



EDICION ESPECIAL

OPEN SOURCE INTELLIGENCE

REQUISITOS

FUENTES DE INFORMACIÓN

ADQUISICIÓN

PROCESAMIENTO

ANÁLISIS

PRESENTACIÓN DE INTELIGENCIA





INVESTIGADOR_Z

INVESTIGADOR_Z

Copyright © 2023 Hack Underway

Todos los derechos reservados. Ninguna parte de este libro puede ser reproducida, pirateada, editada, almacenada en un sistema de recuperación, o transmitida en cualquier forma o por cualquier medio, sin el permiso previo por escrito del editor, salvo en el caso de citas breves incluidas en artículos críticos o reseñas.

En la preparación de este libro (manual) se ha hecho todo lo posible para garantizar la exactitud de la información presentada. Me gustaría recalcar que he dedicado tiempo en realizar este manual y herramientas, así que espero que al comprar este manual también sean discretos en no estar pasando (pirateando) este manual a sus amigos o en grupos, para poder seguir haciendo otros tipos de manuales, que se que le ayudarán en su vida profesional.

No obstante, la información contenida en este libro se vende sin garantía expresa o implícita. Ni el autor, ni Hack Underway, ni sus socios serán responsables de los daños causados directa o indirectamente por este libro, ya que todo es con fines educativos y profesionales.

Quizás de acá a un tiempo algunos enlaces que proporcionaré ya no estén disponibles, ya que vienen actualizándose constantemente, por ello también viendo la acogida que tenga, posteriormente tendrán actualizaciones.

Hack Underway se ha esforzado por proporcionar información sobre marcas comerciales de todas las empresas y productos mencionados en este libro mediante el uso apropiado de mayúsculas, enlaces. No obstante, Hack Underway no puede garantizar la exactitud de esta información.

La herramienta OSINT LATAM, lo pueden solicitar al momento de la compra con este libro en caso lo compren fuera del sitio web, en caso que lo compren desde el sitio web automáticamente se les habilitará las descargas una vez hecho el pago.


«Me gustaría agradecer a mis amigos y familiares, su ayuda tanto en el ámbito profesional y personal. Dar las gracias también a mis compañeros, con los cuales compartí estudios, a todos ustedes fieles seguidores(as) por apoyarme moralmente y materialmente en la realización de este libro».

- Victor Bancayan

Colaboradores

Sobre el autor

Mi nombre es **Victor Bancayan** CEO/FOUNDER/OWNER of [Hack Underway](#), tengo más de 10 años en la informática. Soy titulado de la carrera de “Computación e Informática” en el instituto Cesca. Anteriormente me dedicaba a enseñar ethical hacking en youtube y facebook con el nick de **JEY ZETA**.

Soy un joven que está emprendiendo mediante esta tienda online en Lima – Perú 

Los que me conocen saben que siempre me gustó compartir conocimiento con mis seguidores, soy una persona autodidacta.

Tengo certificaciones en diferentes plataformas online, como en las siguientes:

EC-Council, CertiProf, Cisco, Netzun, Academia, BackTrackAcademy, Eset, Cybrary, Seguridad Cero, Udemy, Tutellus...

“Me considero un novato en busca del conocimiento”

Actualmente estudio inglés.

ÍNDICE

INTRODUCCIÓN.....	2
¿Qué es OSINT?.....	3
Historia del OSINT.....	3
¿En qué te beneficia?.....	4
A quién va dirigido el OSINT.....	4
Fases o ciclos de OSINT.....	5
Sobre las Herramientas.....	6
¿Qué es el doxing?.....	6
Anécdota.....	8
¿Se necesita autorización en investigaciones digitales?.....	9
CONSTRUCCIÓN DE UN LABORATORIO OSINT.....	10
Trace Labs.....	11
Máquinas virtuales.....	12
TAILS.....	14
Efecto Sockpuppet.....	17
¿Qué son las cuentas de Sockpuppet?.....	18
¿Son éticas las cuentas de Sockpuppet?.....	18
Proceso de creación de una cuenta anónima de Sockpuppet.....	19
Fake name generator.....	21
Unreal Person.....	22
Traductores.....	24
Tarjeta virtual.....	26
Navegadores que usaremos.....	27
MOTORES DE BÚSQUEDA OSINT.....	30

Motores de búsqueda comunes.....	31
Motores de búsqueda internacionales.....	32
Buscadores generalistas.....	33
Google.....	33
Microsoft Bing.....	35
Yandex.....	35
Baidu.....	36
DuckDuckGo.....	37
Buscadores tecnológicos.....	38
Shodan.....	38
Zoomeye.....	40
FOFA.....	41
DEEP WEB Y DARK WEB.....	42
Ahmia.Fi.....	43
Configuración de Tor Browser.....	44
Investigación Dark Web (TorBot).....	44
¿Qué es Freenet?.....	45
¿Qué es I2P?.....	46
I2P y Freenet (Configuración).....	47
The Hidden Wiki (Normal).....	48
Herramientas OSINT de la Dark Web.....	51
Herramienta DarkScrape.....	51
Motores de búsqueda en la Dark Web.....	52
Investigación en la Dark Web.....	53
Desarrollo de malware e Investigación en la Dark Web.....	54

GOOGLE HACKING.....	56
Google Dork.....	57
Principales Dorks de Google.....	57
Google Hacking Database.....	59
Pastebin.....	60
¿Qué es un Hash?.....	61
HASH-ID.....	63
Go-Hash.....	63
Hash y cifrado RSA.....	65
OSINT A IMÁGENES / ARCHIVOS / VIDEOS.....	66
Búsqueda inversa de imágenes.....	67
Búsqueda con google imágenes.....	67
Búsqueda con TinEye.....	68
Búsqueda por AI or Not.....	70
Búsqueda con PimEyes.....	71
Visualización de datos EXIF.....	80
De forma online.....	80
FotoForensics.....	81
Search4faces.....	83
Irbis.....	85
Por terminal.....	88
ExifTool.....	88
Búsqueda de archivos.....	91
Búsqueda por Fagan Finder.....	92
Búsqueda por GrayHatWarfare.....	92

Búsqueda de fotos online.....	93
Búsqueda por ImageFinder.....	94
Búsqueda por Shutterstock.....	95
Búsqueda de videos.....	95
Búsqueda por Vimeo.....	96
Motor de búsqueda personalizado.....	97
Búsqueda por Engines Finder.....	97
Búsqueda por Torrent Search.....	98
Buscador de dispositivos.....	99
Búsqueda por censys.....	99
Explotar el motor de búsqueda.....	100
Búsqueda por SPLOITUS.....	101
Búsqueda por Shodan Exploits.....	102
NONBRES DE USUARIOS.....	103
Búsqueda de personas para Investigación.....	104
Búsqueda por BlackBird.....	105
Búsqueda por Snoop.....	107
Búsqueda por SherLock.....	108
Búsqueda por whatsmyname.....	109
Búsqueda por UserRecon.....	110
Búsqueda por Osgint.....	112
Búsqueda por Zen.....	112
Búsqueda por Magma OSINT.....	113
Búsqueda por GvngSearch.....	114
PERSONAS Y EMPRESAS.....	115

Ver información de Bitcoin (wallet).....	116
Búsqueda por Block Cypher.....	116
Búsqueda por BlockChain.....	117
OSINT Framework.....	119
Malfrat's OSINT Map.....	119
OSINT LATAM.....	120
Perú.....	120
Multas Electorales.....	120
Ruc.....	121
Consulta Vehicular.....	123
Colegio de Ingenieros.....	123
Abogados.....	124
México.....	125
Curp.....	126
Venezuela.....	127
Registro Electoral.....	127
Colombia.....	129
Sena.....	129
Chile.....	131
Cédula.....	131
Argentina.....	132
Constancia CUIT.....	132
Ecuador.....	133
Cédula.....	133
Uruguay.....	135

Webmii.....	135
Bolivia.....	136
Email con Epieos.....	136
Paraguay.....	137
Datos.....	137
Métodos privados.....	138
CORREOS ELECTRÓNICOS.....	142
Motor de búsqueda de fugas de datos.....	143
have i been pwned.....	144
Investigación de búsqueda de correo electrónico.....	147
Epieos.....	148
Spokeo.....	151
DuolingoOSINT.....	153
Prot1ntelligence.....	153
Maryan.....	155
Holehe.....	156
Leak Lookup.....	157
Email OSINT.....	159
Breachdirectory.....	160
Mosint.....	160
Api Key.....	162
Requirements.....	162
DeHashed.....	164
GHunt.....	166
¿Qué puede encontrar Ghunt?.....	166

Enlaces externos de OSINT DOJO.....	168
DIRECCIÓN IP.....	169
OSINT para la investigación de direcciones IP.....	170
Maltego.....	171
Obtener IP de usuarios.....	172
Grabify.....	172
IpLogger.....	173
Canary tokens.....	175
Obtener datos geográficos de una IP.....	175
Maxmind.....	175
Sypexgeo.....	176
IPGeolocation.....	176
IpGeo.....	177
H.I.V.E.....	177
GhostTrack.....	177
Otras herramientas.....	179
Servicio Whois.....	179
Exploración DNS, IP inversa.....	180
Reverse IP domain check.....	180
DNSdumpster.....	180
DNSlytics.....	181
Viewdns.....	181
Fugas de datos por dirección IP.....	182
Control de calidad de virus e IP.....	182
VirusTotal.....	183

Internet de las cosas (IoT).....	184
Censys.....	184
Shodan.....	185
Otros enlaces.....	186
Zoomeye.....	186
Marcos para explorar las direcciones IP.....	188
Spiderfoot.....	188
GEOLOCALIZACIÓN / MAPAS.....	192
Google Maps.....	193
Google Earth.....	195
OSINT-SAN.....	198
Mapa de cables submarinos.....	200
Mapa de infraestructuras abiertas.....	201
IP Location.....	201
IPGeolocation.....	204
Seeker.....	205
ngrok.....	205
Enlaces sobre Termux.....	206
Otros recursos extras.....	207
INTELIGENCIA Y RECONOCIMIENTO WEB.....	208
Algunos recursos.....	209
DNSdumpster.....	210
Dnsdmpstr.....	211
DNSRecon.....	211
IndertYwaf.....	212

WAFW00F.....	212
TheHarvester.....	213
Sublist3r.....	214
Scilla.....	215
GoSFinder.....	215
CloudMare.....	216
Cignotrack.....	216
WhatWeb.....	217
WPSeku.....	218
WPScan.....	218
SubDomainizer.....	219
URLExtractor.....	219
FinalRecon.....	220
Wappalyzer.....	221
Shodan.....	222
CheckCloudFlare.....	223
Otras herramientas.....	223
REDES SOCIALES.....	224
Youtube.....	225
Twitter.....	225
TikTok.....	225
Tumblr.....	226
Snapchat.....	226
Skype.....	226
Reddit.....	226

Pinterest.....	226
LinkedIn.....	226
Instagram.....	227
GitHub.....	227
Discord.....	228
Facebook.....	228
Telegram.....	228
Recursos.....	228
WhatsApp.....	229
Ejemplos del mundo real.....	229
Investigación OSINT en Facebook.....	229
Detalles del perfil de Facebook.....	230
User ID de forma manual.....	230
Localiza un grupo de Facebook.....	231
Localizar ID de Fanpage.....	232
Fecha de creación del ID de Facebook.....	233
Opciones de búsqueda en Facebook.....	234
¿Qué es Profile Picture Guard?.....	235
Codificación Base64 de Facebook.....	242
El desglose de la URL anterior es el siguiente.....	243
Interpretar la cadena decodificada.....	244
A continuación se muestra el resultado.....	246
Directorios de Facebook.....	246
Extracción de amigos de Facebook.....	247
User ID, usando LookupID.....	248

OSINT a Youtube.....	249
Video information of youtube.....	249
Youtube Lookup.....	249
OSINT a GitHub.....	251
GitHub URL Hacks.....	251
Public SSH keys.....	251
Profile imagen.....	251
Public GPG keys.....	253
RSS feeds.....	253
Repo commits.....	253
Repo releases.....	254
Repo tags.....	254
User feeds.....	255
Security advisories.....	256
Global timeline.....	256
Diffs.....	256
Osgint.....	257
Zen.....	257
Octosuite.....	258
Uso básico.....	258
Guía de instalación.....	258
Obtener información del perfil de usuario.....	260
Obtener repos de usuario.....	260
Obtener información del perfil de organización.....	263
Obtener los repositorios de organizaciones.....	264

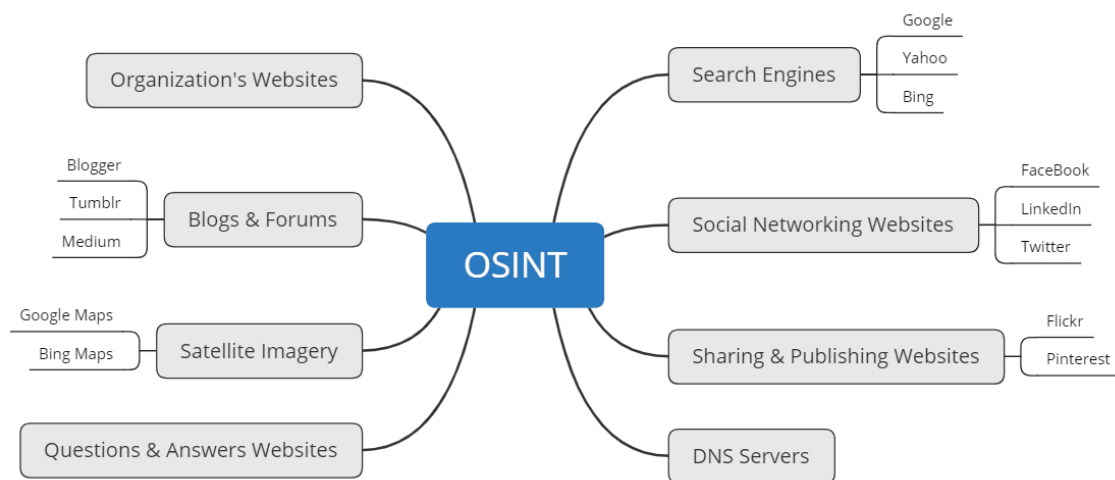
Obtener información sobre el perfil de Repo.....	266
Obtener forks de repo.....	266
OSINT a Instagram.....	267
Instaloader.....	267
OSINT a Twitter.....	269
Tinfoleak.....	169
OSINT a WhatsApp.....	271
WhatsApp-OSINT.....	271
NÚMEROS.....	272
DePerú.....	273
Phonenumbers.....	273
Defastra.....	274
Código Postal.....	276
Epieos.....	277
DeadTrapv2.....	278
GhostTrack.....	279
Ghoulbond.....	279
Otros enlaces.....	281
RECURSOS Y CERTIFICACIONES.....	282
Offensive OSINT.....	282
SANS.....	282
Referencias.....	282
Otros enlaces.....	282
CURSO Y RECOMENDACIONES FINALES.....	284
Hack Underway.....	284

Recomendaciones finales.....	284
Para tomar sus notas.....	284
CherryTree.....	284
Obsidian.....	285
The end.....	286

INTRODUCCIÓN

En esta sección aprenderemos sobre lo que es OSINT, su historia, fases, que herramientas se usan.

A quién va dirigido, en qué nos beneficia, si es legal o no hacer OSINT, sobre doxing, que datos se pueden obtener.



¿Qué es OSINT?

Inteligencia de fuentes abiertas (Open-source intelligence). La importancia de Inteligencia de fuentes abiertas (OSINT) ha crecido en los últimos años. Para la comunidad de inteligencia tradicional, OSINT es probable que siga siendo un componente de una Inteligencia que incluye fuentes clasificadas. Sin embargo, para la mayoría de las agencias gubernamentales, OSINT es la única inteligencia a la que tienen acceso, lo que la convierte en un facilitador estratégico de decisiones y políticas. Los gobiernos deberían considerar la posibilidad de formular un área y el establecimiento de un centro OSINT para permitir la explotación eficaz de fuente de información.

Utilizando OSINT, se puede obtener información de personas y empresas, en este libro nos centraremos en cómo obtener información virtual, sin embargo cabe recalcar que hay diferentes medios de los cuales se puede obtener información, como por ejemplo: Periódicos, revistas, páginas blancas y amarillas, cartas de presentación, fotos físicas, etc.

En pocas palabras el OSINT no es una herramienta, sino una metodología.

Historia del OSINT:

Se tiende a considerar que el OSINT actual nació en 1942, cuando se creó la rama *Research and Analysis* del *Office of Strategic Services* (OSS), la que se encargaba de recopilar toda la información abierta, haciendo traer periódicos del Eje gracias a una nutrida red de embajadas y consulados, escuchando las emisiones de las radios públicas extranjeras, o en general accediendo a librerías y fuentes de información oficiales (CIA, 2013).

Aunque en realidad desde los inicios de los tiempos todos sin querer usamos OSINT, ya sea para saber la dirección de una persona, sus gustos, hasta para buscar alguna tarea en internet.

Sin embargo hay personas que usan mal la información que logran obtener, quiero destacar que hay personas y empresas que tienen mucho acceso a información, por ejemplo: El creador de Facebook, Mark Zuckerberg tiene acceso a todo lo que pasa en esta red social, también las empresas de comunicación como Movistar, ya sea que te den cable, internet, datos, chips, tienen demasiada información de todos sus usuarios en sus sistemas. Y así miles de millones de empresas en todo el mundo, así como los gobiernos y personas que trabajan para el estado, cómo los policías, jueces, fiscales, militares, etc.

¿En qué te beneficia?

Los defensores de OSINT desean destacar su beneficios, quizás el más inmediato de esta es la cuestión del costo. OSINT es considerablemente menos caro que recolectar información vía medios clasificados. Investigadores y periodistas que trabajan en el campo, por ejemplo, son una valiosa fuente de inteligencia. Inteligencia de comunicaciones útil se puede encontrar en los blogs y foros dedicados a varios asuntos, así como en las páginas de cada periódico de calidad.

¿A quién va dirigido el OSINT?

A diferentes ámbitos ó áreas, como son: RRHH, abogados, investigadores privados, policías, militares, periodistas, analistas de seguridad, jueces, fiscales, congresistas, alcaldes, presidentes, etc...



Fases o ciclos de OSINT:

Requisitos: Establecer objetivos, qué información vamos a obtener, que datos con exactitud se debe o necesita encontrar.

Fuentes de información: Dónde vamos a buscar, qué herramientas de búsqueda vamos a utilizar, qué pasos vamos a seguir es esta búsqueda.

Adquisición: Fase de recopilación de datos, suele demorarse un poco más, dependiendo a lo que queremos obtener.

Procesamiento: Dar formato a la información recopilada, generación de inteligencia. (Información clara y comprensible).

Análisis: Fase en la que se genera inteligencia a partir de los datos recopilados y procesados.

Presentación de inteligencia: Cómo presentar la información recopilada, reporte gerencial para tomar las decisiones del caso.



Sobre las Herramientas:

Las herramientas podemos encontrar miles, tanto en modo gráfico, consola, web, en todos los dispositivos tecnológicos que existan, ya que por lo general son multiplataforma y online.

Para ello basta con tener un celular, tablet, laptop, pc, etc. No importa en realidad mucho el sistema operativo que estés usando, ya que desde cualquier equipo con un internet y hardware decente se puede hacer maravillas a la hora de recopilar información.

¿Qué es el doxing?

