



OSINT: herramientas comunes y Cómo usarlos de forma segura

Siobhan Kelleher

Analista sénior de seguridad

Boston College

OSINT: herramientas comunes y cómo usarlas de forma segura

Temas

- ¿Qué es OSINT?
- Uso de OSINT
- Herramientas y recursos
- Mantenerse a salvo
- Usar sus habilidades para el bien



OSINT: herramientas comunes y cómo usarlas de forma segura

¿Qué es OSINT?

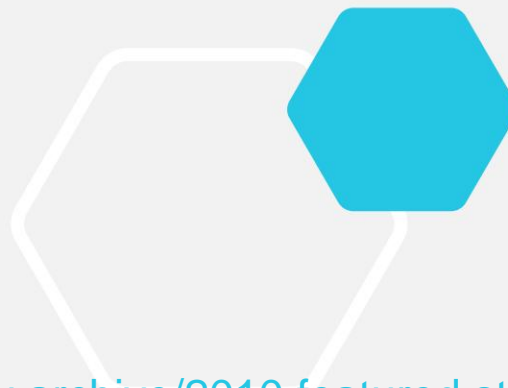
“La inteligencia de código abierto (OSINT) es inteligencia que se produce a partir de información disponible públicamente y se recopila, explota y difunde de manera oportuna a una audiencia adecuada con el fin de abordar un requisito de inteligencia específico”.



OSINT: herramientas comunes y cómo usarlas de forma segura

¿Qué es OSINT?

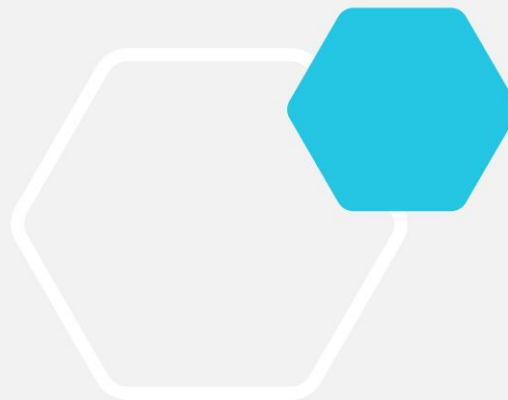
- La Internet
- Medios (por ejemplo, televisión, radio, periódicos, revistas) •
Publicaciones profesionales (revistas, conferencias, estudios)
- Fotos
- Información geoespacial (por ejemplo, mapas y productos de imágenes comerciales)
- ...y más



OSINT: herramientas comunes y cómo usarlas de forma segura

¿Cómo estoy usando OSINT?

- Capacitación para la concientización del usuario
- Correo electrónico malicioso
- Gente desaparecida
- Abuso doméstico



OSINT Landscape v.1 February 2018

Open Source Intelligence (/OSINT – Open Source Investigation)

COVERT SHORES bellingscat
www.hisutton.com



This landscape shows data sources (mostly platforms, tools or apps) that provide publicly available data which may be of use in OSINT. Some tools may charge for data access. It is intended to be extensive, but not exhaustive, and may be updated periodically.

Authors:
H I Sutton, (@CovertShores) Covert Shores and Jane's contributor,
Aliaume Leroy, (@facti) Bellingscat & BBC,
Tony Roper, (@topol_mssj3), planecanada, Jane's contributor

OSINT: herramientas comunes y cómo usarlas de forma segura

Herramientas y recursos

- Redes sociales
 - Tiktok, Twitter, Facebook, Snapchat, aplicaciones de citas...
- Correo electrónico
- Búsqueda inversa de imágenes
- Registros Públicos
 - Dirección, registros de arresto, certificados de defunción
- Otro

