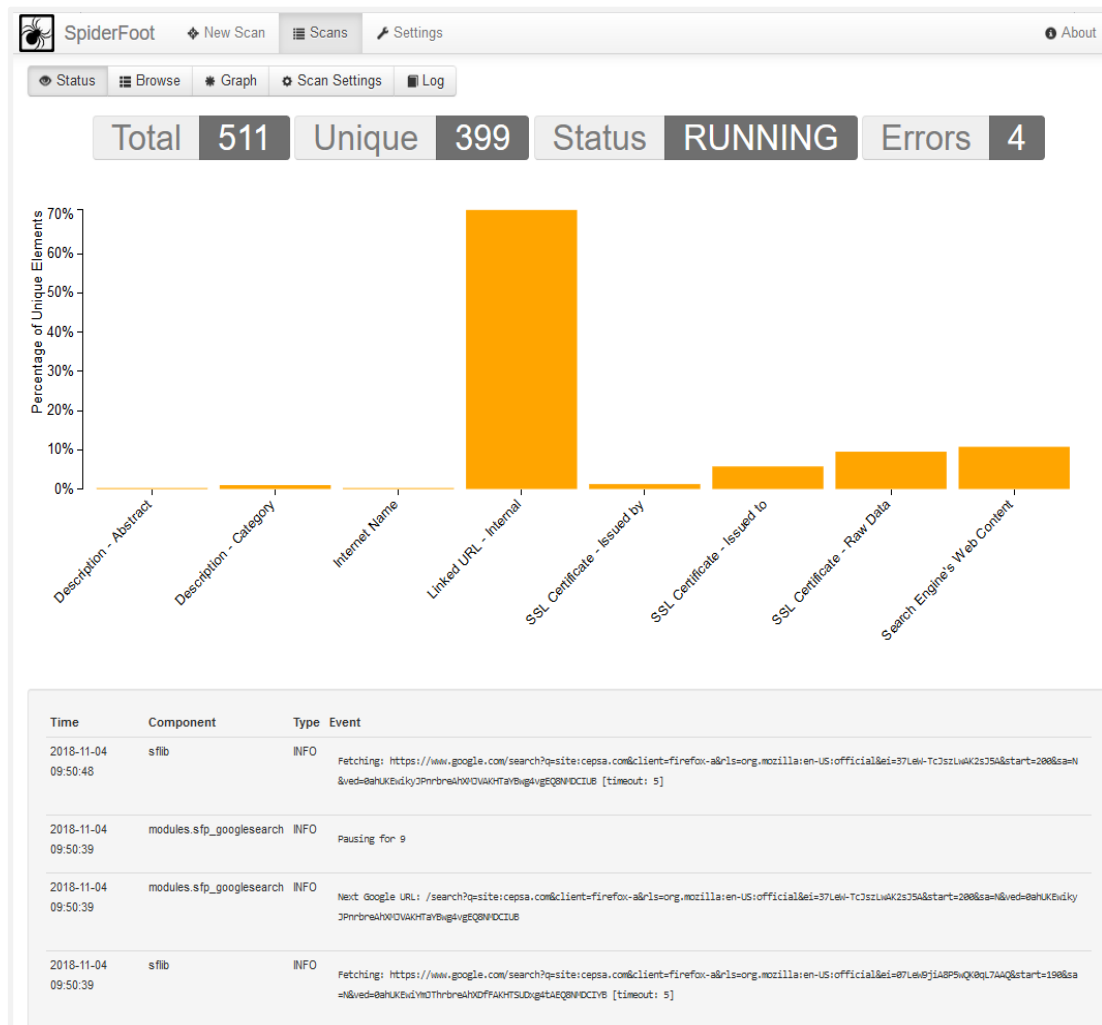
- Dominio
- Subdominio
- IP
- Rango IP
- ASN
- Email
- Username

Se muestran los resultados ofrecidos por SpiderFoot a la búsqueda de un screenshot

SpiderFoot HX – Versión Online

<https://www.spiderfoot.net/hx/>

Herramienta: SpiderFoot Local



SpiderFoot es una herramienta OSINT enfocada a la recopilación de información, permitiendo seleccionar el tipo de investigación mediante fuentes concretas, tipos de datos o caso de uso. Integra multitud de fuentes, tanto privadas como públicas, de manera modular.

Ejemplo de escaneo de un objetivo

OJO: Puede realiza búsquedas activas que dejan trazas

Input:

- Dominio
- Subdominio
- IP
- Rango IP
- Email

Herramienta: SpiderFoot Local

Versión Open Source Instalable

<https://github.com/smicallef/spiderfoot>

Instalación:

- git clone <https://github.com/smicallef/spiderfoot>
- pip3 install -r requirements.txt

Ejecución:

- source spiderfoot/bin/activate
- cd spiderfoot/spiderfoot
- python3 sf.py -l 127.0.0.1:5001

```
(spiderfoot) analista@ubuntu:~/Escritorio/curso/spiderfoot/spiderfoot$ python3 sf.py -l 127.0.0.1:5001
Starting web server at 127.0.0.1:5001 ...

*****
Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:5001
*****

[01/Aug/2020:12:06:23] ENGINE Listening for SIGTERM.
[01/Aug/2020:12:06:23] ENGINE Listening for SIGHUP.
[01/Aug/2020:12:06:23] ENGINE Listening for SIGUSR1.
[01/Aug/2020:12:06:23] ENGINE Bus STARTING
[01/Aug/2020:12:06:23] ENGINE Serving on http://127.0.0.1:5001
[01/Aug/2020:12:06:23] ENGINE Bus STARTED
```

Arranque y ejecución
de spiderfoot

Herramienta: Intelx



IntelligenceX ofrece un repositorio donde consultar datos relacionados sobre leaks, dominios, emails, direcciones IP, usernames, VINs, Hashes, número de teléfonos, perfiles sociales, etc.

Input: Dominio, URL, IP, Email, Rango IP

[Advanced](#)

Filters:

Settings: Sorted by Most Relevant

Categories

Date

Settings

Buckets

☐ Pastes PRO

☐ Darknet: Tor PRO

☐ Darknet: I2P PRO

☐ WikiLeaks

☐ Public Leaks

☐ Dumpster

☐ Whois PRO

Areas

☐ Web: North Korea

☐ Web: Russia

☐ Web: Germany

☐ Government: Russia

Your account has preview access. Upgrade [here](#).

<https://intelx.io/>

Se muestra el buscador de intelx para parametrizar la propia búsqueda consultando un dominio, URL, IP, Email, Rango IP, Dirección de bitcoin

Información de dominios con theHarvester

TheHarvester es una herramienta que permite recopilar información sobre un objetivo de manera pasiva, usando los motores de búsquedas de Bing, Google, Yahoo, Baidu, además de Shodan, ThreatCrowd, y de manera mas activa, realizando Fuerza Bruta DNS. Se pueden obtener emails, subdominios, IPs, nombre de perfiles de usuario en redes sociales.

<https://github.com/laramies/theHarvester>

Instalación:

```
git clone https://github.com/laramies/theHarvester
cd theHarvester
pip3 install -r requirements/base.txt
```

Comando:

```
sudo docker run theharvester -d marca.com -l 300 -b
all > result.txt
```

Input: Dominio



Listado de
Emails

Listado de
Subdominios e IPs

Listado de nombres de
usuarios de Redes Sociales

```
*****
*
* theHarvester
*
* TheHarvester Ver. 2.7
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****

Usage: theharvester options

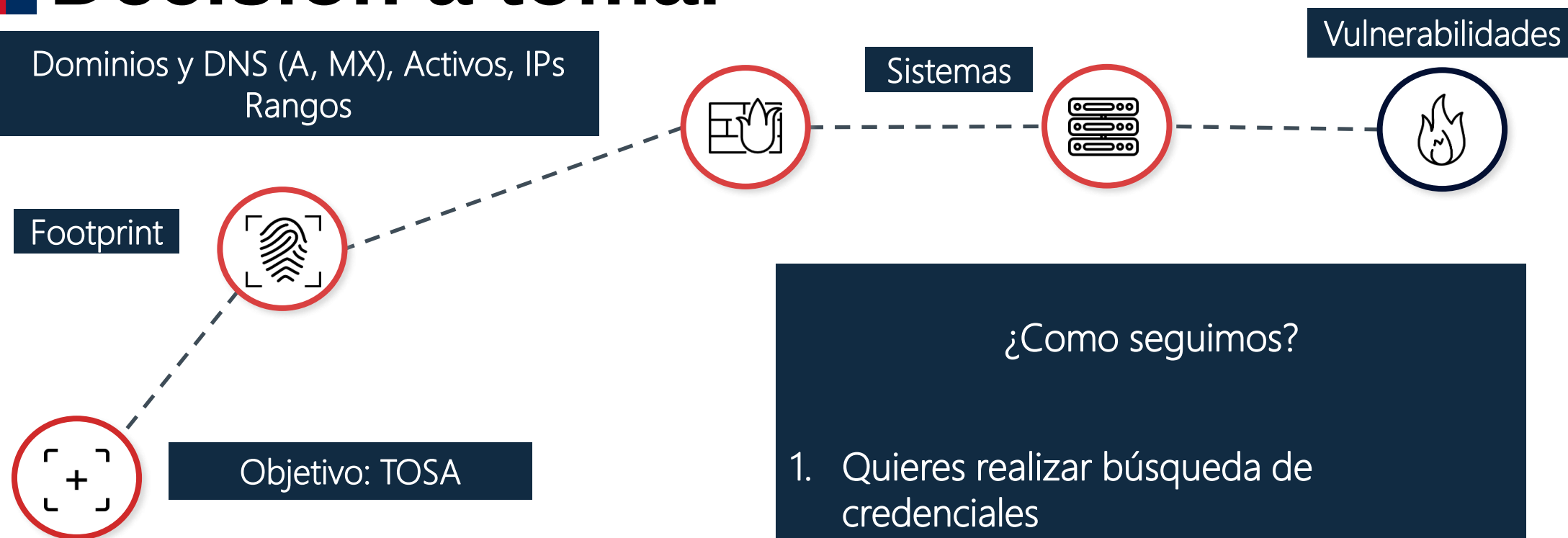
-d: Domain to search or company name
-b: data source: baidu, bing, bingapi, dogpile, google, googleCSE,
    googleplus, google-profiles, linkedin, pgp, twitter, vhost,
    yahoo, all

-s: Start in result number X (default: 0)
-v: Verify host name via dns resolution and search for virtual hosts
-f: Save the results into an HTML and XML file (both)
-n: Perform a DNS reverse query on all ranges discovered
-c: Perform a DNS brute force for the domain name
-t: Perform a DNS TLD expansion discovery
-e: Use this DNS server
-l: Limit the number of results to work with(bing goes from 50 to 50 results,
    google 100 to 100, and pgp doesn't use this option)
-h: use SHODAN database to query discovered hosts

Examples:
theHarvester.py -d microsoft.com -l 500 -b google -h myresults.html
theHarvester.py -d microsoft.com -b pgp
theHarvester.py -d microsoft -l 200 -b linkedin
theHarvester.py -d apple.com -b googleCSE -l 500 -s 300
```



Decisión a tomar



¿Como seguimos?

1. Quieres realizar búsqueda de credenciales
2. Investigar exposición en RRSS
3. Analizar la muestra de malware

Decisión escogida: Investigación malware

Esta mañana un compañero del equipo de gestión de incidentes nos ha pedido ayuda sobre un hash de un proceso detectado en una alerta de seguridad. A priori, el propio proceso aparenta ser inofensivo pero al compañero le ha extrañado el propio nombre del proceso, ya que no ha identificado su aplicación asociada. Necesita que le ayudemos a analizar el hash de dicho proceso para determinar si esta relacionada con alguna amenaza conocida.

El hash es **4b8b49bdfa435d0faba2e3964b04e20bbfc86aa4ffc3c3b8e1449894892f125b**

Objetivo

Identificar posible relación del hash con algún tipo de amenaza

Tipo de investigación

Investigación del hash, junto con las posibles relaciones con otros IoCs

Donde investigamos

- IBM X-Force
- AlienVault OTX
- VirusTotal
- Hybrid Analysis
- Any RUN



Información sobre la muestra

Buscamos el hash en la base de datos de VirusTotal. Detectamos que la muestra ha sido categorizada como maliciosa por 56 motores antivirus.

56

/ 71

Community Score

56 engines detected this file

4b8b49bdafa435d0faba2e3964b04e20bbfc86aa4ffc3c3b8e1449894892f125b

404.50 KB

2020-05-15 18:43:43

%APPDATA%\KQhXCqiZ.exe

Size

6 days

assembly detect-debug-environment direct-cpu-clock-access peexe runtime-modules

DETECTION

DETAILS

RELATIONS

BEHAVIOR

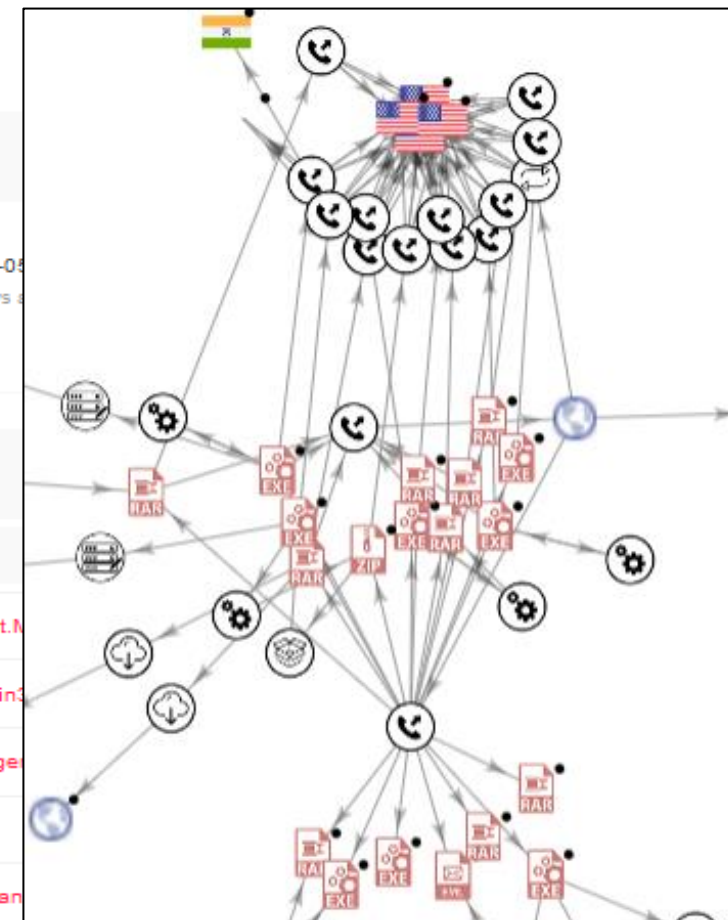
CONTENT

SUBMISSIONS

COMMUNITY 2

2020-05-15T18:43:43

Acrionis	Suspicious	Ad-Aware	Gen:Variant.M
AegisLab	Trojan.Multi.Generic.4!c	AhnLab-V3	Malware/Win32
Alibaba	TrojanSpy:MSIL/Kryptik.8b9f32a9	ALYac	Spyware.Agent
Antiy-AVL	Trojan/Win32.Wacatac	SecureAge APEX	Malicious
Arcabit	Trojan.MSILPerseus.D3485C	Avast	Win32:Trojan
AVG	Win32:TrojanX-gen [Trj]	Avira (no cloud)	HEUR/AGEN.1133788

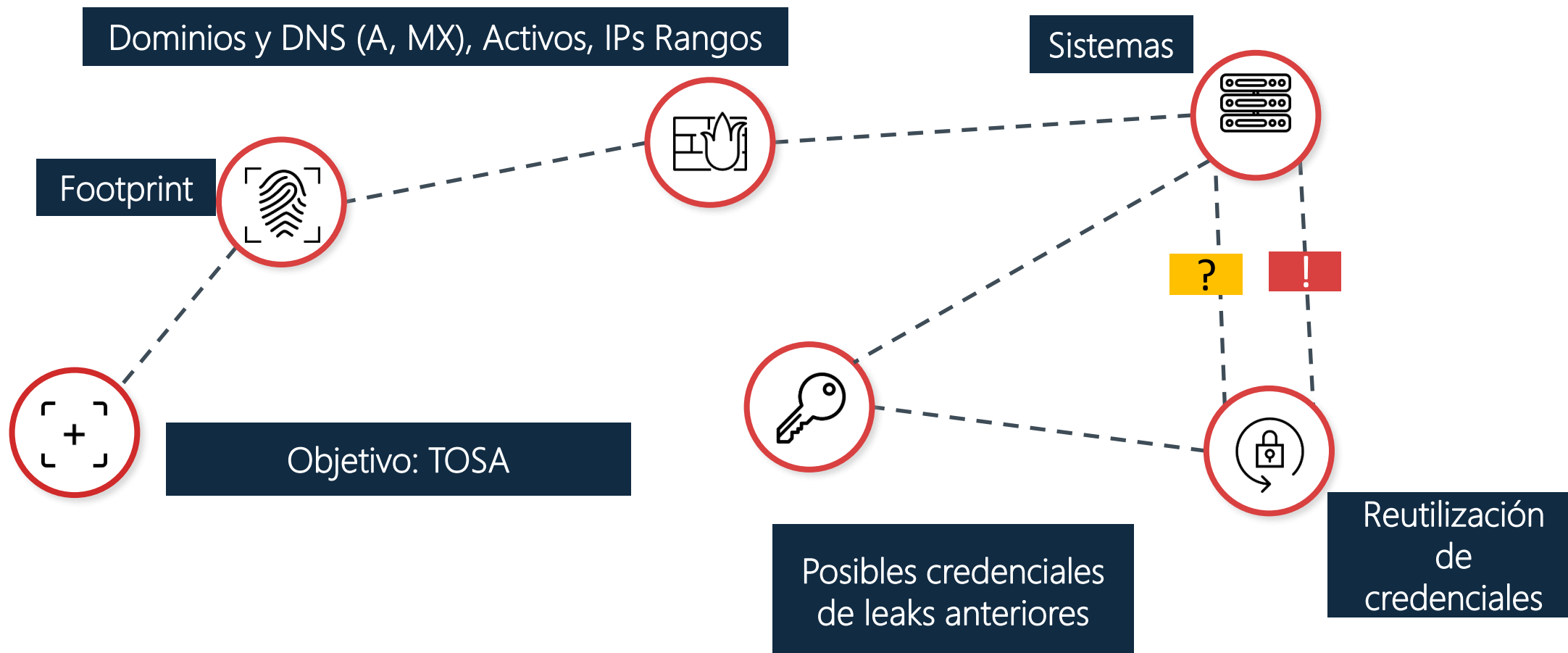


<https://www.virustotal.com/gui/file/4b8b49bdafa435d0faba2e3964b04e20bbfc86aa4ffc3c3b8e1449894892f125b>

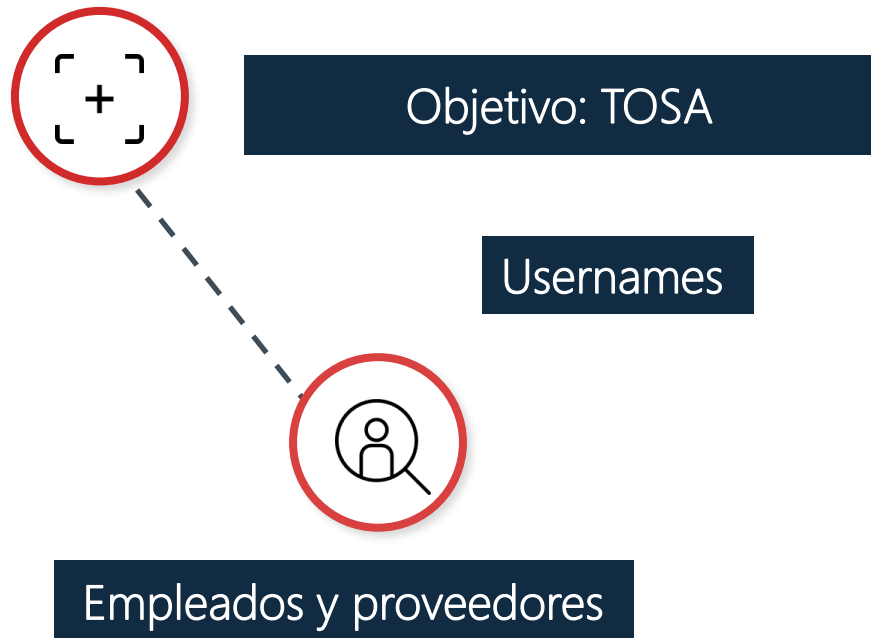
Pivotando en la investigación



Hilando pistas



Explorando la rama SOCMINT



Investigando una identidad digital

1

Qué tenemos

- Nombre de una persona, cuenta/username, identidad o cualquier dato de partida.

2

Qué buscamos

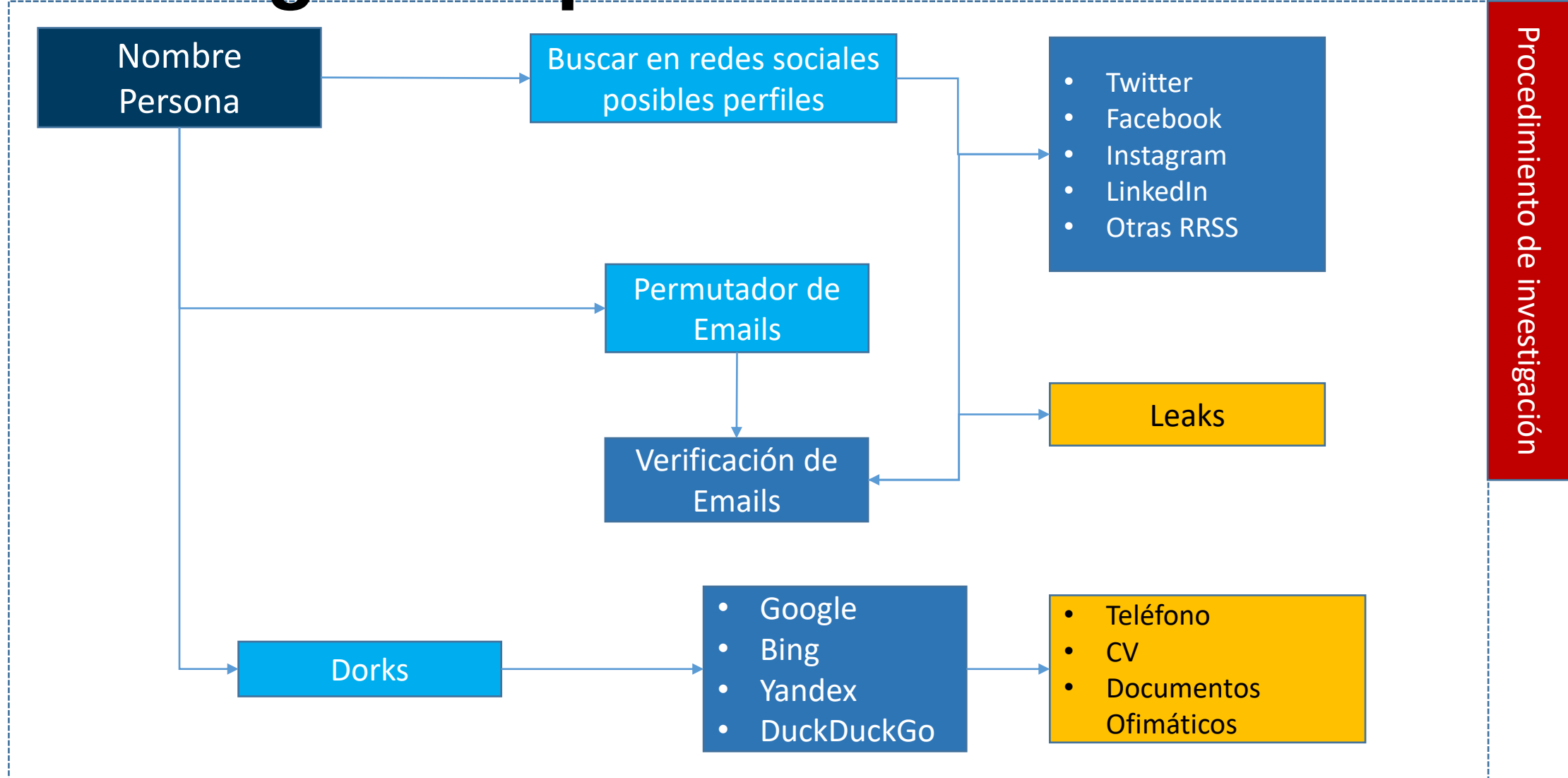
- Perfiles de redes sociales (Twitter, Instagram, Facebook, LinkedIn, etc) que utilicen el username objetivo.
- Comprobación de la existencia de correos electrónicos de cualquier proveedor que usen el username objetivo.
- Búsqueda de correos electrónicos asociados a los perfiles sociales detectados.
- Presencia de los correos electrónicos o del username en Data Leaks filtrados.
- Búsqueda de los usernames o los correos electrónicos asociados utilizando diferentes Dorks en los principales metabuscadore.
- Búsqueda de evidencias asociadas al username en webs de históricos

3

Qué necesitamos

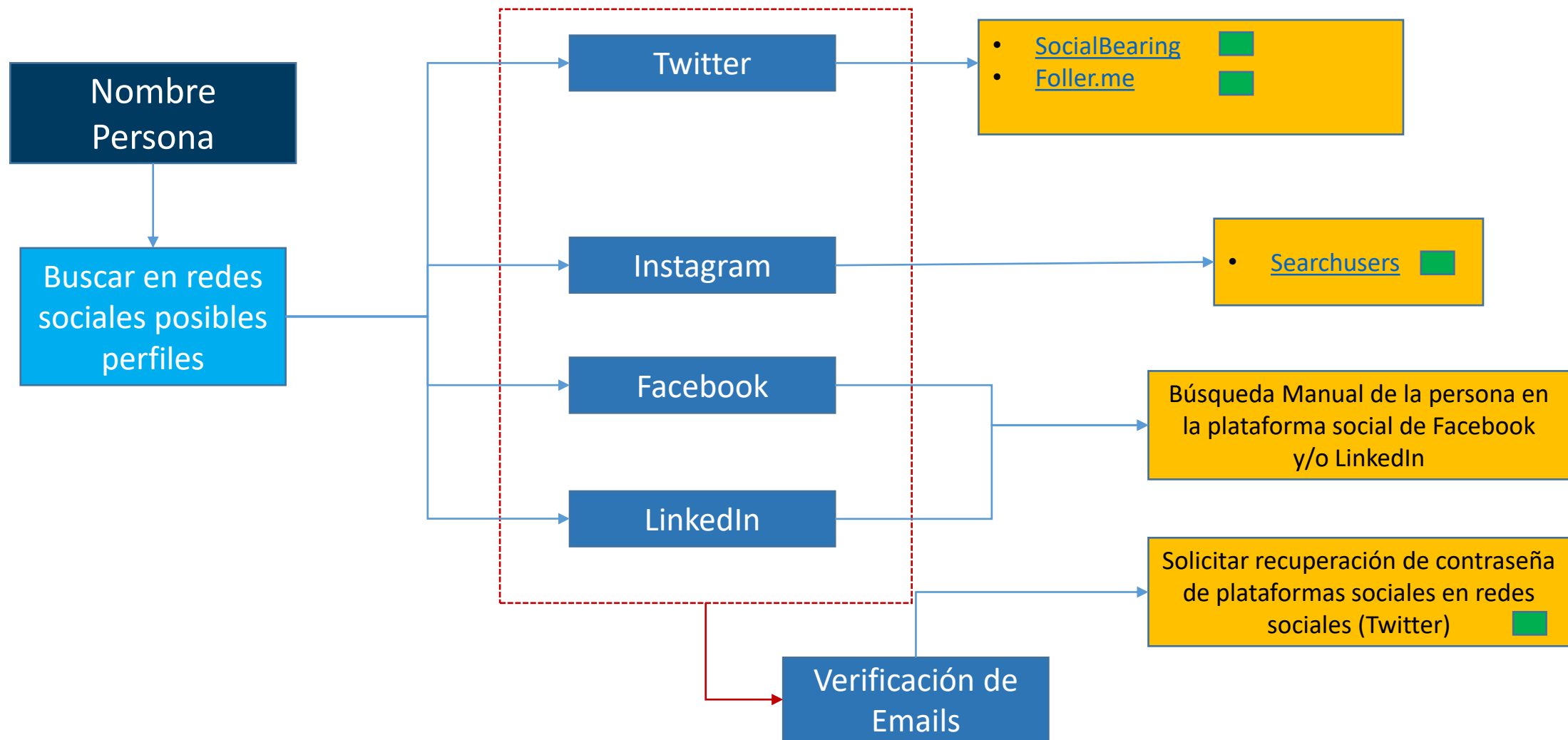
- Establecer las herramientas que podemos usar, tanto de pago como open source.
- Usar la metodología y ciclo de inteligencia para coleccionar y analizar los datos.
- Documentar nuestros hallazgos y generar información de valor.