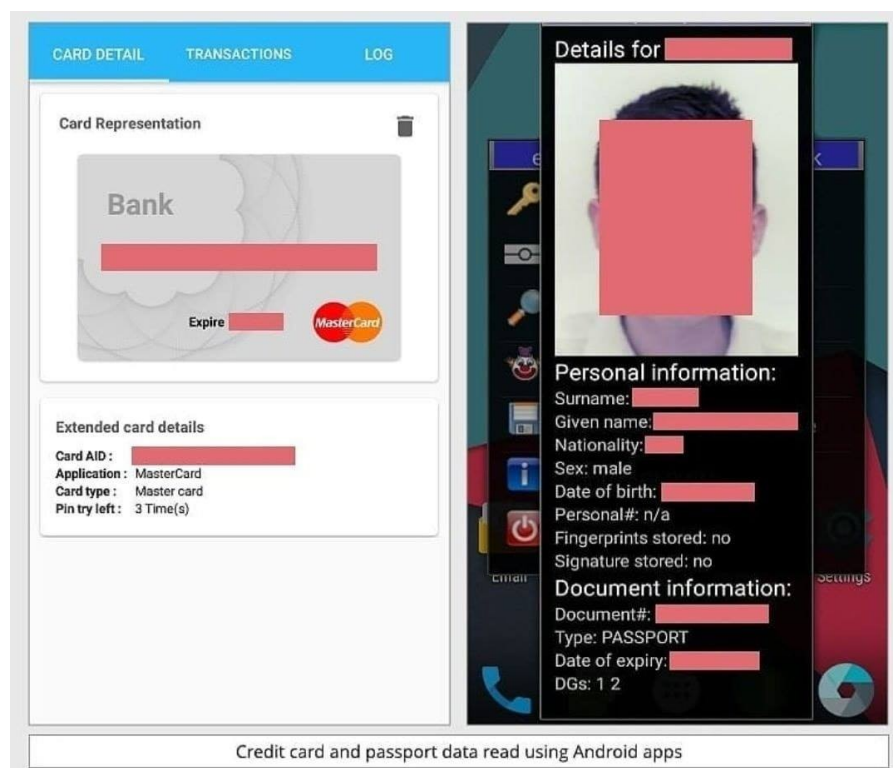
El doxing (a veces escrito como doxxing) consiste en revelar información identificadora de una persona en línea, como su nombre real, dirección particular, lugar de trabajo, teléfono, datos financieros y otra información personal. Luego, esta información se divulga al público sin el permiso de la víctima.

Si bien la práctica de revelar información personal sin el consentimiento del sujeto en cuestión existe desde antes del nacimiento del Internet, el término doxing surgió primero en el mundo de los hackers en la década de 1990, en el que el anonimato se consideraba sagrado. Las disputas entre los hackers rivales a veces provocaban que alguien decidiera “exponer docs” sobre otra persona, quien hasta ese momento solo era conocida por su nombre de usuario o alias. “Docs” se convirtió en “dox” y, finalmente, en su propio verbo (es decir, sin el prefijo “exponer”).

La definición de doxing se ha expandido más allá de la comunidad mundial de hackers y ahora se refiere a la exposición de la información personal. Aunque el término aún se utiliza para describir la acción de desenmascarar a usuarios anónimos, ese aspecto se ha vuelto menos relevante en la actualidad, en que la mayoría de nosotros utilizamos nuestros nombres reales en las redes sociales.

Recientemente, el doxing se ha convertido en una herramienta utilizada en las batallas culturales, ya que los hackers rivales realizan ataques de doxing contra quienes tienen opiniones opuestas a su bando. Los doxers (personas que llevan a cabo el doxing) buscan intensificar el conflicto que tienen con personas en línea llevándolo al mundo real y revelando información como la siguiente:

- Dirección postal
- Detalles del lugar de trabajo
- Números de teléfono personales
- Números del seguro social
- Información de las cuentas bancarias o tarjetas de crédito
- Correspondencia privada
- Antecedentes penales
- Fotos personales
- Detalles personales embarazosos, etc...



Los ataques de doxing pueden variar desde ataques relativamente triviales, como los registros de correo electrónico o las entregas de pizza falsos, hasta los más peligrosos, como acosar a la familia o al empleador de una persona, el robo de identidad, las amenazas u otras formas de acoso en línea, o incluso el acoso en persona.

Anécdota:

Recuerdo estar en comunidades, dónde cada cierto tiempo tenían disputas entre miembros por querer tener el respaldo de la mayoría, ya que siempre tenían diferentes opiniones y formas de pensar, se daban esas peleas virtuales, ya que estando en IRC, las personas eran anónimas, usaban nicks, vpn y diferente seguridad para no ser expuestos, pero aún así he visto con mis propios ojos de cómo personas completamente anónimas y con conocimientos en ciberseguridad, eran doxeados y sus datos expuestos en internet. En esos años se usaba mucho la ingeniería social y cualquier descuido podría llevarte a ser doxeado.

Por esa desunión que vi en habla hispana me retiré de las comunidades y andaba cómo autodidacta aprendiendo por mi cuenta, navegando día y noche en busca del conocimiento.

El mayor descuido que puede hacer un hacktivista es comenzar a dejar huellas en internet luego de sus ataques informáticos, confiar en las personas que lo rodean. Ya que en muchas comunidades hacktivistas hay personas infiltradas, que vienen siguiendo sus pasos, lo digo por experiencia propia, el ego es lo que hace que muchos hacktivistas sean descubiertos, así uses Telegram, correos desechables, VPN, nicks, cifres toda tu información, si cometes un simple descuido se va al tacho de la basura años de estar cuidando tu verdadera identidad.

He llevado casos de investigaciones OSINT, y lo digo porque he visto personas que se cuidan mucho, pero en lo menos pensado bajan la guardia.

Antes de empezar a la práctica debes saber que hay casos donde existe demasiada información y te puedes enredar en ella, ya que probablemente encuentres tanta información que se te hará algo difícil seleccionar y resumirlo.

También debes tener en cuenta de qué tan fiable es la fuente dónde encontraste dicha información, ya que en ocasiones podrías encontrar información errónea e incluso información falsa plantada por la persona o empresa que estén haciendo OSINT, para despistar a los que estén tratando de encontrar algo de ellos.

¿Se necesita autorización en investigaciones digitales?



Como ven la gráfica que publicaron los amigos de ciberpatrulla, hay casos que son sin autorización judicial y otros casos que son con autorización judicial.

Depende mucho del caso, si es complejo debe pedir autorización, ya que hay información que es privada, que solo lo pueden brindar bajo una orden judicial, como es tu historial de búsquedas a tu proveedor de internet, levantamiento de comunicaciones en tu dispositivo móvil, estados de cuenta de banco, etc...

CONSTRUCCIÓN DE UN LABORATORIO OSINT

En esta sección veremos desde la creación de un laboratorio para pruebas OSINT, ya que es fundamental seguir ciertos pasos para la creación de laboratorio y cuentas para la realización de OSINT.

Crear una identidad anónima ó fake (SOCKPUPPET), ya que es importante no usar cuentas personales, cuando haremos trabajos OSINT.

También es importante tener conocimientos sobre la teoría para poder hacer las prácticas necesarias.



Trace Labs:

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

Trace Labs: Es una organización sin ánimo de lucro cuya misión es acelerar la reunificación familiar de las personas desaparecidas a la vez que forma a sus miembros en el arte de la inteligencia de código abierto (OSINT).

Se puede descargar desde el siguiente enlace:

<https://www.tracelabs.org/initiatives/osint-vm>

Downloads			
To get started, download the OVA version of choice below and run it in your choice of VM software (ie. VMware Workstation, Virtualbox etc.). The default credentials to log in to the TL OSINT VM are osint:osint			
VM Release	Size	Install Guide	SHA256 Hash
TL OSINT VM 2022.1 OVA (NA/EU Mirror)	4.7 GB	Install Guide v2.1	62c4a5e6bd8edf1d723f5d031c24163e6c90fcec73bd9228074942868ff7d8fb
TL OSINT VM 2022.1 AMD64 ISO (NA/EU Mirror)	3.8 GB	Install Guide v2.1	442852a5a8ffb4a3756347ac27f616ad7128457b41135d7e75623ce0450bd867
TL OSINT VM 2022.1 MAC M1 ISO	3.5 GB	Install Guide v2.1	32ea9357db1c741ed0d0957f1650d423ed3ebd2e981d41270a2746054fbe2af3

Básicamente este sistema operativo se instala desde una máquina virtual, ya sea que estes en Windows, Linux, Mac OS, en cualquiera puedes instalarlo, y es recomendable usarlo desde una máquina virtual, no como sistema operativo principal, ya que al finalizar podrás eliminarlo sin problemas, así tengas algunos problemas podrás volver a empezar desde cero, eliminar la veces que quieras, ya que sólo es una máquina virtual, no afectará el sistema operativo principal, probablemente si no has usado alguna vez una máquina virtual debes guiarte de vídeos, ya que dependiendo de la BIOS de tu computadora varía la configuración.

Máquinas virtuales:

VMware Workstation

VirtualBox

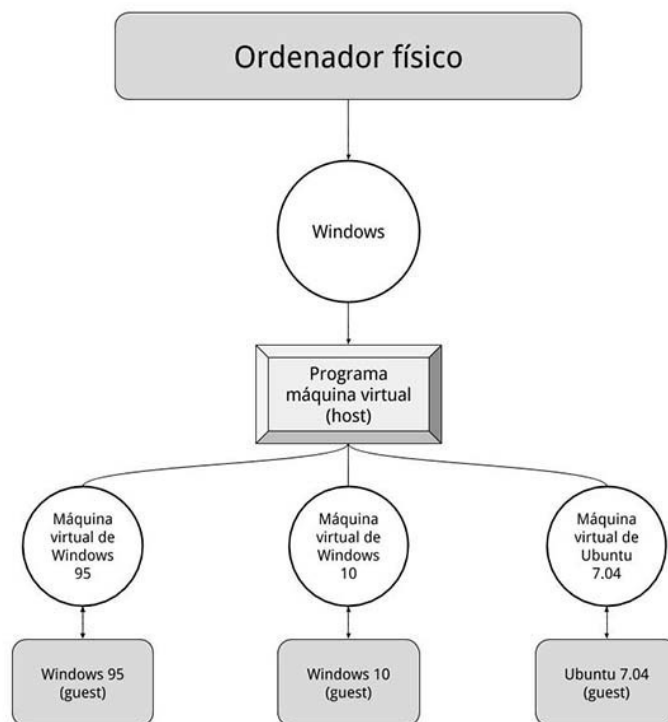
Wineskin Winery

Qemu

Entre otras...



A continuación resumo, lo que es la máquina virtual en una imagen.



En pocas palabras, el sistema operativo principal es el medio donde se va a instalar la maquina virtual, ya que esos programas sirven como emulador, sin afectar el sistema operativo principal, puedes instalar varias máquinas virtuales con diferentes sistemas operativos, cabe mencionar que debes tener al menos

características más que basicas para poder correr bien las máquinas virtuales y no se cuelguen a la hora de ejecutarlos.

Los requerimientos de este sistema operativo.

System Requirements	
Category	Tools/Features
Operating Systems	Windows 10 x64 / Mac OS X / Linux Distribution x64
Processor	Intel Core i3 2.5 Ghz or AMD Phenom II 2.6 Ghz or greater
Memory	8 GB RAM
Storage	40 GB Available
<p>We are continuing to build upon the Trace Labs OSINT VM and welcome any and all feedback. Our goal with this project is to create an OSINT focused VM that provides security, stealthiness and the ability to easily save digital forensic evidence during an investigation all within an easy to use package.</p> <p>Want to contribute tool and configuration suggestions? Log a GitHub Issue on our GitHub page for the project here: https://github.com/tracelabs/tlosint-live</p> <p>Credit for the creation & maintenance of this project goes to Jason Kregting, Tom Hocker (humanDecoded), Swetha Balla, lowprivs, Katniss, and Paul "Krkn" D!</p>	

Algunas herramientas que traen.

Applications Included	
Category	Tools/Features
Domains	<ul style="list-style-type: none">• Sublist3r
Downloaders	<ul style="list-style-type: none">• Browse Mirrored Websites• Metagoofil• Spiderpig• WebHTTrack Website Copier• Youtube-DL
Browsers	<ul style="list-style-type: none">• Chromium Web Browser• Firefox ESR• Tor Browser
Emails	<ul style="list-style-type: none">• Buster• H8mail• Infoga• theHarvester
Data Analysis	<ul style="list-style-type: none">• DumpsterDiver• Exifprobe

Cabe destacar que este sistema operativo está enfocado al OSINT, por eso ya vienen algunas herramientas pre instaladas.

Aunque algunas personas que hacen OSINT usan otros sistemas operativos, ya que depende a su comodidad, ya que básicamente tendremos que instalar ciertas herramientas para el uso de recopilar información, muy aparte de crear cuentas, en diferentes plataformas ya que muchas herramientas nos piden una cuenta y también una API, que lo veremos más adelante.

La instalación es muy simple, ya que al descargar el archivo .OVA, ya viene solo para montarlo a la máquina virtual, sin necesidad de estar instalando el sistema operativo.

Si se preguntan que máquina virtual usar, yo he usado Virtual Box y VMware, pero ya llevo mucho tiempo usando VMware, es cuestión de gustos. Aunque VMware digamos que tiene ciertas características, ya que es un programa de paga (premium).

TAILS:

<https://tails.boum.org/index.es.html>



(The Amnesic Incognito Live System) o "Tails" es una distribución Linux diseñada para preservar la privacidad y el anonimato. Es la siguiente iteración de desarrollo de la distribución Incognito. Está basada en Debian GNU/Linux,

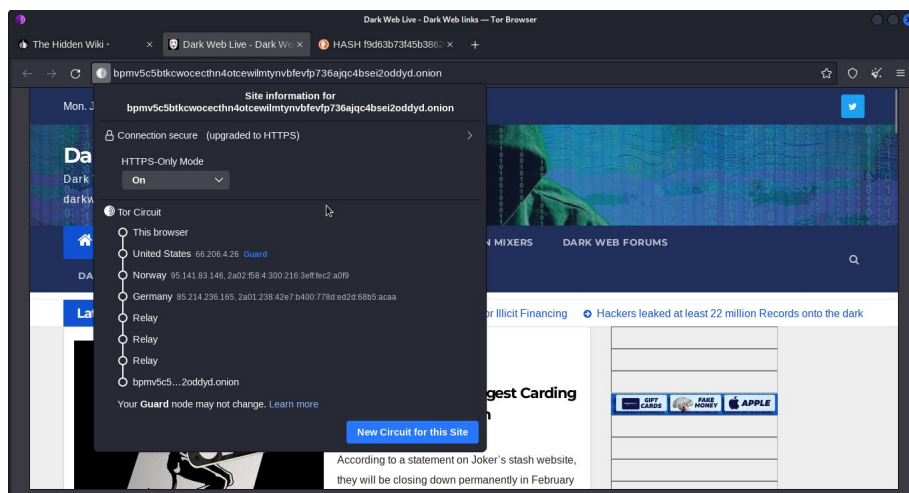
con todas las conexiones salientes forzadas a salir a través de Tor. El sistema está diseñado para ser arrancado como un Live CD o USB sin dejar ningún rastro en el almacenamiento local (por lo general, disco duro) a menos que se indique explícitamente.

https://es.wikipedia.org/wiki/The_Amesic_Incognito_Live_System

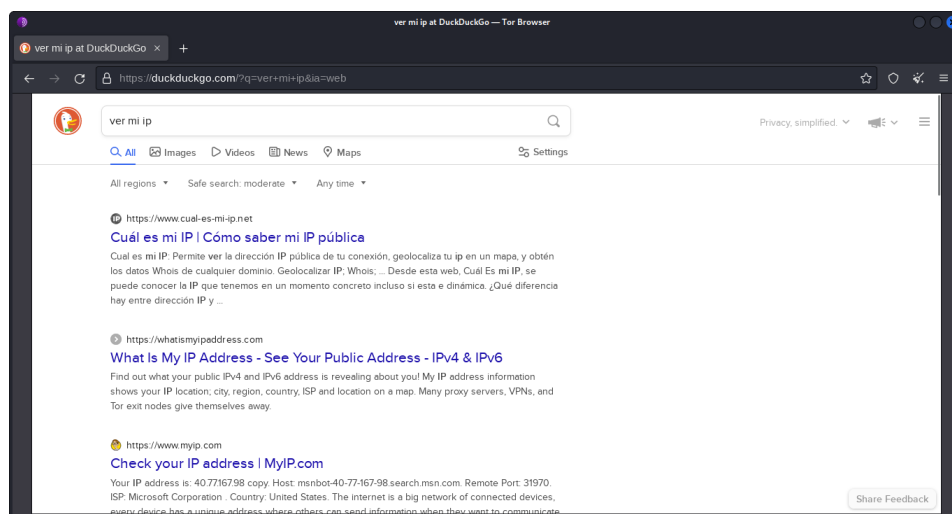
<https://tails.boum.org/about/index.es.html>

<https://www.xn--linuxenespaol-skb.com/distribuciones/tails/>

En este caso usaremos Tor browser.



Quiero destacar que al darle clic al candado en cualquier pagina que estemos, nos muestra la seguridad que nos brinda, nos muestra 6 capas.



Al poner VER MI IP, el el buscador nos muestra varias paginas, vamos a entrar en la primera. (<https://www.cual-es-mi-ip.net/>)



Si queremos geolocalizar la IP, nos muestra el siguiente resultado.

Dirección IP

185.220.101.131

The map shows the location of the IP address 185.220.101.131. A red pin is placed on the map, and a label above it reads 'Su IP: 185.220.101.131'. The map shows the area around Berlin, including Brandenburg, Potsdam, and various smaller towns like Neuruppin, Oranienburg, and Eberswalde.

País	Alemania
Ciudad	Ciudad de Brandeburgo
Latitud	52.6171
Longitud	13.1207
ISP	CIA TRIAD SECURITY LLC

Como plus, puedes cambiar de ip al darle **New Circuit for this Site**, las veces que quiera.

Efecto Sockpuppet:

En el mundo digital un SOCKPUPPET es una falsa identidad en línea, es decir, una cuenta falsa de usuario creada para ensalzar, loar y glorificar a una persona o una organización con un rol de tercera persona.



La creación de cuentas de Sockpuppet, al igual que OSINT, siempre está cambiando.

[https://www.reddit.com/r/OSINT/comments/dp70jr/
my_process_for_setting_up_anonymous_sockpuppet/](https://www.reddit.com/r/OSINT/comments/dp70jr/my_process_for_setting_up_anonymous_sockpuppet/)

<https://javiercantera.com/efecto-sockpuppet/>

¿Qué son las cuentas de Sockpuppet?

Las cuentas Sockpuppet son cuentas anónimas o seudónimas utilizadas para diversos proyectos. Últimamente son noticia por la discordia política. Investigaciones OSINT Investigaciones HUMINT Ingeniería social Y mucho más.

- Últimamente son noticia por la discordia política
- Investigaciones OSINT
- Investigaciones HUMINT
- Ingeniería social
- Y mucho más.

¿Son éticas las cuentas de Sockpuppet?

Esto depende de ti. Sinceramente.

Sockpuppets, una capacidad **OSINT/HUMINT**, se han utilizado generalmente de dos maneras:

- 1.Reconocimiento pasivo. (Generalmente OSINT)
- 2.Infiltración de grupos. (Generalmente HUMINT)

No tengo absolutamente ningún reparo ético en utilizar cuentas ficticias para el reconocimiento pasivo.

Con HUMINT, infiltrarse en grupos objetivo es una necesidad común. En este caso, a menudo tienes que fingir ser alguien que no eres.

Por ejemplo, un investigador contratado para recopilar datos sobre una red de pedofilia en la (dark web) web oscura, tendrá que crear un personaje y convencer de que es uno de ellos para entrar en el grupo.

Generalmente no hago este tipo de trabajos. Me sentiría cómodo si tuviera a las fuerzas del orden (policías, militares, gobierno) respaldándome en esto

porque podría volverse peligroso o ilegal, y me ayudarían a asegurarme de que no estoy infringiendo ninguna ley ni me estoy metiendo en ningún problema del que no puedan sacarme.

Cabe señalar que en EE.UU. Es ilegal hacerse pasar por un empleado del gobierno, especialmente de las fuerzas del orden y del ejército.

Tampoco está bien hacerse pasar por una persona real. Mantén tus sockpuppets inventados (fake).

Proceso de creación de una cuenta anónima de Sockpuppet.

- ✓ Piensa en un personaje para la cuenta.
- ✓ Utiliza el Generador de nombres falsos para crear una persona que creas que encaja con tu personaje de títere.
- ✓ Utiliza a una persona que no existe para generar una imagen. Asegúrate de inspeccionar la imagen detenidamente y de obtener una que no tenga defectos evidentes, como suele ocurrir. Merece la pena adquirir algunos conocimientos de Photoshop, GIMP, Affinity Photo o Designer, u otros conocimientos básicos de manipulación de imágenes para corregirlos y cambiar el fondo de la imagen. Actualización de julio de 2020: Las redes sociales se han dado cuenta de esto y no siempre funciona. He descubierto que "photoshopear" un par de gafas de sol en la cara y cambiar el fondo parece funcionar por ahora.
- ✓ Consigue un teléfono desechable, completamente limpio y nuevo. Puede ser de cualquier marca que acepte una tarjeta SIM de Mint Mobile.
- ✓ Consigue una tarjeta de crédito desechable en Privacy.com para utilizarla en Amazon y, posiblemente, en la configuración de Mint Mobile. Puede que la necesiten para configurar la cuenta.
- ✓ Crea una cuenta de Amazon desechable. Sólo la usaremos una vez.