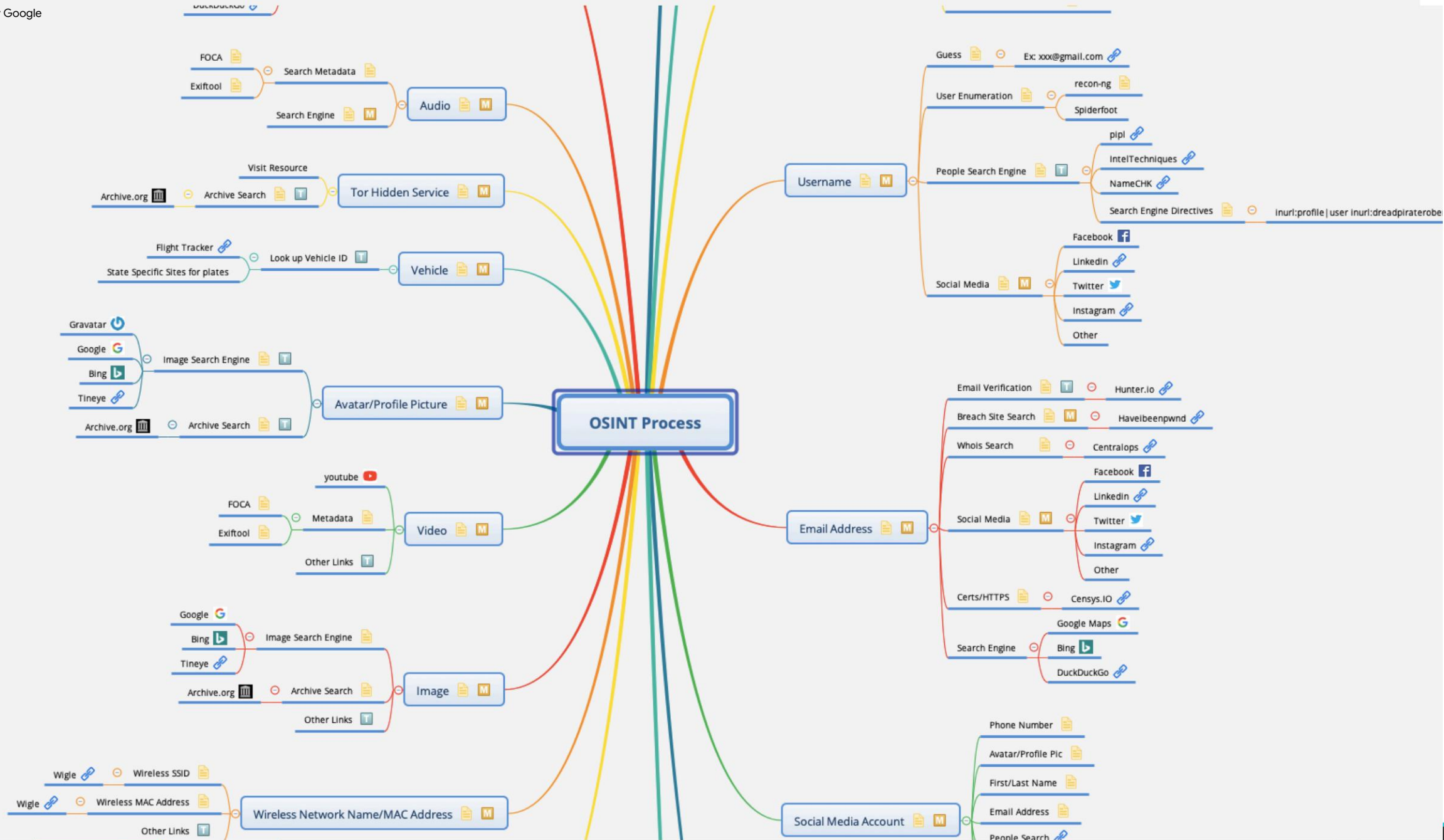


OSINT: herramientas comunes y cómo usarlas de forma segura

Herramientas y recursos

- Mapas Mentales
- Hunchly
- Excel
- Trello
- Compañero de sesión





OSINT: herramientas comunes y cómo usarlas de forma segura

1	OSINT: Jane Doe			
2	https://www.mass.gov/doc/person-missing-poster/download			
3	What	Link	Artifact	Notes
4	Phone number	www.theirnumber.com	8675309	found through this link,
5	Mother	www.mothers	Janet Doe	facebook page is open lists other relatives found through facebook search
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				