Investigación partiendo de un nombre

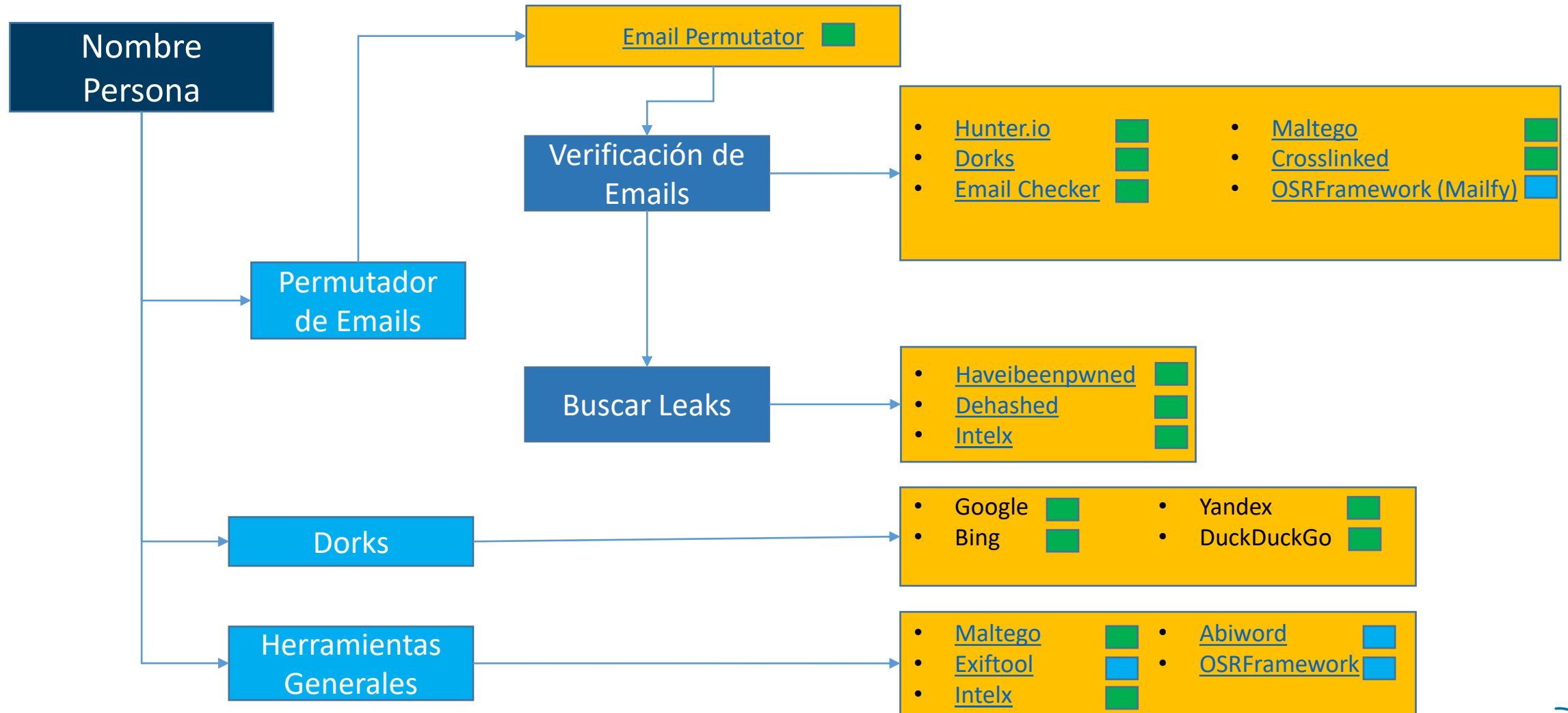


Se ilustra un procedimiento simplificado de cómo investigar partiendo de un nombre de persona como dato de partida.

Investigación partiendo de un nombre



Investigación partiendo de un nombre

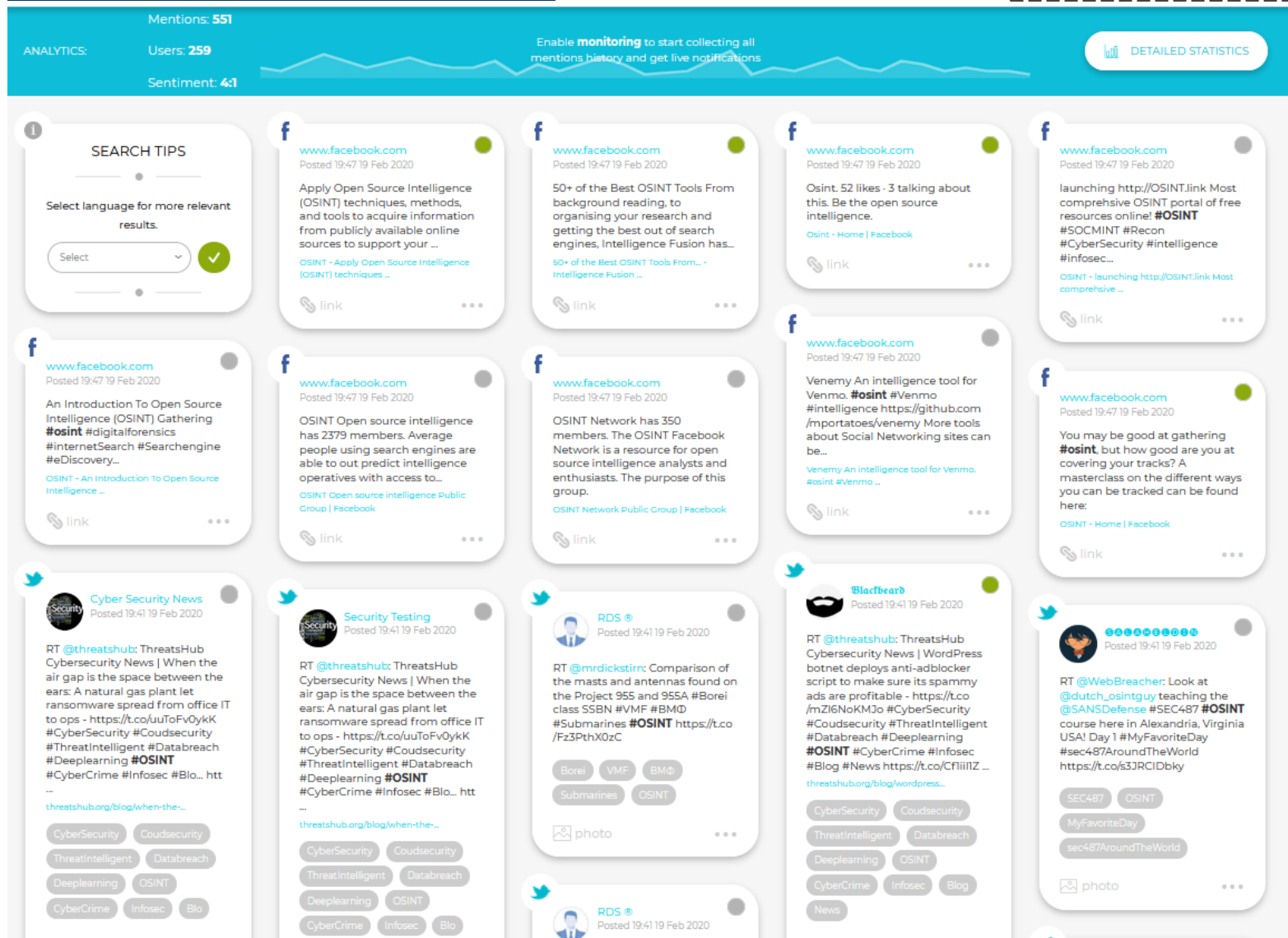


Herramienta Online Script de Nivel de Dificultad Media Script de Nivel de Dificultad Alta

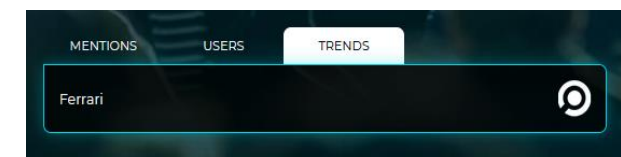
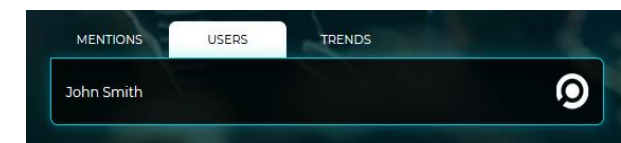
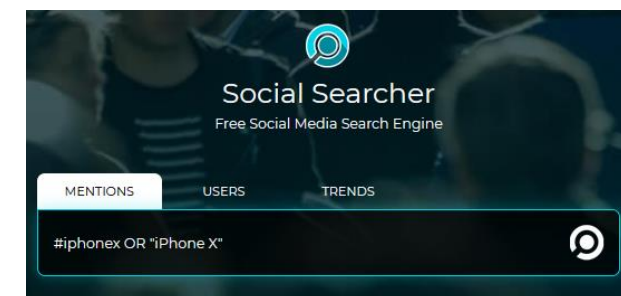
Perfiles a partir del nombre de persona

<https://www.social-searcher.com>

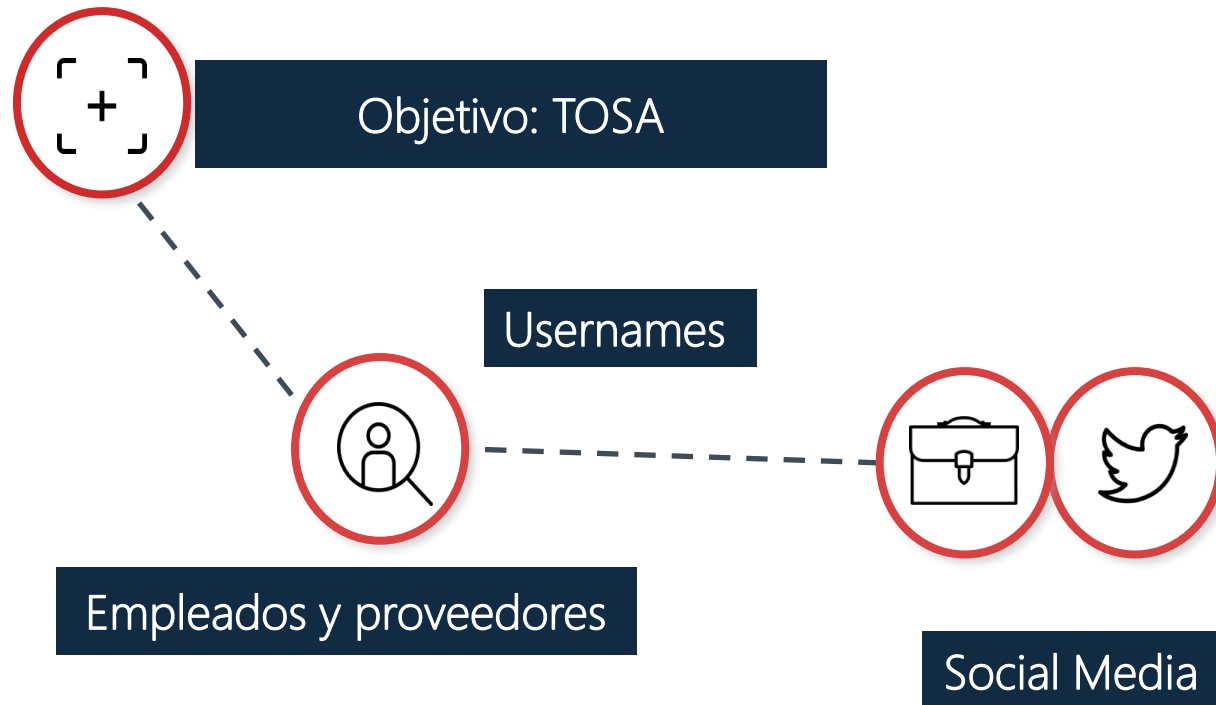
Input: Nombre Persona, Keyword mención



Herramienta que permite investigar usuarios, menciones o cualquier palabra clave en las redes sociales.



Continuamos nuestra investigación



Investigación partiendo de un usuario

1

Qué tenemos

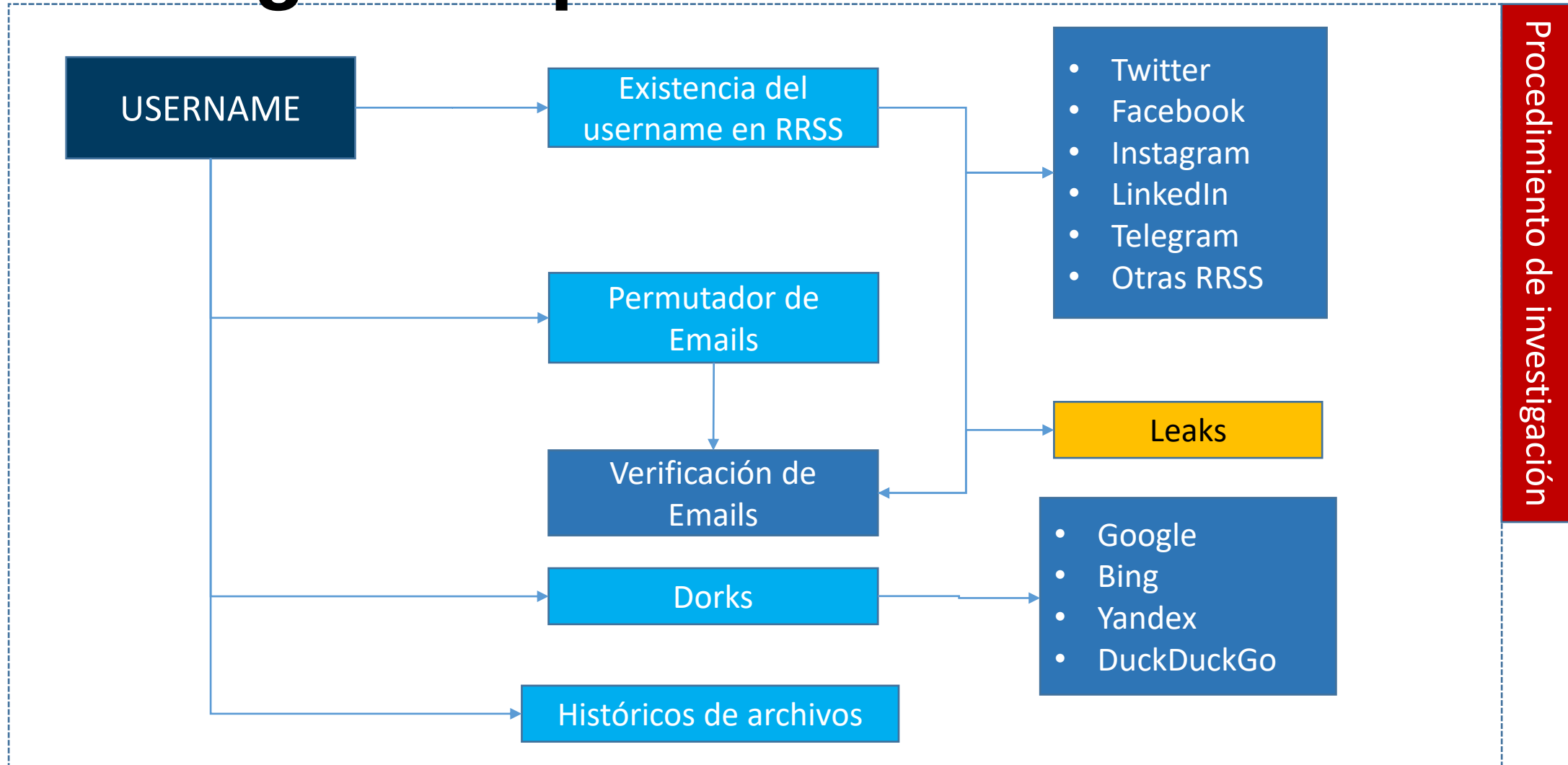
- Username.

2

Qué buscamos

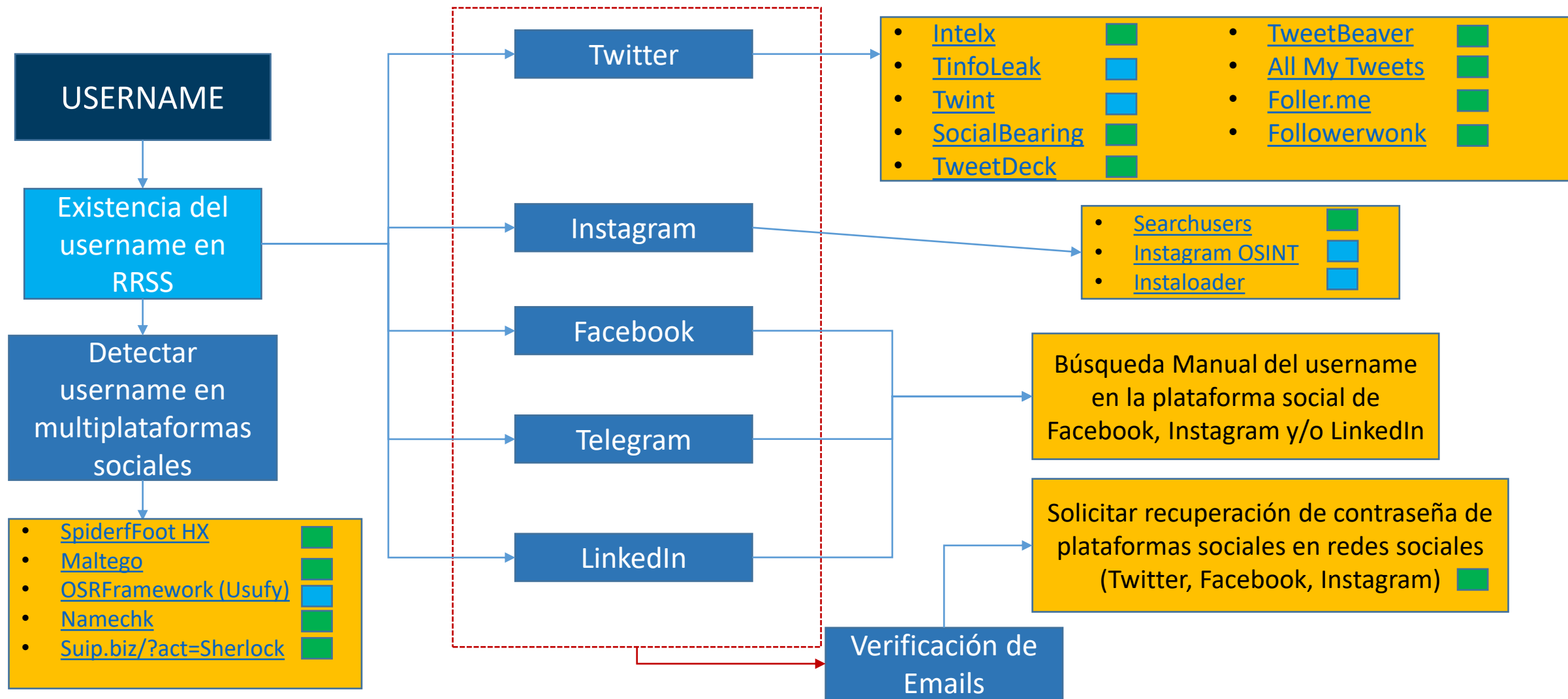
- Perfiles de redes sociales (Twitter, Instagram, Facebook, LinkedIn, etc) que utilicen el username objetivo.
- Comprobación de la existencia de correos electrónicos de cualquier proveedor que usen el username objetivo.
- Búsqueda de correos electrónicos asociados a los perfiles sociales detectados.
- Presencia de los correos electrónicos o del username en Data Leaks filtrados.
- Búsqueda de los usernames o los correos electrónicos asociados utilizando diferentes Dorks en los principales metabuscadore.
- Búsqueda de evidencias asociadas al username en webs de históricos

Investigación partiendo de un usuario



Se ilustra un procedimiento simplificado de cómo investigar partiendo de un dato de usuario/username como dato de partida.

Investigación partiendo de un usuario



Localizar perfiles a partir del username

<https://namechk.com>

Input: Username

https://namechk.com

Username

Facebook	YouTube	Twitter	Instagram	Blogger	Reddit	Ebay	Wordpress	Pinterest	Yelp	Slack	Github
Basecamp	Tumblr	Flickr	Pandora	ProductHunt	Steam	MySpace	Foursquare	OkCupid	Vimeo	Etsy	SoundCloud
BitBucket	CashMe	DailyMotion	About.me	Disqus	Medium	Behance	Photobucket	Coderwall	Fanpop	deviantART	Good Reads
Instructables	Keybase	Kongregate	LiveJournal	Mix	AngelList	last.fm	Slideshare	Tripit	PayPal	Dribbble	Imgur
Tracky	Flipboard	Vk	Kik	Codecademy	Roblox	Gravatar	Trip	Pastebin	blip.fm	Wikipedia	Elo
StreamMe	IFTTT	CodeMentor	Soup.io	Fiverr	Trakt	Hackernews	500px	Spotify	Plenty Of Fish	Houzz	Contently

Localizar emails y perfiles sociales

www.github.com/i3visio/osrframework

Herramienta que permite obtener resultados sobre posibles perfiles sociales según una búsqueda a partir de un username, correo electrónico o nombre de persona.

Se muestran los resultados de OSRFramework sobre una búsqueda de un username dado

[illegible]

Coded with ❤ by **Yaiza Rubio & Félix Brezo**

This program comes with ABSOLUTELY NO WARRANTY. This is free software, and you are welcome to redistribute it under certain conditions. For additional info, visit <https://www.gnu.org/licenses/agpl-3.0.txt>.

```
2020-02-20 09:44:38.135893      Starting search in 216 platform(s)... Relax!
```

Press <Ctrl + C> to stop...

```
2020-02-20 09:45:47.380379 Results obtained (7):
```

Sheet Name: Objects recovered (2020-2-20_9h45m).

com.i3visio.URI	com.i3visio.Alias	com.i3visio.Platform
https://www.canva.com/ivanpormor	ivanpormor	Canva
http://www.bucketlistly.com/users/ivanpormor	ivanpormor	Bucketlistly
https://www.minds.com/ivanpormor	ivanpormor	Minds
https://www.periscope.tv/ivanpormor	ivanpormor	Periscope
https://www.taringa.net/ivanpormor	ivanpormor	Taringa
http://twitter.com/ivanpormor	ivanpormor	Twitter
https://site.douban.com/ivanpormor	ivanpormor	Douban

```
2020-02-20 09:45:47.410711      You can find all the information here:
      ./profiles.csv
```

```
2020-02-20 09:45:47.411309      Finishing execution...
```

```
Total time consumed:      0:01:09.275416
Average seconds/query:    0.32071951851851854 seconds
```

Localizar emails y perfiles sociales

Instalación: pip3 install osrframework

www.github.com/i3visio/osrframework

Módulo Usufy



Permite verificar la existencia de un Username en un total de 306 plataformas.

Comando: usufy -n "username" -p all

Módulo Mailfy



Permite verificar la existencia de un email en los diferentes proveedores de correo.

Comando: mailfy -m correo

Módulo Searchfy



Permite verificar la existencia de perfiles en redes sociales a través del nombre completo de una persona.

Comando: searchfy -q "nombre
persona"

Localizar emails y perfiles sociales

OSRFramework

Coded with ♥ by Yaiza Rubio & Félix Brezo

-- In 'domainfy', use '-t cc' to find domains resolving to ccTLDs. --

Searchfy | Copyright (C) Yaiza Rubio & Félix Brezo (i3visio) 2014-2020

This program comes with ABSOLUTELY NO WARRANTY. This is free software, and you are welcome to redistribute it under certain conditions. For additional info, visit <<https://www.gnu.org/licenses/agpl-3.0.txt>>.

2020-02-18 22:24:40.050277 Starting search in different platform(s)... Relax!

Press <Ctrl + C> to stop...

[*] Launching search using the Facebook module...
[*] Launching search using the Github module...
[*] Launching search using the Instagram module...
[*] Launching search using the KeyServerIO module...
[*] Launching search using the Twitter module...
[*] Launching search using the Youtube module...

2020-02-18 22:24:42.602763 Results obtained:

Sheet Name: Objects recovered (2020-2-18_22h24m).

com.i3visio.Platform	com.i3visio.Alias	com.i3visio.URI
Github	WiktorNykiel	https://github.com/WiktorNykiel
Github	wiktornykielpro	https://github.com/wiktornykielpro

2020-02-18 22:24:42.658569 You can find all the information collected in the following files:
./profiles.csv

2020-02-18 22:24:42.658671 Finishing execution...

Total time used: 0:00:02.608394
Average seconds/query: 2.608394 seconds

Did something go wrong? Is a platform reporting false positives? Do you need to integrate a new one and you don't know how to start? Then, you can always place an issue in the Github project:
<https://github.com/i3visio/osrframework/issues>
Note that otherwise, we won't know about it!

Link to your report: <https://w-e-b.site/?act=report&id=d12412b52abbc9bb38f26f1c04adacch>

<https://suip.biz/?act=searchfy>

Herramienta online que permite ejecutar el modulo **searchfy** de **OSRFramework** sin la instalación de la propia herramienta para buscar coincidencias de perfiles sociales a partir del nombre completo.

Input: Nombre Persona

<https://suip.biz/?act=mailfy>

Herramienta online que permite ejecutar el modulo **mailfy** de **OSRFramework** sin la instalación de la propia herramienta para buscar coincidencias sobre emails utilizados en cualquier plataforma de red social.