- ✓ Compra dos tarjetas SIM de Mint Mobile. Puedes encontrarlas en varios lugares en línea y en tiendas cerca de ti, pero puedes conseguir dos de ellas por \$5 en Amazon (aff). También te dan 1 semana de prueba gratuita con algo así como 100 mensajes de texto, que vamos a utilizar. Esto te da dos tarjetas para dos cuentas sockpuppet por sólo \$ 5.
- ✓ Me gusta usar Amazon para que envíen la tarjeta a una caja de Amazon, que puede ser anónima.
- ✓ Consigue una VPN que puedas configurar en el área física en la que quieres que tu "sockpuppet" "exista".
- ✓ Configura la cuenta de prueba de Mint Mobile en algún lugar lejos de tu casa; tan lejos como estés dispuesto a ir.
- ✓ Utiliza este número de teléfono de prueba de Mint Mobile para configurar todos los sitios web que necesites.
- ✓ Te recomiendo que al menos configures una cuenta de Google y otra de Protonmail. Ambas te serán útiles en diferentes momentos.
- ✓ Una vez que hayas configurado todas las cuentas con tu SIM Mint de prueba, configura 2FA en todas las cuentas.
- ✓ Después de configurar 2FA en todas las cuentas, cambia el número de teléfono a uno al que tengas acceso más permanente, como MySudo o Google Voice.
- ✓ Asegúrate de que todo funciona.
- ✓ Destruye la tarjeta SIM.
- ✓ Borra el teléfono.

Muchos de estos sitios web bloquean MySudo, Google Voice y otros números VoIP. Es por eso que pasamos por el número de teléfono Mint primero.

Dare algunas pautas, para que puedan tener la idea de cómo hacer cuentas anónimas, ya que es recomendable usar cuentas que no suplanten la identidad de una persona, sino que sean de personas que no son reales, para no meternos en líos.

En la siguiente pagina, se puede generar una identidad fake, que no existe, ya sea aleatoriamente, o puedes poner algunas características para que lo genere.

Fake name generator:

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

FAKE NAME GENERATOR™


Name Generator Free Tools Order in Bulk Smiley Generator FAQ

Your Randomly Generated Identity

Gender: Random
Name set: American
Country: United States

These name sets apply to this country: American, Hispanic

[Generate](#) [Advanced Options](#)


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

[Sign in](#)

Peggy S. Irizarry
4361 Hall Street
Overton, NV 89040

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

Mother's maiden name: Sturgill
SSN: 530-85-XXXX
Geo coordinates: 36.329143, -114.316132

PHONE
Phone: 702-484-4686
Country code: 1

Puedes generar aleatoriamente o también elegir esos 3 campos (**Gender, Name set, Country**)

FAKE NAME GENERATOR™


Name Generator Free Tools Order in Bulk Smiley Generator FAQ

Your Randomly Generated Identity

Gender: Male
Name set: German
Country: Italy

These name sets apply to this country: Italian

[Generate](#) [Advanced Options](#)


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

[Sign in](#)

Klaus Wulf
Via Roma, 78
14013-Monale AT

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

Mother's maiden name: Baader
No. Carta d'Identità: BQ67324147
Geo coordinates: 44.869635, 8.034424

PHONE
Phone: 0376 0017715
Country code: 39

BIRTHDAY	
Birthday	April 15, 1970
Age	52 years old
Tropical zodiac	Aries
ONLINE	
Email Address	KlausWulf@armyspy.com <i>This is a real email address. Click here to activate it!</i>
Username	Sullumeent
Password	riqua15Dohng
Website	PublicityHelper.it
Browser user agent	Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko
FINANCE	
MasterCard	5320 3290 8136 8487
Expires	3/2027
CVC2	558
EMPLOYMENT	
Company	Rink's
Occupation	Hospital attendant
PHYSICAL CHARACTERISTICS	
Height	6' 0" (182 centimeters)
Weight	246.2 pounds (111.9 kilograms)
Blood type	A-

TRACKING NUMBERS

UPS tracking number	1Z 994 E35 84 9574 756 0
Western Union MTCN	7633305888
MoneyGram MTCN	67267779

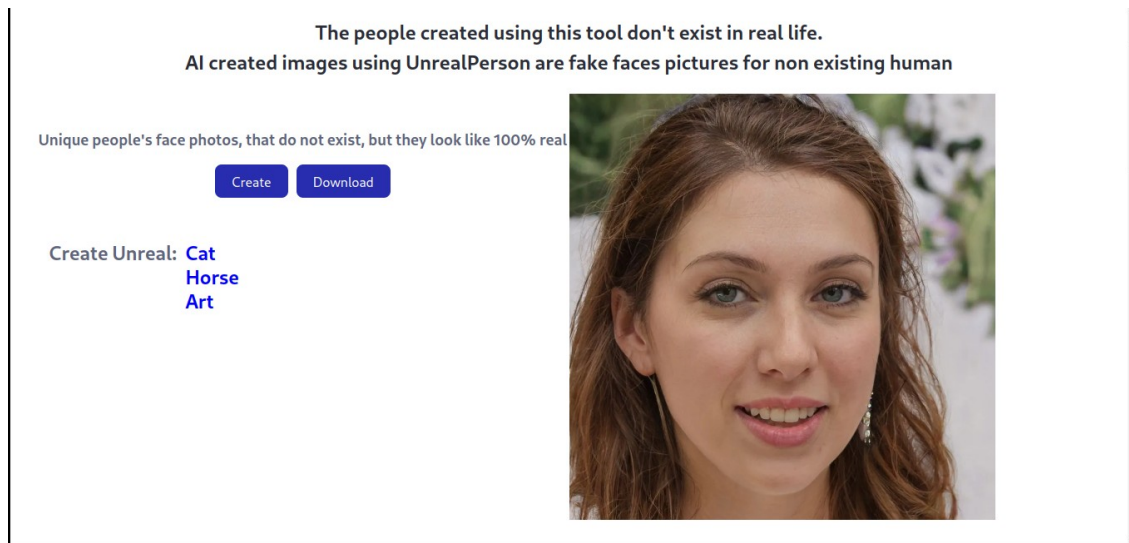
OTHER

Favorite color	Blue
Vehicle	2012 Acura ZDX
GUID	d69d8377-0adc-462e-803a-2e3cb8dede9f
QR Code	Click to view the QR code for this identity

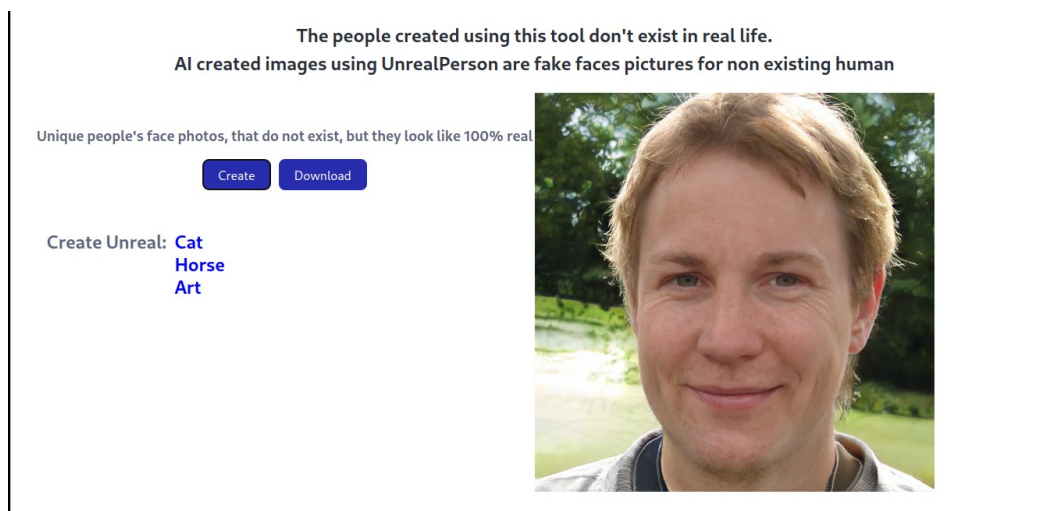
Unreal Person:

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

Las personas creadas con esta herramienta no existen en la vida real. Las imágenes creadas por IA (Inteligencia Artificial) usando UnrealPerson son imágenes de caras falsas de humanos inexistentes.



Si dan clic al botón Create (Crear), podrán generar una nueva imagen aleatoria, es muy importante que tengas en claro algunos términos en inglés, ya que la mayoría de paginas que usaremos están en el idioma inglés.

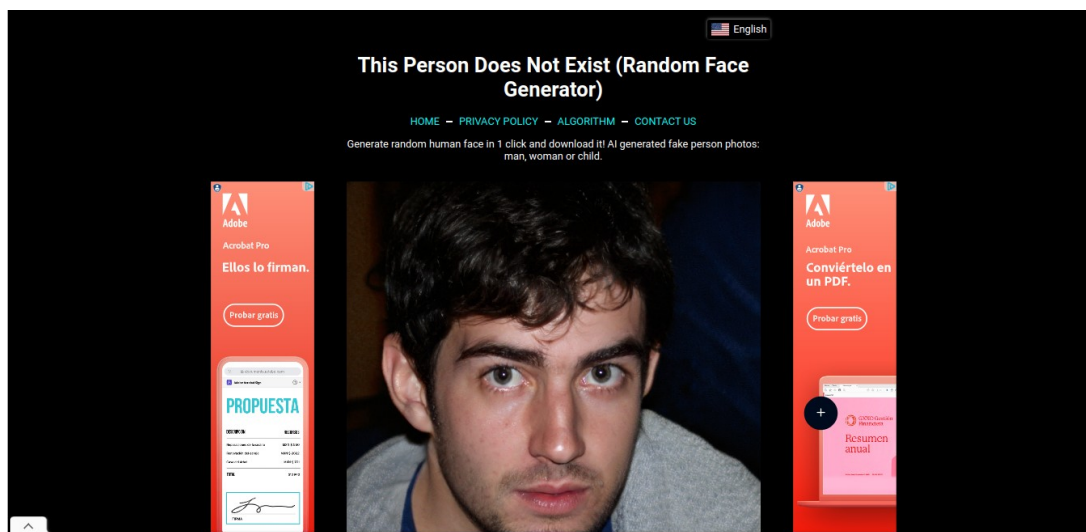


Si gusta pueden descargar, dando clic al botón Download (Descargar) También hay otra web muy usada para generar imágenes que no existen, pero parecen reales.

Ya que son creados con Inteligencia Artificial (IA). Es así como se pone complicado hallar con ese perfil, ya que la imagen no es real de una persona real.

Este es otra pagina web, similar a la que vimos anteriormente.

<https://this-person-does-not-exist.com/en>



Generador de caras aleatorias (Esta persona no existe)

Traductores:

Antes de seguir, debemos tener en cuenta como dije anteriormente, que debemos entender algo de inglés, en todo caso usaremos traductores, ya sea en el navegador, como extensión o como aplicación en el un celular.

<https://translate.google.com/?hl=es>

Es muy usado para traducir idiomas en internet, ya que se usa desde el navegador.

<https://play.google.com/store/apps/details?>

[id=com.google.android.apps.translate&hl=es&gl=US](https://play.google.com/store/apps/details?id=com.google.android.apps.translate&hl=es&gl=US)

También lo pueden usar desde el celular.

En lo personal uso como traductor en el navegador **DeepL Traductor**, como que deja a entender mejor las palabras traducidas al inglés, lo uso desde el navegador y desde la extensión, ya que al tener instalada la extensión, solo basta con seleccionar el texto y nos aparece el logo de la extensión, al darle clic, nos traduce automáticamente el texto seleccionado.

<https://www.deepl.com/es/translator>

<https://apps.apple.com/app/apple-store/id1552407475>

Desde el celular uso **Traductor U**, es muy fácil de usar, además de tener para iPhone y Android.

[https://play.google.com/store/apps/details?](https://play.google.com/store/apps/details?id=com.youdao.hindict&hl=es_PE&gl=US)

[id=com.youdao.hindict&hl=es_PE&gl=US](https://play.google.com/store/apps/details?id=com.youdao.hindict&hl=es_PE&gl=US)

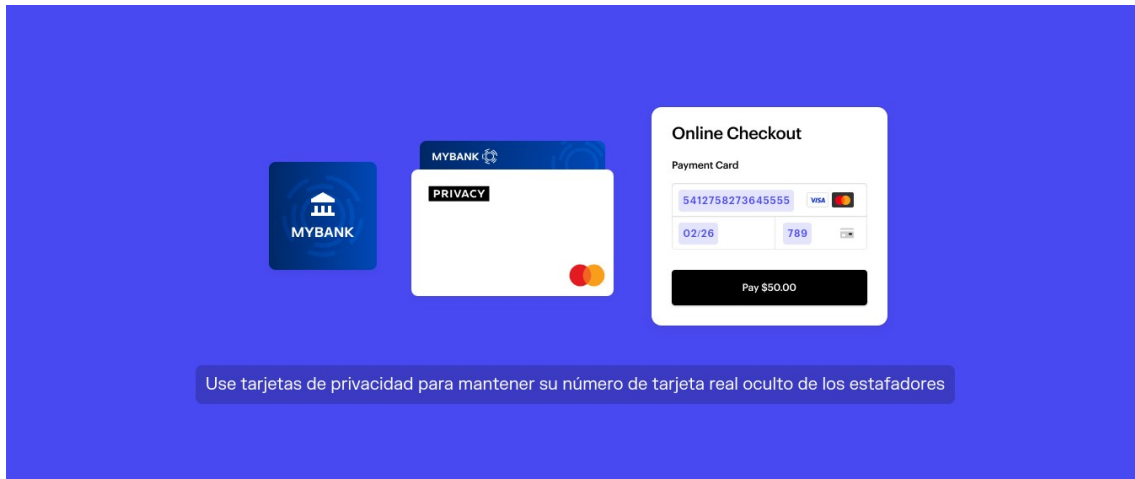
[https://apps.apple.com/co/app/traductor-u-inkl%C3%A9s-espa%C3%B1ol/](https://apps.apple.com/co/app/traductor-u-inkl%C3%A9s-espa%C3%B1ol/id1319771553)
[id1319771553](https://apps.apple.com/co/app/traductor-u-inkl%C3%A9s-espa%C3%B1ol/id1319771553)



Es necesario a la hora de hacer OSINT, mantener el anonimato, no usar nuestras cuentas personales para estar buscando información, como recomendación sería usar una identidad que no exista pero que parezca real, usar un sistema operativo en modo Live o virtualizado, para mantener la seguridad de nuestras búsquedas, y eliminar al final todo.

Targeta virtual:

Privacy - (<https://privacy.com/>)



Una tarjeta virtual es un número de tarjeta único de 16 dígitos con un código CVV y una fecha de vencimiento que puede generarse instantáneamente y usarse para realizar compras en línea o por teléfono. Piense en ello como una tarjeta de crédito o débito normal, pero sin la tarjeta de plástico física. Una tarjeta de privacidad es una tarjeta virtual que oculta su información de pago real. Al usar una tarjeta de privacidad para pagar, puede mantener su verdadera información financiera privada de comerciantes, terceros malintencionados y actores fraudulentos. Las tarjetas de privacidad tienen funciones de seguridad adicionales que lo protegen contra fraudes y transacciones injustificadas. Con esta targeta puedes hacer compras sin dejar rastros. (Funciona en distitos navegadores y dispositivos).

Obtener privacidad para Chrome

Obtener privacidad para Firefox

Obtenga privacidad para iOS

Obtener Privacidad para Android

También podemos usar BTC (Bitcoin), para mantener el anonimato al máximo.

Mientras no hagas cosas ilegales siéntete seguro usando btc, mucho más si eres un policía o autoridad, ya que tienes el respaldo del gobierno.

No hay nada 100% seguro, pero si medidas a tomar en cuenta para ampliar la seguridad.

Navegadores que usaremos:

https://www.google.com/intl/es_es/chrome/

Google Chrome: Es un navegador web de código cerrado, desarrollado por Google, aunque derivado de proyectos de código abierto. Está disponible gratuitamente. El nombre del navegador deriva del término en inglés usado para el marco de la interfaz gráfica de usuario.

https://en.wikipedia.org/wiki/Google_Chrome



<https://brave.com/es/>

Brave: Es un navegador web de código abierto basado en Chromium, creado por la compañía Brave Software en el año 2016, fundada por el cofundador del Proyecto Mozilla y creador de JavaScript, Brendan Eich. A partir de 2019, Brave ha sido lanzado para Windows, macOS, Linux, Android e iOS.

[https://es.wikipedia.org/wiki/Brave_\(navegador_web\)](https://es.wikipedia.org/wiki/Brave_(navegador_web))



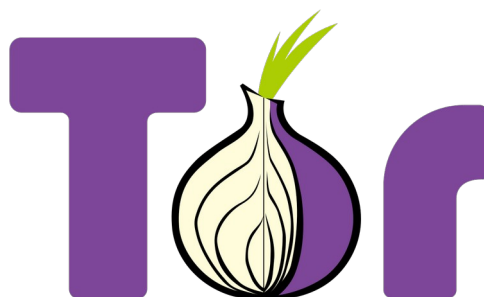
<https://www.torproject.org/es/>

Tor (sigla de The Onion Router ,en [español](#): “El Enrutador Cebolla”) es un proyecto cuyo objetivo principal es el desarrollo de una red de comunicaciones distribuida de baja [latencia](#) y [superpuesta](#) sobre [internet](#), en la que el [encaminamiento](#) de los mensajes intercambiados entre los usuarios no revela su identidad, es decir, su [dirección IP](#) (anonimato a nivel de red) y que, además, mantiene la integridad y el secreto de la información que viaja por ella. Por este motivo se dice que esta tecnología pertenece a la llamada [darknet](#) o red oscura, que no se debe confundir con la *deep web* o [web profunda](#).

El Navegador Tor está disponible para Linux, Mac y Windows, y desde entonces ha sido portado a móviles. Si usas Android, encuentra OrBot u OrFox en Google Play Store o F-Droid. Los usuarios de iOS pueden descargar OnionBrowser de la App Store de Apple.

https://es.wikipedia.org/wiki/Tor_%28red_de_anonimato%29

<https://www.shellfire.es/blog/tor-browser-anonimo-seguro/>



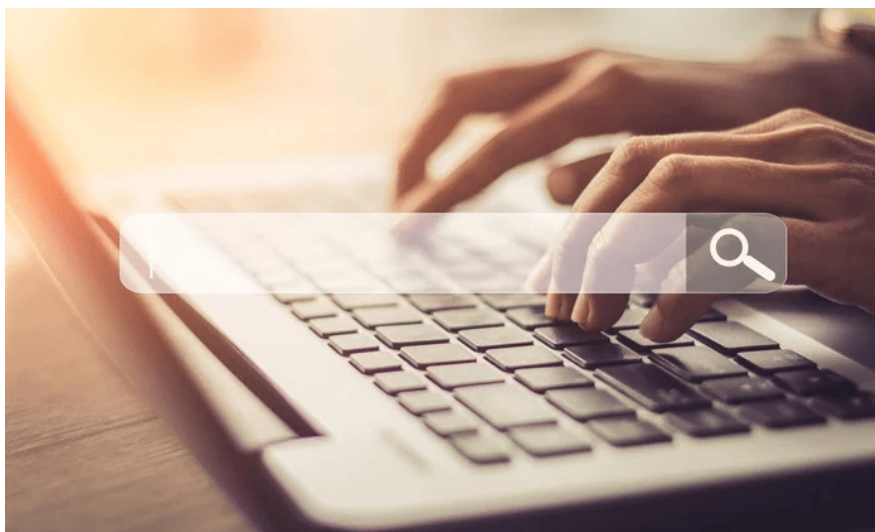
La instalación de estos navegadores, es muy simple y lo bueno que es multiplataforma, pueden buscar por internet cientos de tutoriales de la instalación de estos navegadores en diferentes idiomas.

MOTORES DE BÚSQUEDA OSINT

Veremos el uso de diferentes opciones para la búsqueda de información, como los navegadores, motores de búsqueda, ya que hoy en día hay demasiada información que se expone en internet.