D.S. RP

☆

OSINT DA RP

Free

Team Visible

S

Invite

Artifacts Found

Account

Account

Images

Association

+ Add another card

Under Investigation

Second username

+ Add another card

Good Artifact

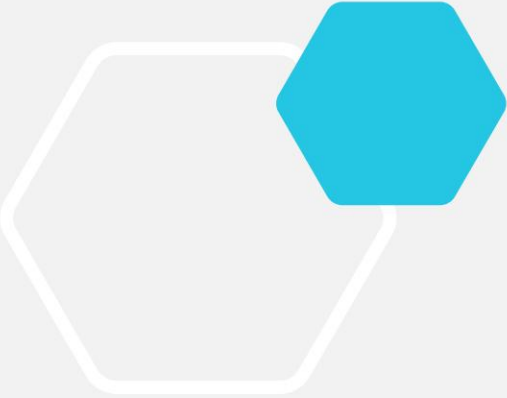
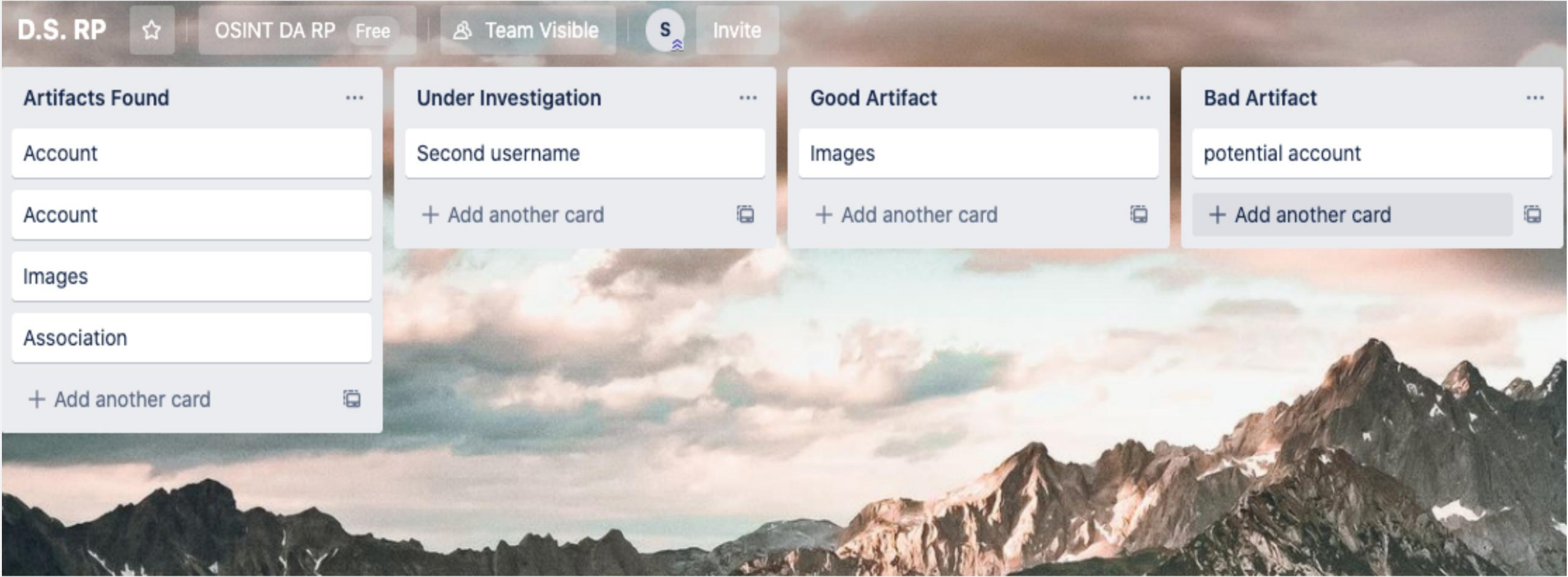
Images