Input: Email

Se muestran los resultados de OSRFramework sobre una búsqueda de un nombre de persona dado

Investigar perfil a partir del username

SOCIALBEARING
Insights & analytics
for tweets & timelines



Tweets @Handle Geo People Followers Friends

Enter keywords, hashtag or website (it's free) **SEARCH**

Find tweets that contain keywords or hashtag ☐ Exact match **Advanced Search** ▼

Se muestra la
página principal
de socialbearing

<https://socialbearing.com/>

Input: Username, Nombre Persona, Geolocalización, Hashtag

Twitter search & analytics for 'ciberinteligencia'

[New Twitter Search »](#)

TWEETS

100

[LOAD MORE](#)

TIMEFRAME

9 days

REACH

284.901

IMPRESSIONS

340.297

TOTAL RT'S

1233

TOTAL FAVES

1237

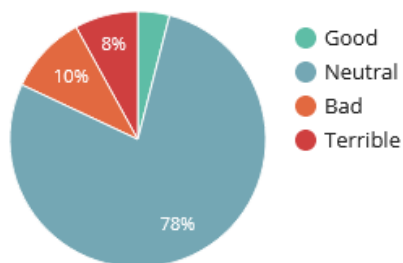
REPLIES

3

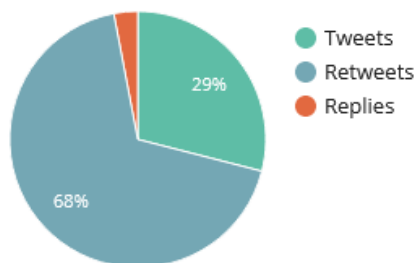
HIDDEN

0

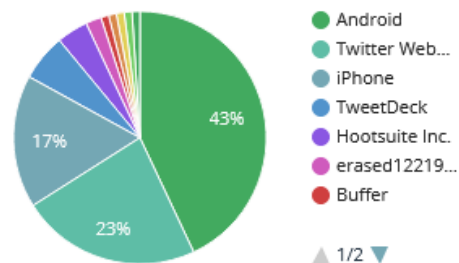
TWEETS BY SENTIMENT



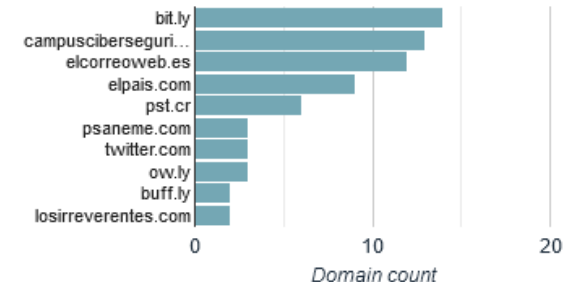
TWEETS BY TYPE



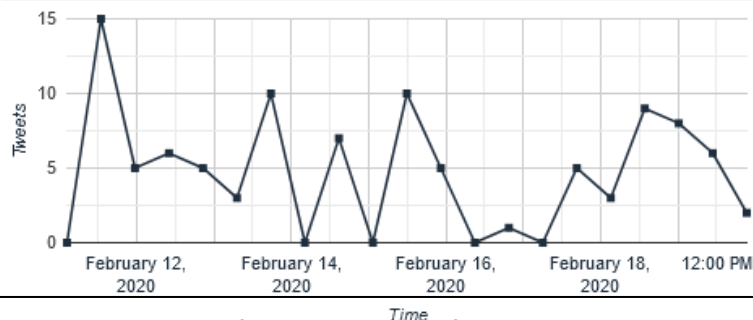
TWEETS BY SOURCE



TOP DOMAINS SHARED



TWEETS OVER TIME



HASHTAG CLOUD



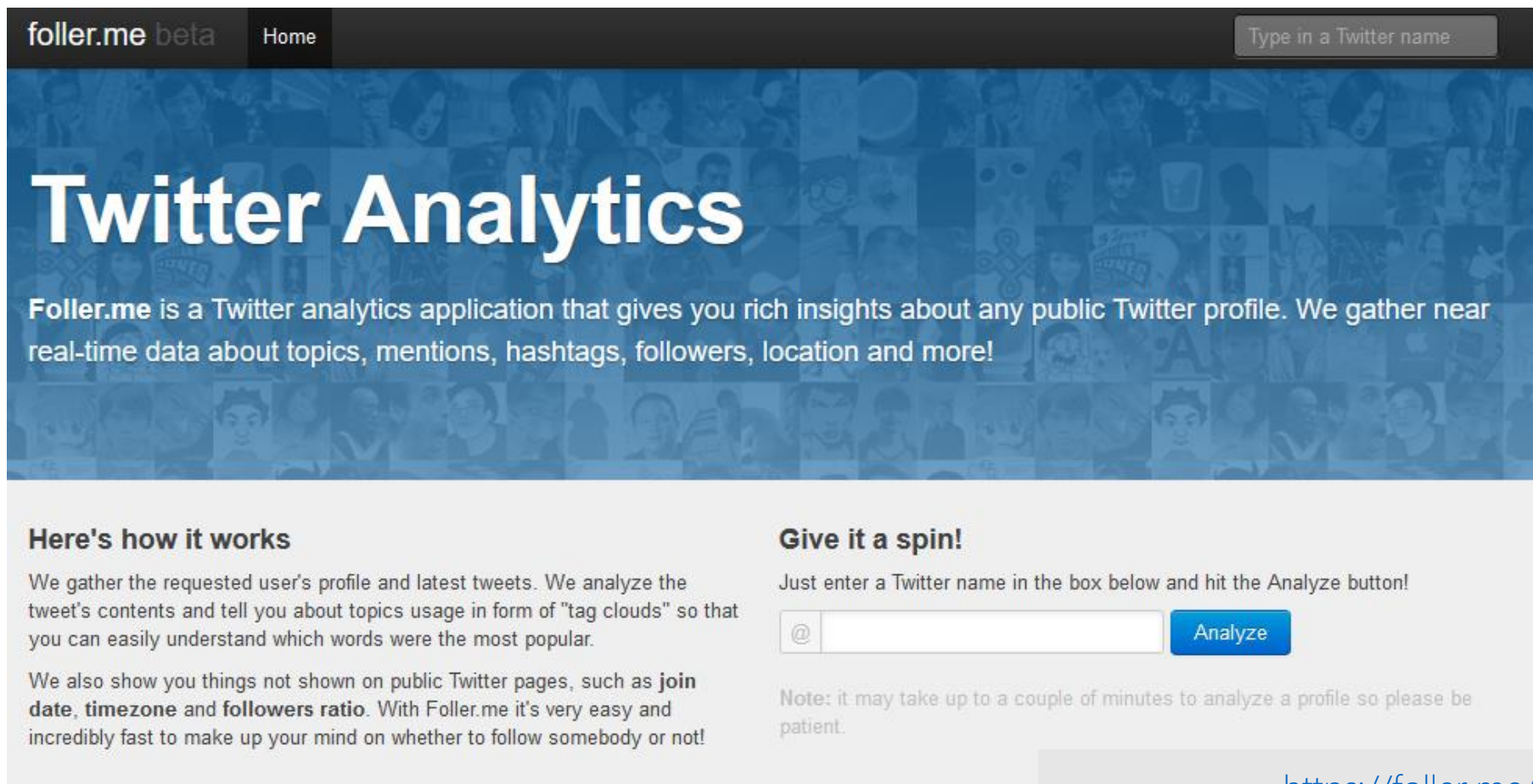
WORD CLOUD



Se muestran los resultados proporcionados por SocialBearing de la palabra ciberinteligencia

Investigar perfil a partir del username

Herramienta que permite la obtención de información relacionada con un perfil de Twitter como **datos básicos del perfil, estadísticas de tweets, seguidores, seguidos, listas incluidas, menciones, hashtags mas utilizadas, topics y un timeline**



The screenshot shows the Foller.me website. At the top, there's a dark navigation bar with 'foller.me beta' on the left, a 'Home' link in the center, and a search input field on the right labeled 'Type in a Twitter name'. Below the navigation bar is a large blue banner with a collage of profile pictures. The banner contains the text 'Twitter Analytics' in large white letters, followed by a paragraph: 'Foller.me is a Twitter analytics application that gives you rich insights about any public Twitter profile. We gather near real-time data about topics, mentions, hashtags, followers, location and more!'. Below the banner, the page is divided into two columns. The left column is titled 'Here's how it works' and contains two paragraphs explaining the tool's functionality. The right column is titled 'Give it a spin!' and contains a text input field with a '@' icon, an 'Analyze' button, and a note: 'Note: it may take up to a couple of minutes to analyze a profile so please be patient.'

Input: Username

Se muestra la
página oficial de
foller.me

<https://foller.me/>



Obtenición de información de Twitter

Twint esta desarrollado en **python3.6** y por lo tanto es necesario disponer de dicho lenguaje de programación instalado y el **pip3** para la instalación de librerías necesarias en el mismo.

Puede instalarse tanto en sistemas **Linux** como **Windows** siempre que tenga Python 3.6 instalado.

Comando de instalación

```
pip3 install --user --upgrade  
git+https://github.com/twintproject/twint.git@origin/master#egg=twint
```

<https://github.com/twintproject/twint/>

Uso de Twint

Posibilidades de uso:

- **twint -u username** → Scraping de todos los tweets del usuario especificado
- **twint -u username -s keyword** → Scraping de todos los tweets de una keyword dada del usuario especificado
- **twint -u username --since "2019-12-20 20:30:15"** → Scraping de todos los tweets del usuario especificado y desde una fecha dada
- **twint -u username --year 2020** → Scraping de todos los tweets de un año dado del usuario especificado
- **twint -u username --email --phone** → Scraping de todos los tweets del usuario especificado con coincidencias de emails y números de teléfono
- **twint -u username --followers** → Scraping de todos los tweets de los seguidores del usuario especificado
- **twint -u username --following** → Scraping de todos los tweets de los seguidores seguidos por el usuario especificado

Uso de Twint

Posibilidades de uso:

- `twint -u username --following --user-full` → Recolección de información de los usuarios de los seguidores seguidos por el usuario especificado
- `twint -u username --favorites` → Scraping de todos los tweets del usuario especificado que sea favorito
- `twint -u username --profile-full` → Recolección de todos los tweets/RT del perfil de un usuario especificado
- `twint -u username --user-full` → Recolección de información de un usuario especificado
- `twint -u username --retweets` → Recolección de los últimos 900 tweets de un usuario
- `twint -u username -o file.csv --csv` → Scraping de todos los tweets del usuario especificado exportando resultados en csv

Uso de Twint

Posibilidades de uso:

- **twint -g="40.416933529263936, -3.706192548676933,1km" -o file.csv --csv** → Scraping de todos los tweets en un radio de 1km en una geolocalización dada, exportando resultados en csv
- **twint -u username -o file.json --json** → Scraping de todos los tweets del usuario especificado exportando resultados en JSON
- **twint -u username --database tweets.db** → Scraping de todos los tweets del usuario especificado exportando resultados a una BBDD SQLite
- **twint -u username -es localhost:9200** → Scraping de todos los tweets del usuario especificado exportando resultados a una BBDD Elasticsearch
- **twint -u noneprivacy --csv --output none.csv --lang en --translate --translate-dest es --limit 100 (BETA)**
→ Traducción a español de los últimos 100 tweets en ingles

Uso de Twint

The screenshot shows the Google Maps interface for the location of Sol in Madrid. The URL in the address bar is <https://www.google.com/maps/place/Sol,+Madrid/@40.4169335,-3.7061925,17z/data=!3m1!4b1!4m5!3m4!1s0xd42287e1463b6cf:0x14a34120b93...>. The coordinates `@40.4169335,-3.7061925,17z` are highlighted with a red box. The map shows the area around Sol, including the Gran Vía and the Real Madrid Official Stores. A 'Compartir' (Share) dialog is open, showing the 'Insertar un mapa' (Insert map) tab. The dialog displays the coordinates and a link to the map: `<iframe src="https://www.google.com/maps/embed?pb=!1m18!1m12!1s0xd42287e1463b6cf:0x14a34120b93...">`. The left sidebar shows the search bar with 'sol' entered, and the bottom section shows the 'Información resumida' (Summary information) for Sol, stating 'Sol es el corazón de Madrid, con numerosas calles'.

Se muestra como extraer las coordenadas de un lugar en concreto por medio de Google Maps

Localizar emails presentes en hibp



Mediante esta herramienta es posible obtener información sobre los emails que estén presentes en cualquier Data Breach dado.

have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username pwned?

183 pwned websites 2,051,020,243 pwned accounts 43,869 pastes 40,402,537 paste accounts

Top 10 breaches

- myspace 359,420,698 MySpace accounts
- NetEase 234,842,089 NetEase accounts
- in 164,611,595 LinkedIn accounts
- Adobe 152,445,165 Adobe accounts
- Badoo 112,005,531 Badoo accounts
- VK 93,338,602 VK accounts
- Рамблер/ 91,436,280 Rambler accounts
- Dropbox 68,648,009 Dropbox accounts



Notify me

Get notified when future pwnage occurs and your account is compromised.

enter your email address

Just to make sure you're not a robot, please solve this puzzle first:

☐ No soy un robot reCAPTCHA

notify me of pwnage

email@wiktornykiel.com pwned?

Oh no — pwned!

Pwned on 1 breached site and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security

Start using 1Password.com

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

<https://haveibeenpwned.com/>

Input: Email

Localizar más fugas de información



Mediante esta herramienta es posible obtener información sobre los emails que estén presentes en cualquier Data Breach dado.

DEHASHED

IS YOUR **PERSONAL** DATA AMONG THE **12,387,953,776** COMPROMISED ASSETS?

Regex enabled — Disable true wildcard by wrapping text with quotation marks — e.g. "example" — or by using search operators below. ⓘ

Search for anything... "searchterm" OR email:"my@email.com" OR email:"*@yourcompany.com"

SEARCH

Search for specific fields by adding 'fieldname:' before query or using some premade buttons below. ⓘ

(default searches for all fields including ones not listed, and wildcards the search) ⓘ

ALL FIELDS (DEFAULT)

EMAIL

USERNAME

IP ADDRESS

NAME

ADDRESS

PHONE NUMBER

VIN

<https://dehashed.com>

Input: Email

Caso de estudio



TOSA Tiendas Online SA

Itinerario de introducción que abarca las disciplinas de OSINT y SOCMINT

Tiendas TOSA S.A ha sido comprometida y tendrás que averiguar quién está detrás de ello y por qué.

Modalidad:Teleformación (On-line)

<https://angeles-elearning.ccn-cert.cni.es/course/view.php?id=170>



OSINT Case Study (TOSA)

Introductory itinerary covering OSINT and SOCMINT disciplines

Tiendas TOSA S.A. has been compromised and you will have to find out who is behind it and why.

Modalidad:Teleformación (On-line)

Caso de estudio



**Invicador Innovación
Redes Sociales**

Invicador Innovación - Redes Sociales

Escenario de simulación para el entrenamiento en la aproximación práctica al trazado de un contenido en redes sociales

Modalidad:Teleformación (On-line)

<https://angeles-elearning.ccn-cert.cni.es/course/view.php?id=163>



**Invicador Innovación
Social Networks**

Invicador Innovación - Social Networks

Simulation scenario for training in the practical approach to the layout of content on social networks

Modalidad:Teleformación (On-line)

<https://angeles-elearning.ccn-cert.cni.es/course/view.php?id=167>

Caso de estudio



**Vinos de la Vega
OSINT Web**

Vinos de la Vega - Web

Escenario de simulación para el entrenamiento
en la aproximación práctica al trazado de un
contenido en web

Modalidad:Teleformación (On-line)

<https://angeles-elearning.ccn-cert.cni.es/course/view.php?id=178>



**Vinos de la Vega
OSINT Web**

OSINT Web Case Study (Vinos de la Vega)

Simulation scenario for training in the practical
approach to web content mapping

Modalidad:Teleformación (On-line)

<https://angeles-elearning.ccn-cert.cni.es/course/view.php?id=158>

Índice

- 01 Conceptos esenciales
- 02 Sobre Elena
- 03 Un ejemplo real: Counterfeit en comercios web
- 04 Un ejemplo de caso de investigación en Elena
- 05 Seguridad Operativa en actividades de cibervigilancia
- 06 Inteligencia de imágenes
- 07 Dorking con buscadores genéricos
- 08 Dorking con buscadores especializados
- 09 Reportando y entregando el producto
- Anexos



OPSEC – Seguridad Operativa

- ✓ Ser paranoico proactivamente.
- ✓ Planifica. No contar planes, ni detalles.
- ✓ No confiar en nadie.
- ✓ No hablar en público. Si se habla, usar palabras clave.
- ✓ No tener evidencias que nos podrían incriminar al descubierto.
- ✓ Aislar la infraestructura.
- ✓ Aislar nuestros avatares, evitar que se contaminen.
- ✓ Separar de nuestra vida personal.

OPSEC

OPERATIONS SECURITY

Ciberprotección y anonimización

1

Creación de diferentes avatares para cada investigación

Correos como protonmail.com o emails desechables. Creación de avatares lo más realistas posibles (gmail, outlook, yahoo). Usar keepass para almacenar las contraseñas, generar contraseñas aleatorias, no guardarlas en el navegador.

2

Uso de entornos aislados, anti tracking y revisión de privacidad

Evitar elementos que se puedan trackear, revisar configuraciones de privacidad de las cuentas creadas. Usa plugins de Firefox para contenerización, privacidad y anonimato. Valora entornos como Tails, Whonix, Qubes OS.

3

Conexiones: uso de VPN para privacidad (proteger los datos), TOR para anonimato (proteger a la persona)

riseup.com, freeproxylists.net, protonvpn.
Comprobar nuestra IP en en.utrace.de o similares, ver si exponemos datos (<http://check.torproject.org>)

4

Usar métodos pasivos frente a activos de acceso a la información

Usar paginas cacheadas, no realizar enumeraciones de puertos directas (ej. nmap). Recuerda que hay búsquedas que dejan rastro (búsqueda activa) y otras que no (información cacheada). Es mejor no dar pistas de lo que estamos buscando.

5

Cifra la información obtenida

Usa particiones ficheros o ficheros cifrados para almacenar la información.

N

Creando avatares

1

No usar la **fecha de nacimiento real**, asegurarse de que es aleatoria cada vez que se introduce.

2

No usar tu **nombre real** o nombre completo.

3

Si no tienes que usar tu **ubicación** real, entonces no lo hagas.

4

Preguntas de seguridad si son necesarias, utilice la función de llenado de formularios del administrador de contraseñas para generar una cadena aleatoria que se guardará en esa cuenta, generalmente en notas o keepass.

Creando avatares

5

Para las **fotos de perfil**, si se requiere una pública, entonces ten cuidado con la que uses, para todas las demás cuentas, <https://this-person-does-not-exist.com/en> está bien, o una foto al azar de un gato, un perro o un objeto inanimado está bien. Además, asegúrate de que sean **únicas** en todos los sitios para que no puedan ser enlazadas a través de la **búsqueda inversa de imágenes**.

6

Utiliza la configuración de privacidad para asegurarte de que las direcciones de **correo electrónico se hagan privadas/ocultas del público**, especialmente en **Twitter**, donde el restablecimiento de la contraseña muestra parte de tu correo electrónico /teléfono.

7

Utilice direcciones de correo electrónico de un solo uso cuando se registre en los sitios, asegúrese de que no pueda ser rastreada hasta usted, es decir, regístrese con la VPN y no deje marcadores de identificación, como nombres u otros datos personales.

Correo seguro y anónimo

1

ProtonMail

About Security Blog Careers Support Enterprise ▾

LOG IN

SIGN UP

2

Secure Email Based in Switzerland

3

Secure Your Communications with ProtonMail

GET YOUR ENCRYPTED EMAIL ACCOUNT

4

5

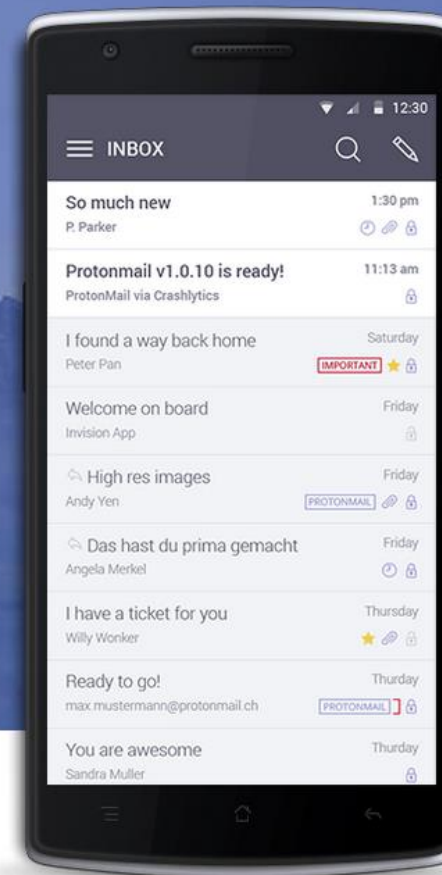
N

The ProtonMail mobile apps are now available worldwide.

Introducing Encrypted Email for Your Mobile Device



<https://protonmail.com>



Tarea:

1. Crear cuenta de correo lo más real posible.
2. Guardar credenciales de forma segura.

Se muestra la página principal de
<https://protonmail.com>

Números de teléfono “gratis”

1

2

3

4

5

N

RECEIVE-SMS-ONLINE.INFO

Receive SMS Online
Receive-SMS-online.info is FREE service for receive Dynamic Sender ID feature.
How to use?
Select one of the numbers listed below and you can

United Kingdom
+447727411978
SMS received:7197

Estonia
+37253706220
SMS received:3101

Bangladesh
+8801645787953
SMS received:8711

India
+918727923596
SMS received:26442

• This site have any limitations ?
Receive-sms-online.info has no limitation when SM

• If you use the numbers above for **Phone Verificati**

• What countries are currently available ?
Currently We support few countries numbers like: US

<http://receive-sms-online.info>

ABOUT IT

SMS-Receive.net is a website that contains vi
Yahoo, Microsoft, serverloft, CloudSigma, Face

We've detected that you're using AdBlock Plus

USA +16173408061
Total SMS: 1361

Belgium +32460234463
Total SMS: 998

<http://sms-receive.net>

Receiveasms.com

Spain

Status: **Online**
Number: **+349110674**
Please **Reload** the page to update any r

Three minute delay turn off **Adblock** to re

Show 6 entries

Time	From	Mess
2020-02-18 19:14:39	+85254724000	As2in1
2020-02-18 18:12:55	+85254724000	As2in1
2020-02-18 15:43:08	+34626562617	From: 93396 para co 20,00 XX973

Tarea:

1. Recibir SMS de validación en un teléfono temporal.

<https://receiveasms.com/>

Números virtuales de pago

1



Protect Your Privacy

Burner is the original second phone number app for picture messaging. Stay safe and anonymous with a burner number.

GET STARTED

2

3

4

5

N

https://hushed.com



Plans & Pricing

Features

About Us

Private Phone Numbers, Talk & Texting

★★★★★ 25K  ★★★★★ 50K 

The best second phone number app for any occasion. Make private calls, send texts, picture messages, and manage multiple numbers... all in one easy-to-use app.

Stay protected and stay anonymous with Hushed.

Get Started



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

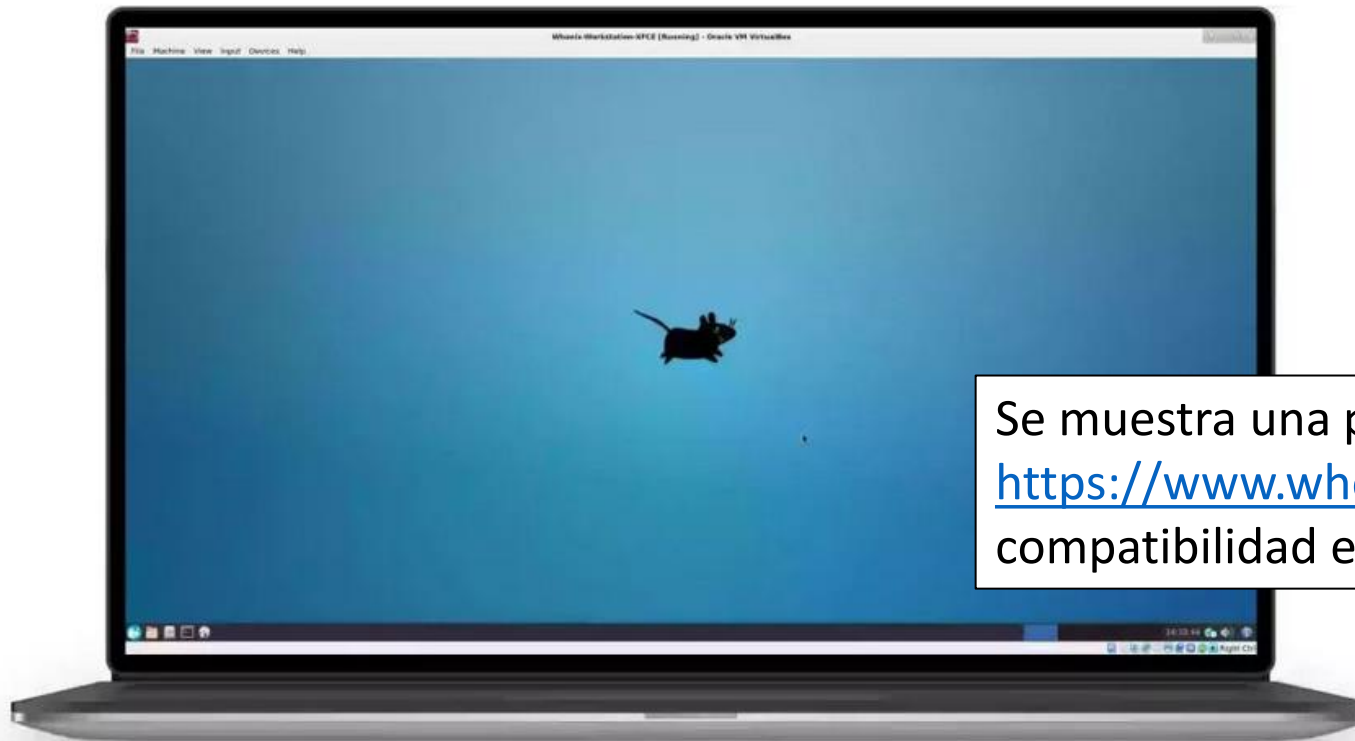


<https://hushed.com/>

Sistemas operativos



Anonymize Everything You Do Online



Se muestra una parte de la página principal de <https://www.whonix.org/> y una imagen con la compatibilidad entre sistemas



<https://www.whonix.org/>

Navegadores vitaminados

Excelentes complementos de privacidad para Firefox

1

Mejora tu privacidad con estos excelentes complementos para Firefox.

Impide el rastreo con Privacy Badger



Privacy Badger es un complemento para el navegador que impide que los anunciantes y seguidores de terceros de manera secreta puedan rastrear qué páginas visitas de Internet. Privacy Badger aprende sobre los rastreadores mientras navegas inspeccionando peticiones de sitios webs externos. Tenga en cuenta que Google Analytics no es considerado como un seguidor de terceros por Privacy Badger, lo que significa que Google Analytics no será bloqueado si no utiliza otro bloqueador como uBlock Origin.

2

Bloquea la publicidad y los rastreadores con uBlock Origin



Un eficiente bloqueador de amplio espectro que no consume mucha memoria, y además puede cargar y aplicar más filtro que otros bloqueadores más populares que existe. No tiene una estrategia de monetización y es completamente de código abierto. Recomendamos Firefox pero uBlock Origin también funciona con otros navegadores como Safari, Opera o Chromium. A diferencia de AdBlock Plus, uBlock no tiene eso llamado "publicidad aceptable".

Borra automáticamente las cookies con Cookie AutoDelete



Elimina automáticamente las cookies cuando ya no son usadas por las pestañas abiertas en tu navegador. Con las cookies, las sesiones persistentes, así como la información utilizada para espiar, serán eliminadas.

3

Cifrado con HTTPS Everywhere



Una extensión para Firefox, Chrome, y Opera que cifra tus comunicaciones con la mayoría de sitios web, haciendo tu navegador más seguro. Una colaboración entre el proyecto Tor y Electronic Frontier Foundation.

Bloquea contenido de redes de distribución de contenido con Decentraleyes



Emula sistemas de distribución de contenido de manera local interceptando peticiones, encontrando los recursos necesarios e inyectándolos al entorno. Esto ocurre de manera instantánea, automática y no se necesita una configuración previa. Código fuente: [GitLab \(auto-hospedado\)](#).

4

Informate mediante Terms of Service; Didn't Read



"He leído y estoy de acuerdo con los términos" Es la mayor mentira de Internet. Este complemento trata de solucionar eso dando una puntuación a los sitios web basada en sus acuerdos de sus Términos de uso del Servicio y ofrece un breve resumen. Código fuente: [GitHub](#).

Snowflake



"Snowflake es un nuevo *pluggable transport* del Proyecto Tor. Si tienes una conexión sin censura, al ejecutar esta extensión de manera voluntaria puedes hacer que tu conexión pueda ser utilizada como una conexión proxy Snowflake para ayudar a los usuarios que no pueden conectarse a la red Tor. Tu IP no será visible a los sitios que los usuarios visitan utilizando tu proxy, ya que esta extensión no te hará ser un nodo de salida de la red. Si tu acceso a la red Tor está bloqueada, esta extensión no te ayudará y deberías utilizar el Navegador Tor. Código fuente: [Servicio Git](#).

5

Las siguientes extensiones requieren una cierta interacción del usuario para hacer que las cosas funcionen. Algunas web puede que no funcionen correctamente hasta que hayas configurado las extensiones.

Detén las peticiones de sitios cruzados mediante uMatrix



Muchos sitios web integran características que permiten a otros sitios web rastrear, como los botones de "Me Gusta" de Facebook o Google Analytics. uMatrix te da el control de esas peticiones que hacen los sitios web a otras webs. Esto te ofrece y te garantiza que tendrás un mayor control sobre la información que vas filtrando en tu actividad en la red.