Con tan solo poner diferentes búsquedas por dorks y usar buscadores como Shodan, son los que nos facilitan a la hora de encontrar cierta información, ya que se indexa por estos motores de búsqueda.

Muchas empresas y personas no configuran sus dispositivos y sistemas, pensando que nadie podría acceder a su información, muchos gobiernos utilizan esto para tener ventaja de la competencia, inclusive para espionaje gubernamental.



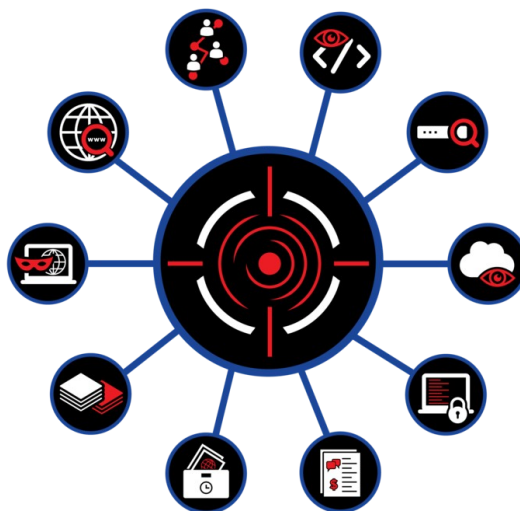
Motores de búsqueda comunes:

- [Google](#)
- [Bing](#)
- [Yahoo](#)
- [AOL](#)
- [Infospace](#)
- [Lycos](#)
- [Exalead](#)
- [ASK](#)
- [Ecosia](#)
- [entireweb](#)
- [teoma](#)
- [yippy](#)
- [I Search From](#): Simula el uso de la Búsqueda de Google desde una ubicación o dispositivo diferentes, o realiza una búsqueda con una configuración.
- [millionshort](#): Permite eliminar la parte superior de los resultados del motor de búsqueda.



Motores de búsqueda internacionales:

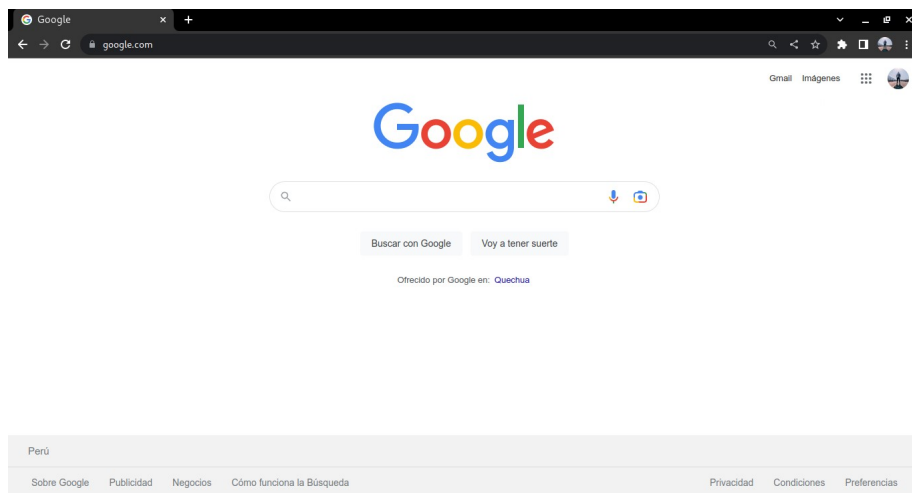
- [Yandex](#): Russia
- [Search](#): Switzerland
- [Alleba](#): Philippines
- [Baidu](#) | [so](#) | [bhanvad](#) China
- [Eniro](#): Sweden
- [Daum](#): South Korea
- [Goo](#): Japan
- [Onet](#): Poland
- [Parseek](#): Iran
- [SAPO](#): Portugal
- [AONDE](#): Brazil
- [Lableb](#): Arabic based search engine
- [arabo](#): Arabic Search engine



Buscadores generalistas:

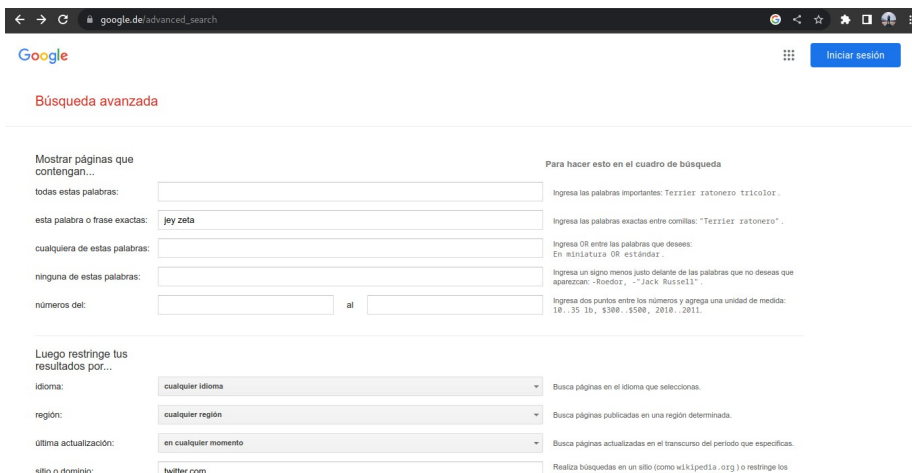
<https://www.google.com/>

Google: La Búsqueda de Google es un buscador completamente automatizado que utiliza programas de software denominados “rastreadores web” para explorar la Web periódicamente en busca de páginas que pueda añadir a su índice. Google ofrece búsqueda en Internet y otros servicios como mapas, navegador, traductor, pasajes de vuelos, transporte público, taxi, clima, noticias, etc...



https://www.google.de/advanced_search

Cabe recalcar que también se pueden hacer búsquedas avanzadas desde Google.



Luego restringe tus resultados por...

idioma:	<input type="text" value="cualquier idioma"/>	Busca páginas en el idioma que seleccionas.
región:	<input type="text" value="cualquier región"/>	Busca páginas publicadas en una región determinada.
última actualización:	<input type="text" value="en cualquier momento"/>	Busca páginas actualizadas en el transcurso del periodo que especificas.
sitio o dominio:	<input type="text" value="twitter.com"/>	Realiza búsquedas en un sitio (como wikipedia.org) o restringe los resultados a un dominio como .edu, .org o .gov.
términos que aparecen:	<input type="text" value="En cualquier parte de la página"/>	Busca términos en toda la página, en su título o en su dirección web, o vínculos que le dirijan a la página que estás buscando.
SafeSearch	<input type="text" value="Mostrar resultados explícitos"/>	Indica a SafeSearch si quieres que filtre contenido sexualmente explícito.
tipo de archivo:	<input type="text" value="Cualquier formato"/>	Busca páginas del formato que prefieras.
derechos de uso:	<input type="text" value="Páginas cuyo uso no requiera de licencias"/>	Busca páginas que puedas usar libremente.

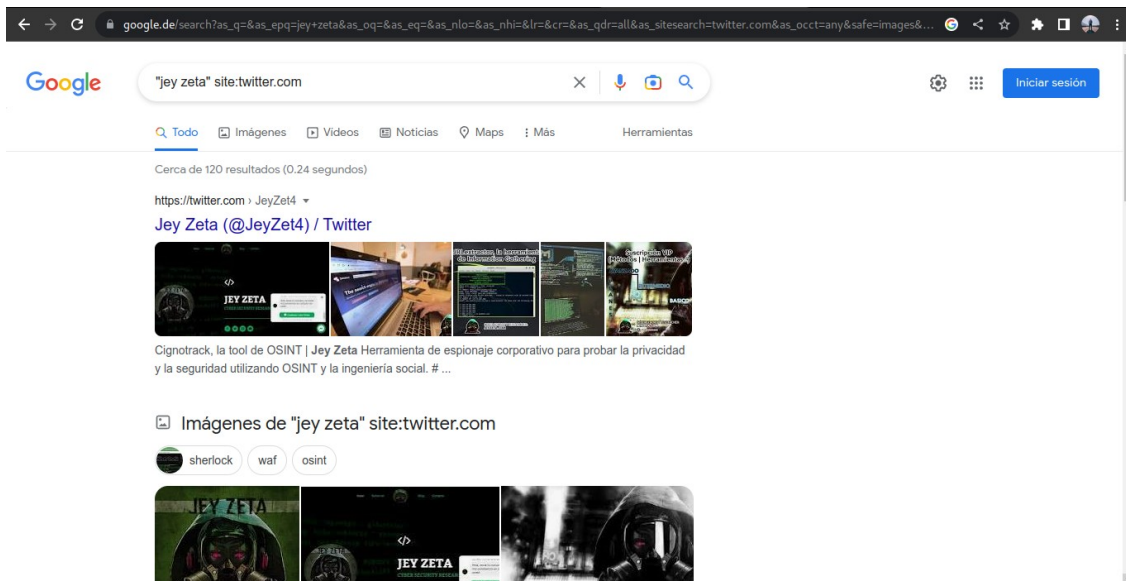
[Búsqueda avanzada](#)

También puedes...

- [Buscar páginas similares a una URL](#)
- [Buscar las páginas visitadas](#)
- [Usar los operadores del cuadro de búsqueda](#)
- [Personalizar la configuración de búsqueda](#)

Perú

Nos muestra como una DORK de Google, que lo veremos un poco más adelante.



Google es muy usado al momento de hacer nuestras búsquedas, será probablemente la herramienta que más usemos diariamente.

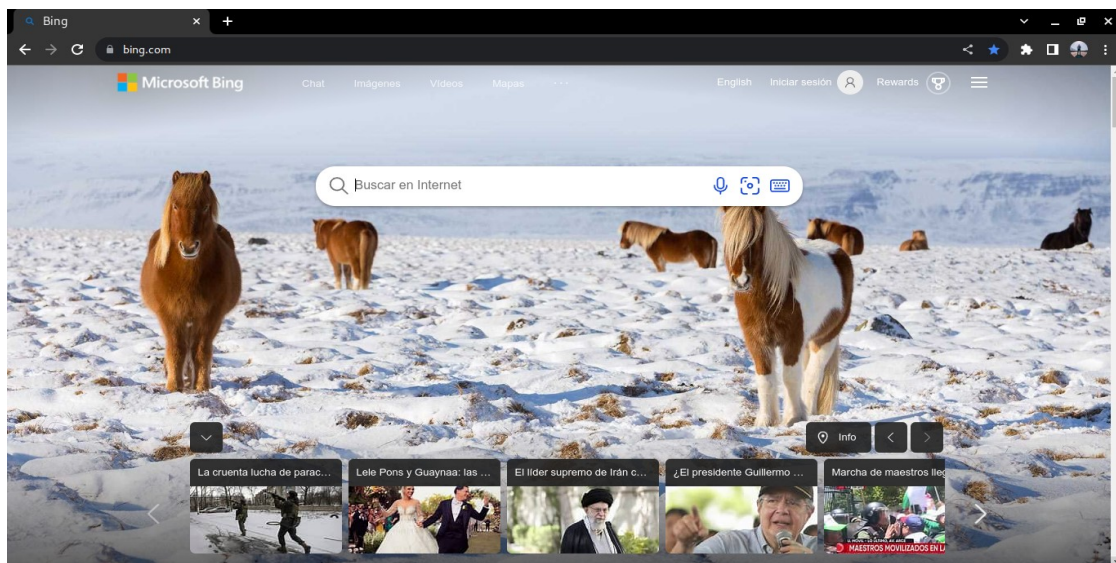
En realidad se puede encontrar mucha información, como también poca, depende los datos que tengas, los rastros que deje la target que estés investigando.

Por otro lado, puedes usar diferentes navegadores, como los siguientes:

Google Chrome, Mozilla Firefox, Safari (macOS), Microsoft Edge, Opera, Brave, Vivaldi, etc.

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

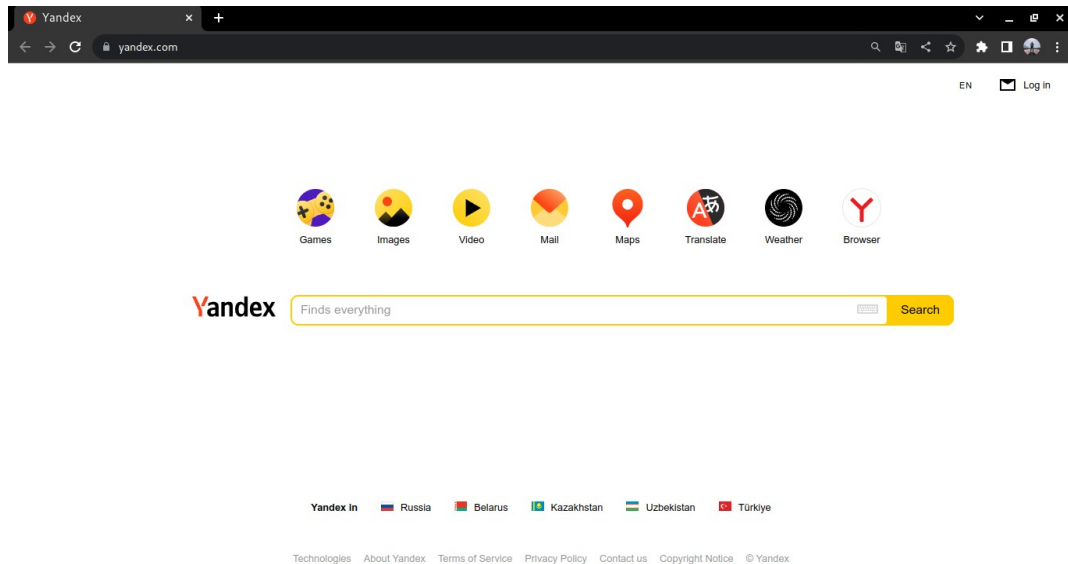
Microsoft Bing: Es un motor de búsqueda web de Microsoft. El servicio tiene su origen en los anteriores motores de búsqueda de Microsoft: MSN Search, Windows Live Search y posteriormente Live Search. Bing proporciona varios servicios de búsqueda, incluidos productos de búsqueda web, de vídeo, de imágenes y de mapas.



<https://yandex.com/>

Yandex: Se trata del buscador más utilizado en Rusia y algunos de los países pertenecientes a la antigua Unión Soviética, al mismo tiempo que también es

una de las páginas más visitadas en este país, con más de 65 millones de visitantes diarios. Yandex ofrece búsqueda en Internet y otros servicios como mapas, navegador, transporte público, taxi, clima, noticias, etc...



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

Baidu: Se traduce literalmente como «cientos de veces» y representa la persistencia en la búsqueda de lo ideal. Se alude habitualmente a Baidu como «el Google chino» debido a su similitud con éste. Incluye la posibilidad de búsqueda de noticias, imágenes y canciones, entre otras funciones.



<https://duckduckgo.com/>

DuckDuckGo: Es un motor de búsqueda que hace hincapié en la protección de la privacidad de los buscadores y en evitar la burbuja de filtros de los resultados de búsqueda personalizados. DuckDuckGo no muestra resultados de búsqueda procedentes de granjas de contenido.



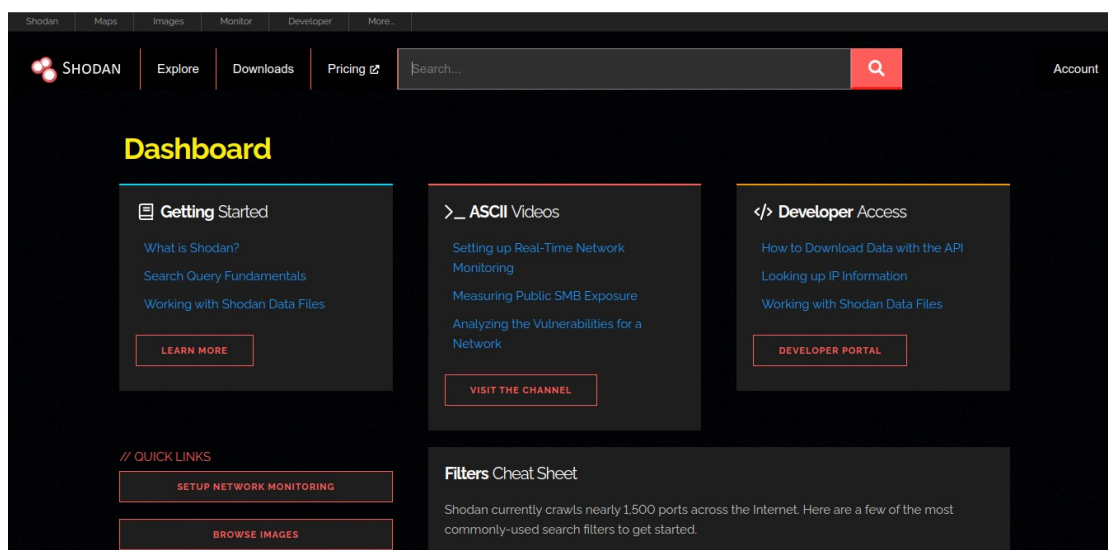
<https://techglimpse.com/duck-duck-go-search-engine-goodies-tricks/>

CheatSheet for DuckDuckGo			
Everyday use		Geeks / Techies	
Calculate no. of days between dates	e.g: days between 01/31/2013 01/31/2014	Calculate freq. of characters in text	e.g: frequency of all characters in sample
Conversions	e.g: 100usd in eur	Expand short URLs	e.g: expand http://bit.ly/a
Calculate time interval	e.g: 1am to 4:30pm	Check status of website	e.g: is techglimpse.com up?
Temperature Conversion	e.g: 6 fahrenheit in celsius	Convert ASCII,hex,numbers	e.g: foo in binary
Food Conversions	e.g: calories in 2 eggs	Data rate conversions	e.g: 6GB/700KB/s in min
Find new coupons	e.g: samsung coupon	Find your IP address	e.g: ip address
Formulas	e.g: volume of a sphere	Find service running on port	e.g: port 23
Find Google+ users	e.g: google+ techglimpse	Identify Browser details	e.g: useragent
Detect Language	e.g: detect language こんにちは	Decode HTML entities	e.g: !
Pronounce Words	e.g: pronounce wow	Count no. of characters	e.g: chars test
Find latest tweets of a user	e.g: @techglimpse		
Get Flight Information	e.g: AA 102		
Find flash version	e.g: flash version		
Cyptography		System Administration	
Generate a random password	e.g: password 15 strong	Convert unix epoch time	e.g: 12343435 time
Generate QR code for website	e.g: qrcode http://techglimpse.com	Display Private n/w info	e.g: private network
Find HASH function Type	e.g: hash 624d420035fc9471f6e16766b7132ddeb34ea62	Display Public DNS info	e.g: public dns
Convert Roman, Arabic Numerals	e.g: roman numeral MCCCXXXVII	IP address Lookup	e.g: 64.207.122.151
Get Plain text or hash of input	e.g: leakdb 21232f297a57a5a743894a0e4a801fc3	Translate Crontab	e.g: crontab 0 0 * * * /bin/sh
MD5 or SHA word	e.g: md5 word, sha word	Find WHOIS Data	e.g: whois duckduckgo.com
Web Design		Regular expressions	e.g: regex /./ ddg
Display ASCII table	e.g: ascii table	Current time in epoch	e.g: epoch
Display Color codes	e.g: color codes	Textual info of unix permission	e.g: chmod 755
Display HTML chars	e.g: html chars		
URL escape codes	e.g: url escape		
Find HEX color combinations	e.g: #368798, color(12,120,15)		
HSL & HEX Information	e.g: hsl 194 0.53 0.79		
Generate HEX codes in RGB	e.g: rgb 173 216 230		
References		Fun & Others	
https://duckduckgo.com/goodies	How to use these tricks	Mirror texts	e.g: mirror techglimpse
http://thenextweb.com	1. Go to http://duckduckgo.com	Fetch recent meme	e.g: xkcd
	2. Type any of the above command in search box	I'm feeling lucky	e.g: add slash front to query
		!Bangs	
		https://duckduckgo.com/bang.html	
DuckDuckGo is a search engine that does not track you and, has more instant answers and less spam/clutter. This is only part of Goodies present in DuckDuckGo.		TECHGLIMPSE	
		@techglimpse	

Buscadores tecnológicos:

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

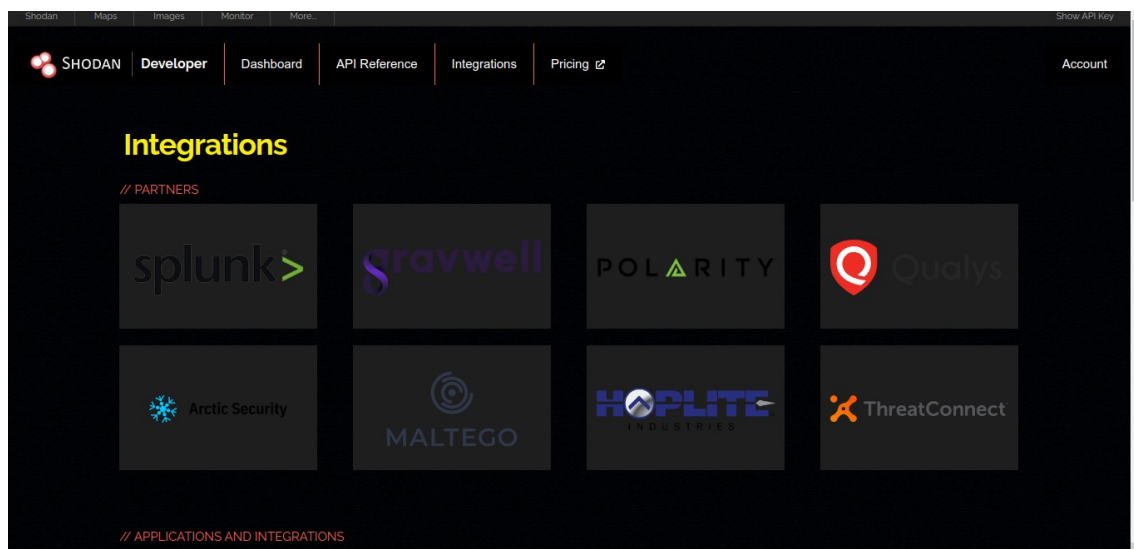
Shodan: Es un motor de búsqueda de dispositivos y servicios y productos que adquieren los servidores funcionan con ciertos comandos para realizar las búsquedas, además que cuenta con un “mapbox” que es un mapa digital para realizar búsquedas vía “map con su geo localización, ciudad y región” puedes realizar búsquedas también a través de su “Word Map” o de por medio de “3D Map Shodan” cada uno cuentan con buenos gráficos para realizar las búsquedas e identificar los servidores o ordenadores y dispositivos conectados afiliados a internet por medio de ciertos “Puertos” y “Productos” famosos modelos de hardware y software.