+ Add another card

Bad Artifact

potential account

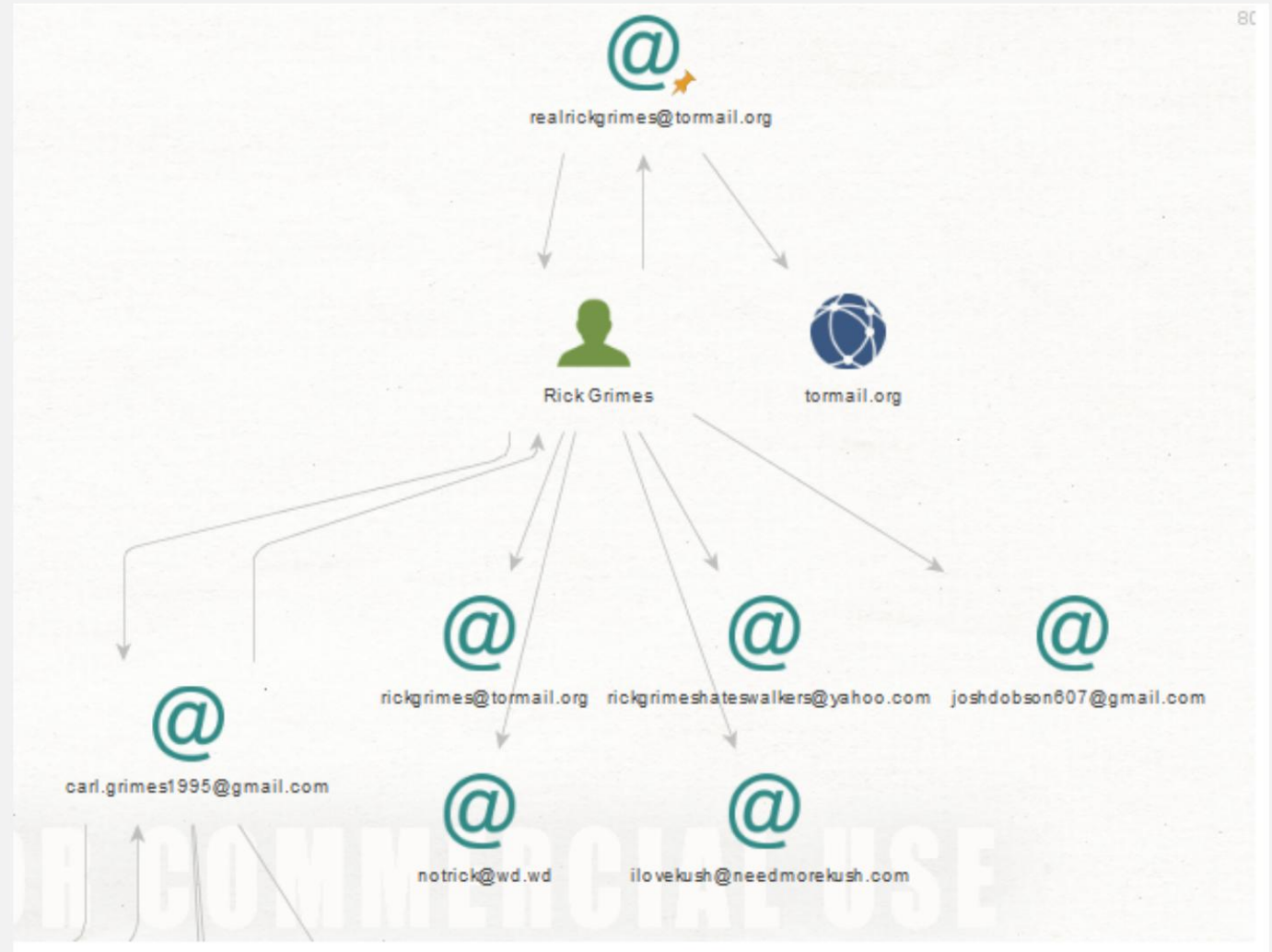
+ Add another card



OSINT: herramientas comunes y cómo usarlas de forma segura

Herramientas y recursos

Maltego



gle

site:twitter.com intext:"malware"

×

All

News

Images

Books

Videos

More

Settings

Tools

About 726,000 results (0.32 seconds)

twitter.com › hashtag › malware

#malware hashtag on Twitter

Cybersecurity tip: To best protect your business you'll need both #antivirus and anti-malware programmes. Antivirus software offers protection against classic ...

You visited this page on 8/10/20.

People also ask

Can you get malware from twitter?

What are the 4 types of malware?

How do I remove malware from my computer?

Which is an example of a malware?