N



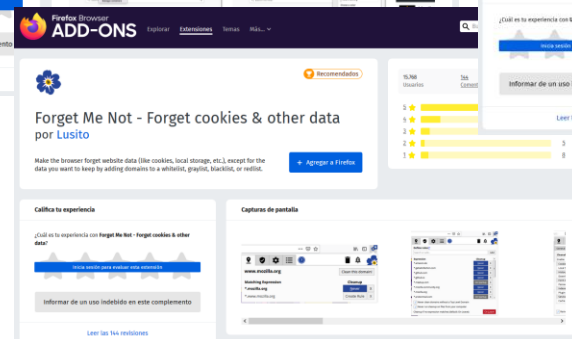
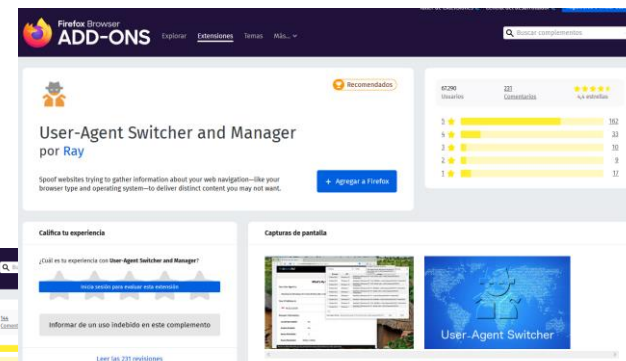
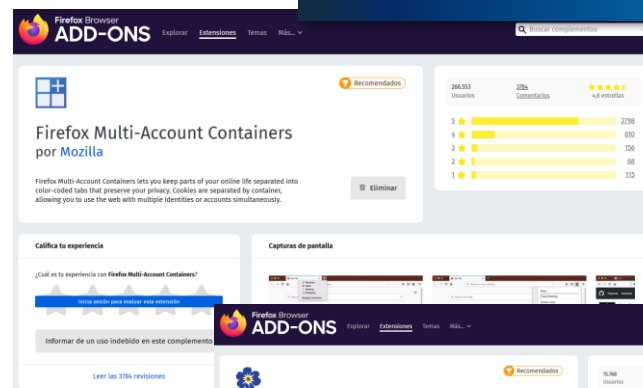
<https://victorhck.gitlab.io/privacytools-es/#addons>

Complementos para navegadores Web

Privativo*	Recomendaciones Libres		
Ghostery	Decentraleyes Protégete contra rastreo a través de entr... Android BSD GNU/Linux macOS Windows	HTTPS Everywhere Cifra tus comunicaciones en millones de ... Android BSD GNU/Linux macOS Windows	
	Mailvelope Cifrado OpenPGP para servicios webmail. BSD GNU/Linux macOS Windows	Multi-Account Containers Manual identity isolation for Firefox. BSD GNU/Linux macOS Windows	
	NoScript Activa JavaScript, Java y Flash solament... Android BSD GNU/Linux macOS Windows	Privacy Badger Tracking blocker that tries to learn who is... Android BSD GNU/Linux macOS Windows	
	Temporary Containers Per-tab identity isolation for Firefox.	uBlock Origin An efficient blocker for Firefox and Chrom... Windows	



<https://prism-break.org/es/all/>



Extensiones

1

2

3

4

5

N

The screenshot shows the Firefox Add-ons page for the 'Firefox Multi-Account Containers' extension. The header includes the Firefox logo, 'Firefox Browser', and 'ADD-ONS'. Navigation links are 'Explorar', 'Extensiones' (underlined), 'Temas', and 'Más...'. The extension card features a blue icon with a plus sign, the title 'Firefox Multi-Account Containers por Mozilla', and a description: 'Firefox Multi-Account Containers lets you keep parts of your online life separated into color-coded tabs that preserve your privacy. Cookies are separated by container, allowing you to use the web with multiple identities or accounts simultaneously.' It has a 'Recomendados' badge, a star rating of 5 stars, and 266,553 users. A 'Eliminar' button is present. Below the card are sections for 'Califica tu experiencia' (with a question '¿Cuál es tu experiencia con Firefox Multi-Account Containers?' and a bar chart) and 'Capturas de pantalla' (showing browser tabs with different container themes like Personal, Work, Banking, and Shopping).

Tarea:

1. Personalizar navegador.

Se muestra la página de instalación del Add-on Firefox Multi-Account Containers de firefox

Configuración avanzada

1

🏠 Servicios ▾ Navegador ▾ Software ▾ Sistemas operativos ▾ Participa Acerca de Comparte ▾ Dona Código

Preparación:

1. Escribe "about:config" (sin comillas) en la barra de direcciones de Firefox y presiona la tecla Enter.
2. Presiona el botón "Tendré cuidado, lo prometo"
3. Sigue las instrucciones que se detallan a continuación...

2

Empezando:

1. **privacy.firstparty.isolate = true**
 - Un resultado del esfuerzo de [Tor Uplift](#), esta preferencia aísla todas las fuentes de identificación (por ejemplo cookies) al primer dominio, con el fin de reducir el rastreo a través de dominios diferentes.
2. **privacy.resistFingerprinting = true**
 - Como resultado del esfuerzo de [Tor Uplift](#), esta preferencia hace a Firefox más resistente a la identificación del navegador.
2. **privacy.trackingprotection.enabled = true**
 - Esta es la nueva oferta de Mozilla como protección del rastreo. Utiliza el listado de filtros de Disconnect.me, que es redundante si ya estás utilizando Origin 3rd party, además deberías ajustarlo a "false" si estás utilizando las funcionalidades del complemento.
2. **browser.cache.offline.enable = false**
 - Inhabilita la cache "offline".
2. **browser.safebrowsing.malware.enabled = false**
 - Inhabilita las comprobaciones de malware de la navegación segura de Google. Tiene riesgos de seguridad pero mejora la privacidad.
2. **browser.safebrowsing.phishing.enabled = false**
 - Inhabilita la protección de la navegación segura de Google y la protección de "phishing". Tiene riesgos de seguridad pero mejora la privacidad.
2. **browser.send_pings = false**
 - El atributo debería ser útil para permitir a los sitios web rastrear los clics de los visitantes.
2. **browser.sessionstore.max_tabs_undo = 0**

3

4

5

N



https://victorhck.gitlab.io/privacytools-es/#about_config

2. **dom.battery.enabled = false**
 - Los propietarios de sitios web pueden rastrear la actividad de la batería de tu dispositivo.

Tarea:

1. Personalizar navegador.
2. Firefox
3. about:config

Se muestran distintas configuraciones que se pueden cambiar en Firefox para mejorar la ciberprotección y anonimización

Comprobación de la configuración

1

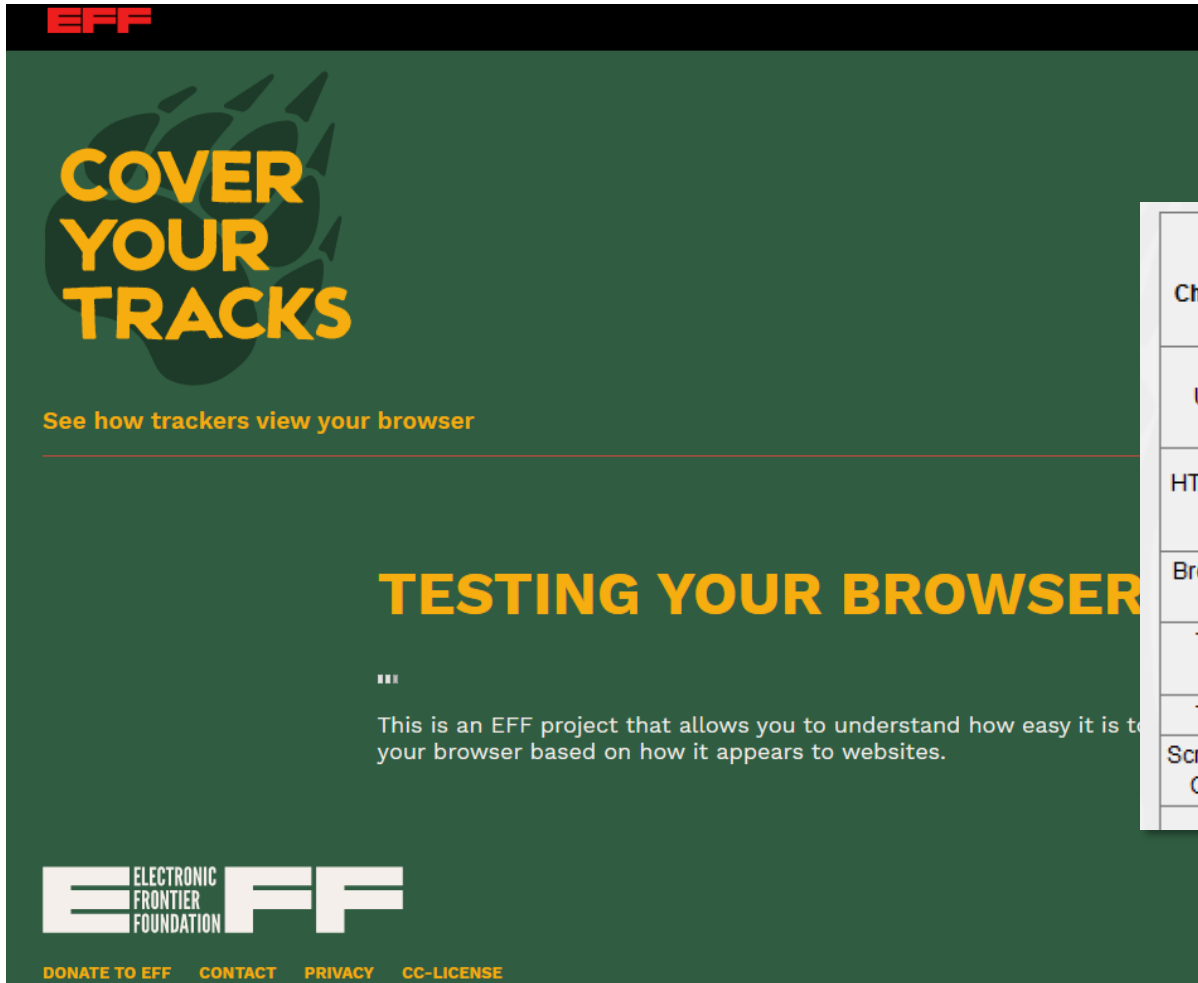
2

3

4

5

N



<https://victorhck.gitlab.io/privacytools-es/#browser>

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	17.98	258291.0	AZXd6q8hRHCIRw ToycZo9Z (Windows NT NT 10.0; Win64; x64; rv:76.0) WSFZHaZYO939 TZifjS99qv2 ZVjt9xT9Y59S Z8sUQsbkAJj Firefox/5.0 9f GZRvh9Zc5r9 Mozilla/20100101 9nwxXh9CM7
HTTP_ACCEPT Headers	17.98	258291.0	gf9gz/7zjx, */*; q=0.01, bq9fo/pdzjffo, yzk99/vpk9z, text/html br, deflate, k8l 8nxdl, szzee8, kjsomwu, gzip, hrrfj2be, enbz, 1trsy9z, hc8o ar-ly, ms, es-ES, en; q=0.3, es-bo, es; q=0.8, en-US; q=0.5, sl
Browser Plugin Details	0.84	1.79	undefined
Time Zone Offset	6.13	70.25	-600
Time Zone	6.45	87.41	Europe/Madrid
Screen Size and Color			

Se muestran las páginas principales de <https://coveryourtracks.eff.org/> y de <https://victorhck.gitlab.io/privacytools-es/#browser>



<https://coveryourtracks.eff.org/>

Comunicaciones seguras

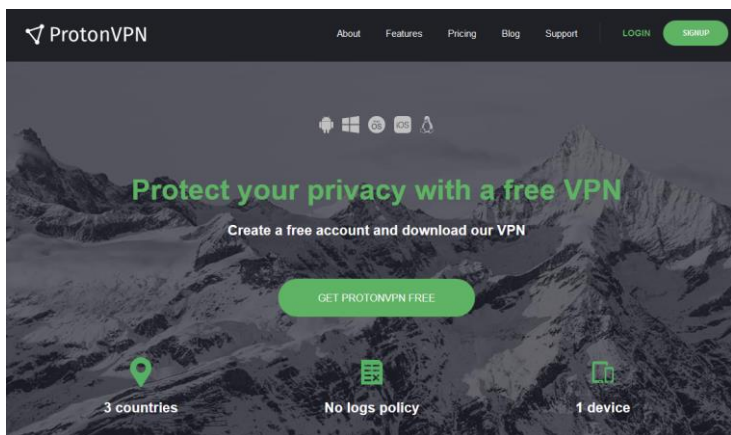
1



2



3



4

Red Privada Virtual (VPN)

Privativo*	Recomendaciones Libres		
 Cisco VPN  Hola!	 Bitmask LEAP platform client. Experimental Android GNU/Linux macOS	 Mullvad No-log WireGuard VPN provider. Servicios Web	 WireGuard Fast, modern, secure VPN tunnel. Android BSD GNU/Linux iOS macOS Servidores
 Riseup Cuentas de correo seguras y privadas. Servicios Web			

5

<https://protonvpn.com/support/tor-vpn/>

N

Fuentes “pasivas”

1



2



3



4



5

N

The Most Complete View of the Internet

Censys is the most reputable, exhaustive, and up-to-date source of Internet scan data in the world, so you see everything.

Search IPv4



Search Certificates



Search Websites



228,628,886

Active IP Addresses



2,029

Ports



36

Protocols Scanned



676,641,933

Active Services



40

Risk Classifications



3,519,772,418

Certificates



225,267,600

Domain Names



228,982

Software Packages

Protección de la información

1

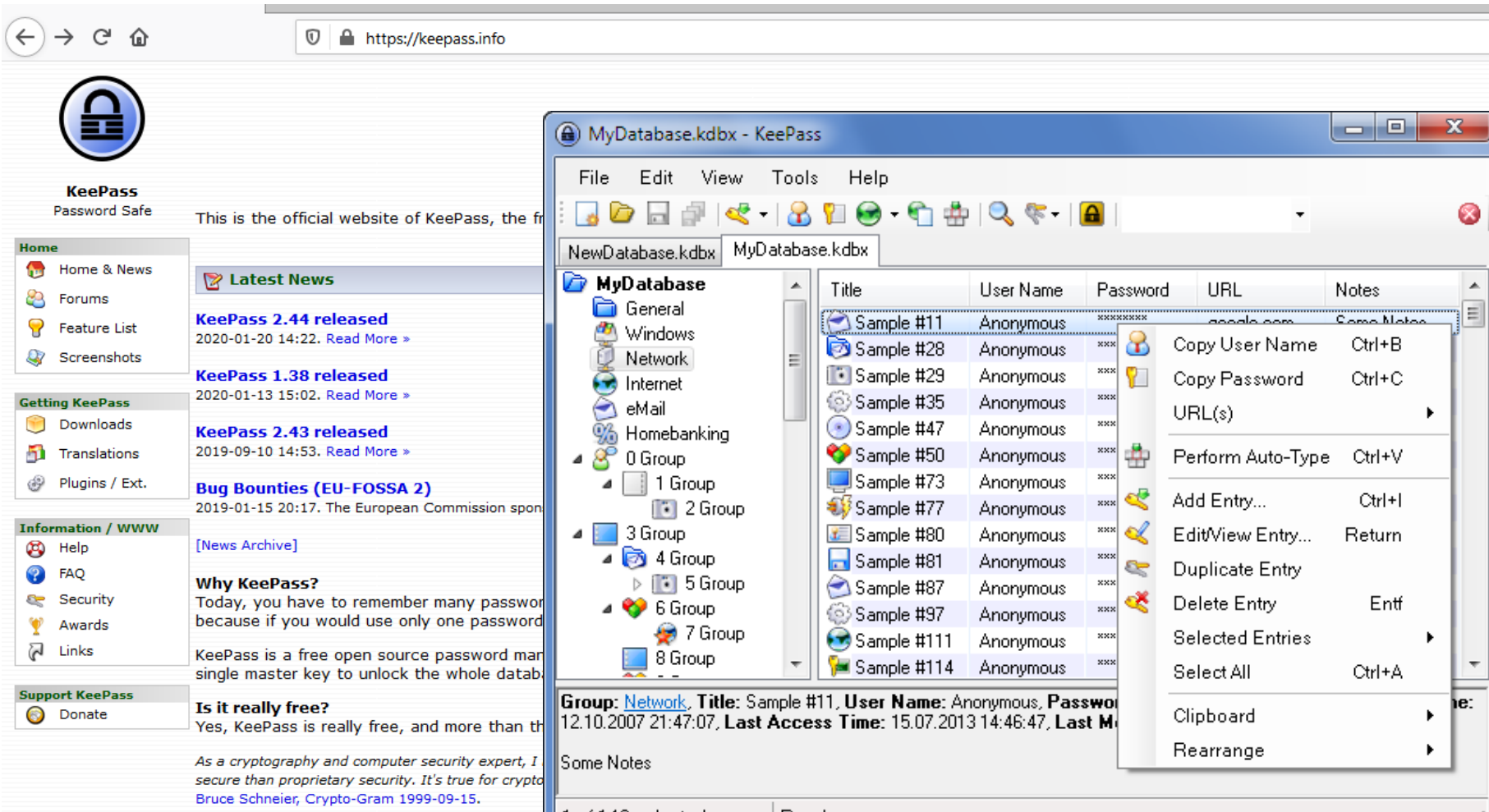
2

3

4

5

N



Tarea:
1. Guardar credenciales de forma segura.



<https://keepass.info/>

Se muestran una imagen de la página de descarga de KeePass y otra imagen del software en uso

Alternativas <https://victorhck.gitlab.io/privacytools-es/#pw>

Protección de la información

1

2

3

4

5

N



Home

Source Code

Downloads

Documentation

Donate

Forums

VeraCrypt is a free open source disk encryption software for Windows, Mac OSX and Linux. Brought to you by IDRIX (<https://www.idrix.fr>) and

VeraCrypt main features:

- Creates a **virtual encrypted disk** within a file and mounts it as a real disk.
- Encrypts an **entire partition or storage device** such as USB flash drive or hard drive.
- Encrypts a **partition or drive where Windows is installed** ([pre-boot authentication](#)).
- Encryption is **automatic, real-time(on-the-fly) and transparent**.
- [Parallelization](#) and [pipelining](#) allow data to be read and written as fast as if the drive was not encrypted.
- Encryption can be [hardware-accelerated](#) on modern processors.
- Provides [plausible deniability](#), in case an adversary forces you to reveal the password: [Hidden volume](#) (steganography) and [hidden operating system](#).
- More information about the features of VeraCrypt may be found in the [documentation](#)

[Donate to help the project](#)



Flattr

[Release Notes / Changelog](#)

[Frequently Asked Question](#)

[Android & iOS Support](#)

[Contributed Resources & Downloads \(Tutorials, PPA, ARM, Raspberry Pi...\)](#)



<https://www.veracrypt.fr/>

Alternativas: <https://victorhck.gitlab.io/privacytools-es/#encrypt>

Tarea:

1. Descargar VeraCrypt.
2. Crear volumen cifrado.
3. Guardar contraseña en KeePass.

Comprobación final

Id	Checklist	Estado
1	Sistema Operativo seguro	Si / No
2	Revisada configuración de los dispositivos (bluetooth, camara, etc)	Si / No
3	TOR (anonimato)	Si / No
4	VPN (privacidad)	Si / No
5	Geolocalización no estándar / WiFi o datos Burner SIM	Si / No
6	Firefox personalizado (Configuración y Plugins)	Si / No
7	Comms: Signal, Session, Telegram	Si / No
8	Números de teléfono desechables – Verificación de cuentas	Si / No
9	Avatares únicos para la investigación	Si / No
10	Segregación y aislamiento del entorno de investigación	Si / No
11	Credenciales únicas y complejas para el avatar – KeePass	Si / No
12	Información cifrada (Arranque o contenedor VeraCrypt)	Si / No
13	Nombres en clave / Alias para el objetivo	Si / No
14	Análisis de riesgos realizado	Si / No
15	Contramedidas aplicadas	Si / No
16	No comentar nada de la investigación	Si / No
17	No revelar datos personales, no hablar de hobbies, etc	Si / No

Laboratorio



<https://angeles-elearning.ccn-cert.cni.es/course/view.php?id=160>



<https://angeles-elearning.ccn-cert.cni.es/course/view.php?id=164>

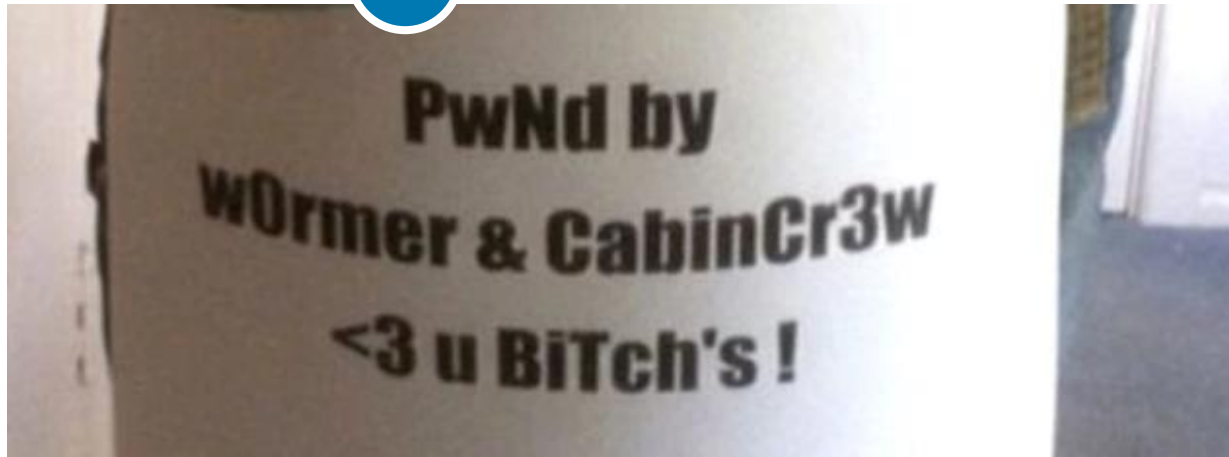
Índice

- 01 Conceptos esenciales
- 02 Sobre Elena
- 03 Un ejemplo real: Counterfeit en comercios web
- 04 Un ejemplo de caso de investigación en Elena
- 05 Seguridad Operativa en actividades de cibervigilancia
- 06 Inteligencia de imágenes
- 07 Dorking con buscadores genéricos
- 08 Dorking con buscadores especializados
- 09 Reportando y entregando el producto
- Anexos



Inteligencia de imágenes en el tiempo

2012



<https://www.infobae.com/2012/04/17/642702-el-fbi-atrapo-un-peligroso-hacker-gracias-foto-su-novia/>

Se encuentran imágenes y enlaces a dos noticias, una sobre como localizaron a un hacker gracias a una foto de su novia y la otra sobre dónde estaban los alborotadores del Capitolio cuando publicaron videos de asedio de Parler.

En ambas noticias vemos que se exponen coordenadas GPS ubicadas en las fotos expuestas

2021



<https://www.dailymail.co.uk/news/article-9142985/GPS-data-Parler-hack-shows-users-app-stormed-Capitol-Building.html>



Una imagen con todas las líneas papilares

Un traficante vendía marihuana en la Dark Web de forma anónima: lo identificaron gracias a una foto de sus dedos



Se muestra una imagen y el enlace a una noticia sobre como identificaron a un traficante gracias a una foto de sus dedos

<https://www.xataka.com/otros/traficante-vendia-marihuana-dark-web-forma-anonima-identificaron-gracias-a-foto-sus-dedos>

Ejemplos reales

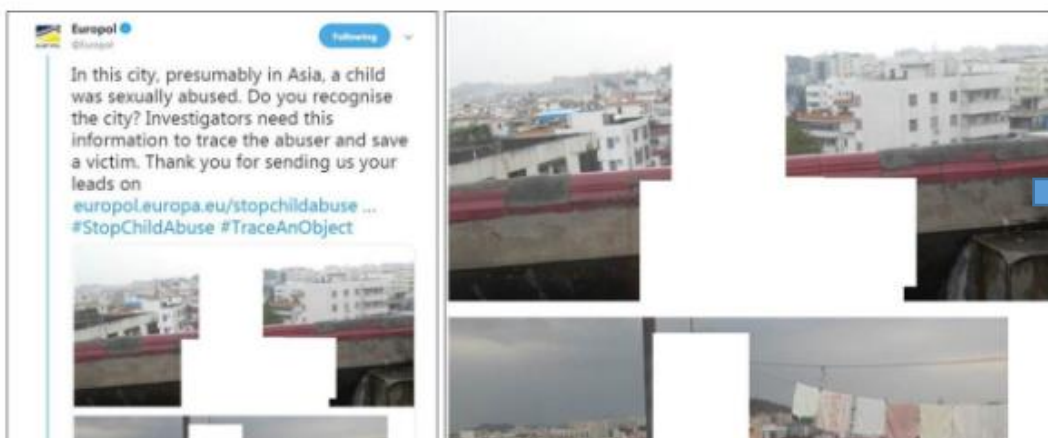
Europol's Asian City Child Abuse Photographs Geolocated

November 8, 2018 #StopChildAbuse China

Translations: [Русский](#)

Since 2017 the European Union Agency of Law Enforcement Cooperation, better known as Europol, has been crowdsourcing parts of or heavily censored photographs, related to child abuse crimes in their "[Stop Child Abuse – Trace an Object](#)" campaign.

Within two weeks after the start of their campaign Europol received 10.000 contributions from the public. Bellingcat, among many others, shared this [campaign](#) on the crowdsourcing platform [Check](#). Many followers of this campaign have helped by identifying objects and/or geolocating photographs. The location of a photograph in a hotel room was proved to be taken in a [hotel on Mauritius](#) within 48 hours after Europol shared the photograph on Twitter.



Conclusion

This research shows that in a complex investigation tiny details can be very important. The architecture, the tiles with red and orange colors, the blue roof and the mountainous area narrowed down the research to Southern China. Details in a video lead us to an eastern suburb of Shenzhen with similar architecture. Another video shows us GSM antennas and a satellite dish, also visible in the photographs, and lead us to a northern suburb of Shenzhen. Tiny details as buildings that are not visible in the photographs, but are visible in satellite imagery, and GSM antennas missing in the photographs, but which are visible in street view, show the photographs are at least five years old, likely even older.

It takes hours of research, and a complex investigation as this one clearly can not be solved by one person or a small team; a crowdsourced wisdom is required to solve cases like this. When even with crowdsourcing a location or an object can't be found, it can feel very frustrating. Yet, when a photograph is geolocated or an object is recognized, you realize that there is a chance that the case will be solved and someone will get arrested for a serious crime — and it was you who contributed to that.

Research by Daniel Romein and Timmi Allen, editing by Natalia Antonova.



Se muestran varias imágenes sobre la noticia de como se geolocalizó al delincuente a través de esas imágenes y sus elementos colindantes. El enlace hace referencia a procedimientos de investigaciones usando búsqueda inversa de imágenes.

<https://www.bellingcat.com/resources/how-tos/2019/12/26/guide-to-using-reverse-image-search-for-investigations/>

Busqueda inversa de imágenes



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

Imágenes visualmente similares



<https://www.archimadrid.org> > index.php > 2-madrid ▾

[La parroquia de Lavapiés celebra la ... - Archidiócesis de Madrid](#)



300 × 200 · 10 ago 2017 — Enclavada en el castizo barrio de Lavapiés, la parroquia de San Lorenzo (c/Doctor Piga, 2 – Metro Lavapiés) festeja a su santo patrono este ...

<https://callejartemadrid.com> > 2016/09/08 > la-iglesia-... ▾

[la iglesia de las "chinchas" | - Callejarte Madrid](#)



584 × 452 · 8 sept 2016 — Seguro que no conocías este apodo para la Iglesia de San Lorenzo, ... consagrada como parroquia el 8 de septiembre de 1670, la actual tras ...

Se muestran los resultados que devuelve Google Imágenes de la búsqueda de una imagen de la Parroquia de San Lorenzo, donde la identifica y devuelve imágenes muy similares

Busqueda inversa de imágenes

Yandex Uploaded image X Search

Web Images Video News Translate Disk Mail Ads

Register Log in

Press to select an item in this image

Размер изображения: 300x300 Select crop area

Image appears to contain

мужчина ведение бизнеса джефф олсон бизнес ...