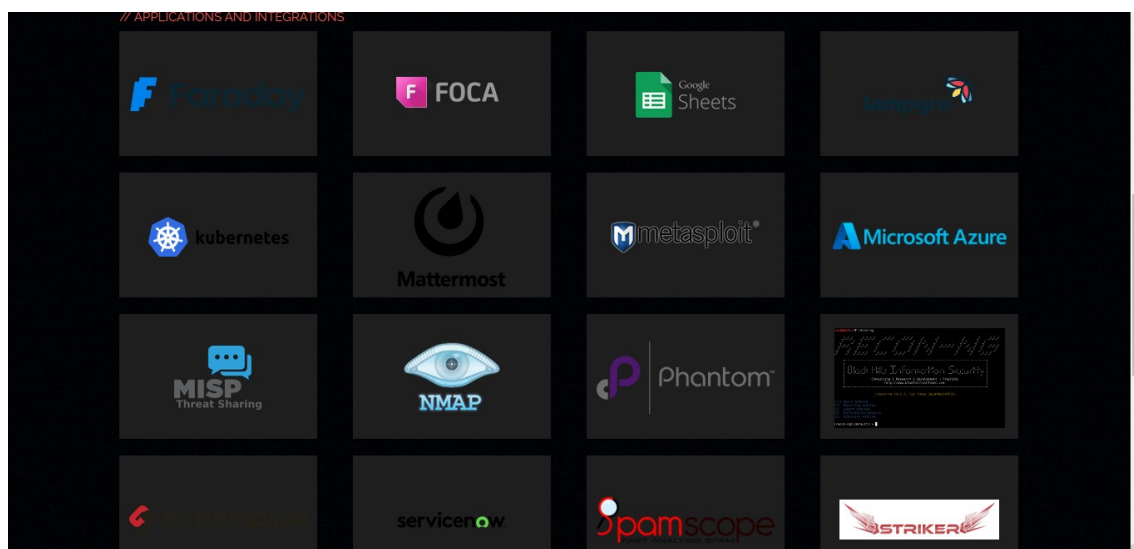
Shodan es sin dudas un motor de búsqueda efectivo a la hora de buscar credenciales, camaras de seguridad, puertos abiertos, etc

Lo bueno de shodan, que se puede integrar con multiples aplicaciones, inclusive uno mismo puede hacer sus propias herramientas.

<https://developer.shodan.io/apps>



Se puede integrar con Maltego, Foca, Nmap, RECON-NG, etc.



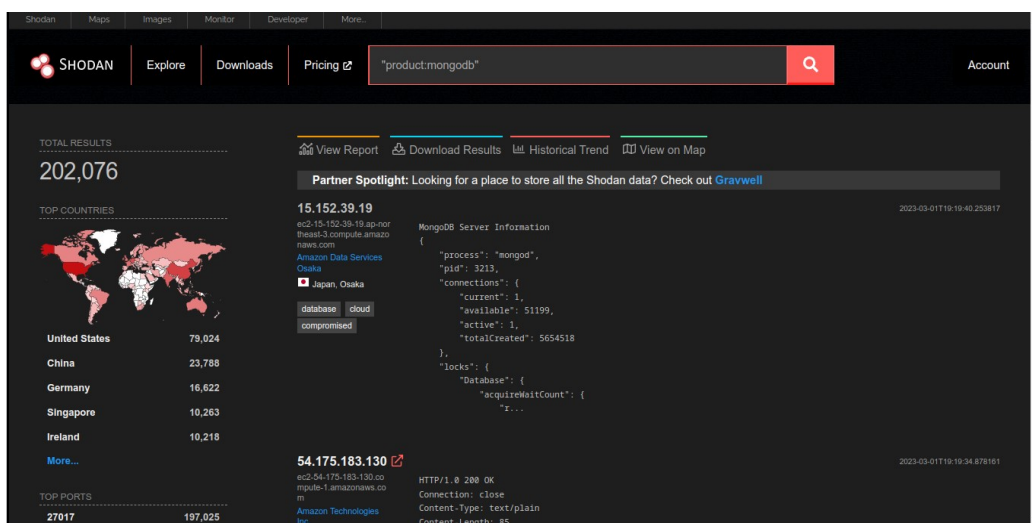
En estos enlaces pueden encontrar comandos de Shodan:

<https://github.com/JavierOlmedo/shodan-filters>

<https://cheatography.com/j-johnson138/cheat-sheets/shodan-io/>

Depende a su búsqueda deberán poner los comandos, cabe resaltar que deben crearse una cuenta en Shodan, hay gratis y premium, en este caso usaré la premium, pero pueden usar la gratis sin problemas.

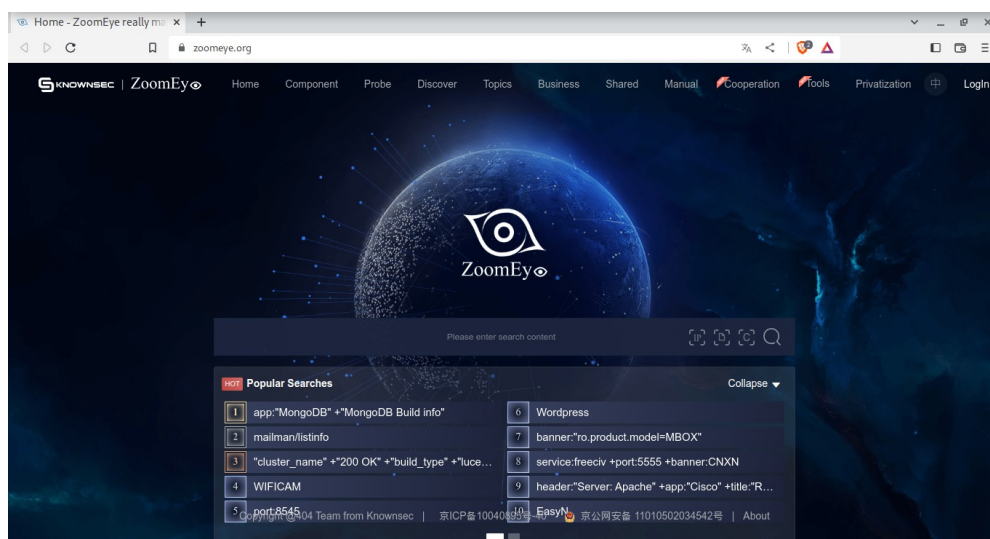
Por ejemplo una búsqueda rápida en Shodan.



Nos muestra ese resultado, también podemos buscar por países o ciudades, dependiendo lo que quieran encontrar, más adelante veremos un poco más de su uso.

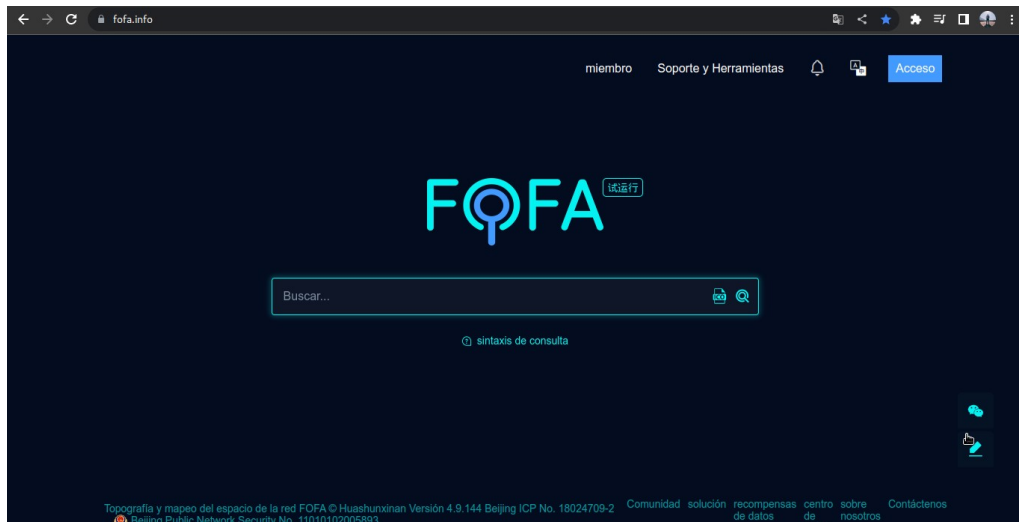
<https://www.zoomeye.org/>

Zoomeye: Es un buscador de origen Chino, es catalogado por ciertos investigadores de seguridad, como la hermana de shodan, tiene ciertas características similares y diferentes a Shodan, para ver camaras web, host, etc.

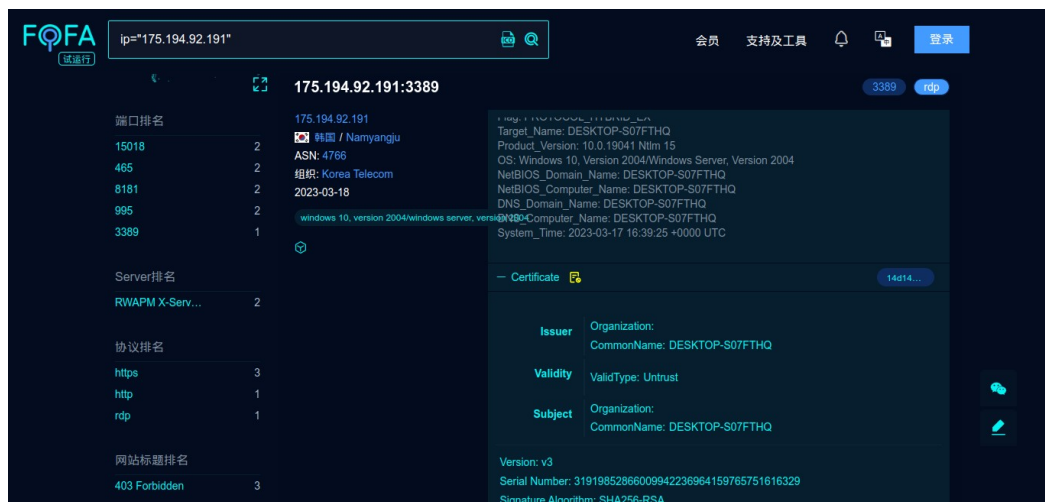


<https://fofa.info/>

FOFA: Indica dónde está alojado el sitio web (país, ciudad), quién es el propietario de la IP y qué otros servicios/puertos están abiertos.



Los usuarios que han usado shodan, se sentirán más cómodos, ya que tiene algo en particular.



Quiero dejar en claro que iré nombrando herramientas, pero no usaré todas, trataré de nombrar las que he usado en casos particulares, ya que depende mucho de tu objetivo, usarás la que más te convenga.

DEEP WEB Y DARK WEB

Abarcaremos sobre la deep web, desde su configuración y búsquedas.

También dejaré notas sobre la Freenet e IP2, ya que es fundamental saber esto.

Por ejemplo los que empiezan en el OSINT, en sus principios buscan información en la Surface Web, la internet que todos conocemos a diario.

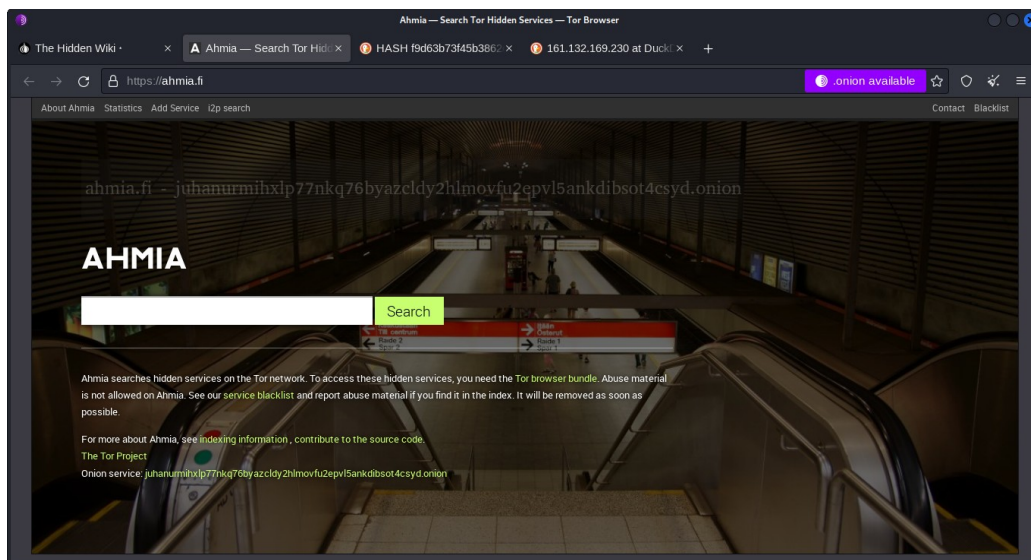
Es necesario, ya que lo más probable que te llegue a tocar varios casos sobre cómo hacer OSINT en la Deep Web o Dark Web, se pueden usar herramientas online, cómo también herramientas desde nuestra terminal. Es indispensable que te adaptes a todos los escenarios.

Ya que si eres un policía o un profesional en OSINT, debes llevar la ventaja al recolectar información, en el peor de los casos, si te llegarán a contratar para ver quién está detrás de una cuenta en la Dark Web, tengas las nociones de dónde empezar.



Ahmia.Fi: Buscador sobre TOR e I2P.

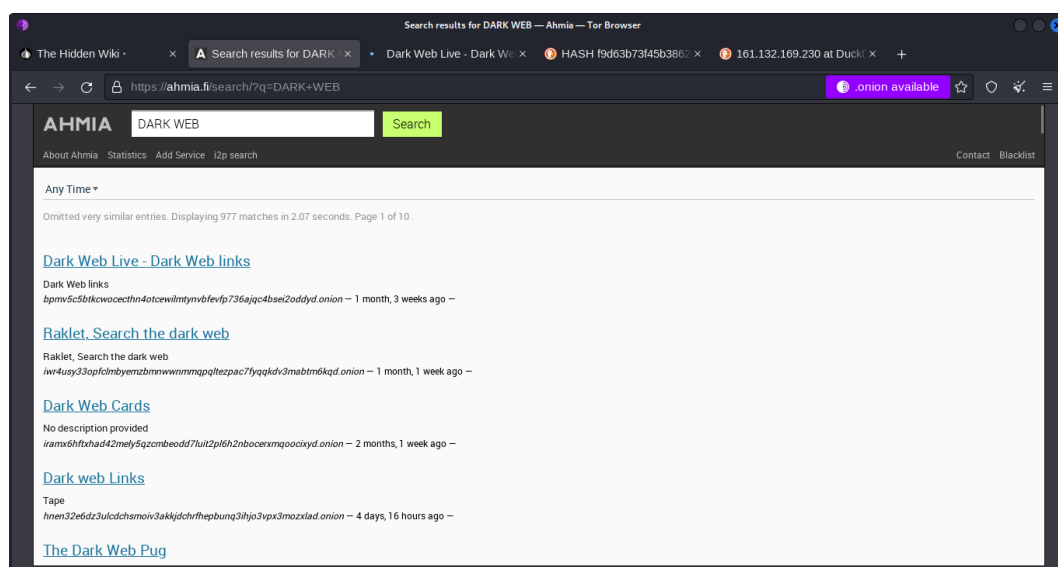
<https://ahmia.fi/>

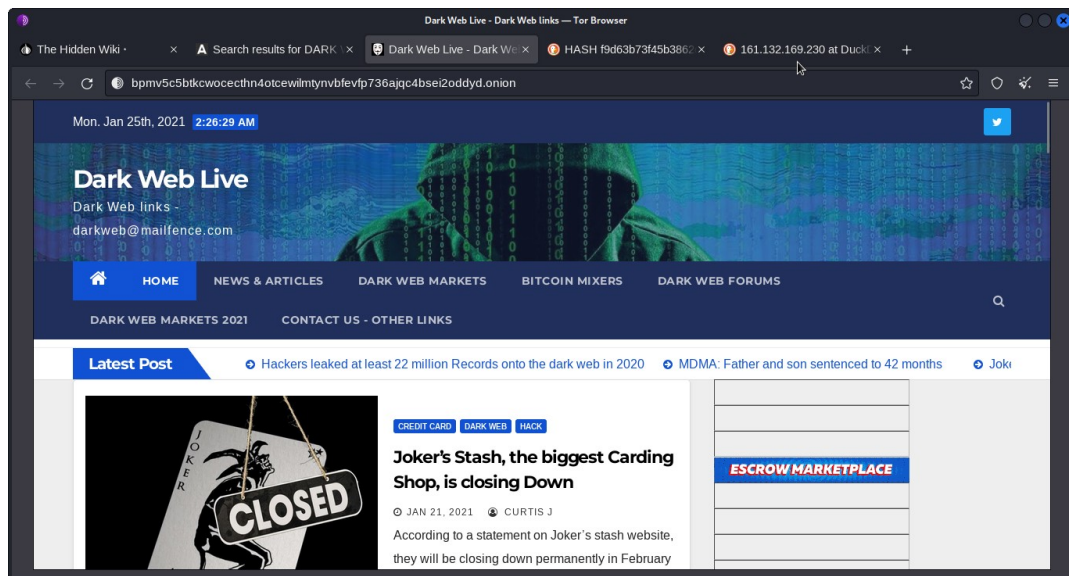


Ahora lo estamos usando desde Tor Browser, que lo veremos un poco más adelante.

En este buscador se puede buscar diferentes palabras.

Por ejemplo: Buscamos “Dark Web” al ver el primer resultado nos muestra una pagina .onion, que viene a ser un post sobre la Dark web.





Nota: Onion Link y TORCH, ya no están disponibles, es necesario que tengan muy en claro que hay servicios online que con el tiempo no estarán disponibles, pero lo bueno es que siempre salen otras para cubrir ciertas búsquedas.

Al usar Tor, pueden usar la configuración por defecto, pero si quieren una personalizada y sentirse más seguros, pueden configurarlo, les dejo el enlace para que se puedan guiar.