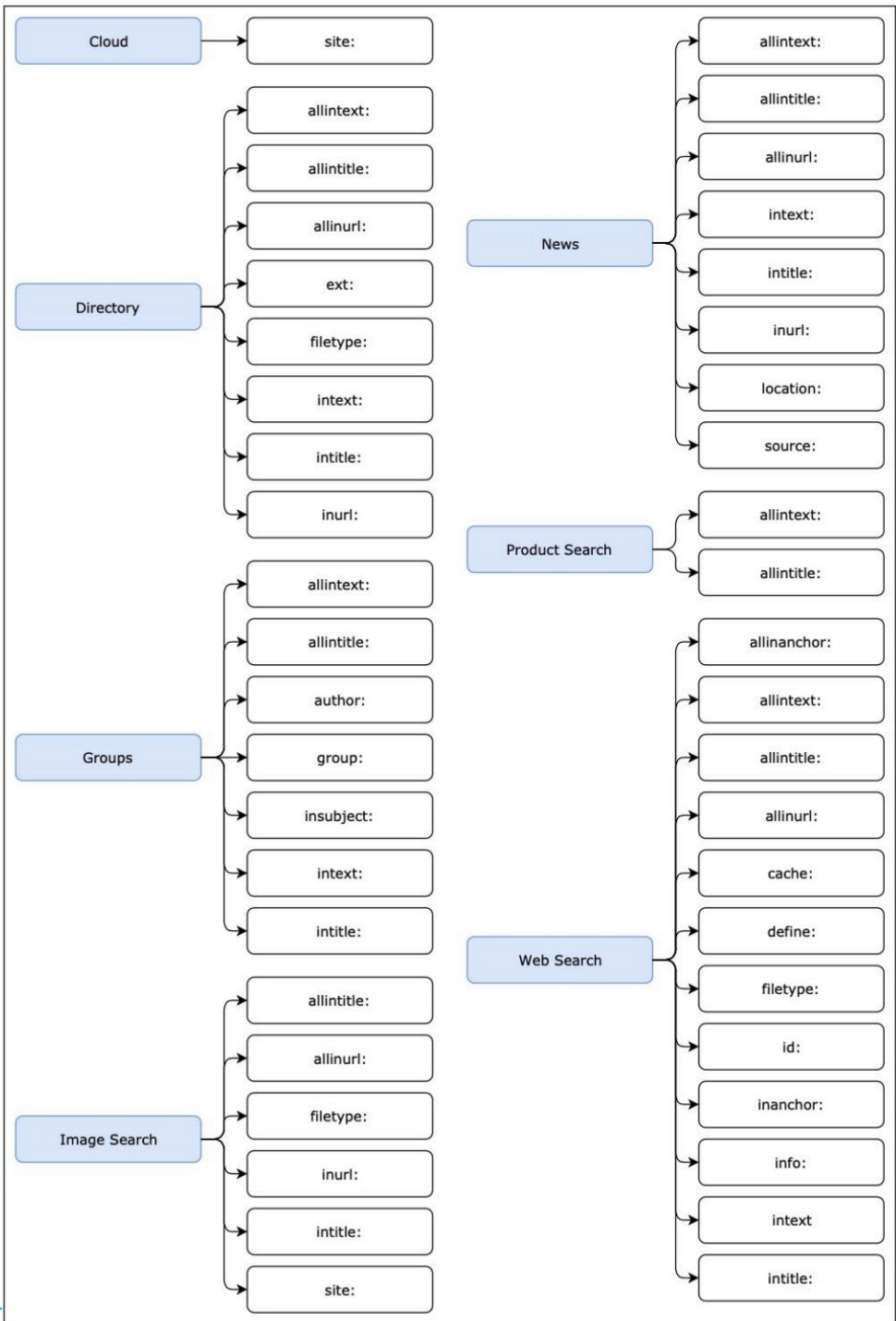
Feedback

twitter.com › web › status

Brad on Twitter: "2020-08-10 - #Emotet infection with #Qakbot ...

1 hour ago - Brad · @malware_traffic. Sharing information on malicious network traffic and malware samples. 127.0.0.1.

Imagen: https://twitter.com/velstadt_com/status/1206902436469911552





OSINT: herramientas comunes y cómo usarlas de forma segura

Herramientas y recursos

- SpiderFoot •

Edición de pasatiempo gratuita basada en

la web • Descargable de código abierto gratuito

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



OSINT: herramientas comunes y cómo usarlas de forma segura

Herramientas y recursos

Proyecto Escila

scylla.sh/search?q=name%3A*.edu

ning Tools Slack PSI-BC infosec wiki Tickets Security Issue Tra... GDrive Industry News BCHR Work | Trello

a, please report bugs to [the scylla github repo](#)

name: *.edu

domain	email	password	ip	name
000webhost.com	giaovienit1@gmail.com		117.6.3.147	trongbang.edu
000webhost.com	ewagner@gm.slc.edu		201.253.213.228	ewagner@gm.slc.edu
000webhost.com	alhamd.edu@gmail.com		41.233.55.181	alhamd.edu
000webhost.com	cleel2@wellesley.edu		98.169.59.134	cleel2@wellesley.edu
000webhost.com	brandon@ucdavis.edu		24.7.168.71	Brandon@ucdavis.edu
000webhost.com	physeekshop@gmail.com		118.138.161.16	jenny.keating@monash.edu
000webhost.com	dbittinger@dcccd.edu		144.162.48.139	dbittinger@dcccd.edu
000webhost.com	xfh174@my.utsa.edu		70.123.242.111	xfh174@my.utsa.edu
000webhost.com	lfield@bu.edu		73.218.234.191	lfield@bu.edu
000webhost.com	efrain.pacheco@upr.edu		136.145.209.2	efrain.pacheco@upr.edu
000webhost.com	ssutton1@live.maryville.edu		97.91.223.50	ssutton1@live.maryville.edu
000webhost.com	aigat001@odu.edu		184.2.73.130	aigat001@odu.edu
000webhost.com	cstover@rtc.edu		98.247.92.185	cstover@rtc.edu
000webhost.com	travis.langer@yellowjackets.bhsu.edu		198.177.154.139	travis.langer@yellowjackets.bhsu.edu