Similar images

Other image sizes

No matching images found

Sites containing information about the image

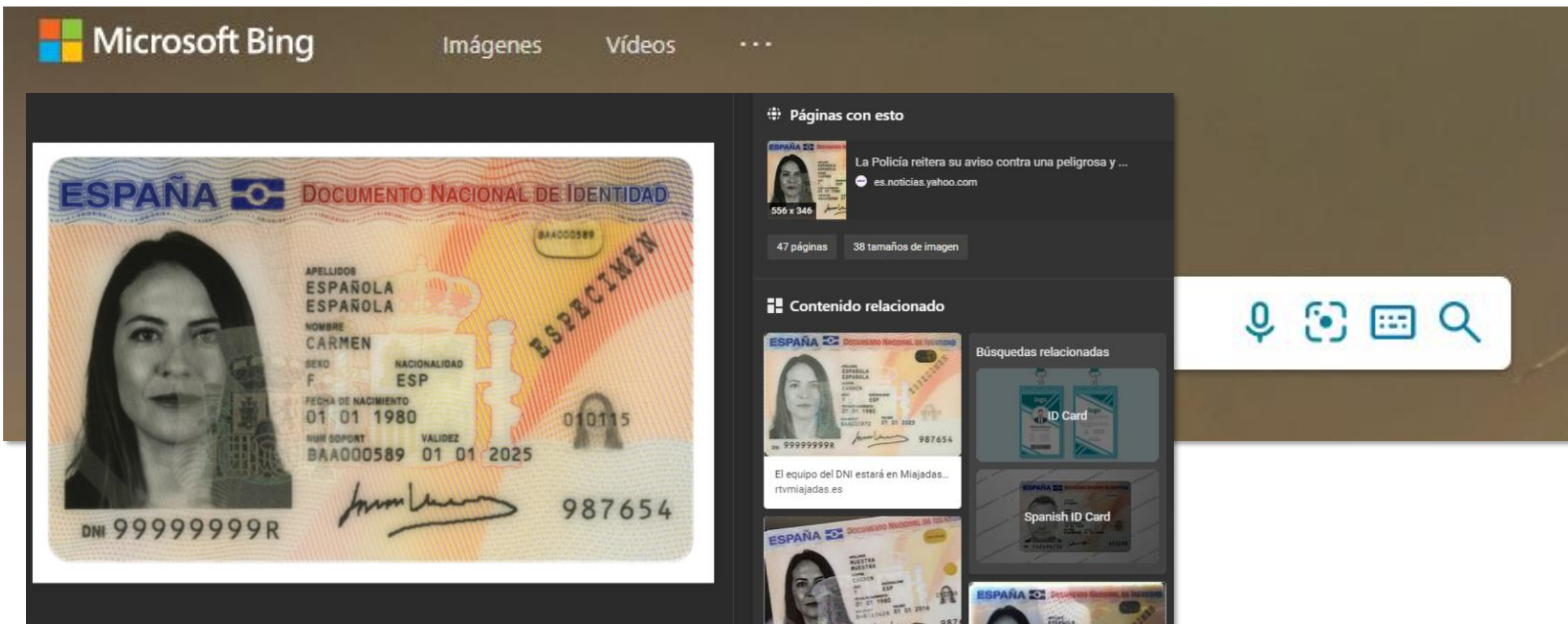
Speakers
ccn-cert.cni.es
Ponente

Ponentes XIII JORNADAS STIC CCN-CERT
ccn-cert.cni.es
Ponentes XIII JORNADAS STIC CCN-CERT

<https://yandex.com/images/>

Se muestran los resultados que devuelve Yandex de la búsqueda de una imagen de una persona de inicio desconocida, donde la identifica y devuelve imágenes muy similares indicándonos el nombre y webs donde aparece la misma

Busqueda inversa de imágenes



<https://www.bing.com/images/search>

Se muestra los resultados que devuelve Bing Imágenes de la búsqueda de una imagen de un dni, devuelve imágenes muy similares

Comparativa de buscadores de imágenes

Los servicios de **búsqueda reversa de imágenes** nos permiten verificar la exposición de las mismas, identificando así otros dominios en los que aparecen y obteniendo información relativa a éstas.

Existen diferentes herramientas entre las que destacan: **Google Imágenes**, **Yandex**, **Bing Imágenes** y **TinEye**.

	 Elements Identified	 Faces	 Structures	 Places	 Digital/ Logos	 Alternate Sizes	 Flipped or Altered
Google	1	Neutral	Great	Great	Great	Good	Neutral
Yandex	2+	Great	Great	Great	Good	Good	Good
Bing	3+	Good	Good	Good	Good	Neutral	Great
TinEye	1	Neutral	Neutral	Neutral	Great	Great	Good

Laboratorio



Laboratorio IMINT

Laboratorio IMINT



Laboratorio de investigación a partir de imágenes. (IMINT)

Modalidad:Teleformación (On-line)

<https://angeles-elearning.ccn-cert.cni.es/course/view.php?id=153>



Laboratory IMINT

Laboratory IMINT



Laboratory of Imagery intelligence (IMINT)

Modalidad:Teleformación (On-line)

<https://angeles-elearning.ccn-cert.cni.es/course/view.php?id=155>

Índice

- 01 Conceptos esenciales
- 02 Sobre Elena
- 03 Un ejemplo real: Counterfeit en comercios web
- 04 Un ejemplo de caso de investigación en Elena
- 05 Seguridad Operativa en actividades de cibervigilancia
- 06 Inteligencia de imágenes
- 07 Dorking con buscadores genéricos
- 08 Dorking con buscadores especializados
- 09 Reportando y entregando el producto
- Anexos



Definición de dorks

El término “**Dorks**” hace referencia a una serie de comandos u operadores de búsqueda disponibles en algunos buscadores, que permiten acotar y especificar la información en las consultas generadas; de este modo, a través de este tipo de consultas, se puede llegar incluso a obtener información sensible expuesta, previamente indexada.

A su vez, el uso de estos operadores, como técnica para extraer información sensible a través de Google, se conoce habitualmente como **Google Hacking**; de forma análoga, también se puede hablar de los términos **Bing Hacking** o **Shodan Hacking**, al hacer uso de esta técnica en estos buscadores.

Tipos de buscadores

1

—— **Buscadores genéricos u horizontales**

Son los buscadores que todo el mundo suele usar en su día a día, como por ejemplo, Google, Bing o Yahoo. Su objetivo es rastrear e indexar la máxima información posible.

2

—— **Buscadores especializados o verticales**

Buscadores especializados en un sector, temática o nicho concreto de información. Únicamente rastrean un número limitado de páginas específicas, por lo que su índice es más limitado pero mucho más específico.

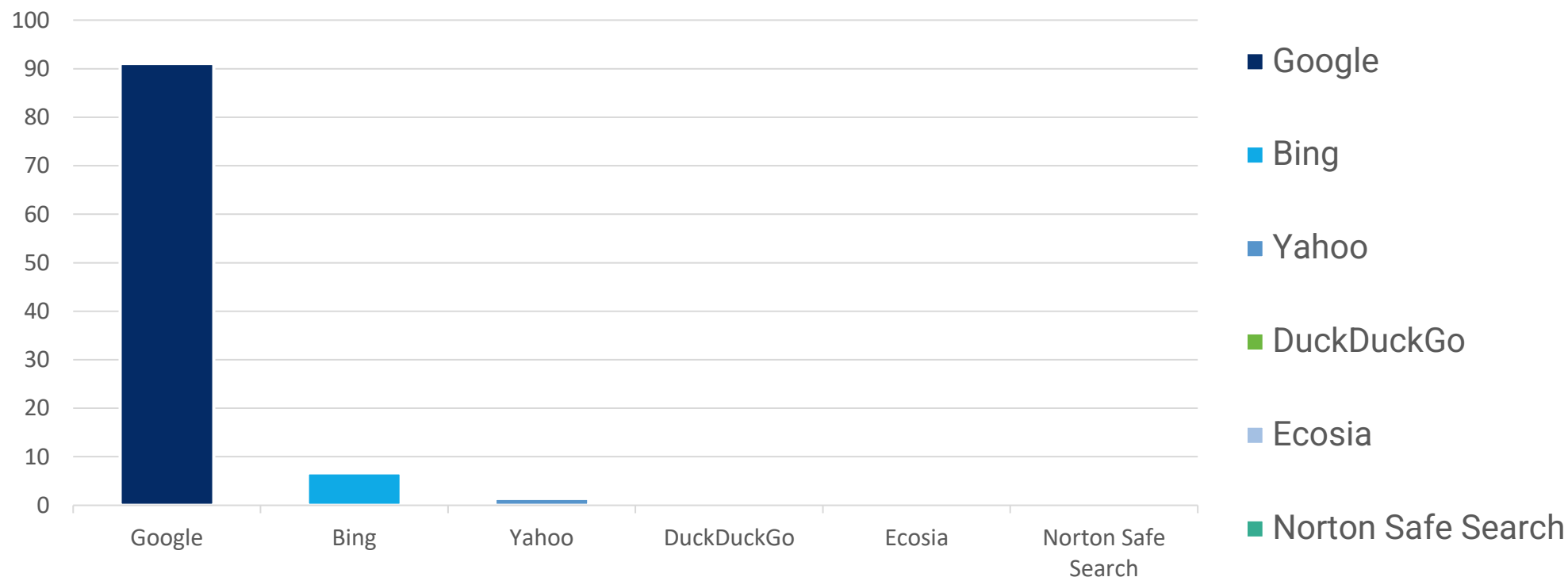
3

—— **Metabuscadore**s

Buscadores que permiten buscar en varios buscadores al mismo tiempo.

Buscadores genéricos

En **España**, hay un claro predominio de Google con más del 91,06% de cuota de mercado:



Google	bing	Yahoo!	DuckDuckGo	Ecosia	Norton Safe Search
91.06%	6.67%	1.39%	0.46%	0.29%	0.03%

* Search Engine Market Share in Spain - December 2020

Buscadores genéricos

Operador	Descripción
"Search Term"	Search for the exact phrase within " "
-	Remove pages that mention a given term from the search results
+	Force Google to return common words that might ordinarily be discarded
OR	Search for a given search term OR another term
site:	Search within a given domain
filetype:	Search for a certain file type
intitle:	Search for sites with the given word(s) in the page title
inurl:	Search for sites with the given word(s) in the URL
intext:	Search for sites with the given word(s) in the text of the page
inanchor:	Search for sites that have the given word(s) in links pointing to them
cache:	Show most recent cache of a webpage

inurl:intranet filetype:doc confidential

intitle:"Live view / – AXIS"

anonymous "#op*"

intitle:index of inurl://whatsapp/

"Dumped database"

site:reddit.com + "leak" | "bank" | "breach"

cache:intelcon.ginseg.com

Buscadores genéricos

Google

Búsqueda avanzada

Buscar páginas con...

todas estas palabras:

esta palabra o frase exactas:

cualquiera de estas palabras:

ninguna de estas palabras:

números desde el: hasta

A continuación, limitar los resultados por...

idioma:

región:

última actualización:

sitio o dominio:

los términos que aparecen:

Búsqueda Segura:

tipo de archivo:

derechos de uso:

Haz lo siguiente en el cuadro de búsqueda

Escribe las palabras importantes: terrier ratonero tricolor

Escribe las palabras exactas entre comillas: "terrier ratonero"

Escribe OR entre todas las palabras que quieras: miniatura OR estándar

Añade un signo menos delante de las palabras que no quieras que aparezcan: -roedor, -"Jack Russell"

Escribe dos puntos seguidos entre los números y añade una unidad de medida: 10..35 kg, 300..500 euros, 2010..2011

Busca páginas en el idioma que selecciones.

Busca páginas publicadas en una región determinada.

Busca páginas actualizadas en el periodo de tiempo especificado.

Busca un sitio (como wikipedia.org) o limita los resultados a un dominio como, por ejemplo, .edu, .org o .gov.

Busca términos en toda la página, en el título de la página o en la dirección web, o enlaces a la página que estás buscando.

Indica a Búsqueda Segura si quieres que filtre contenido sexualmente explícito.

Busca páginas en el formato que prefieras.

Busca páginas que puedas utilizar libremente.

"password" site:pastebin.com

Q Todo Imágenes Videos Noticias Shopping Más Configuración

Cualquier país Cualquier idioma Últimas 24 horas Todos los resultados Borrar

username : utuhkajung password : riski266 username ...
https://pastebin.com > NNpPKUt4 Traducir esta página
hace 5 horas - username : utuhkajung password : riski266 username : tomokboys02.
password : s0219995690. username : TINBELIKMAL27 password : Granita123.

username : batamcrow789 password : ldssurya3rv username ...
https://pastebin.com > bxaMQEMx Traducir esta página
hace 22 horas - password : ldssurya3rv. username : pj066. password : strippink05.
username : pahlawanpro. password : mess262roko1. username : senti428. password : ...

username : KRWsantuy password : karawang123 username ...
https://pastebin.com > ... Traducir esta página
hace 15 horas - password : karawang123. username : rsudpb780. password : tongbores148.
username : hedohedu. password : heidia03654. username : heidia007. password : ...

username : corazon0101 password : andresusilo131 ...
https://pastebin.com > SPjtHyeE Traducir esta página
hace 3 horas - password : andresusilo131. username : yumi6636. password : bowo6636.
username : jabar12345. password : anakmamah123. username : incom2345.

username : dullah007 password : mamapapa00123 ...
https://pastebin.com > ... Traducir esta página
hace 1 hora - password : galfila25. username : sempakkuda123456. password :
sempakkuda123. username : frozz310. password : sman14sketsa. username : siakew2.



https://www.google.es/advanced_search

Base de conocimiento de Google Dorks

The screenshot displays the 'Google Hacking Database' interface on the website <https://www.exploit-db.com/google-hacking-database>. The page features a sidebar with navigation icons and a main content area with a table of dorks. A callout box points to the table, stating: 'Se muestran distintos dorks que se pueden usar para acceder a bases de datos'.

Date Added	Dork	Category	Author
2020-02-20	intitle:"index of" "env.bak"	Files Containing Juicy Info	Hilary Soita
2020-02-20	intitle:"index of" "smtp.log"	Files Containing Juicy Info	Magratur Alam Sofily
2020-02-20	inurl:ReportViewer.aspx	Advisories and Vulnerabilities	rhinofense.com
2020-02-20	inurl:/swagger/index.html	Various Online Devices	MuckT
2020-02-20	intitle: index of "*db.tar.gz"	Files Containing Juicy Info	berat isler
2020-02-20	intext:"username=" AND "password=" ext:log	Files Containing Passwords	Hilary Soita
2020-02-20	intitle:"index of/" "db.sql"	Files Containing Juicy Info	Ishan Saha
2020-02-19	intitle:index.of "awsconfig.json"	Files Containing	
2020-02-19	intitle:index.of "db.zip"	Sensitive Dir	
2020-02-18	intitle:VMware intext:"VMware, Inc. All rights reserved." AND "Powered by VMware Studio"	Pages Containing	
2020-02-18	site:bamboo.* ext:action build	Footho	
2020-02-17	intext:"SECRET_KEY" ext:py inurl:mysite -site:stackoverflow.com -site:github.com	Files Containing	
2020-02-17	intitle:index.of "backwpup"	Sensitive Dir	
2020-02-14	intitle:index.of "keys.txt"	Files Containing Juicy Info	CANCOM #RedTeam
2020-02-14	intitle:"index of" intext:"access.txt"	Files Containing Juicy Info	CANCOM #RedTeam

Showing 1 to 15 of 5,254 entries

Pagination: FIRST PREVIOUS 1 2 3 4 5 ... 351 NEXT LAST

Automatización de alertas - Google Alerts

1

Monitorización de protestas
Ejemplo: anonymous and España

2

Estar al día en los temas de interés
Ejemplo: España or Manifestación site:twitter.com

3

Monitorización de nuestra identidad
Ejemplo: Nombre Apellido

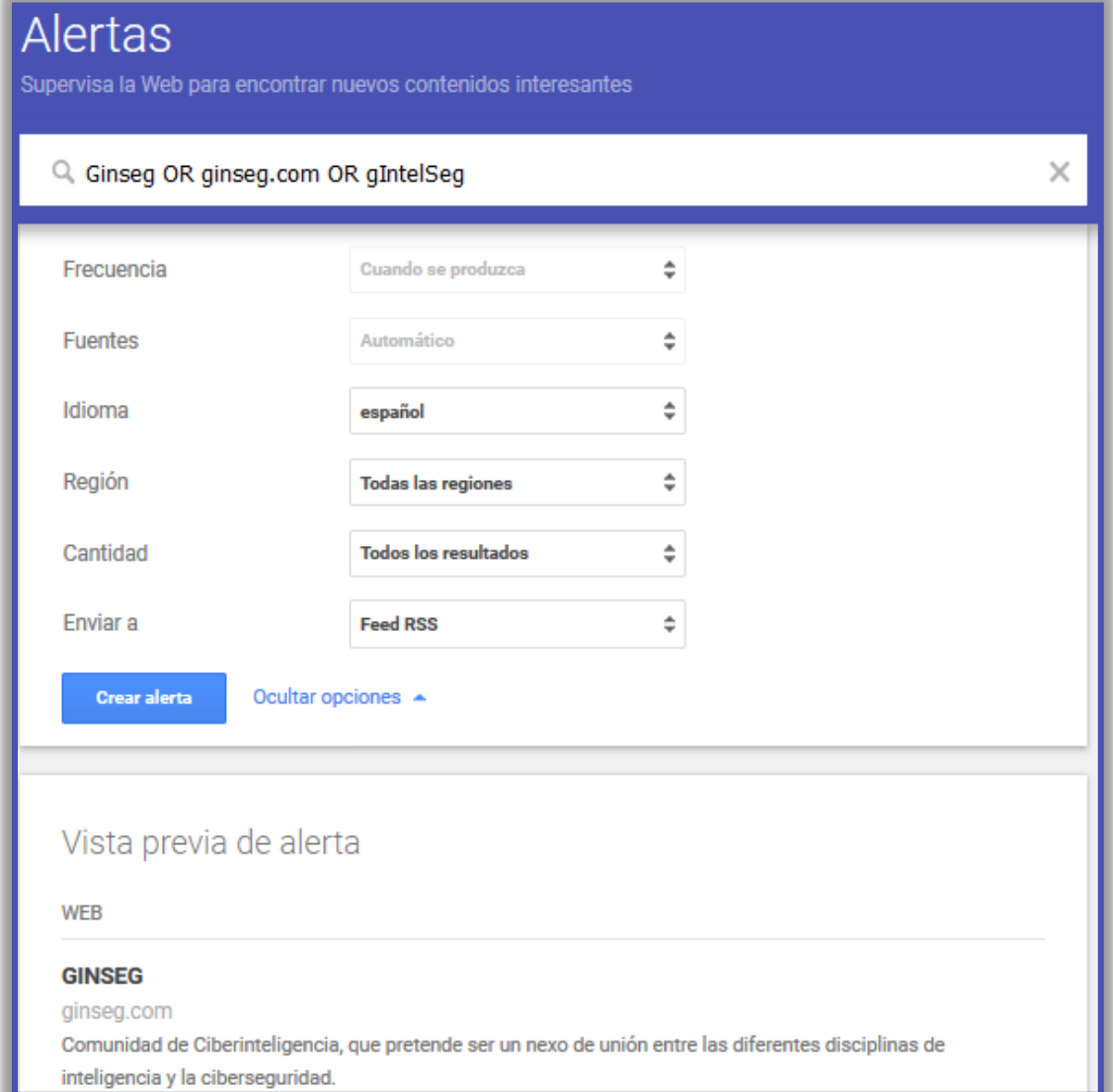
4

Buscando ofertas de trabajo
Ejemplo: oferta de trabajo + analista inteligencia

5

Subvenciones
Ejemplo: Location:España subvención
investigación cyber or cyber research

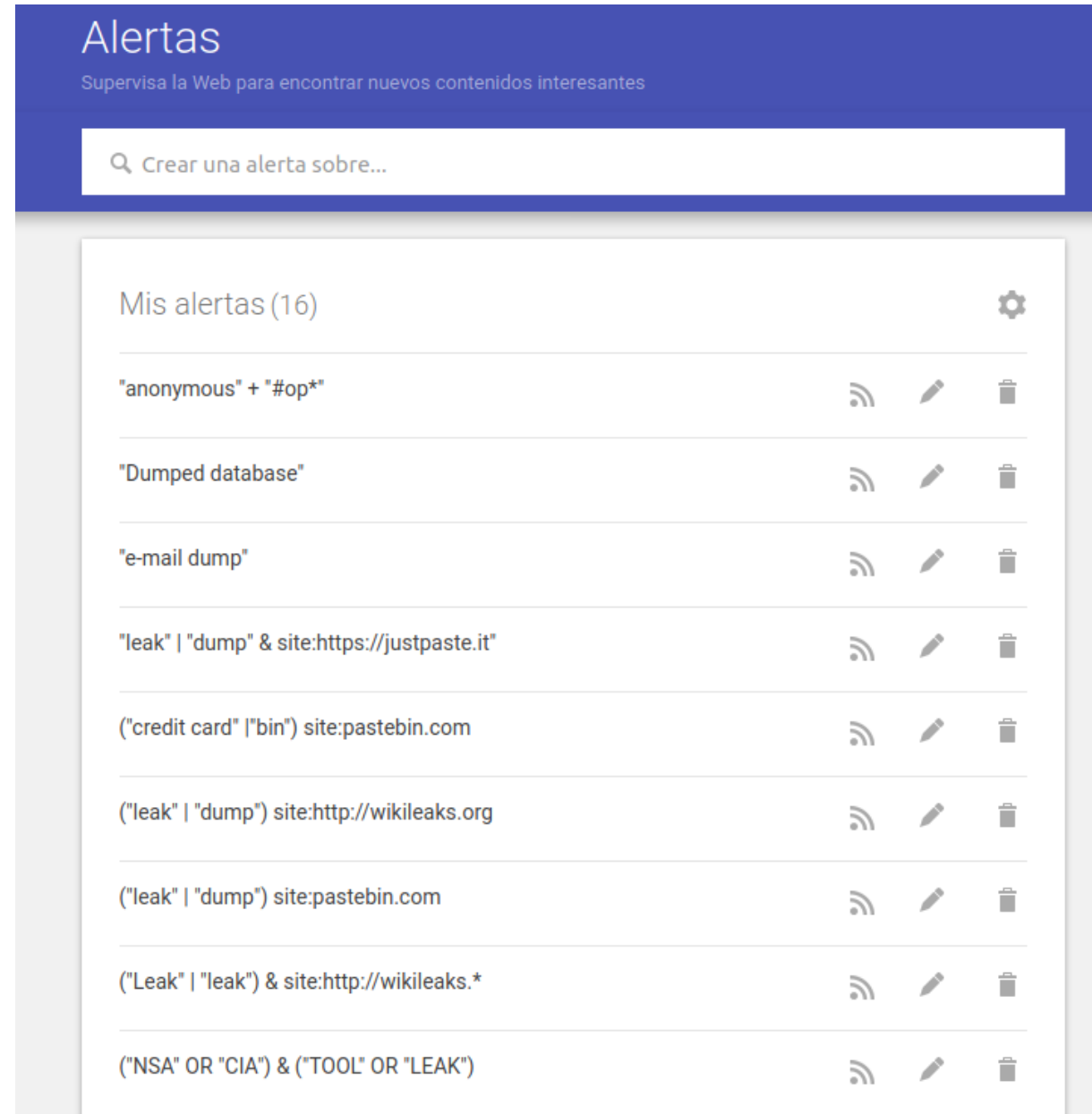
N



The screenshot displays the Google Alerts configuration page. At the top, the title 'Alertas' is followed by the subtitle 'Supervisa la Web para encontrar nuevos contenidos interesantes'. Below this is a search bar containing the query 'Ginseg OR ginseg.com OR gIntelSeg'. To the right of the search bar is a close button (X). Below the search bar, there are several dropdown menus for configuring the alert: 'Frecuencia' (set to 'Cuando se produzca'), 'Fuentes' (set to 'Automático'), 'Idioma' (set to 'español'), 'Región' (set to 'Todas las regiones'), 'Cantidad' (set to 'Todos los resultados'), and 'Enviar a' (set to 'Feed RSS'). Below these menus are two buttons: 'Crear alerta' (highlighted in blue) and 'Ocultar opciones' (with a small upward arrow). Below the configuration section, there is a 'Vista previa de alerta' (Alert preview) section. It shows a sample alert entry for 'GINSEG' from 'ginseg.com', with a description: 'Comunidad de Ciberinteligencia, que pretende ser un nexo de unión entre las diferentes disciplinas de inteligencia y la ciberseguridad.'

Automatización de alertas - Google Alerts

- 1 Elegimos las keywords que queremos monitorizar
- 2 Creamos una alerta por cada monitorización a realizar
- 3 Elección de envío a feed RSS



The screenshot shows the Google Alerts web interface. At the top, there's a blue header with the word "Alertas" and the subtitle "Supervisa la Web para encontrar nuevos contenidos interesantes". Below this is a search bar with the placeholder text "Crear una alerta sobre...". The main content area is titled "Mis alertas (16)" and lists 16 individual alerts. Each alert entry consists of a keyword phrase, an RSS icon, an edit icon (pencil), and a delete icon (trash). The keywords listed are:

- "anonymous" + "#op**"
- "Dumped database"
- "e-mail dump"
- "leak" | "dump" & site:https://justpaste.it"
- ("credit card" | "bin") site:pastebin.com
- ("leak" | "dump") site:http://wikileaks.org
- ("leak" | "dump") site:pastebin.com
- ("Leak" | "leak") & site:http://wikileaks.*
- ("NSA" OR "CIA") & ("TOOL" OR "LEAK")

Laboratorio



<https://angeles-elearning.ccn-cert.cni.es/course/view.php?id=159>



<https://angeles-elearning.ccn-cert.cni.es/course/view.php?id=165>

Buscadores genéricos - Bing

Comillas "" Permiten buscar cadenas de texto concretas.

Guion - Permite negar expresiones o términos en la búsqueda.

site Permite listar toda la información de un dominio concreto.

filetype Permite hacer búsquedas por tipo de fichero.

ext Permite hacer búsquedas por la extensión del archivo, por ejemplo, pdfs, imágenes, png, jpg, etc.

feed Permite buscar directamente un feed RSS de una página web.

intitle Permite buscar páginas que contiene términos específicos en el título.

instreamset:(url):xxxx Permite buscar páginas que contienen términos específicos en la dirección URL.

Buscadores genéricos - Bing



The screenshot shows the Microsoft Bing search engine interface. The search bar at the top contains the query 'domain:ginseg.com'. Below the search bar, the 'TODO' filter is selected. The search results show 21 results. The first result is titled 'Introducción a la Inteligencia - GINSEG' with a URL 'https://ginseg.com/2018/897/inteligencia/introduccion-a-la-inteligencia'. The second result is titled 'IntelCon | Congreso de Ciberinteligencia Online' with a URL 'https://intelcon.ginseg.com'. The interface includes filters for 'Fecha', 'Idioma', and 'Región', and a toggle for 'Abrir vínculos en una pestaña nueva'.

Microsoft Bing

domain:ginseg.com

TODO

21 Resultados Fecha Idioma Región Abrir vínculos en una pestaña nueva

[Introducción a la Inteligencia - GINSEG](https://ginseg.com/2018/897/inteligencia/introduccion-a-la-inteligencia)
<https://ginseg.com/2018/897/inteligencia/introduccion-a-la-inteligencia>
En este post vamos a describir los conceptos introductorios relacionados con la Inteligencia comenzando por su propia definición. Especificaremos el proceso por el que es indispensable que un dato sea transformado en información, para posteriormente obtener la inteligencia necesaria que podrá ser utilizada en una toma de decisiones acertadas.

[IntelCon | Congreso de Ciberinteligencia Online](https://intelcon.ginseg.com)
<https://intelcon.ginseg.com>
El objetivo del congreso es la difusión de conocimientos de calidad sobre Ciberinteligencia de forma gratuita y en sus diferentes áreas asociadas, para formar ...



<https://www.bing.com>

Buscadores genéricos - Bing



ip: 151.101.53.50

TODO IMÁGENES VÍDEOS MAPAS NOTICIAS SHOPPING

24.000.000 Resultados Fecha Idioma Región Abrir vínculos en una pestaña nueva

[Telva - Revista de Moda y Belleza](https://www.telva.com) ✓
<https://www.telva.com> ▾
Tu revista de moda y belleza. Toda la actualidad sobre celebrities, pasarelas y tendencias. Consejos, estilo de vida, fitness...
[Moda](#) · [Cocina](#) · [Belleza](#) · [Estilo de Vida](#) · [Recetas](#)

[NFL 2020: Los líderes en las estadísticas de la temporada ...](https://us.marca.com/claro/futbol-americano/nfl/album/2021/01/05/5ff4b...) ✓
<https://us.marca.com/claro/futbol-americano/nfl/album/2021/01/05/5ff4b...> ▾
5/1/2021 · mpletando así los 256 partidos de la fase regular. 14 equipos siguen con aspiraciones de ganar el Super Bowl LV, mientras que otros 18 ya piensan en la siguiente temporada, poniendo la mira en el Draft. ¿Quiénes fueron los jugadores más destacados en las 17 semanas de la temporada 2020? Aquí te presentamos a los líderes en las principales categorías: yardas, anotaciones...



<https://www.bing.com>

Buscadores genéricos - Baidu



<http://www.baidu.com/>



百度一下

Cuarto proveedor de búsqueda en cuota de mercado a nivel mundial, también conocido como el “Google Chino”.

En **China** es el principal motor de búsqueda; sin embargo, está limitado por la férrea censura estatal china que supervisa de cerca y bloquea gran parte de los sitios internacionales, promoviendo así ciertas plataformas y webs locales en su lugar.