Configuración de Tor Browser:

<https://thesafety.us/tor-browser-setup>

<https://tb-manual.torproject.org/running-tor-browser/>

Investigación Dark Web (TorBot):

- <https://github.com/DedSecInside/TorBot>
- <https://haxf4rall.com/2019/06/27/torbot-osint-dark-web/>

También pueden usar Freenet e i2P.

¿Qué es Freenet?

Freenet es un software gratuito que le permite compartir archivos de forma anónima, navegar y publicar "sitios libres" (sitios accesibles sólo a través de Freenet) y chatear en foros sin temor a la censura. Freenet está descentralizado para que sea menos vulnerable a ataques y, si se utiliza en modo "darknet", donde los usuarios se conectan sólo con sus amigos, es muy difícil de detectar.

<https://freenetproject.org/>



- Las comunicaciones de los nodos de Freenet están encriptadas y se enrutan a través de otros nodos para que sea extremadamente difícil determinar quién solicita la información y qué contiene.
- Los usuarios contribuyen a la red proporcionando ancho de banda y una parte de su disco duro (denominada "almacenamiento de datos") para guardar archivos. Los archivos se conservan o eliminan automáticamente en función de su popularidad,

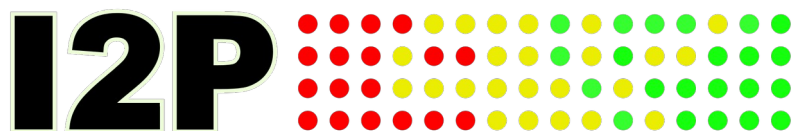
- Los menos populares se descartan para dar paso a contenidos más nuevos o populares. Los archivos están encriptados, así que, por lo general, el usuario no puede averiguar fácilmente lo que hay en su almacenamiento de datos y es de esperar que no se le pueda responsabilizar de ello.
- Ser considerado responsable de ello. Los foros del chat, los sitios web y las funciones de búsqueda se construyen sobre este almacén de datos distribuido.
- Freenet se ha descargado más de 2 millones de veces desde que comenzó el proyecto y se utiliza para la distribución de información censurada en todo el mundo, incluidos países como China y Oriente Medio. Las ideas y conceptos de Freenet han tenido un impacto significativo en el mundo académico.

<https://es.wikipedia.org/wiki/Freenet>

¿Qué es I2P?

El Proyecto Internet Invisible (I2P) es una capa de red privada totalmente encriptada que ha sido desarrollada con privacidad y seguridad por diseño para proporcionar protección de su actividad, ubicación e identidad. El programa incluye un router que te conecta a la red y aplicaciones para compartir comunicarse y construir.

<https://geti2p.net/en/>



- I2P oculta el servidor al usuario y el usuario al servidor. Todo el tráfico I2P es interno a la red I2P. El tráfico dentro de I2P no interactúa directamente con

Internet. Es una capa superior a Internet. Utiliza túneles cifrados unidireccionales entre tú y tus pares. Nadie puede ver de dónde nadie puede ver de dónde viene el tráfico, adónde va o cuál es el contenido. Además, I2P ofrece resistencia al reconocimiento de patrones y al bloqueo por parte de los censores. Como la red se basa en pares para reenviar el tráfico, también se reduce el bloqueo por localización.

<https://es.wikipedia.org/wiki/I2P>

Es muy importante ser cuidadosos al momento de navegar por Tor, para ello dejaré unos post para la configuraciones necesarias, ya que lo primordial es navegar seguros al momento de estar recolectando información.

Es necesario usar de la mejor manera las herramientas que brindo en este libro, ya que hacer OSINT no es un juego, es para hacerlo de la manera más profesional posible.

I2P y Freenet (Configuración):

- <https://geti2p.net/pt-br/about/browser-config>
- <https://freenetproject.org/pages/help.html>

Otros enlaces que pueden servir.

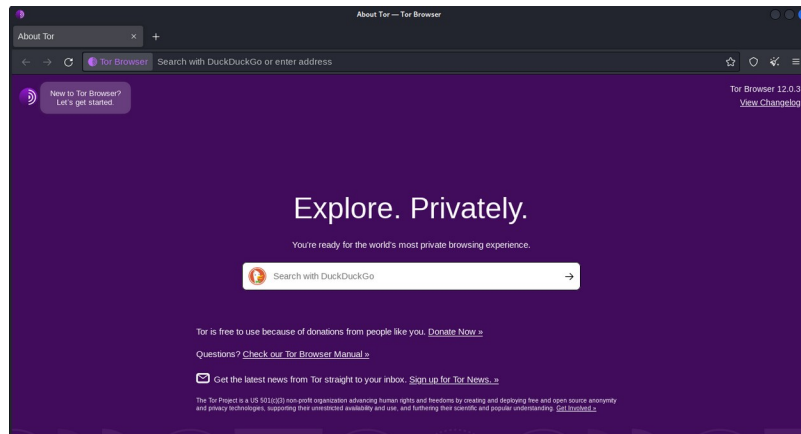
<https://github.com/DedSecInside/TorBot>

<https://github.com/htrgouvea/nipe>

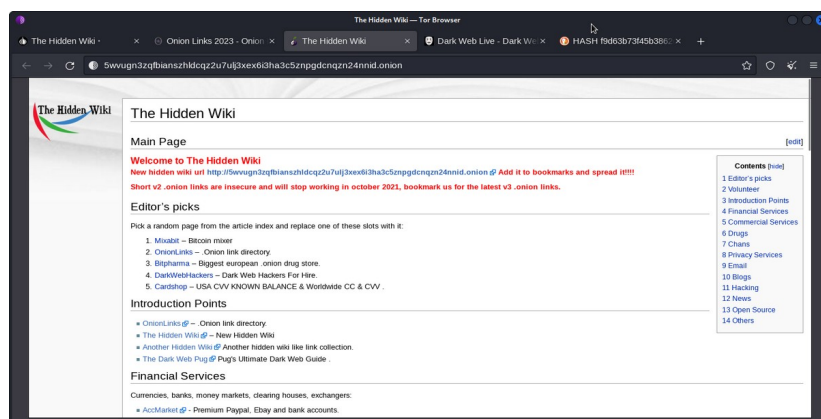
<https://github.com/radio24/TorBox>

<https://www.torbox.ch/>

Lo bueno que al usar Tor browser nos viene por defecto el buscador DuckDuckGo, para mantener mejor nuestra privacidad.

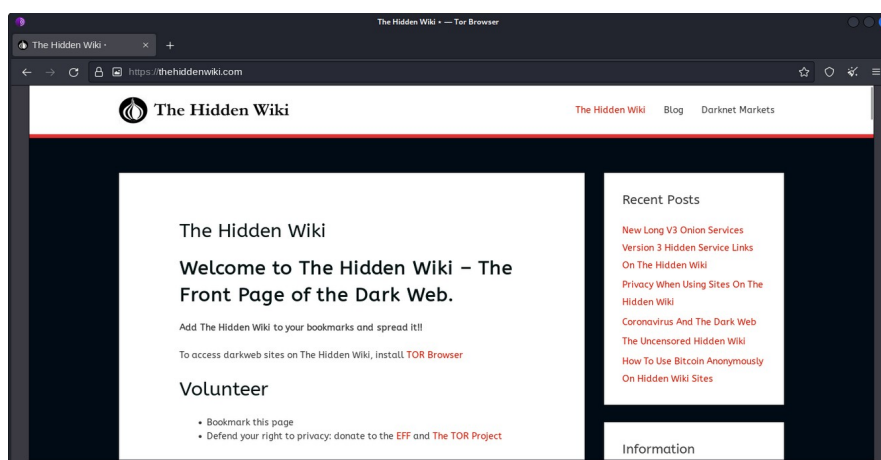


<http://5wvugn3zqfbianszhldcq2u7ulj3xex6i3ha3c5znpqgdcnqzn24nnid.onion/>



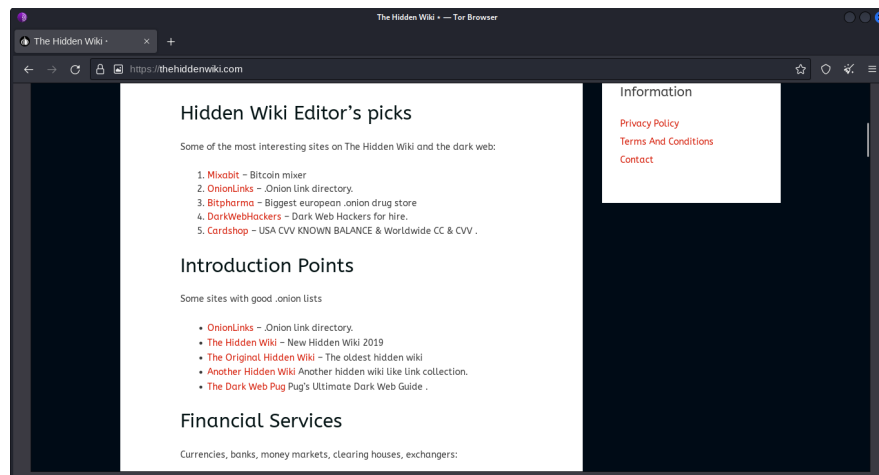
The Hidden Wiki (Normal):

<https://thehiddenwiki.com/>

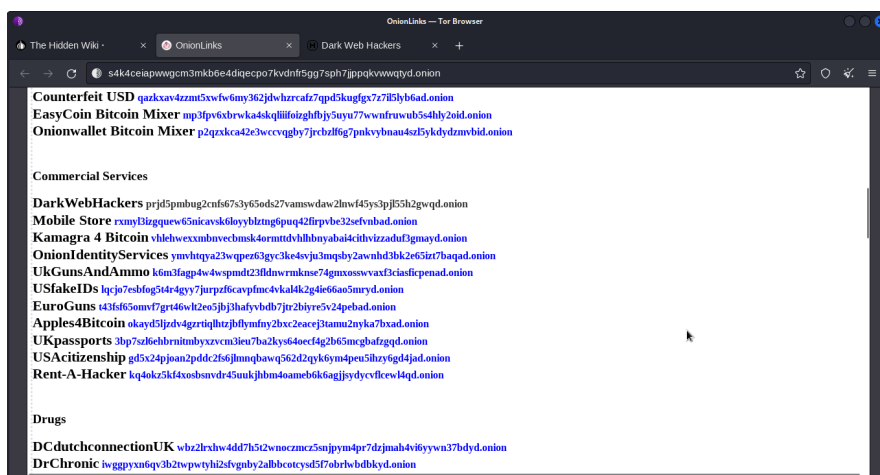


Nos muestra varios enlaces .onion

Están separados por categorías, en este caso solo veremos algunos ejemplos.



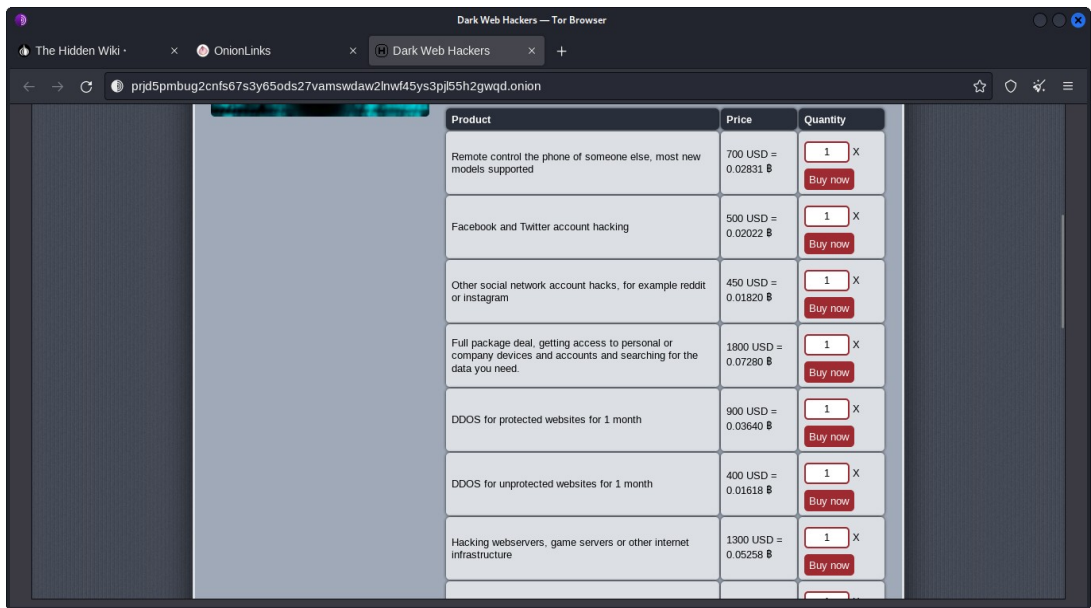
Entramos en el primer enlace que nos muestra una web de BTC.



Vemos cualquier enlace.



Nos muestra un foro dónde hacen trabajos black hat.



En este caso, solo lo muestro para que tengan la idea de lo que pueden llegar a encontrar en estos sitios. Hay una gran ventaja al usar ciertos buscadores, dependiendo sea el caso, por ejemplo si usamos DuckDuckGo, podemos hacer que busque un hash y ver que tipo de HASH es, y también usaremos una herramienta que viene instalada en Kali Linux, para corroborar cierta

información. Es importante usar varias herramientas para ver que resultado nos es más útil y precisa.

Herramientas OSINT de la Dark Web:

- Hunchly - <https://www.hunch.ly/darkweb-osint/>
- Tor66 Fresh Onions - <http://tor66sewebgixwhcqfnp5inzp5x5uohhdy3kvtnyfx2e5mxih34iid.onion/fresh>
- Onionscan - <https://github.com/s-rah/onionscan>
- Onioff - <https://github.com/k4m4/onioff>
- Onion-nmap - <https://github.com/milesrichardson/docker-onion-nmap>
- TorBot - <https://github.com/DedSecInside/TorBot>
- TorCrawl - <https://github.com/MikeMeliz/TorCrawl.py>
- VigilantOnion - <https://github.com/andreyglauzer/VigilantOnion>
- OnionIngestor - <https://github.com/danieleperera/OnionIngestor>

Herramienta DarkScrape:

- <https://github.com/itsmehacker/DarkScrape>
- <https://www.geeksforgeeks.org/darkscrape-osint-tool-for-scraping-dark-websites/>
- Descargar medios
- Scraping desde una Url
- Reconocimiento facial

- Scraping de archivos
- Txt
- Csv
- Excel

Motores de búsqueda en la Dark Web:

- [ahmia](#)
- [Onion Search Engine](#)
- [darksearch](#)
- [Torch](#)
- [Not Evil](#)
- [Candle](#)
- [The Uncensored Hidden Wiki](#)
- [Parazite](#)
- [TorLinks](#)
- [gibiru](#)
- [HayStack](#)
- [TorDex](#)

Si nos dirigimos a Onion Search Engine.

Buscamos “dark web” (<https://onionengine.com/search.php?search=dark+web&submit=Search&rt=>)



Onion Search Engine

"No cookies, no javascript, no trace. We protect your privacy"




* Onion service: [Hidden 1](#), [Hidden 2](#)




☒ Onion Network | ☐ Standard Network | ☐ Images | ☐ Video |

[Adding / Updating a URL](#) | [Mail](#) | [MyDrive](#) | [PGP Suite](#) | [Images](#) | [Video](#) | [Tor2Web](#) | [Short URL](#) | [Helpdesk](#) | [Contact](#)

You searched for **dark web**

2684 results found !

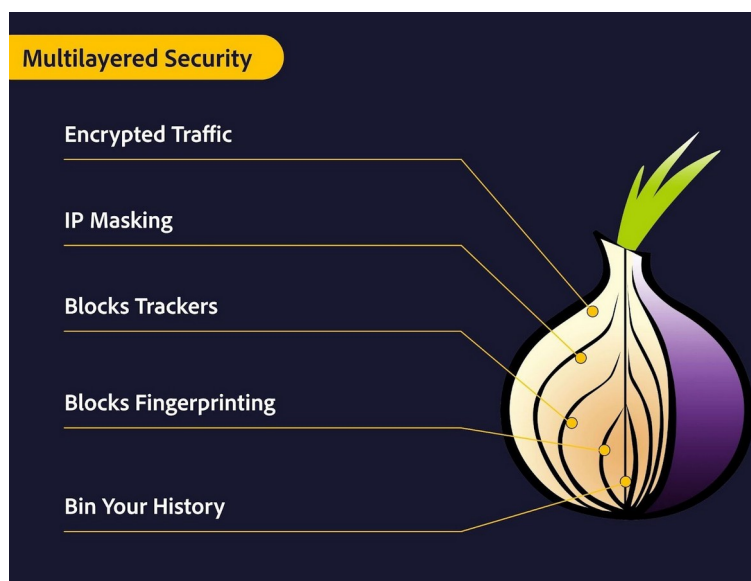
 [SCAMADVISOR | Full base of unreliable sellers in Darknet - Trusted Dark Web Services List - Dark web](#)
<http://l5jcgrava4h2joxfcnyas7qvkqjdzeyvnsqntmwwqpfq7u4rz2iwjzyd.onion/>
SCAMADVISOR | Full base of unreliable sellers in Darknet - Trusted Dark Web Services List - Dark web
scam list - deep web scammer list Full base of unreliable s...
 [Online](#) |  [Report abuse](#) | [Tor2Web](#)

 [SCAMADVISOR | Full base of unreliable sellers in Darknet - Trusted Dark Web Services List - Dark web](#)
<http://fricesdlxrwld7dgmzmzfmsiww43b3cty5fklfb5odmtfpmmbmvpzid.onion/>
SCAMADVISOR | Full base of unreliable sellers in Darknet - Trusted Dark Web Services List - Dark web
scam list - deep web scammer list Full base of unreliable s...
 [Online](#) |  [Report abuse](#) | [Tor2Web](#)

Nos muestra mucha información, solo que para entrar a esos enlaces, debemos hacerlo desde Tor Browser, ya que son .onion

Investigación en la Dark Web: Investigación OSINT en sitios .onion

<https://www.osintme.com/index.php/2019/11/24/darknet-diving-conducting-osint-on-onion-sites/>



Desarrollo de malware e Investigación en la Dark Web:

- <https://www.secjuice.com/osint-daily-dose-of-malware/>
- [IntelMQ](#) - Una herramienta para CERTs para el procesamiento de datos de incidentes usando una fila de mensajes.
- [IOC Editor](#) - Un editor gratuito para archivos XML IOC.
- [ThreatTracker](#) - Un script Python para monitorizar y generar alertas basadas en IOCs indexados por un conjunto de motores de búsqueda personalizados de Google.
- [ioc_writer](#) - Biblioteca Python para trabajar con objetos OpenIOC, de Mandiant.
- [TIQ-test](#) - Visualización de datos y análisis estadístico de feeds de Inteligencia de Amenazas.
- [Massa Octo Spice](#) - Anteriormente conocido como CIF (Marco de Inteligencia Colectiva). Acumula IOCs de varias listas. [Comisariada por la fundación de dispositivos CSIRT](#).
- [AbuseHelper](#) - Estructura de código abierto para recibir y redistribuir feeds de abusos y amenazas Intel.
- [MISP](#) - Plataforma de compartición de información sobre malware gestionada por el proyecto MISP.
- [PassiveTotal](#) - Busca, conecta, marca y comparte IPs y dominios.
- [Combinar](#) - Herramienta para reunir indicadores de Inteligencia de amenazas de fuentes públicamente disponibles.
- [PyIOCe](#) - Un editor Python OpenIOC.
- [ThreatCrowd](#) - Un motor de búsqueda de amenazas, con visualización gráfica.
- [Fileintel](#) - Extrae inteligencia por hash de archivo.

- <https://portswigger.net/daily-swig/fbis-dark-web-investigations-hampered-by-inefficiencies-overlapping-objectives-of-different-units>
- <https://www.pulsarsecurity.com/services/dark-web-assessment>
- [Hostintel](#) - Inteligencia de extracción por host.
- [AbuseHelper](#) - Un framework de código abierto para recibir y redistribuir feeds de amenazas y abusos de Intel.
- [PassiveTotal](#) - Buscar, conectar, etiquetar y compartir IPs y dominios.
- [AlienVault Open Threat Exchange](#) - Comparte y colabora en el desarrollo de Inteligencia de Amenazas.
- [Combine](#) - Herramienta para recopilar indicadores de Inteligencia de Amenazas de fuentes disponibles públicamente.
- [IntelMQ](#) - Una herramienta para CERTs para procesar datos de incidentes usando una cola de mensajes.
- [Pasta Octo Spice](#) - Anteriormente conocido como CIF (Collective Intelligence Framework). Acumula IOCs de múltiples listas. Gestionado por la CSIRT Devices Foundation.
- [MISP](#) - Plataforma de intercambio de información sobre malware comisariada por el proyecto MISP .
- [Threatagggregator](#) - Agrega amenazas a la seguridad de diversas fuentes, incluidas algunas de las enumeradas a continuación en Otros recursos .
- [ThreatCrowd](#) - Motor de búsqueda de amenazas, con visualización gráfica.
- [ThreatTracker](#) - Un script Python para monitorizar y generar alertas basadas en IOC indexados por un conjunto de motores de búsqueda personalizados de Google .