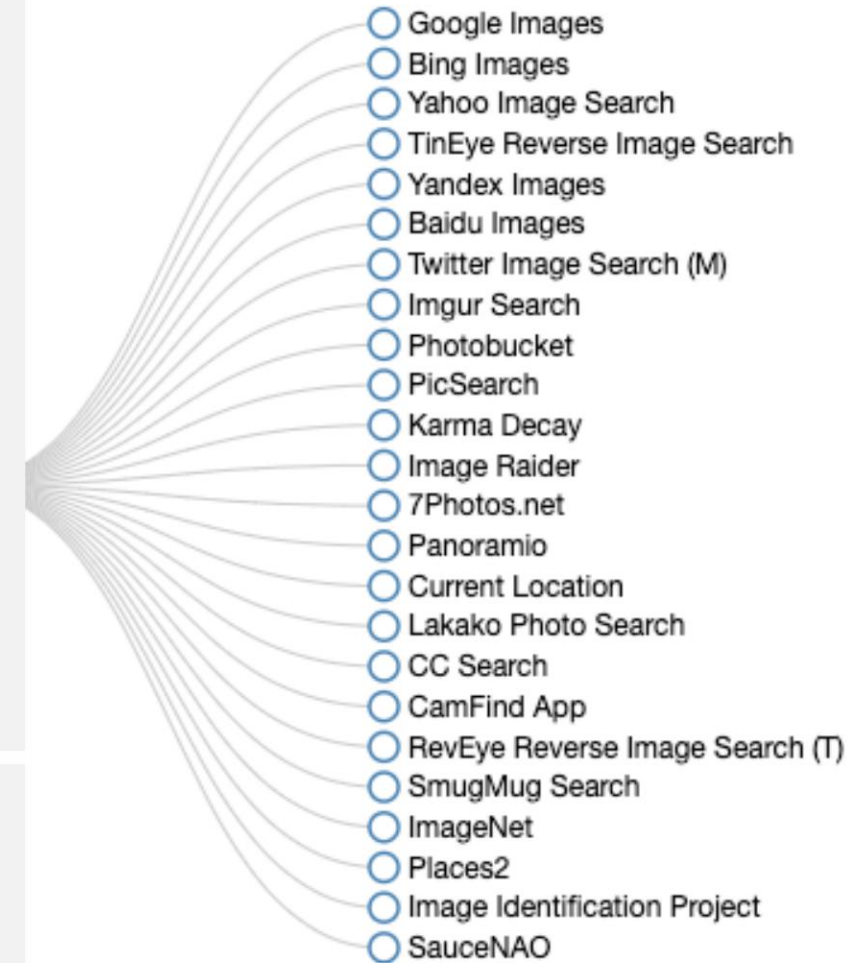
OSINT: herramientas comunes y cómo usarlas de forma segura