Buscadores genéricos - Baidu

Comillas "" Permiten buscar cadenas de texto concretas

Guion - Permite negar expresiones o términos en la búsqueda

site Permite listar toda la información de un dominio concreto

filetype Permite hacer búsquedas por tipo de fichero

domain Permite listar toda la información de un dominio concreto

intitle Permite buscar páginas que contiene términos específicos en el título

Inurl Permite buscar páginas que contiene términos específicos en la URL

Buscadores genéricos - Yandex



 <https://yandex.com/>

Yandex

Quinto proveedor de búsqueda más grande del mundo, que controla más del 61% de las búsquedas en **Rusia** y en otros países de su área idiomática, como **Kazajstán, Bielorrusia y Ucrania**.



Buscadores genéricos - Yandex

Comillas "" Permiten buscar cadenas de texto concretas.

! Permite buscar palabras concretas.

* Permite reemplazar cero o más caracteres.

site Permite listar toda la información de un dominio concreto.

url o host o domain Permite listar toda la información de una URL concreta o las páginas asociadas a un dominio

mime Permite hacer búsquedas por tipo de fichero

date Permite buscar coincidencias mediante fechas dadas. (Entre dos fechas < date:YYYYMMDD..YYYYMMDD>)

Title[keyword] Permite buscar páginas que contiene términos específicos en el título.

Inurl Permite buscar páginas que contiene términos específicos en la URL.

Buscadores genéricos - Archive

Archive permite realizar búsquedas de páginas webs y de usuarios de redes sociales para visualizar el contenido cacheado en su Base de Datos.




Internet Archive is a non-profit library of millions of free books, movies, software, music, websites, and more.

								
411B	23M	5.5M	9.0M	2.0M	520K	3.4M	213K	720K

[Advanced Search](#)

Announcements

Archiving Information on the Novel Coronavirus (Covid-19)

Our Social Media is Broken. Is Decentralization the Fix?

Libraries and Publishing Now— Viva la Library!

[SEE MORE](#)

<https://archive.org/>

Buscadores genéricos - Archive

Archive dispone de múltiples filtros de búsqueda totalmente personalizables y de un repositorio de históricos de screenshot sobre páginas web.

Advanced Search returning JSON, XML, and more

This will return results in the format of your choice.

Query:

Fields to return (pick one or more):

avg_rating
backup_location
btih
call_number
collection
contributor
coverage
creator
date
description
downloads
external-identifier
foldoutcount
format
genre
headerImage
identifier
imagecount
indexflag
item_size
language
licenseurl
mediatype
members
month
name
noindex
num_reviews
oai_updatedate
publicdate
publisher
related-external-id
reviewdate

(optional) Sort results by:

▼
▼
▼

Number of results:

50

Page:

1

JSON format: ☒

XML format: ☐

save to file: ☒

HTML table: ☐

CSV format: ☐

[\(show/hide help\)](#)

RSS format: ☐

("Fields to return" ignored)

Search

Advanced Search

This form allows you to perform an advanced search. You only need to fill in one field below. This can be combined with other fields. You must select one other field.

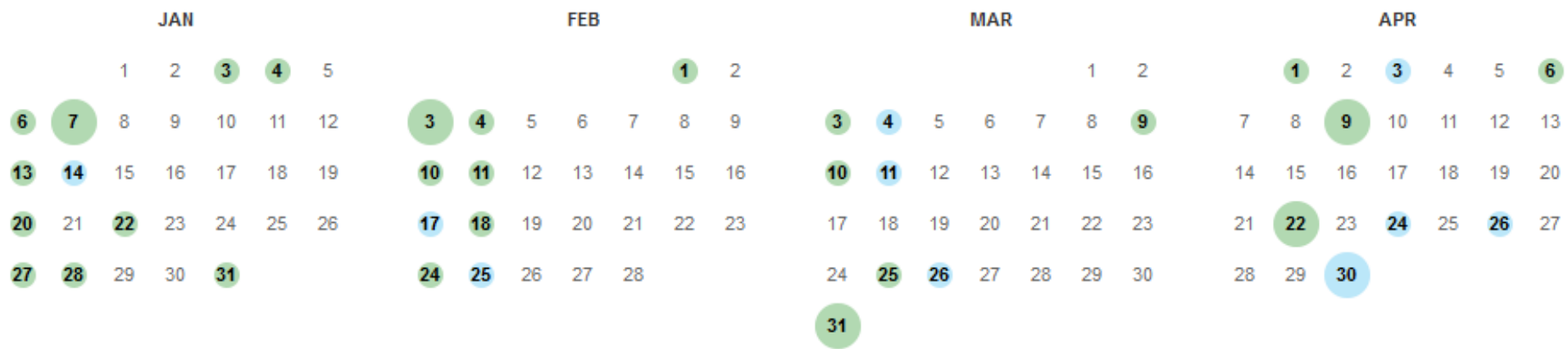
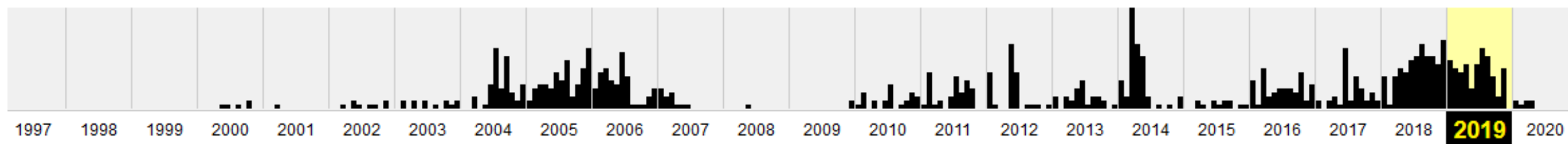
AND	Any field:	contains						
AND	Title:	contains						
AND	Creator:	contains						
AND	Description:	contains						
AND	Collection:	is						
AND	Mediatype:	is	All mediatypes					
AND		Custom field						
AND		Custom field						
AND		Custom field						
AND	Date:	YYYY	MM	DD				
AND	Date range:	YYYY	MM	DD	TO	YYYY	MM	DD

Search

Buscadores genéricos - Archive

Archive dispone de **múltiples filtros de búsqueda** totalmente **personalizables** y de un repositorio de históricos de screenshot sobre páginas web.

Saved **825 times** between **May 11, 2000** and **April 6, 2020**.



Buscadores genéricos - Archive

También permite **generar de forma manual un screenshot**, sobre el contenido que queramos registrar e indexar en su Base de Datos, pudiendo así consultar este contenido posteriormente aunque sea eliminado.

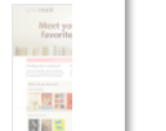


INTERNET ARCHIVE
WayBackMachine

DONATE

Explore more than 468 billion [web pages](#) saved over time





 **Tools**

[Wayback Machine Availability API](#)
[Chrome Extension](#)
[Firefox Add-on](#)
[Safari Extension](#)
[iOS app](#)
[Android app](#)

 **Subscription Service**

Archive-It enables you to capture, manage and search collections of digital content without any technical expertise or hosting facilities. [Visit Archive-It to build and browse the collections.](#)

 **Save Page Now**

Capture a web page as it appears now for use as a trusted citation in the future.



<https://web.archive.org/save>

También permite **generar de forma manual un screenshot**, sobre el contenido que queramos registrar e indexar en su Base de Datos, pudiendo así consultar este contenido posteriormente aunque sea eliminado.

[DONATE](#)

INTERNET ARCHIVE

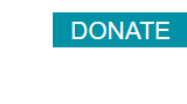
WayBackMachine

 Save Page Now

☒ Save error pages (HTTP Status=4xx, 5xx)

SAVE PAGE

Capture a web page as it appears now for use as a trusted citation in
[Sign in](#) to use extra features: "Save outlinks", "Save screen shot" and "M...



INTERNET ARCHIVE

WayBackMachine

DONATE

Saving page <http://ginseg.com>

✓ Done!

A snapshot was captured. Visit page: <http://web.archive.org/web/20210117101736/http://ginseg.com/>

http://ginseg.com/

https://ginseg.com/

https://c0.wp.com/c/5.5.3/wp-includes/css/dist/block-library/style.min.css

https://c0.wp.com/c/5.5.3/wp-includes/css/dashicons.min.css

https://c0.wp.com/p/jetpack/9.2/css/jetpack.css

https://c0.wp.com/c/5.5.3/wp-includes/js/jquery/jquery.js

https://c0.wp.com/c/5.5.3/wp-includes/js/Utils.min.js

https://c0.wp.com/c/5.5.3/wp-includes/js/underscore.min.js

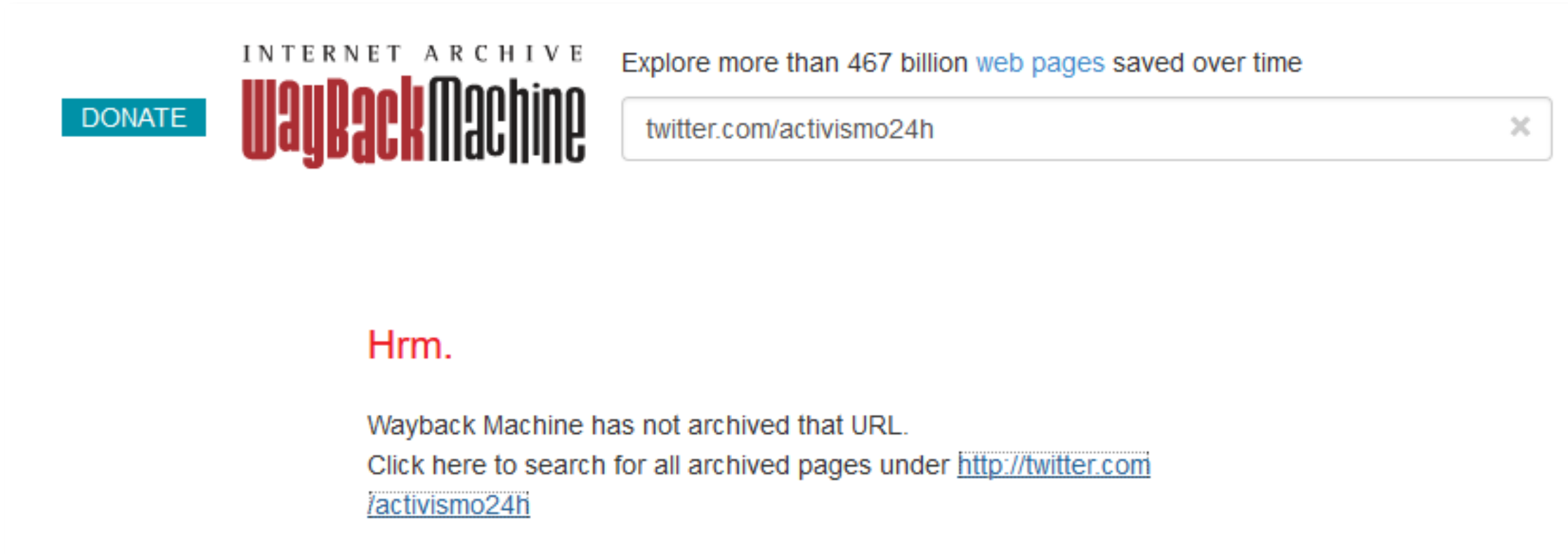
https://fonts.googleapis.com/css?family=Montserrat

https://ginseg.com/wp-content/plugins/buddypress/bp-members/css/blocks/member.min.css?ver=6.4.0

Downloaded elements: 73

Buscadores genéricos - Archive

Archive permite realizar búsquedas de páginas webs y de usuarios de redes sociales para visualizar el contenido cacheado en su Base de Datos.



INTERNET ARCHIVE

WayBackMachine

DONATE

Explore more than 467 billion web pages saved over time

twitter.com/activismo24h

Hrm.

Wayback Machine has not archived that URL.

Click here to search for all archived pages under <http://twitter.com/activismo24h>

 <https://web.archive.org/>

Buscadores genéricos - Archive

Archive permite realizar búsquedas de páginas webs y de usuarios de redes sociales para visualizar el contenido cacheado en su Base de Datos.

INTERNET ARCHIVE

DONATE

WayBackMachine

Go Wayback!

380 URLs have been captured for this domain.

Filter results (i.e. '.txt'):							URL or MIME Type
URL	MIME TYPE	FROM	TO	CAPTURES	DUPLICATES	UNIQUES	
https://twitter.com/Activismo24h/status/1015553564205305856	text/html	Mar 10, 2020	Mar 10, 2020	1	0	1	
https://twitter.com/Activismo24h/status/1037746470508797953	text/html	Jun 5, 2020	Jun 5, 2020	1	0	1	
https://twitter.com/Activismo24h/status/1104096166977945600	text/html	Mar 8, 2020	Mar 8, 2020	1	0	1	
https://twitter.com/Activismo24h/status/1226828086202626048	text/html	Mar 6, 2020	May 12, 2020	2	0	2	
https://twitter.com/Activismo24h/status/1232375628600631299	text/html	Feb 25, 2020	Feb 25, 2020	1	0	1	
https://twitter.com/Activismo24h/status/1232379309966471169	text/html	Feb 25, 2020	Feb 25, 2020	1	0	1	



<https://web.archive.org/>

Índice

- 01 Conceptos esenciales
- 02 Sobre Elena
- 03 Un ejemplo real: Counterfeit en comercios web
- 04 Un ejemplo de caso de investigación en Elena
- 05 Seguridad Operativa en actividades de cibervigilancia
- 06 Inteligencia de imágenes
- 07 Dorking con buscadores genéricos
- 08 Dorking con buscadores especializados
- 09 Reportando y entregando el producto
- Anexos



Buscadores especializados

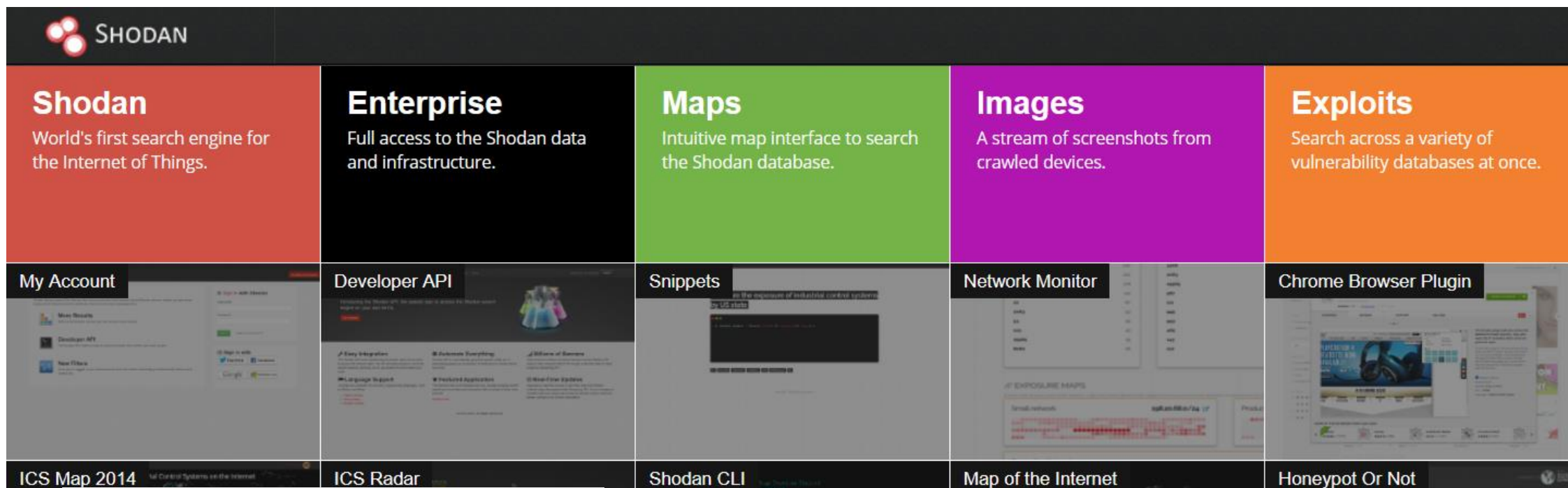


Tal como se ha indicado previamente, los buscadores especializados o verticales permiten obtener gran información relevante sobre una cuestión o tema específico.

A pesar de que existe gran cantidad de subtipos, resulta fundamental destacar entre estos los orientados al Internet de las Cosas (IoT), que identifican e indexan en su índice otro tipo de información, tal como direcciones IP, puertos y servicios de dispositivos expuestos a Internet.

Buscadores especializados - Shodan

Herramienta que realiza un ZMAP hacia todos los **dispositivos, dominios, direcciones IP** conectados a **Internet**, ofreciendo información relacionada mediante un buscador. En **desarrollo y evolución constante**, como puede ser el **módulo de Exploits** para realizar búsquedas sobre vulnerabilidades o el **módulo de Honeypot or Not**.



<https://www.shodan.io>



Buscadores especializados - Shodan

country	Permite filtrar por sistemas publicados en un país concreto.
city	Permite filtrar por la ciudad en la que se encuentre un sistema.
geo	Permite filtrar por las coordenadas de latitud y longitud.
port	Permite filtrar por puertos específicos.
net	Permite filtrar por una IP específica o por rangos de IP.
os	Permite filtrar por sistema operativo.
hostname	Permite para filtrar por nombre de host.
before/after	Permite filtrar la búsqueda a un periodo concreto.

Buscadores especializados - Shodan

intitle:"Live view / - AXIS"

image is displayed, there might be too many viewers, or the ...

es-la.facebook.com › theviperxxsy › posts › live-view-... ▼

Assaf - Live view - AXIS 206M Network Camera version 4.11 ...

Ver más de Assaf en Facebook. Iniciar sesión. ¿Olvidaste tu cuenta? o. Crear cuenta nueva. Ahora no. Páginas relacionadas. Eset Mobile Security. Teléfono/ ...

vroomshoopwebcam.mine.nu ▼ Traducir esta página

Live view / - AXIS 205 version 4.03

CENTRUMBRUG VROOMSHOOP. If no image is displayed, the browser configuration will probably have to be changed.



<http://vroomshoopwebcam.mine.nu/>

Se muestra como se accede a una cámara haciendo la búsqueda de Google de intitle:"Live view / - AXIS"



AXIS 205 Network Camera

Live View

View Size:



Greetings from Vroomshoop by dutchmanrenzo.nl Thu.1.1.1970 06:08:57

Buscadores especializados



SCANNERS

TOOLS

Use this **DNS lookup** tool to easily view the standard DNS records for a domain.

vroomshoopwebcam.mine.nu

GET THE DNS RECORDS

A : 213.184.127.123

Se muestra como se accede a la IP de un dominio con hackertarget.com/dns-lookup/ y después con se hace búsqueda de esa IP en shodan y se encuentra un puerto abierto con una cámara



<https://hackertarget.com/dns-lookup/>

Buscadores especializados - Shodan

🌐 213.184.127.123 123-127-184-213.dynamic.caiway.nl

City	Enschede
Country	Netherlands
Organization	DELTA Fiber Nederland B.V.
ISP	DELTA Fiber Nederland B.V.
Last Update	2021-04-23T19:45:44.983455
Hostnames	123-127-184-213.dynamic.caiway.nl
ASN	AS15435

⚡ Web Technologies

Se muestra como se accede a la IP de un dominio con hackertarget.com/dns-lookup/ y después con se hace búsqueda de esa IP en shodan y se encuentra un puerto abierto con una cámara



<https://www.shodan.io/host/213.184.127.123>

🔌 Ports

79	80	81	82
----	----	----	----

🔌 Services

79	HTTP/1.0 400 Bad Request
tcp	X-Frame-Options: sameorigin
newline-tcp	Date: Fri, 26 Mar 2021 00:14:03 GMT
	Accept-Ranges: bytes
	Connection: close
	Content-Type: text/html; charset=ISO-8859-1
	<HTML><HEAD><TITLE>400 Bad Request</TITLE></HEAD>
	<BODY><H1>400 Bad Request</H1>
	Your client has issued a malformed or illegal request.
	</BODY></HTML>

80	HTTP/1.0 200 OK
tcp	X-Frame-Options: sameorigin
http	Content-Length: 5731
	Last-Modified: Wed, 07 Apr 2021 14:02:02 GMT
	Cache-Control: no-cache
	Content-Type: text/html



Buscadores especializados - Shodan

The screenshot displays the Shodan search engine interface. At the top, the search bar contains the query 'product:AXIS'. Below the search bar, there are navigation tabs for 'Exploits', 'Maps', 'Share Search', 'Download Results', and 'Create Report'. The main content area shows search results for the query 'product:AXIS'. On the left, there is a section titled 'TOTAL RESULTS' showing '7,236' results. Below this is a 'TOP COUNTRIES' section with a world map and a list of countries: United States (2,814), Russian Federation (424), France (418), Mexico (381), and Germany (289). On the right, there is a 'New Service' banner for 'Shodan Monitor'. Below the banner, there are two search results. The first result is for IP '150.201.136.221', identified as 'Central Methodist University' in the 'United States, Cape Girardeau'. The second result is for IP '87.130.17.125', identified as 'Deutsche Telekom AG' in 'Germany, Ilmenau'. Both results show a list of implemented commands: USER, QUIT, PASS, SYST, HELP, PORT, PASV, LIST, NLST, RETR, STOR, TYPE, MKD, RMD, DELE, PWD, CWD, SITE, CDUP, RNFR, RNTD, ...

SHODAN product:AXIS

Explore Downloads Reports Pricing Enterprise Access

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
7,236

TOP COUNTRIES

United States 2,814
Russian Federation 424
France 418
Mexico 381
Germany 289

TOP SERVICES

FTP 7,111

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

150.201.136.221
Central Methodist University
Added on 2021-01-17 12:24:01 GMT
United States, Cape Girardeau

220 AXIS Q6034-E PTZ Dome Network Camera 5.51.6.1 (2019) ready.
530 Login incorrect.
214-The following commands are implemented.

USER	QUIT	PASS	SYST	HELP	PORT	PASV	LIST
NLST	RETR	STOR	TYPE	MKD	RMD	DELE	PWD
CWD	SITE	CDUP	RNFR	RNTD	...		

87.130.17.125
Deutsche Telekom AG
Added on 2021-01-17 12:23:51 GMT
Germany, Ilmenau

220 AXIS Q6114-E PTZ Dome Network Camera 6.50.3.1 (2019) ready.
530 Login incorrect.
214-The following commands are implemented.

USER	QUIT	PASS	SYST	HELP	PORT	PASV	LIST
NLST	RETR	STOR	TYPE	MKD	RMD	DELE	PWD
CWD	SITE	CDUP	RNFR	RNTD	...		

Se muestra una imagen donde se está realizando una búsqueda en Shodan con el filtro product: AXIS y se ven los diferentes resultados que se devuelven



Buscadores especializados - Censys



Herramienta similar a Shodan, siendo el buscador desarrollado para Scans.io y poder localizar activos conectados a Internet relacionados a **IPv4**, **Sitios Webs** y **certificados**.



<https://censys.io>

The Most Complete View of the Internet

Censys is the most reputable, exhaustive, and up-to-date source of Internet scan data in the world, so you see everything.

Search IPv4



Search Certificates



Search Websites



228,628,886

Active IP Addresses



2,029

Ports



36

Protocols Scanned



676,641,933

Active Services



40

Risk Classifications



3,519,772,418

Certificates



225,267,600

Domain Names



228,982

Software Packages

Buscadores especializados - Censys

<https://censys.io/ipv4>

Search Censys Data

Search IPv4



Search Certificates



Search Websites



Se muestra los resultados que devuelve la página de Censys haciendo un filtrado por IPv4

The screenshot displays the Censys search interface. At the top, there is a search bar with a dropdown menu set to 'IPv4 Hosts'. Below the search bar, a 'Quick Filter' section lists 'IPv4 Hosts', 'Websites', and 'Certificates'. The main results area shows a list of Autonomous Systems (ASes) on the left and detailed information for selected IP addresses on the right. The selected IP addresses are 109.222.183.92 and 46.36.197.169. The first result, 109.222.183.92, is associated with France Telecom - Orange (3215) and is located in La Couronne, Nouvelle-Aquitaine, France. It is also associated with Raspberry Pi and Raspbian 10deb9u5. The second result, 46.36.197.169, is associated with PUREBROADBAND (201508) and is located in Hull, England, United Kingdom. Both results are associated with 22/ssh.

Search results for IPv4 Hosts:

- 109.222.183.92 (apoitiers-655-1-479-92.w109-222.abo.wanadoo.fr.)
 - France Telecom - Orange (3215)
 - La Couronne, Nouvelle-Aquitaine, France
 - Raspberry Pi
 - Raspbian 10deb9u5
 - 22/ssh
- 46.36.197.169 (no-dns-yet.purebroadband.net.197.36.46.in-addr.arpa.)
 - PUREBROADBAND (201508)
 - Hull, England, United Kingdom
 - 22/ssh

Buscadores especializados - Censys

<https://censys.io/certificates>

Search Censys Data

Search IPv4 →

Search Certificates →

Search Websites →

Se muestra los resultados que devuelve la página de Censys haciendo un filtrado por certificados



Q Certificates

Search

Quick Filters

For all fields, see [Data Definitions](#)

Tag:

2640.1M CT

2600.63M Leaf

2534.57M DV

2512.78M Google CT

2429.1M Expired

[More](#)

Issuer:

2285.69M Let's Encrypt

357.33M cPanel, Inc.

124.79M CloudFlare, Inc.

105.35M Sectigo Limited

70.22M COMODO CA Limited

[More](#)

Certificates

Page: 1/145,639,591 Results: 3,640,989,762 Time: 8898ms Query Plan: [expanded](#)

[OU=Domain Control Validated, OU=PositiveSSL, CN=www.flourishgardens.co.nz](#)

Sectigo RSA Domain Validation Secure Server CA

2019-08-21 – 2020-09-03

flourishgardens.co.nz, www.flourishgardens.co.nz

[CN=www.fulle-keramik.de](#)

Encryption Everywhere DV TLS CA - G1

2019-08-20 – 2020-09-03

fulle-keramik.de, www.fulle-keramik.de

[CN=ssltest.datalou.com](#)

Amazon

2019-08-20 – 2020-09-20

ssltest.datalou.com

Buscadores especializados - Censys

<https://censys.io/domain>

Search Censys Data

Search IPv4



Search Certificates



Search Websites



Se muestra los resultados que devuelve la página de Censys haciendo un filtrado por dominio

 **Censys**

Q Websites Search

Quick Filters

For all fields, see [Data Definitions](#)

Protocol:

- 830.5K 443/https
- 672.57K 80/http
- 667.47K 80/http_www
- 633.6K 443/https_www
- 470.32K 25/smtp

Tag:

- 867.61K http
- 638.62K https
- 470.32K smtp
- 910 rsa-export

Websites

Page: 1/36,865 Results: 921,611 Time: 262ms Query Plan: [expanded](#)

-  [google.com \(216.58.211.46\)](#)
 - ★ 1 ⚙ 25/smtp, 443/https, 443/https_www, 80/http, 80/http_www
 - 🏠 Google 🔒 *.google.com, *.android.com, *.appengine.google.com
-  [youtube.com \(216.58.201.174\)](#)
 - ★ 2 ⚙ 25/smtp, 443/https, 443/https_www, 80/http, 80/http_www
 - 🏠 YouTube 🔒 *.google.com, *.android.com, *.appengine.google.com
-  [tmall.com \(140.205.130.99\)](#)
 - ★ 3 ⚙ 25/smtp, 443/https, 443/https_www, 80/http, 80/http_www
 - 🏠 天猫tmall.com-理想生活上天猫 🔒 *.tmall.com, *.1688.com, m.intl.taobao.com

Buscadores especializados - Censys

Se permiten los siguientes términos: and (y), or (o) y not (no mostrar en los resultados).

[] Permite filtrar por rangos numéricos inclusivos.

{ } Permite filtrar por rangos numéricos exclusivos.

? Permite reemplazar un solo carácter.

* Permite reemplazar cero o más caracteres.

^ Permite dar mayor relevancia a un término en la búsqueda.

ip: xxx.xxx.xxx.xxx/xx (rango IP concreto) o ip: [xxx.xxx.xxx.xxx TO xxx.xxx.xxx.xxx] (una serie de direcciones IP específicas).

[xxxx-xx-xx TO xxxx-xx-xx] (rango de fecha exacto) o [xxxx-xx-xx TO *] (rango de fecha abierto).

a:dominio.com o mx:dominio.com Permite realizar consultas DNS.