GOOGLE HACKING

En esta sección veremos cómo se puede usar Google para hacer OSINT, ya sea por búsquedas usando Dorks, búsquedas avanzadas.

Google hacking se usa a diario, por ejemplo cuando quieres buscar un curso, tema, tarea, etc. Al comienzo hay búsquedas que están como escondidas y usando dorks y personalizando nuestras búsquedas podemos encontrar desde errores xss, sqli, información personal, bases de datos, contraseñas, usuarios, cursos premium, libros digitales de todo tipo, etc.



Google Dork:

Google Hacking es una técnica en informática que utiliza operadores para filtrar información en el buscador de Google. Además podemos encontrar otras aplicaciones de agujeros de seguridad en la configuración y el código informático que se utilizan en las páginas web.

En términos más simples, un Google Dork es una búsqueda avanzada, la cual admite una serie de parámetros para realizar búsquedas en Google y obtener resultados concretos o información más relevante para el usuario.

https://es.wikipedia.org/wiki/Google_Hacking



Principales Dorks de Google:

`"keyword1 keyword2"`

`keyword1 AND keyword2`

`keyword1 OR keyword2`

`-keyword`

`*keyword`

site:example.com

intitle:keyword

allintitle:keyword1

keyword2

inurl:keyword

allinurl:keyword1 keyword2

info:example.com

intext:keyword

allintext:keyword1

keyword2

related:example.com

ext:pdf

cache:example.com

link:example.com



```
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
NORMAL google_Dorks.txt text utf-8[unix] 21,676 words 0% 1/9863 ln : 1
"google_Dorks.txt" 9863L, 293687C
```

Más dorks:

https://github.com/BullsEye0/google_dork_list

<https://github.com/BullsEye0/dorks-eye>

Google Hacking Database:

<https://www.exploit-db.com/google-hacking-database?category=6>

The screenshot shows the 'Google Hacking Database' page on the Exploit Database website. The page has a dark blue header with the 'EXPLOIT DATABASE' logo. Below the header, there's a search bar and a 'Category' dropdown menu set to 'Vulnerable Servers'. The main content area displays a table of search results. The table has columns for 'Date Added', 'Dork', 'Category', and 'Author'. The results are filtered to show 15 items. The first few rows of the table are as follows:

Date Added	Dork	Category	Author
2022-06-16	intitle:"HFS" AND intext:"httpserver 2.3" AND -intext:"remote"	Vulnerable Servers	Alexander Ahmann
2021-11-15	inurl:adm/login.jsp.bak	Vulnerable Servers	Md Anzaruddin
2021-09-24	intitle:"TileServer GL - Server for vector and raster maps with GL styles"	Vulnerable Servers	Jan-Jaap Korpershoek
2021-09-16	intitle:"index of" "/views/auth/passwords"	Vulnerable Servers	J. Igor Melo
2021-09-08	intitle:"Icecast Streaming Media Server" "Icecast2 Status" .com	Vulnerable Servers	Mugdha Peter Bansode
2021-06-25	inurl:/editor/filemanager/connectors/uploadtest.html	Vulnerable Servers	Alexandros Pappas

Puedes elegir la categoría dependiendo el uso que le quieras dar a las dorks.

<https://pastebin.com/3D1ruRSw>

The screenshot shows a Pastebin post titled 'New Dorks Dorklist 2017 Sql and more'. The post is dated APR 22ND, 2017, and has 807 views. The content of the post is a list of 18 dorks, numbered 1 through 18, which are SQL injection payloads targeting various parts of a website. The dorks are as follows:

1. inurl:index.php?id= site:gov.il
2. inurl:index.php?id= site:gov
3. inurl:news.php?id= site:gov.il
4. inurl:oferta.php?id= site:gov.il
5. inurl:trainers.php?id= site:gov.il
6. inurl:article.php?ID= site:gov.il
7. inurl:play_old.php?id= site:gov.il
8. inurl:declaration_more.php?decl_id= site:gov.il
9. inurl:Pageid= site:gov
10. inurl:pagina.php?left= site:gov.il
11. inurl:layout.php?id=120'= site:gov.il
12. inurl:principal.php?id=123'= site:gov.il
13. inurl:standard.php?base_dir= site:il
14. inurl:home.php?where= site:gov.il
15. inurl:page.php?sivu= site:il
16. inurl:inc*.php?adresa= site:gov
17. inurl:padrao.php?str= site:gov
18. inurl:include.php?mv= site:gov il

Las dork son búsquedas específicas, para encontrar cierta información, pueden encontrar documentos confidenciales, contraseñas, usuarios, correos, bases de datos, paneles de administración, etc.

Es muy importante saber hacer estas búsquedas, ya que les servirán tanto para hacer OSINT, como para hacer una auditoría de seguridad.

Pastebin: (<https://pastebin.com/3D1ruRSw>)

Un pastebin es una aplicación web que permite a sus usuarios subir pequeños textos, generalmente ejemplos de código fuente, para que estén visibles al público en general.



<https://es.wikipedia.org/wiki/Pastebin>

En esta imagen vemos algo general, en realidad los dorks se van actualizando, dependiendo tus necesidades, vas usando la que más se adapte a ti, más adelante veremos un ejemplo de dork personalizada, que un amigo realizó.

	A	B	C	D	E	F
1	FUNCIONALIDAD	GOOGLE DORK	BING DORK	YANDEX DORK	SHODAN DORK	DUCKDUCKGO
2	Búsqueda literal	"osint"	"osint"	"osint"		
3	Búsqueda por dominio	site:example.com	site:example.com	site:example.com	hostname:example.com	site:example.com
4	Búsqueda de una palabra en el título	intitle:"osint"	intitle:"osint"		title:"Web Scada"	
5	Búsqueda de una palabra dentro de una URL	inurl:"osint"	Lo realiza por defecto			
6	Búsqueda por tipos de fichero	ext:pdf	filetype:pdf	mime=docx		ext:pdf
7	Exclusión de una palabra dentro de una búsqueda completa	"aplicación de técnicas osint" -"humint"	-osint		city:"Lima"	
8	Resultados que cumplan al menos un término entre dos términos propuestos (OR)	"osint" OR "humint"	"osint" OR "humint"	"osint" "humint"	port:23 port:1023	"osint" OR "humint"
9	Resultados que cumplan obligatoriamente dos términos (AND)	"osint" AND "humint"	"osint" AND "humint"	osint +humint		"osint" AND "humint"
10	Búsqueda en caché	cache:example.com				
11	Búsqueda que nos proporcione páginas similares	related:example.com				
12	Búsqueda por puerto				port:23,1023	
13	Búsqueda por dirección IP		ip:"93.184.216.34"		net:93.184.216.34	
14	Información del dominio	info:example.com				
15	Límite la búsqueda a una fecha o ámbito de fechas					
16	Realizar un hash MD5 de una palabra					osint md5
17	Búsqueda por comodines	"aplicación de * osint"		"aplicación de * osint"		
18	Búsqueda en texto de sitio web	intext:"osint"	inbody:"osint"			
19	Sitios web que poseen link específico	link:www.example.com	findfromdomain:example.com			
20	Buscar entre rango de números	1..51 mejores tecnicas osint		date:20071215..20080101, date:>20091231		
21	Búsqueda url concreta		url:www.example.com	url:www.example.com		
22	Búsqueda feed RSS		feed:osint			
23	Sitios webs localizados en Ips relativos a un país		loc:es			
24	Dar importancia		prefer			
25	Enlaces a un tipo de fichero concreto		contains:pdf			

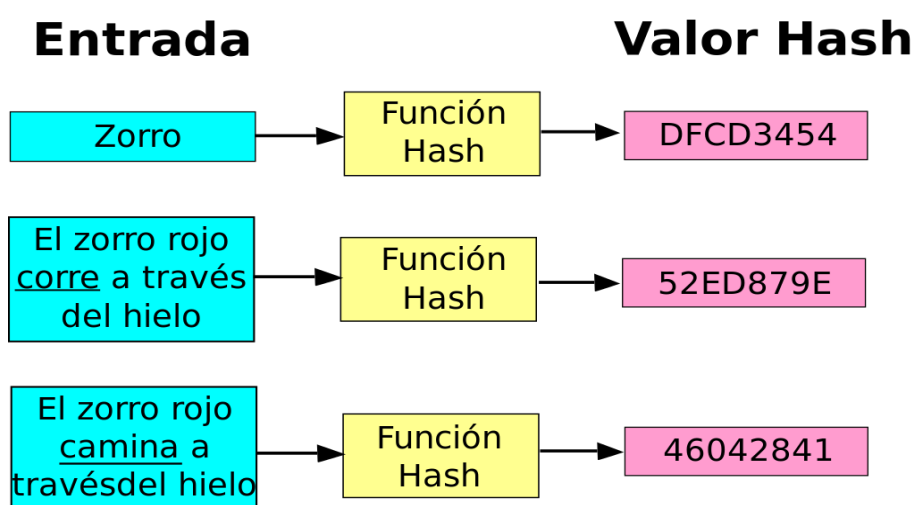
Podemos ver, como una especie de resumen, aunque en realidad es mucho más extendido, ya que diariamente se actualizan las dorks.

Depende en que buscador pones la dork, ya que cada uno tiene lo suyo, y debes saber implementarlo en el mejor de los casos.

26	Búsqueda en delimitador		inanchor:osint			
27	Búsqueda por idioma concreto		"osint" language:es	lang:en		
28	Búsqueda de sitios web en site específico con fuentes RSS o Atom		site:example.com	hasfeed:osint		
29	Búsqueda keyword concreta en metadatos				filename:apache	
30	Búsqueda por ciudad				city:"Madrid"	
31	Búsqueda por país				country:"España"	
32	Búsqueda por categoría				category:ics	
33	Búsqueda por Organización				org:"Verizon Wireless"	
34	Búsqueda por sistema operativo				os:linux	
35	Búsqueda por rango IP				net:93.184.216.0/24	
36	Para buscar por el contenido html de una página web				http.html:"comentario"	
37	Búsqueda subdominios			host:com.example.*		
38	Bang					!g
39	Aparición orden exacto			!aplicación de técnicas losint		
40	Búsqueda host			host:example.com		
41	Realizar un hash SHA256 de una palabra					sha256 osint
42	Búsqueda por fecha			date:200712*		

¿Qué es un Hash?

Una función criptográfica hash usualmente conocida como “hash”, es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.



Es muy importante saber estos términos, ya que cuando hagamos la práctica tendremos la base necesaria, hace mucho tiempo personalmente no me gustaba la teoría, pero con el pasar del tiempo, supe que es necesario saber primero la teoría y luego ya ponerlo en práctica, antes omitía la teoría, y quizás usted también quisiera full práctica, pero es necesario tratar de explicar y dar las fuentes, para que tengan esa base que necesitan.

En estos enlaces puedes encontrar mayor información:

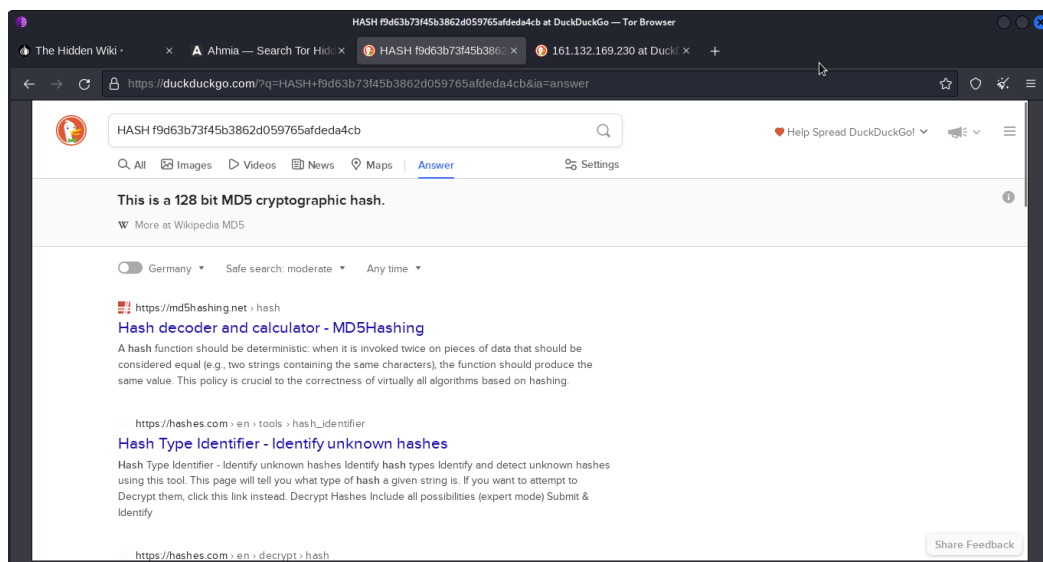
https://es.wikipedia.org/wiki/Funci%C3%B3n_hash

<https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/>

[https://keepcoding.io/blog/que-es-una-funcion-hash/#:~:text=Una%20funci%C3%B3n%20hash%20es%20un,que%20se%20tenga%20la%20clave\).](https://keepcoding.io/blog/que-es-una-funcion-hash/#:~:text=Una%20funci%C3%B3n%20hash%20es%20un,que%20se%20tenga%20la%20clave).)

Por ejemplo, si ponemos en el buscador DuckDuckGo, lo siguiente:

HASH f9d63b73f45b3862d059765afdeda4cb



Vemos que nos muestra en la primera búsqueda, que pertenece a MD5, y en efecto esta con ese tipo de HASH.

HASH-ID:[illegible]

También podemos usar la siguiente herramienta, que es más actualizada y también multiplataforma.

Go-Hash:

<https://github.com/HunxByts/Go-Hash>



```
jeyzeta@JeyZeta: ~/Go-Hash
Archivo Acciones Editar Vista Ayuda

(jeyzeta@JeyZeta)-[~/Go-Hash]
$ python3 gohash.py

  GO-HASH
  <----- CODE BY HUNX ----->
  < Hash identified >

[+] Enter Your Hash : f9d63b73f45b3862d059765afdeda4cb
===== Show Algorithm Hash =====

[+] Hash : f9d63b73f45b3862d059765afdeda4cb
[+] Algorithm : MD5

Do you want to identify the hash again? Y/N : █
```

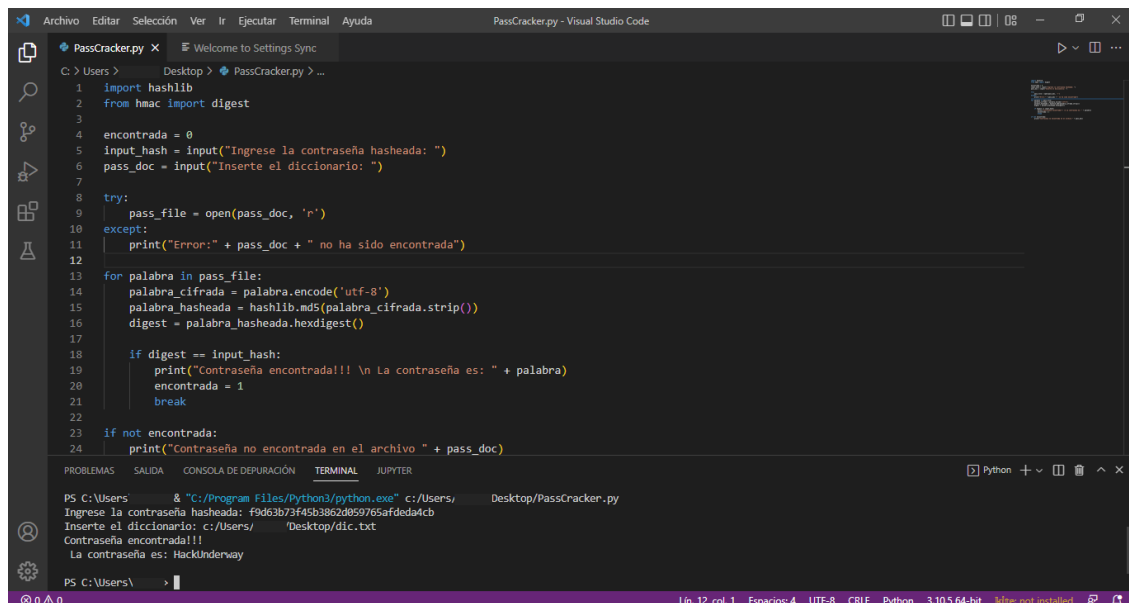
Inclusive pueden usar esta herramienta para crackear contraseñas con HASH.

<https://github.com/HackUnderway/PassCracker>

Crackeador de contraseñas (HASH) SHA-224, SHA-256, SHA-384, SHA-512 además de versiones optimizadas de plataforma de MD5 y SHA1. Usando HASHLIB en Python.

En mi pagina web tengo un post al respecto.

<https://hackunderway.com/pass-cracker/>



```
PassCracker.py
1 import hashlib
2 from hmac import digest
3
4 encontrada = 0
5 input_hash = input("Ingrese la contraseña hasheada: ")
6 pass_doc = input("Inserte el diccionario: ")
7
8 try:
9     pass_file = open(pass_doc, 'r')
10 except:
11     print("Error:" + pass_doc + " no ha sido encontrada")
12
13 for palabra in pass_file:
14     palabra_cifrada = palabra.encode('utf-8')
15     palabra_hasheada = hashlib.md5(palabra_cifrada.strip())
16     digest = palabra_hasheada.hexdigest()
17
18     if digest == input_hash:
19         print("Contraseña encontrada!!! \n La contraseña es: " + palabra)
20         encontrada = 1
21         break
22
23 if not encontrada:
24     print("Contraseña no encontrada en el archivo " + pass_doc)
```

PROBLEMAS SALIDA CONSOLA DE DEPURACIÓN TERMINAL JUPYTER

PS C:\Users\ & "C:/Program Files/Python3/python.exe" c:/Users/ Desktop/PassCracker.py
Ingrese la contraseña hasheada: f9d63b73f45b3862d059765afdeda4cb
Inserte el diccionario: c:/Users/ Desktop/dic.txt
Contraseña encontrada!!!
La contraseña es: HackUnderway

PS C:\Users\ >

Lo que haces es decifrar el HASH usando un diccionario, dependerá mucho de lo complejo que sea el HASH y lo efectivo que sea el diccionario.

Para cifrar y decifrar texto con hash, pueden usar estas paginas.

<https://www.md5hashgenerator.com/>

<https://www.md5online.org/md5-encrypt.html>

<https://www.base64encode.org/>

Hay muchos tipos de cifrado, pero por lo general te vas a topar con MD5.

Hash y cifrado RSA:

<https://blog.signaturit.com/es/que-es-un-hash>

<https://hackingenvivo.blogspot.com/2017/11/cifrado-rsa.html>

OSINT A IMÁGENES / ARCHIVOS / VÍDEOS

En este punto se verán temas para encontrar metadatos de imágenes.

También se verá sobre encontrar la fuente de las imágenes, usando diferentes herramientas en terminal y online.