Herramientas y recursos

- Búsqueda inversa de imágenes
 - Encuentra otras cuentas

<https://tineye.com/>

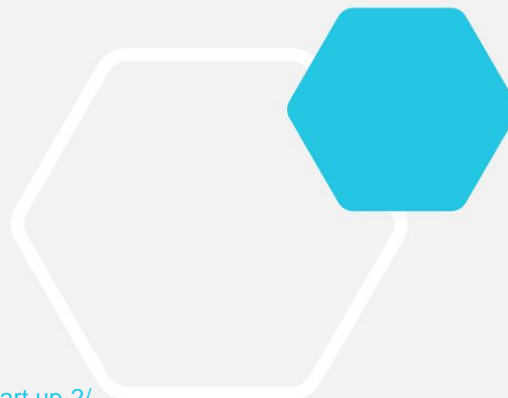
<https://images.google.com/>



OSINT: herramientas comunes y cómo usarlas de forma segura

Herramientas y recursos

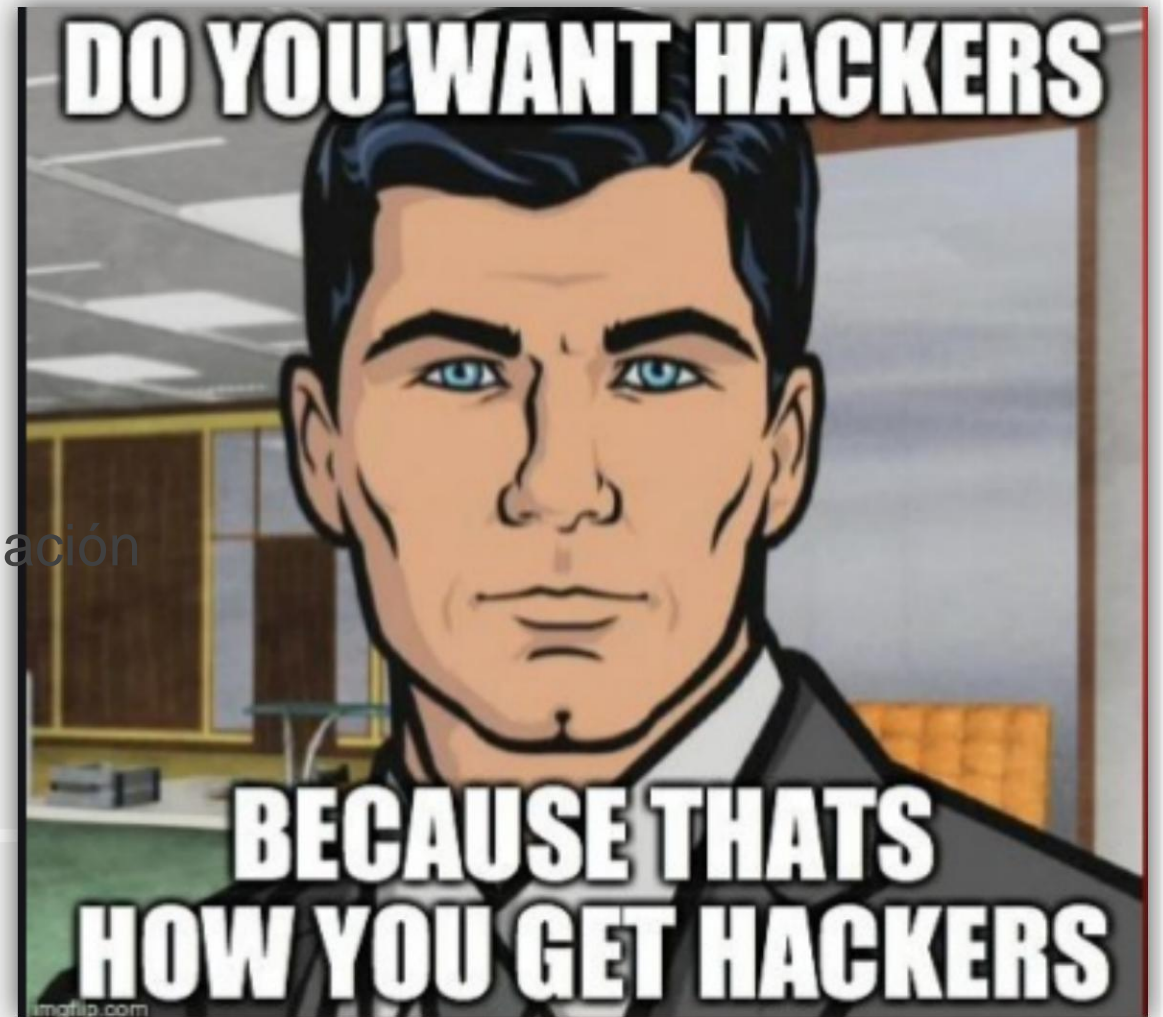
- Búsqueda en redes sociales
 - Lo simple a veces es mejor



OSINT: herramientas comunes y cómo usarlas de forma segura

Mantenerse a salvo

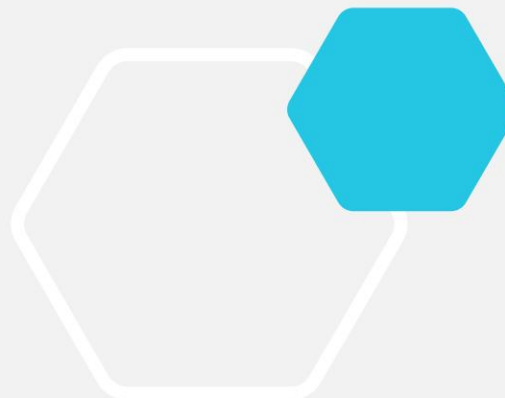
- ¡Por qué es importante!
- Protéjase
- Aísle al objetivo proteja la investigación



OSINT: herramientas comunes y cómo usarlas de forma segura

Mantenerse a salvo

- Reconocimiento pasivo o “sin contacto”:
 - Sin interacción con el objetivo • No invasivo
 - Sin piratería ilegal
 - Reconocimiento activo:
 - Iniciar sesión en las cuentas de los objetivos •
- Ponerse en contacto con el objetivo/amigos/familiares



OSINT: herramientas comunes y cómo usarlas de forma segura

Mantenerse a salvo

- Usar una VM (máquina virtual)
 - Grabelo cuando termine • VPN
- (red privada virtual) • Proton
- Valiente
- Norte •
- Acceso privado a Internet (PIA)