Casos de estudio



Dorking con buscadores
genéricos y especializados

Modalidad: Teleformación (On-line)

<https://angeles-elearning.ccn-cert.cni.es/course/view.php?id=244>



Dorking with generic and
specialized search engines

Simulation scenario for training in the practical
approach to the different dorks of general and
specific search engines

Modalidad: Teleformación (On-line)

<https://angeles-elearning.ccn-cert.cni.es/course/view.php?id=166>

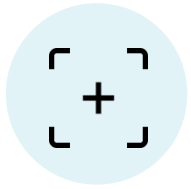
Índice

- 01 Conceptos esenciales
- 02 Sobre Elena
- 03 Un ejemplo real: Counterfeit en comercios web
- 04 Un ejemplo de caso de investigación en Elena
- 05 Seguridad Operativa en actividades de cibervigilancia
- 06 Inteligencia de imágenes
- 07 Dorking con buscadores genéricos
- 08 Dorking con buscadores especializados
- 09 Reportando y entregando el producto

Anexos



Haciendo las preguntas oportunas



Identificación de ataques ad-hoc



Asociar la huella a un
atacante



Enumeración de recursos en
la red externa



Identificación de vulnerabilidades
críticas y altas que pueden ser
explotadas



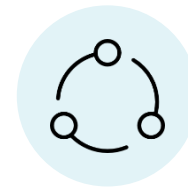
Entender al atacante y su
objetivo



Proteger accesos a los sistemas
físicos y lógicos



Enumeración de vías de intrusión



Evaluación continua según e ciclo de
inteligencia

Enfocar las preguntas al nivel del interlocutor

Información relevante que se convierte en inteligencia a través de un ciclo dinámico de colección, análisis, integración y producción.

Esta **inteligencia** puede ser **consumida** por los **equipos de seguridad** así como por **altos cargos**.



Es importante **ajustar el mensaje al interlocutor adecuado**, proporcionando la información clave con el nivel exacto de detalles para cada una de las partes receptoras de la inteligencia.

Niveles de interlocutores

Información relevante que se convierte en inteligencia a través de un **ciclo dinámico de colección, análisis, integración y producción.**

Estratégico

Información de alto nivel.

Impacto financiero de la actividad cibernética, las **tendencias de ataque** y las áreas que pueden afectar las **decisiones comerciales** de alto nivel.

 Junta directiva / CEO.

 Otros altos responsables en la toma de decisiones.

Operacional

Es información sobre ataques específicos que llegan a la organización.

 Personal de seguridad y defensa.

Táctico

Tácticas, técnicas y procedimientos (TTP) es información sobre cómo los actores pretenden o están realizando sus ataques.

 CISOs, DPO, CTO & Security Architects.

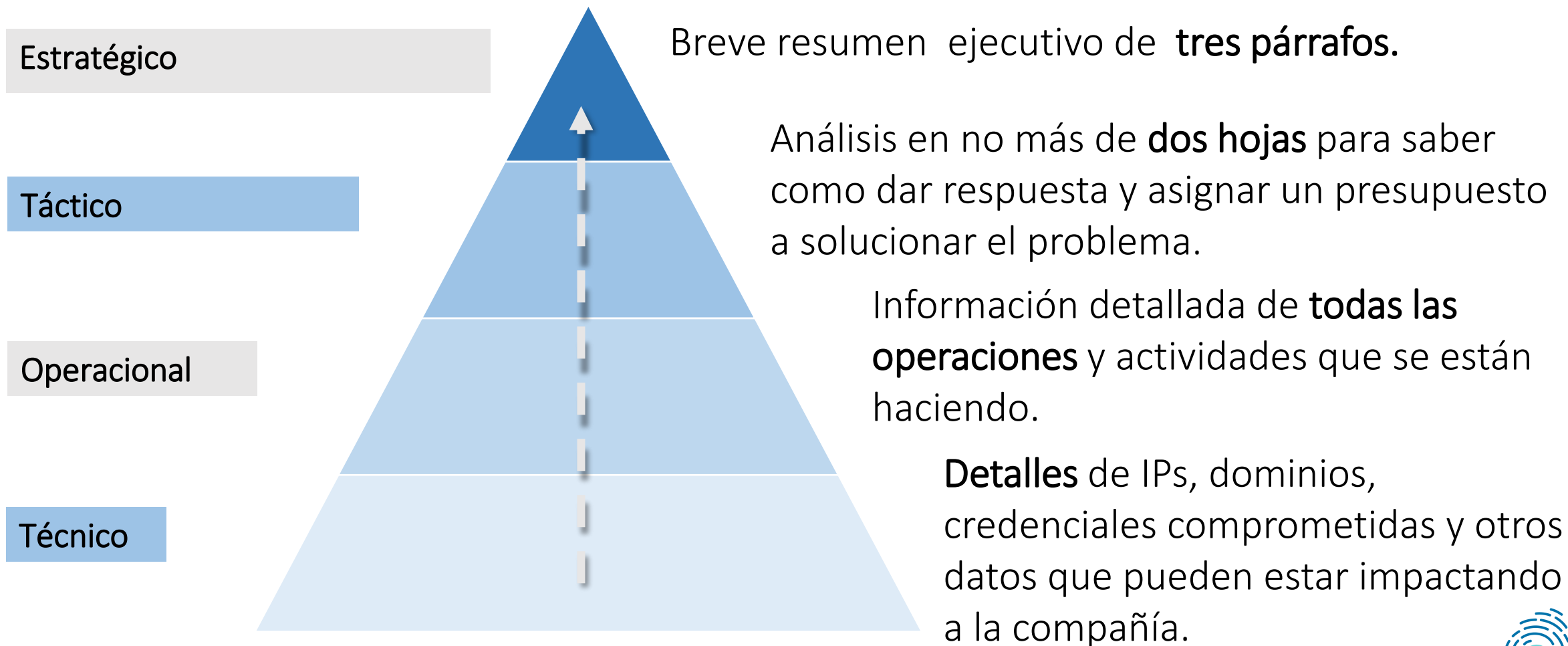
Técnico

Datos o información sobre indicadores de sucesos específicos. La inteligencia de amenaza técnica generalmente alimenta las funciones de investigación o supervisión de una empresa.

 Analistas, SOCs, IR, SysAdmins. e IT Staff.

Adaptar el mensaje y el volumen

Es importante **ajustar el mensaje al interlocutor adecuado**, proporcionando la información clave con el nivel exacto de detalles para cada una de las partes receptoras de la inteligencia.



Tomando requisitos

Amenazas interesantes para el cliente

- On Demand Investigations
- Trend Reports
- Newsletter
- Periodic Reports
- Proactive investigations
- Information Leaks
- Hacktivism, activism in the network
- DDoS detection
- Breach of Security Controls
- Credential theft
- Detection of Suspicious Domains
- Unauthorised Use of Brand, Logo or Image
- Offensive Contents
- Counterfeit
- Digital Identity Monitoring
- Phishing
- Pharming
- Carding
- Malware
- Detection of Suspicious Mobile App



Interés

Muy alto
Alto
Medio
Bajo
Muy bajo



Frecuencia Reporte

Inmediato
Diario
Semanal
Mensual
Trimestral
Semestral
Anual



Contacto

Protocolo de comunicación
Vía Mail / dirección email
Teléfono
Horario normal / urgencias
Detalle técnico /alto nivel
Idioma

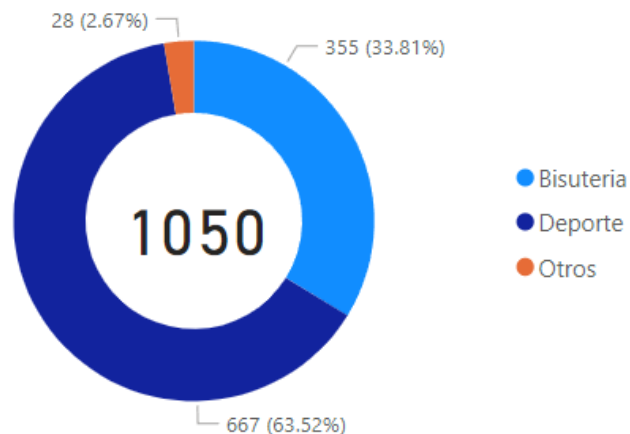
Elaborando el producto

Fases para la elaboración del producto

Fases para la elaboración del producto				
Inicio	Elaboración y revisión			Cierre
Objetivo	Elaboración	Redacción	Revisión	Conclusiones y plan de acción
¿Por qué y para qué? Respuesta a una petición para alertar, proponer o informar. Muy importante alcanzar los objetivos marcados. Comunicación eficaz 1. Elaborar 2. Redactar 3. Revisar	Durante la fase de elaboración debemos fijarnos estos cuatro puntos: 1. Ideas principales 2. Ideas secundaras 3. Ordenar 4. Determinar el mensaje	Regla de las 5 "C" La redacción debe ser: 1. Clara 2. Concisa 3. Concreta 4. Completa 5. Coherente Debemos cuidar la corrección en nuestra redacción.	Comprobar que hemos respondido a las preguntas: 1. ¿Qué? 2. ¿Cuándo? 3. ¿Dónde? 4. ¿Cómo? 5. ¿Quién? 6. ¿Por qué? 7. ¿Para que? 8. ¿Y ahora qué? Revisar 1. Ortografía 2. Gramática 3. Sintaxis	

Cuantificando los resultados

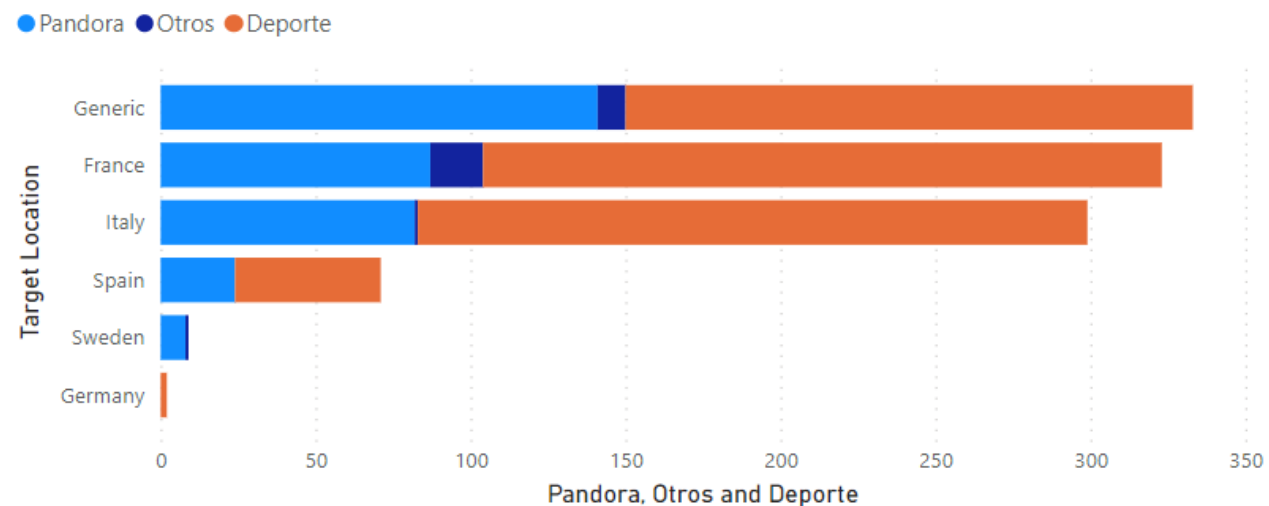
Bisuteria, Deporte and Otros



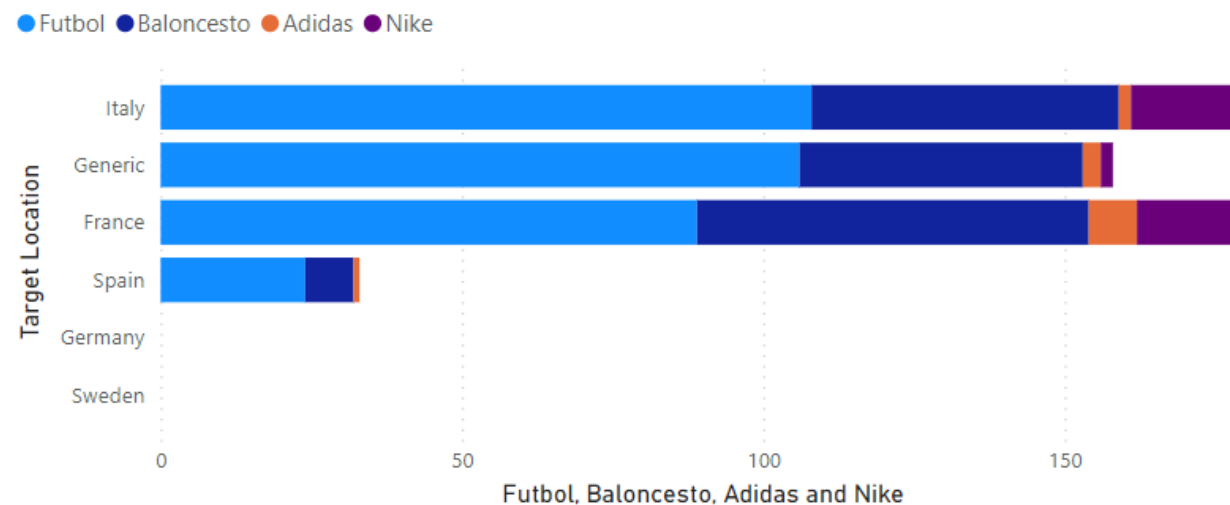
11K

Gasto anual en dominios

Pandora, Otros and Deporte by Target Location



Futbol, Baloncesto, Adidas and Nike by Target Location



Índice

- 01 Conceptos esenciales
- 02 Sobre Elena
- 03 Un ejemplo real: Counterfeit en comercios web
- 04 Un ejemplo de caso de investigación en Elena
- 05 Seguridad Operativa en actividades de cibervigilancia
- 06 Inteligencia de imágenes
- 07 Dorking con buscadores genéricos
- 08 Dorking con buscadores especializados
- 09 Reportando y entregando el producto

Anexos

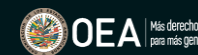


#STICPUNTACANA

III JORNADAS STIC

CAPÍTULO REPÚBLICA DOMINICANA

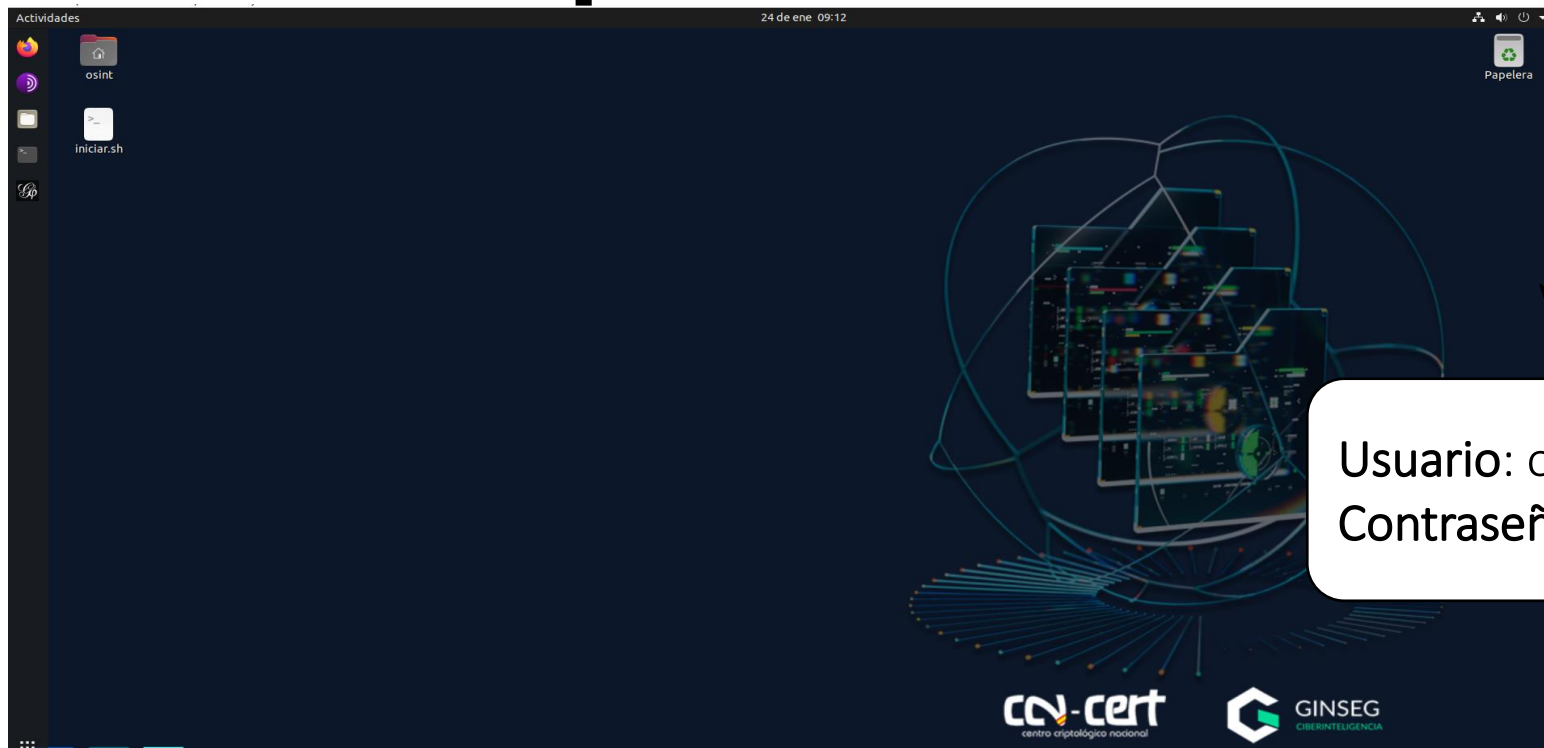
Anexo: Entorno de trabajo y kit de herramientas



Máquina virtual para entrenar e investigar

<http://curso-cibervigilancia.ginseg.com/CursoCibervigilancia.ova>

Recursos para el analista



Máquina para el analista

Máquina virtual desarrollada y configurada específicamente para esta formación.

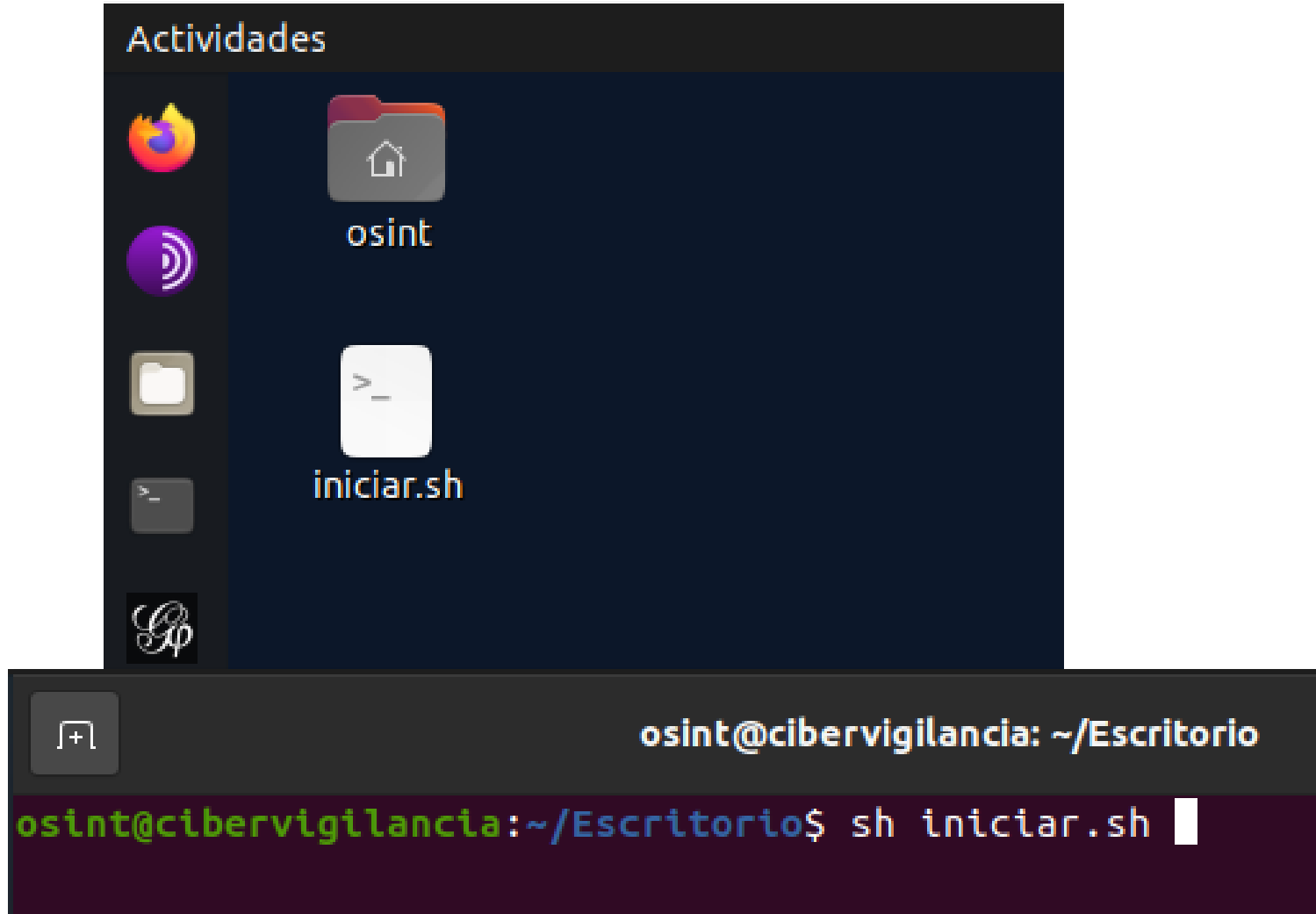
Requiere realizar la instalación del resto de herramientas con script *iniciar.sh*

Herramientas incluidas:

- PyCharm
- Python3
- Tor Browser
- Firefox
- Plugins privacidad y anonimato
- Keepass
- Veracrypt
- The Harvester
- Riseup VPN
- Twint
- Gephi
- Tinfoleak
- Maltego
- OSRFramewor k
- instagramOSI NT
- instaloader
- Karma
- Spiderfoot
- Desarrollos a medida para la formación
- Otras herramientas complementarias

Primer arranque

Curso Cibervigilancia [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda



Pasos de instalación de herramientas:

1. Dar botón derecho del ratón en el Escritorio.
2. Hacer clic en “Abrir en una terminal”.
3. Escribir “sh iniciar.sh” en la terminal.
4. Comenzará el proceso de instalación automático y desatendido.
5. Si solicita introducir una contraseña deberemos escribir “osint”.
6. Al finalizar escribir “exit”



osint



iniciar.sh



Papelerera



Se ven como es la pantalla del escritorio de la máquina virtual

cn-cert
centro criptológico nacional

GINSEG
CIBERINTELIGENCIA

Índice

- 01 Conceptos esenciales
- 02 Sobre Elena
- 03 Un ejemplo real: Counterfeit en comercios web
- 04 Un ejemplo de caso de investigación en Elena
- 05 Seguridad Operativa en actividades de cibervigilancia
- 06 Inteligencia de imágenes
- 07 Dorking con buscadores genéricos
- 08 Dorking con buscadores especializados
- 09 Reportando y entregando el producto

Anexos

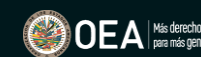


#STICPUNTACANA

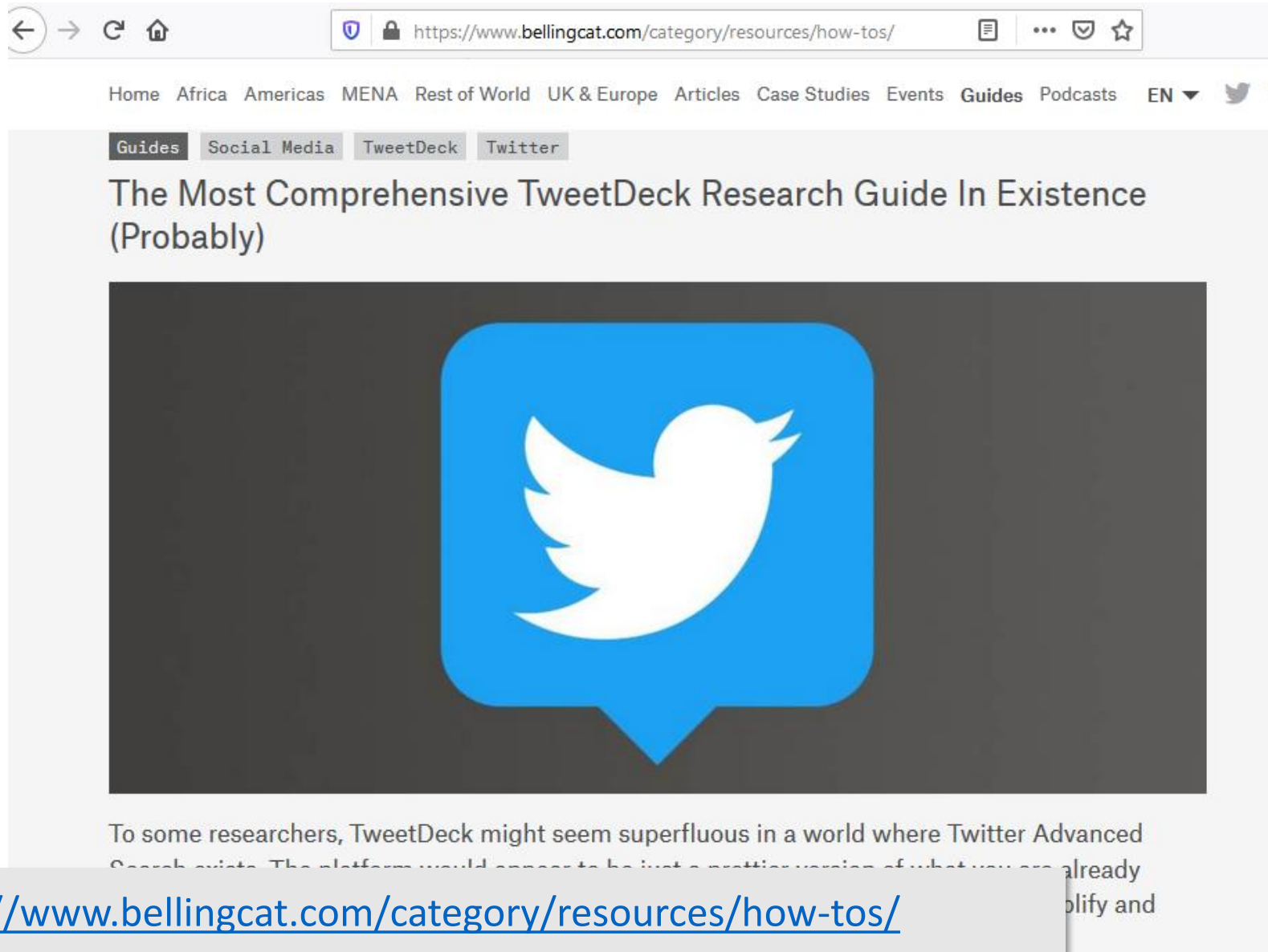
III JORNADAS STIC

CAPÍTULO REPÚBLICA DOMINICANA

Anexo: Referencias para seguir aprendiendo



Recursos digitales – Guías y How Tos



<https://www.bellingcat.com/category/resources/how-tos/>

Recursos digitales – Awesome OSINT

<https://github.com/jivoi/awesome-osint>

Social Media Tools

Twitter

- Backtweets
- Blue Nod
- burrrd.
- Crate
- doesfollow
- Fake Follower Check
- FirstTweet
- First Tweet
- Foller.me
- FollowCheck
- Followerwonk
- Geochirp
- GeoSocial Footprint
- GetTwitterID
- Gigatweeter
- Ground Signal
- HappyGrumpy
- Harvard TweetMap
- Hashtagify
- Hashtags.org
- ManageFlitter
- Mentionmapp
- OneMillionTweetMap
- Queryfeed
- Rank Speed

Major Social Networks

1. [Draugiem \(Latvia\)](#)
2. [Facebook](#)
3. [Facenama \(Iran\)](#)
4. [Instagram](#)
5. [Linkedin](#)
6. [Mixi \(Japan\)](#)
7. [Odnoklassniki \(Russia\)](#)
8. [Pinterest](#)
9. [Qzone \(China\)](#)
10. [Reddit](#)
11. [Taringa \(Latin America\)](#)
12. [Tinder](#)
13. [Tumblr](#)
14. [Twitter](#)
15. [Weibo \(China\)](#)
16. [VKontakte](#)
17. [Xing](#)

Real-Time Search, Social Media Search, and General Social Media Tools

1. [Audiense](#)
2. [Bottlenose](#)
3. [Brandwatch](#)
4. [Buffer](#)
5. [Buzz sumo](#)
6. [Geocreepy](#)
7. [Geofeedia](#)
8. [Hootsuite](#)
9. [Hashtatit](#)
10. [Icerocket](#)
11. [Klear](#)
12. [Kred](#)
13. [MustBePresent](#)
14. [Netvibes](#)
15. [OpinionCrawl](#)
16. [Rival IQ](#)
17. [RSS Social Analyzer](#)
18. [SocialBakers](#)
19. [SociaBlade](#)
20. [Social DownORNot](#)
21. [Social Searcher](#)
22. [Tagboard](#)
23. [Trackur](#)
24. [UVRX](#)

Social Media Tools

Twitter

1. [Backtweets](#)
2. [Blue Nod](#)

4. [Crate](#)
5. [doesfollow](#)
6. [Fake Follower Check](#)
7. [FirstTweet](#)
8. [First Tweet](#)
9. [Foller.me](#)
10. [FollowCheck](#)
11. [Followerwonk](#)
12. [Geochirp](#)
13. [GeoSocial Footprint](#)
14. [GetTwitterID](#)
15. [Gigatweeter](#)
16. [Ground Signal](#)
17. [HappyGrumpy](#)
18. [Harvard TweetMap](#)
19. [Hashtagify](#)
20. [Hashtags.org](#)
21. [ManageFlitter](#)
22. [Mentionmapp](#)
23. [OneMillionTweetMap](#)
24. [Queryfeed](#)
25. [Rank Speed](#)
26. [Riffle](#)
27. [RiteTag](#)
28. [Sentiment140](#)
29. [SnapBird](#)
30. [Sleeping Time](#)
31. [Social Bearing](#)
32. [Social Rank First Follower](#)
33. [Spoonbill](#)
34. [Tagdef](#)
35. [TeachingPrivacy](#)
36. [Tinfoleak](#)
37. [Trends24](#)
38. [TrendsMap](#)
39. [Twazzup](#)
40. [twbirthday](#)
41. [TwChat](#)
42. [tweepsect](#)
43. [TweetArchivist](#)
44. [TweetDeck](#)
45. [Tweeten](#)
46. [TweetMap](#)
47. [TweetMap](#)
48. [Tweetpaths](#)
49. [TweetPsych](#)
50. [Tweetch](#)
51. [TweetStats](#)

53. [TweetTunnel](#)
 54. [Twellow](#)
 55. [Tweriod](#)
 56. [Twiangulate](#)
 57. [Twicsy](#)
 58. [Twilert](#)
 59. [Twipho](#)
 60. [Twitonomy](#)
 61. [TwitRSS](#)
 62. [Twitter Advanced Search](#)
 63. [Twitter Audit](#)
 64. [Twitterfall](#)
 65. [Twitter Search](#)
- #### Facebook
1. [Agora Pulse](#)
 2. [Commun.it](#)
 3. [DumpItBlue](#)
 4. [Fanpage Karma](#)
 5. [Facebook Search](#)
 6. [Facebook Search Tool](#)
 7. [FaceLIVE](#)
 8. [Fb-sleep-stats](#)
 9. [Find my Facebook ID](#)
 10. [LikeAlyzer](#)
 11. [Lookup-ID.com](#)
 12. [SearchIsBack](#)
 13. [Wolfram Alpha Facebook Report](#)
 14. [Zesty Facebook Search](#)
- #### Instagram
1. [Hashtagify](#)
 2. [Iconosquare](#)
 3. [Picodash](#)
 4. [SnapMap](#)
 5. [Social Rank](#)
 6. [Tofo.me](#)
 7. [Worldcam](#)
- #### Pinterest
1. [Pingroupie](#)
- #### Reddit
1. [Imgur](#)
 2. [Mostly Harmless](#)
 3. [Reddit Archive](#)
 4. [Reddit Suite](#)
 5. [Reddit Investigator](#)
 6. [Reddit Metrics](#)
 7. [Reddit User Analyzer](#)
 8. [SnoopSnoo](#)
 9. [Subreddits](#)



<https://github.com/jivoi/awesome-osint>

■ Informes de amenazas



<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3776-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-edicion-2019-1/file.html>



Se muestran dos informes del CCN-CERT sobre amenazas y hacktivismo

IntelCon – Congreso Gratuito

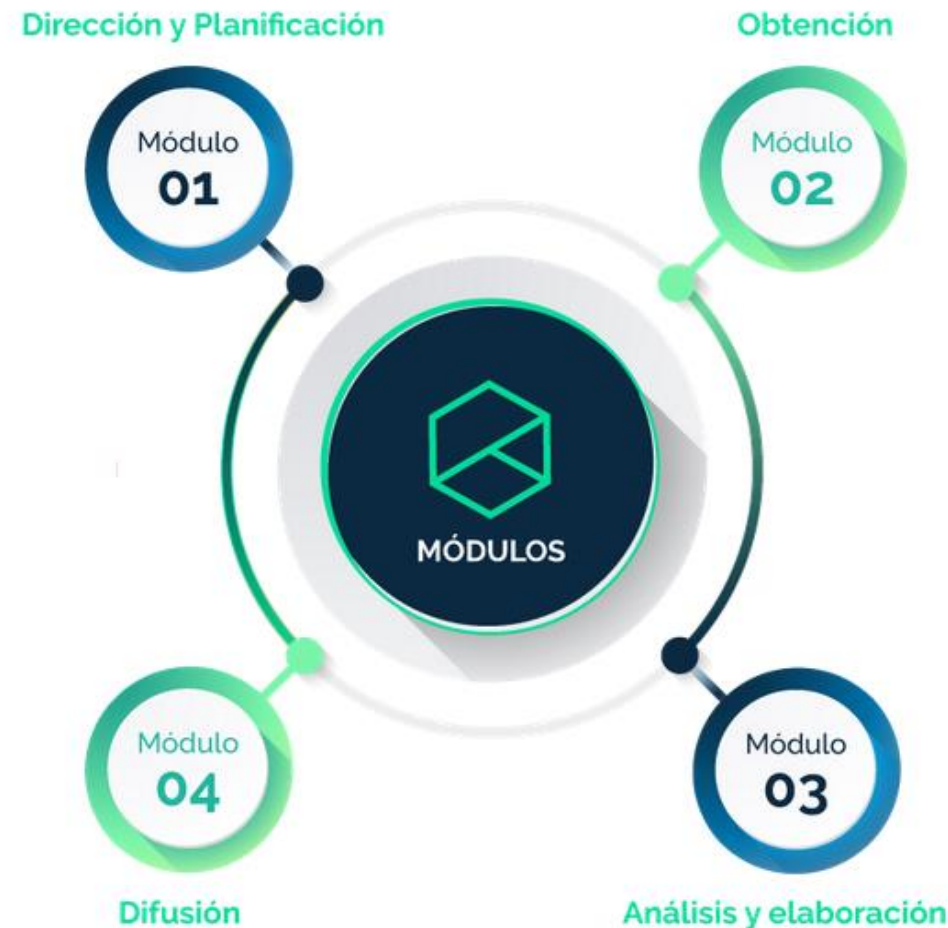


EN STREAMING GRATIS

Congreso **Online** de Ciberinteligencia **2023**
DEL 24 AL 28 DE JULIO 2023

#InteligenciaDeAmenazas #OSINT #SOCMINT #VirtualHUMINT
#DeepWeb #RespuestaIncidentes #TécnicasAnálisis #Herramientas #Ciberamenazas

<https://intelcon.ginseg.com/>



Canal de Youtube de IntelCon



IntelCon
1410 suscriptores

INICIO

VÍDEOS

LISTAS

COMUNIDAD

CANALES

MÁS INFORMACIÓN



SUSCRITO



Subidas

▶ REPRODUCIR TODO



IntelCon 2020 - Last of us, Apocalyptic days for a...

67 visualizaciones •
hace 6 meses



IntelCon 2020 - Estafas en plataformas de alquiler de...

95 visualizaciones •
hace 6 meses



Taller IntelCon 2020 - Elige tu propia aventura de OSIN...

272 visualizaciones •
hace 6 meses



IntelCon 2020 - Metacharla ~ Redes sociales, Física y...

89 visualizaciones •
hace 6 meses



IntelCon 2020 - De la desinformación online a la...

136 visualizaciones •
hace 6 meses



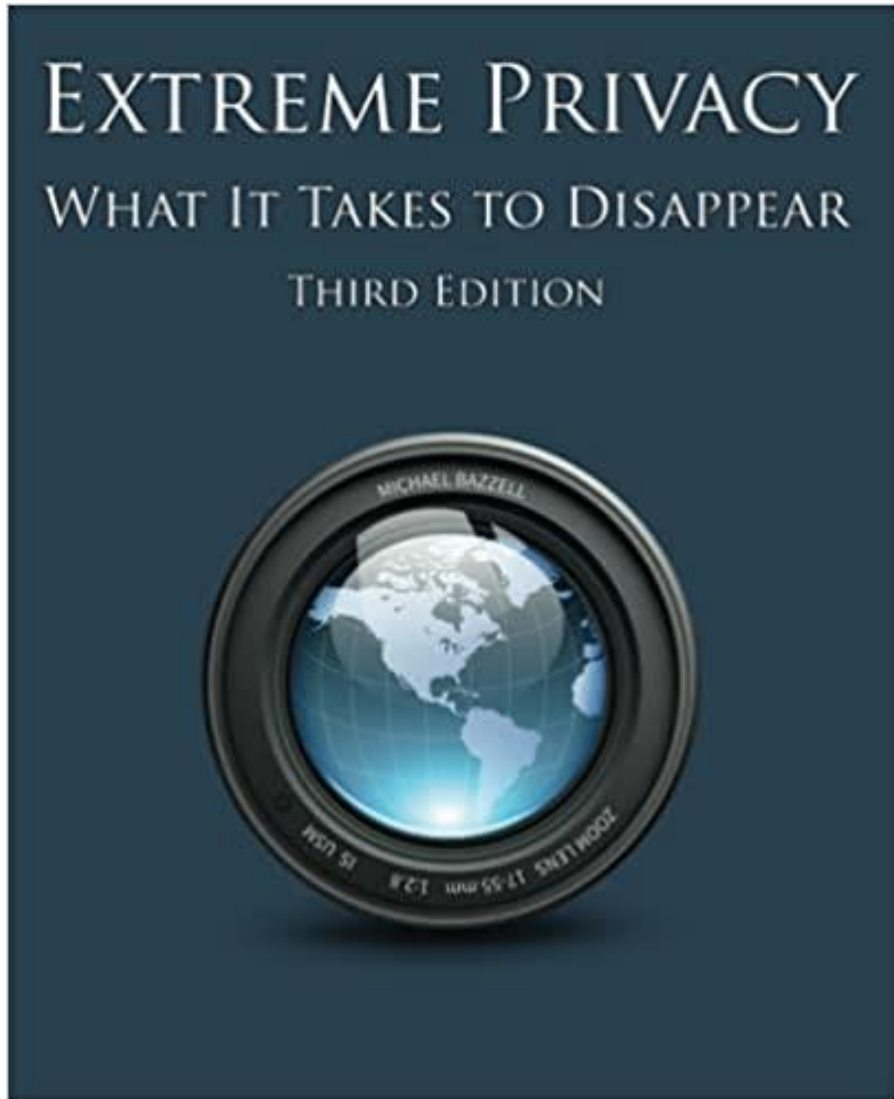
IntelCon 2020 - Datos inteligentes para...

104 visualizaciones •
hace 6 meses



<https://www.youtube.com/intelcon>

Referencias para seguir aprendiendo



Título: Extreme Privacy: What It Takes to Disappear

Autor: Michael Bazzell

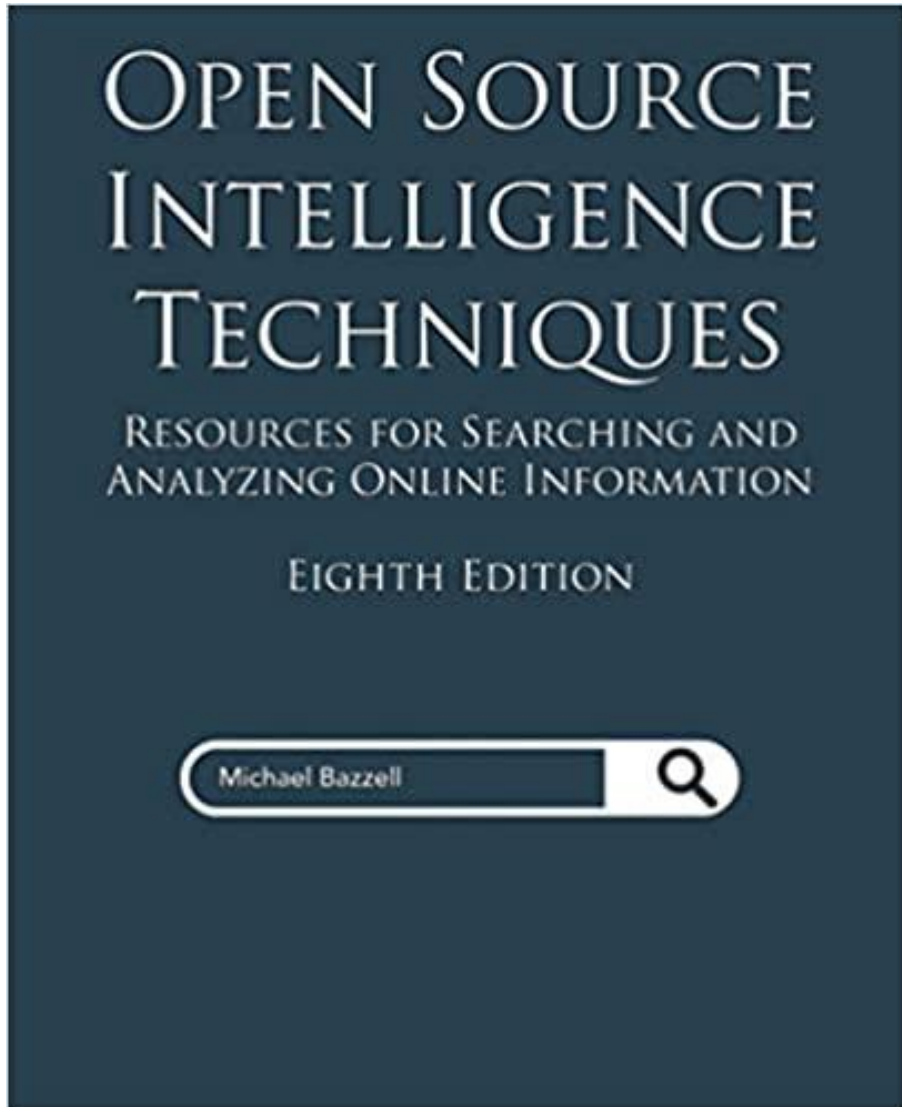
Temática: OPSEC, Privacidad



<https://www.amazon.es/dp/B094LDWKGZ/>

Se muestra portada de libro

Referencias para seguir aprendiendo



Título: Open Source Intelligence Techniques

Autores: Michael Bazzell

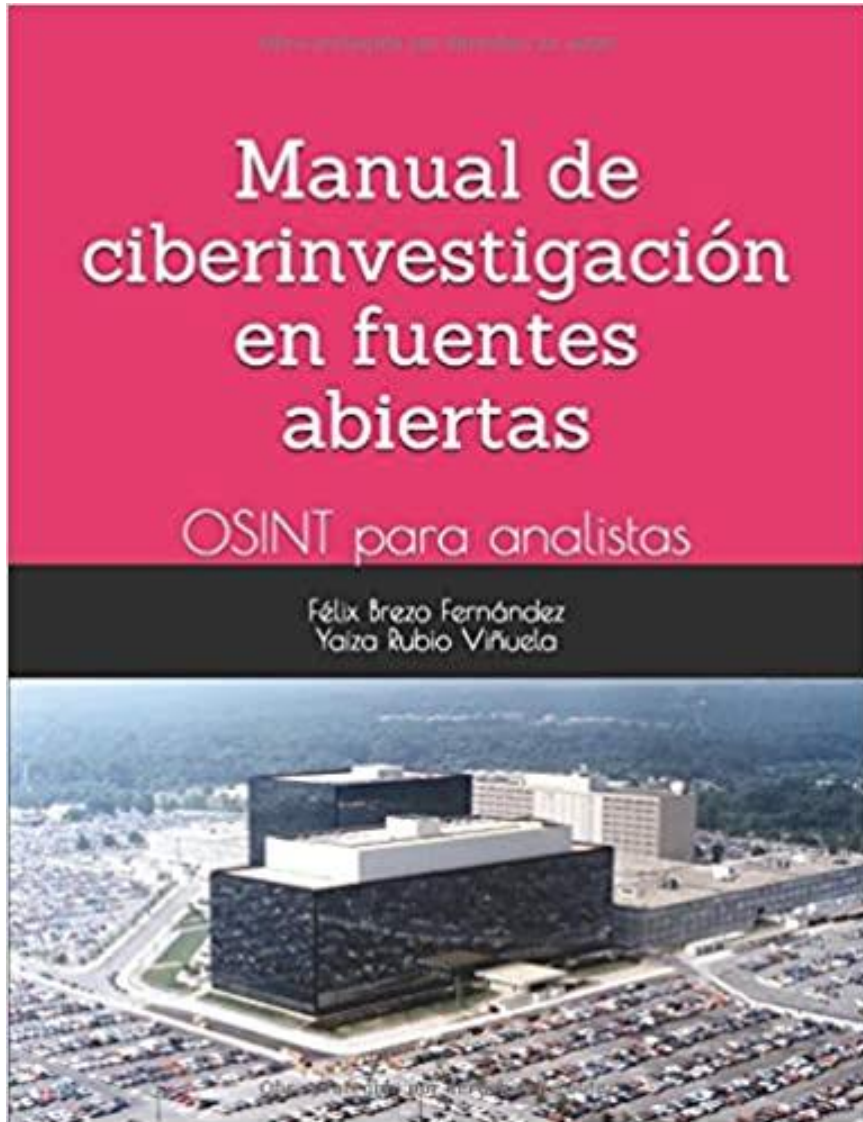
Temática: Técnicas de investigación OSINT



<https://www.amazon.es/dp/B08RRDTFF9/>

Se muestra portada de libro

Referencias para seguir aprendiendo



Título: Manual de ciberinvestigación en fuentes abiertas

Autores: Félix Brezo y Yaiza Rubio

Temática: Técnicas de investigación OSINT



<https://www.amazon.es/dp/1650895747/>

Se muestra portada de libro

Referencias para seguir aprendiendo

Open Source INTelligence (OSINT)

Investigar personas e Identidades en Internet

Carlos Seisdedos

Prólogo de Pedro Baños

Vicente Aguilera



Título: Open Source INTelligence (OSINT):
Investigar personas e Identidades en Internet

Autores: Vicente Aguilera y Carlos Seisdedos

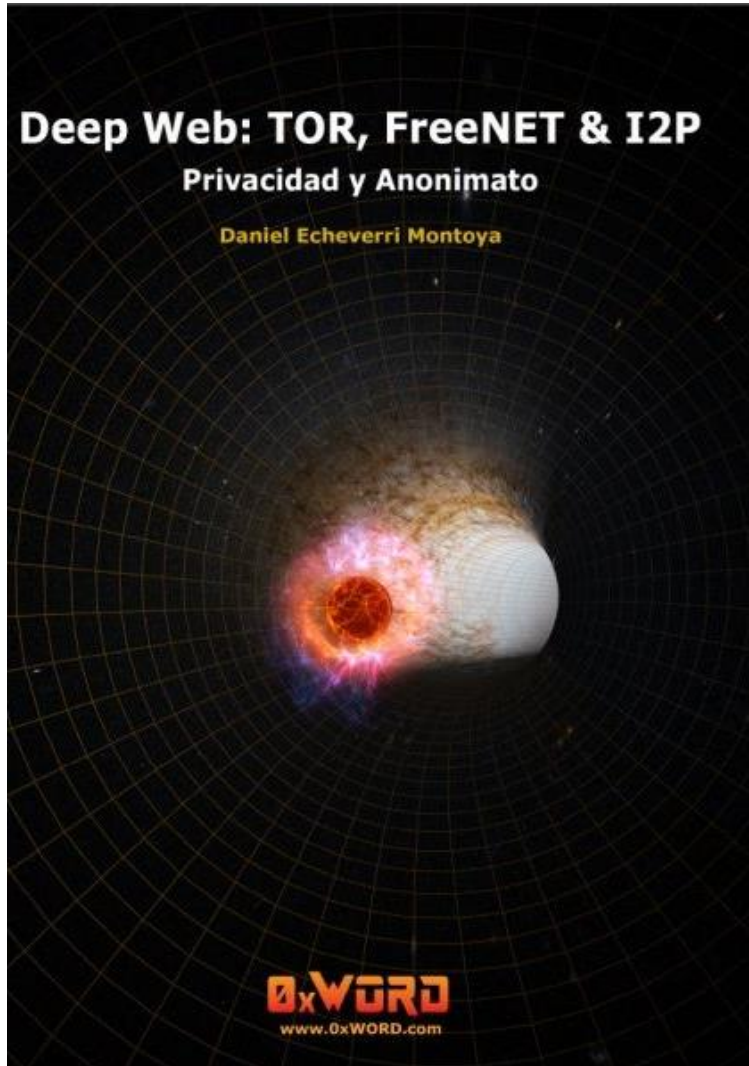
Temática: Técnicas de investigación OSINT



<https://0xword.com/es/libros/162-open-source-intelligence-osint-investigar-personas-e-identidades-en-internet.html>

Se muestra portada de libro

Referencias para seguir aprendiendo



Título: Deep Web: TOR, FreeNET & I2P - Privacidad y Anonimato

Autores: Daniel Echeverri aka Adastra

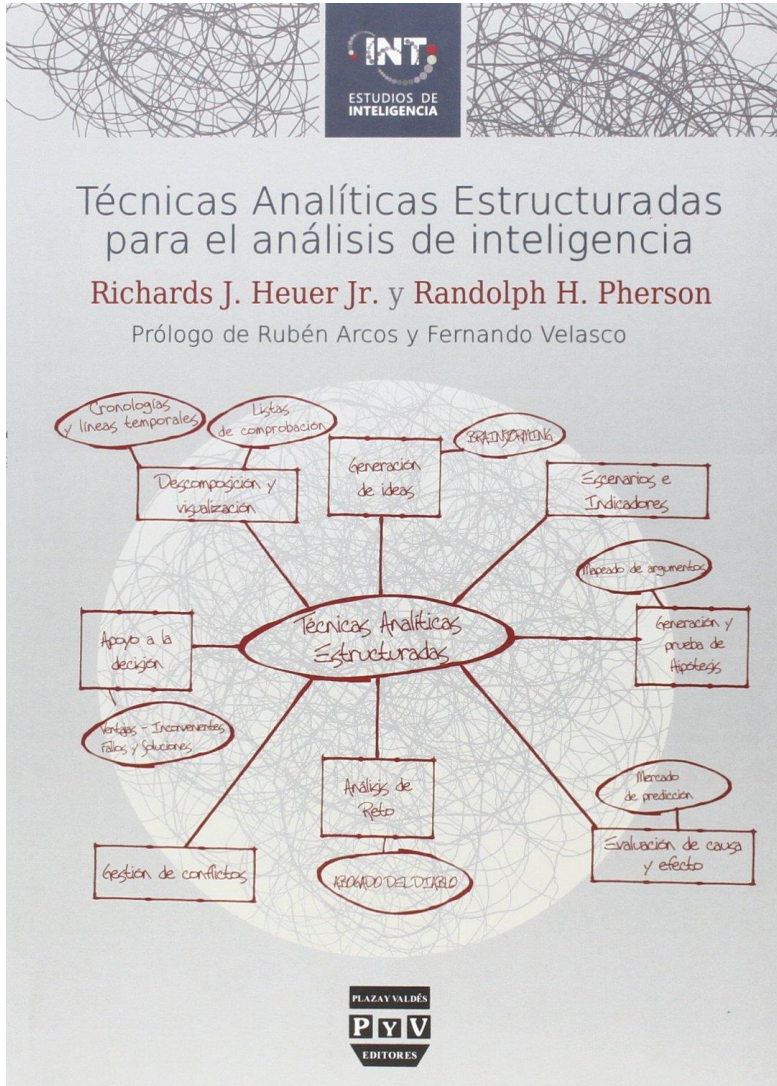
Temática: Deepweb, Privacidad, Anonimato



<https://0xword.com/es/libros/75-deep-web-tor-freenet-i2p-privacidad-y-anonimato.html>

Se muestra portada de libro

Referencias para seguir aprendiendo



Título: Técnicas de Analíticas Estructuradas para el análisis de inteligencia

Autores: Richards J. Heuer y Randolph H. Person

Temática: Técnicas de análisis de inteligencia



<https://www.amazon.es/dp/8415271670/>

Se muestra portada de libro

Referencias para seguir aprendiendo

GINSEG - Comunidad de Ciberinteligencia Colectiva

3.285 miembros

[Mensaje anterior](#)

Comunidad GINSEG Bienvenidos a todos los integrantes del grupo!!

LISTADO DE TAGS

Generales

#Amenaza #Riesgos #Legal #IngenieriaSocial #Seguridad #Leaks
#Hacking #Forense #RedTeam #Vulnerabilidad #Honeypot #Tools
#Fuente #Feed #API #Crawling #DeepWeb #Darkweb #Darknet
#Tor #I2P #Freenet

Inteligencia

#Inteligencia #Ciberinteligencia #CTI #ThreatIntel #OSINT
#SOCMINT #HUMINT #SIGINT

Investigación y Análisis

#Investigacion #Perfilado #Persona #Telefono #Geolocalizacion
#Mapas #Analisis #Taxonomia #Bayesiano #Brainstorming #DAFO
#Prospectiva #Metricas
#SATs #CicloInteligencia

Amenazas

#Malware #Ransomware #Botnet #APT #Actor #Phishing #IoC
#STIX #Hash #IP #Yara #Hunting #Sample

Otros tags

#Congreso #CFP #CTF #Articulo
#Formacion #Master #Libro #Empleo

GINSEG

IntelCon archivos - GINSEG

Ponencias y talleres impartidos en el congreso sobre



GINSEG - Comunidad de Ciberinteligencia Colectiva

Lucía Taco se unió al grupo

16:37



Cyber Threat Intel News

Nuevas sesiones de formación sobre cibervigilancia El Equipo...

vie



Grupo Analisis de inteligencia español

Alal: ,

17:55

<https://t.me/ginseg>

Se muestra imagen del grupo de Telegram de GINSEG



Referencias para seguir aprendiendo

Cyber Threat Intel News

3.964 suscriptores

Cyber Threat Intel News

Desde @ginseg hemos decidido fijar la fecha de la Segunda Edición de #IntelCon del 30 de agosto al 3 de septiembre de 2021

El objetivo del congreso es la difusión de conocimientos de calidad sobre #Ciberinteligencia de forma gratuita y en sus diferentes áreas asociadas. Para cumplir dicho objetivo proponemos una serie de ponencias que formen parte de un itinerario siguiendo lo que se conoce como el Ciclo de Inteligencia. Mediante el mismo, el asistente podrá descubrir como generar un producto de inteligencia a través de sesiones que cubrirán y explicarán de forma detallada cada una de sus fases, introduciendo la teoría para culminar con un enfoque práctico.

<https://youtu.be/Prz8Sdy9Mhc>
<https://intelcon.ginseg.com>

Las temáticas relacionadas con el congreso son variadas abarcando:

#Inteligencia #OSINT #SOCMINT #HUMINT
#DeepWeb #TécnicasAnálisis #Ciberamenazas #CTI

Por favor, #comparte #IntelCon2021, gracias.

Fuente: <https://t.me/ThreatIntelligence/1275>



GINSEG - Comunidad de Ciberinteligencia Colectiva

16:37

Lucía Taco se unió al grupo



Cyber Threat Intel News

vie

Nuevas sesiones de formación sobre cibervigilancia El Equipo...



Grupo Analisis de inteligencia español

17:55

Alal: ,

<https://t.me/ThreatIntelligence>

Se muestra imagen del CANAL de Telegram de GINSEG



**III JORNADAS
STIC**

CAPÍTULO REPÚBLICA DOMINICANA

MUCHAS

GRACIAS

#STICPUNTACANA