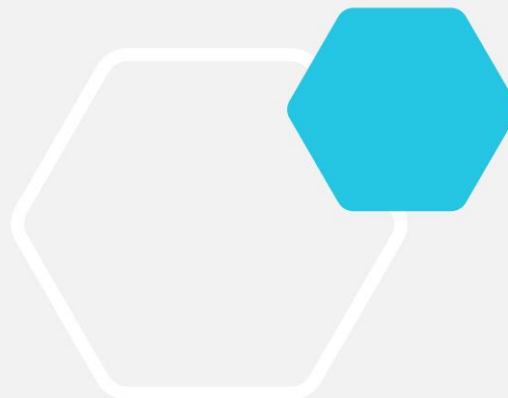
OSINT: herramientas comunes y cómo usarlas de forma segura

Mantenerse a salvo

- Cuentas de títeres de calcetín •

Cuenta falsa utilizada para reconocimiento

- Nunca use sus cuentas personales de redes sociales para investigaciones OSINT • Aísle su información personal



OSINT: herramientas comunes y cómo usarlas de forma segura

Mantenerse a salvo

- Cuentas de títeres de calcetín

- Teléfono quemador

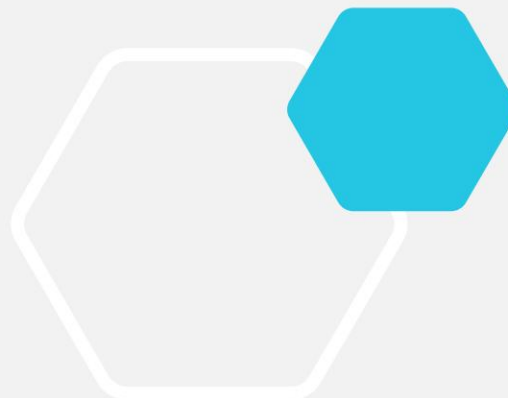
- Proxy inteligente

- Wi-Fi

- Generadores de identidades falsas

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

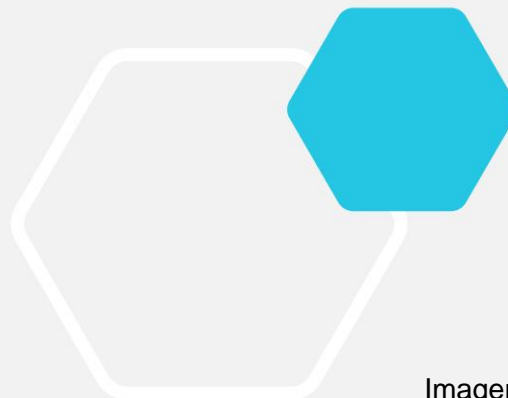
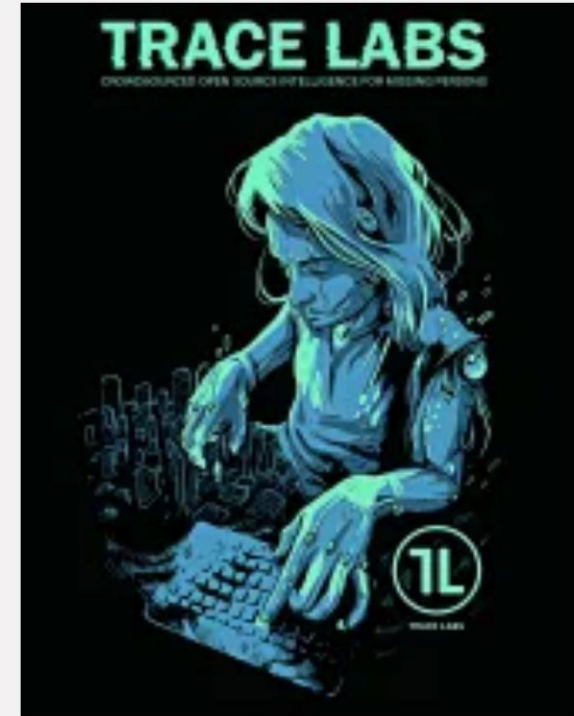
<https://www.generadordenombresfalsos.com/>



OSINT: herramientas comunes y cómo usarlas de forma segura

Usando tus habilidades para el bien

- TraceLabs
 - CTF- ¡Premios y gloria!
 - Casos colaborativos mensuales



OSINT: herramientas comunes y cómo usarlas de forma segura

Resumen

- Si puedes googlear puedes hacer esto
 - Empezando:

- máquina virtual

- VPN

- Google •

Cuaderno

- Deseo de ayudar •

Manténgase organizado





Gracias

👤 Siobhan Kelleher

✉ siobhan.kelleher@bc.edu