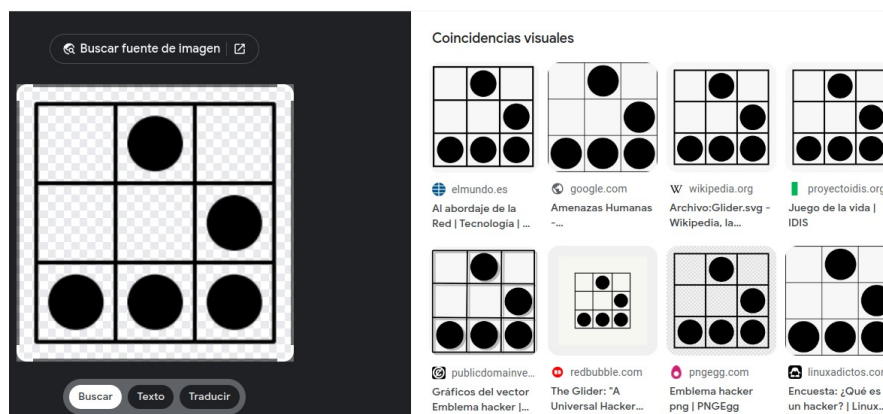


Búsqueda inversa de imágenes:

- [Google reverse search](#)
- [Karmadecay](#)
- [TinEye](#)
- [Yandex reverse image search](#)
- [Bing visual search](#)
- [REVERSE IMAGE SEARCH](#)
- [Cam finds App](#): Se trata de una aplicación disponible para dispositivos Android y Apple. Utiliza tecnología de búsqueda visual para reconocer la imagen subida y ofrecer resultados instantáneos sobre ella, como imágenes relacionadas, resultados de compras locales y una amplia selección de resultados web.
- [Image Identification Project](#)
- [Picsearch](#)
- [Yahoo search engine](#)

Búsqueda con google imágenes:

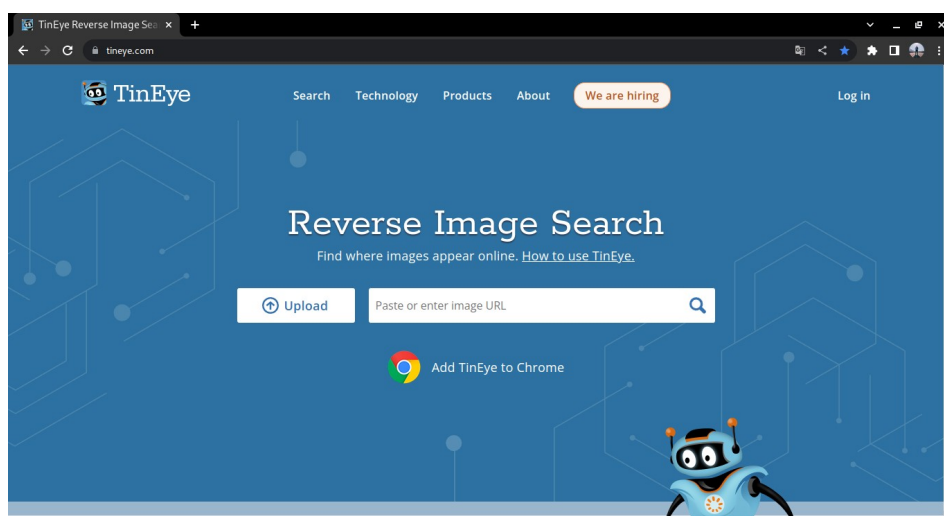
<https://www.google.com/imghp>



Búsqueda con TinEye:

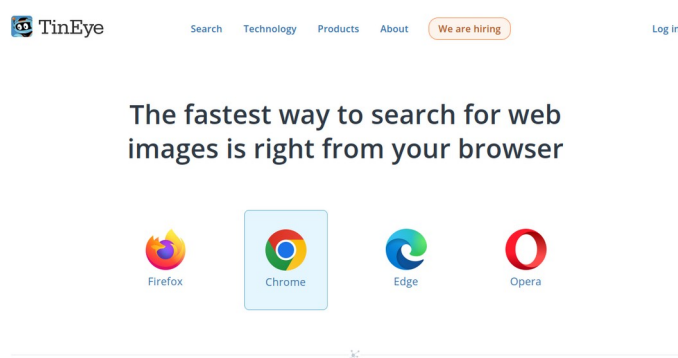
<https://tineye.com/>

TinEye: Es un motor de búsqueda de imágenes inversas desarrollado y ofrecido por Idée, Inc., una empresa con sede en Toronto, Ontario, Canadá. Es el primer motor de búsqueda de imágenes en la web que utiliza tecnología de identificación de imágenes en lugar de palabras clave, metadatos o marcas de agua.

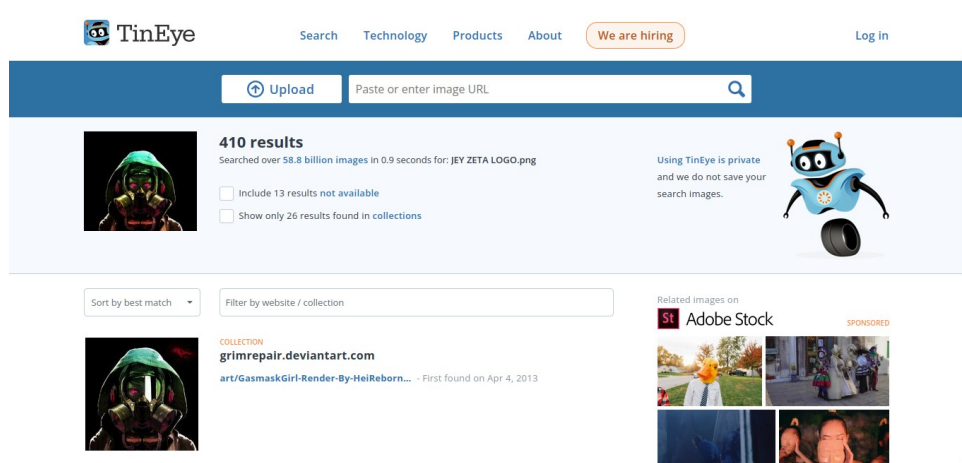


<https://tineye.com/extensions>

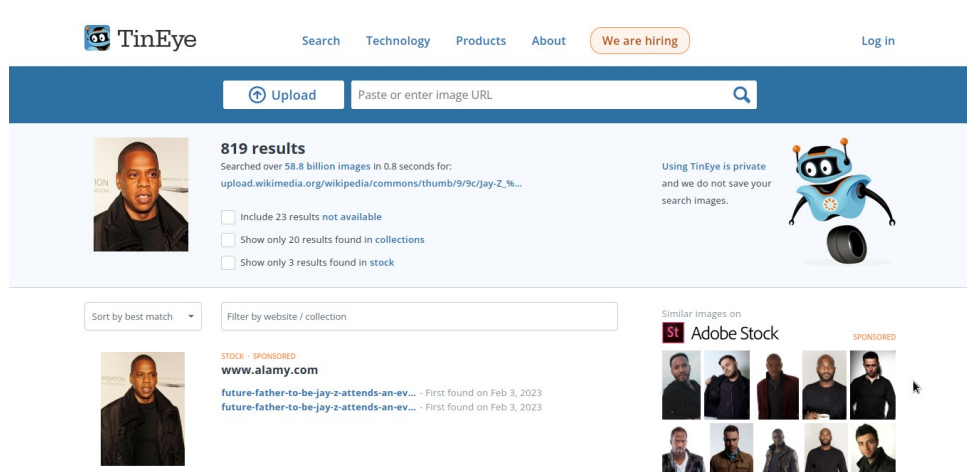
También se puede añadir las extensiones para los siguientes navegadores.



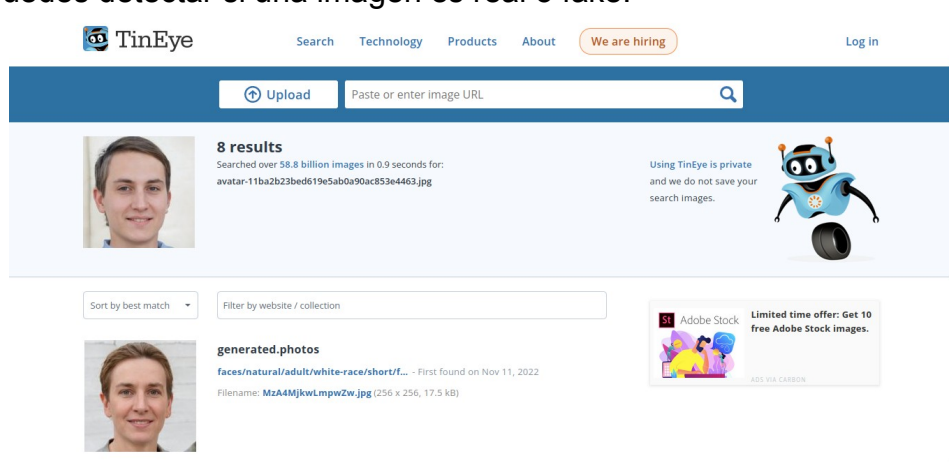
A continuación vemos la búsqueda de una imagen que está desde nuestra computadora, previamente descargada.



También se puede buscar desde un enlace



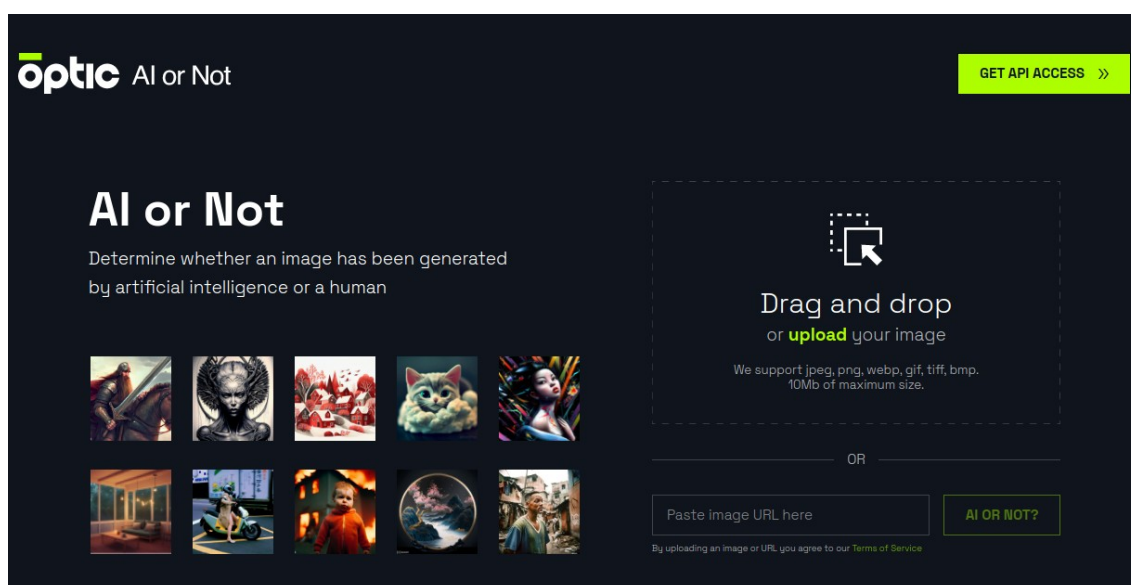
Por ejemplo he buscado esta imagen que ha sido creada (generada) con inteligencia artificial (IA), como lo vimos a un principio, pero ya sabes que con esto puedes detectar si una imagen es real o fake.



Búsqueda por AI or Not:

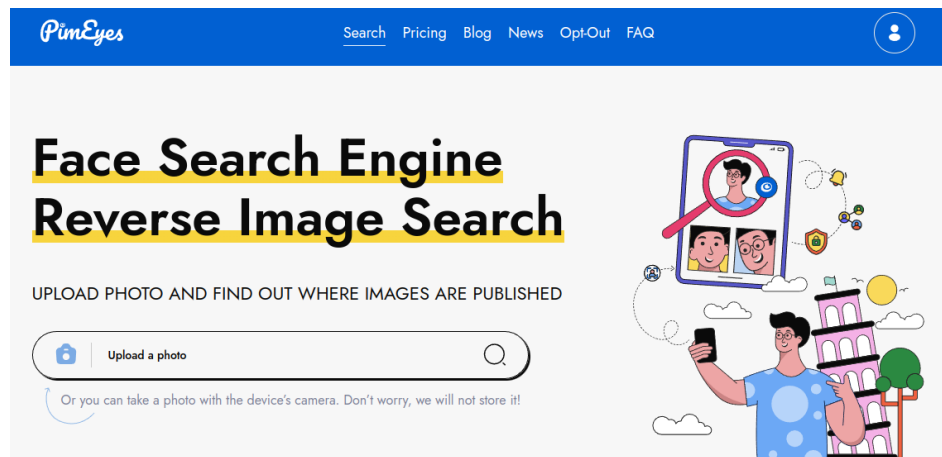
<https://aiornot.optic.xyz/>

AI or Not es una herramienta online para determinar si una imagen ha sido generada por inteligencia artificial o por un ser humano. Lo usamos al momento de hacer OSINT a imágenes, también es usado por forenses, para determinar si una imagen es real o fake. Puede subir la imagen desde su dispositivo o desde una url.

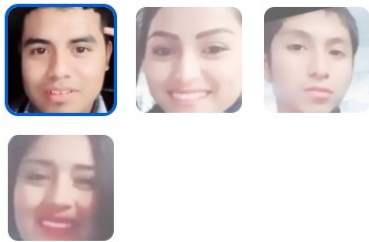


Búsqueda con PimEyes:

<https://pimeyes.com/en>



Choose your face



Select photo(s) of your face to proceed with the search

Proceed to the Face Search

Face search



Add more photos for better results

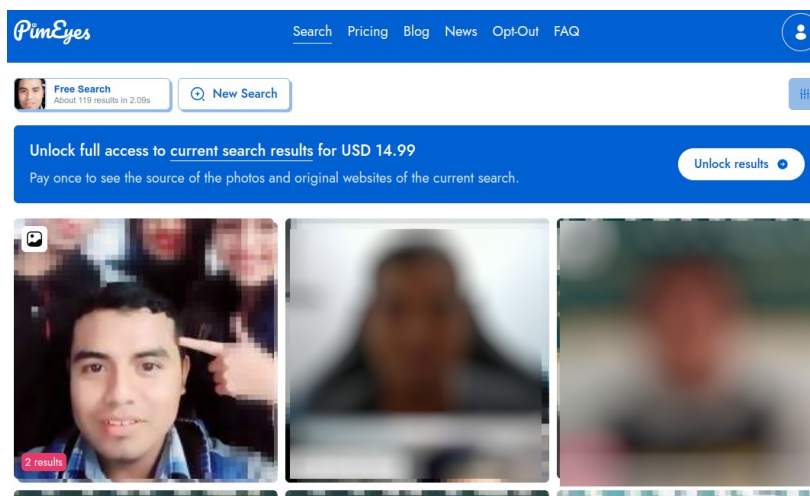
Choose Search Time: Any Time

Safe Search Deep Search

Start Search

Free searches available: 1/1

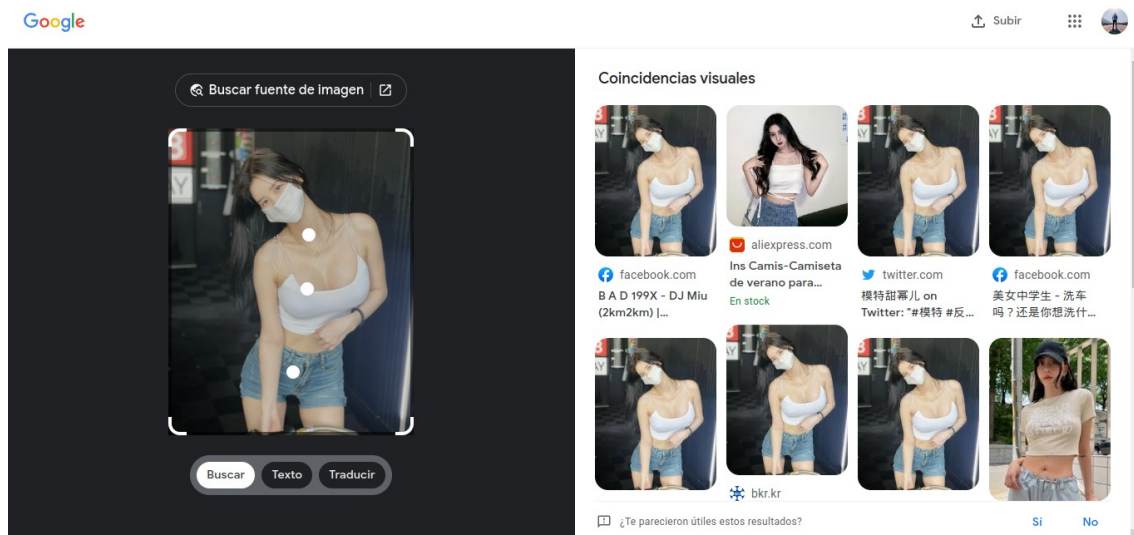
Nos muestra los resultados de la imagen seleccionada.



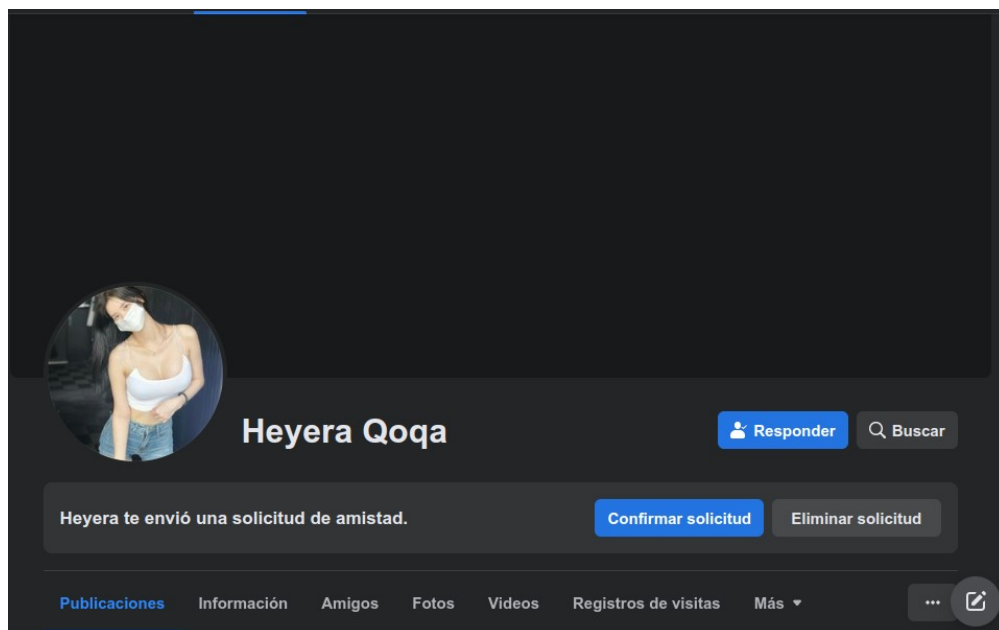
Si hacemos una búsqueda con Google Imágenes.

<https://www.google.com.pe/imghp?hl=es-419&tab=ir&ogbl>

Me muestra el siguiente resultado.



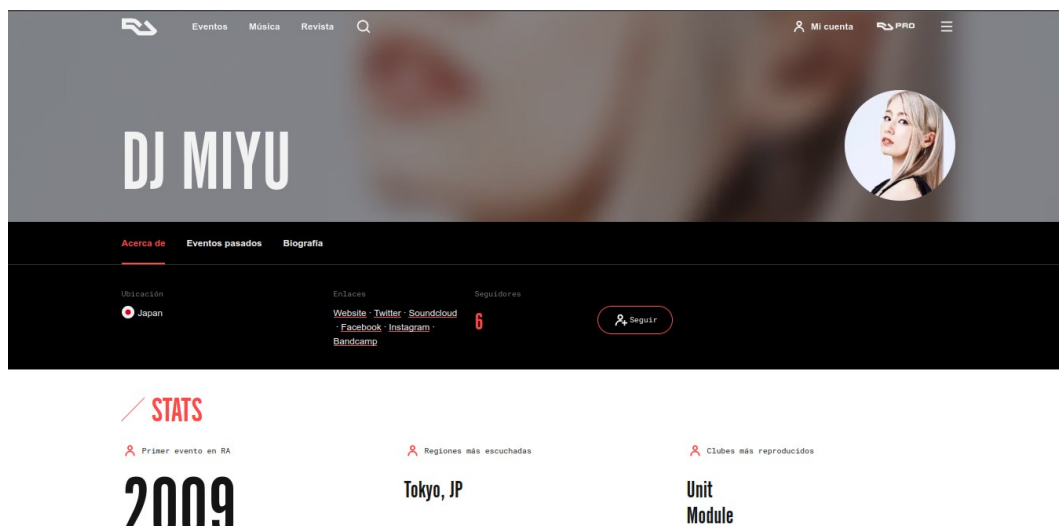
Quizas se pregunten, porqué busqué esa imagen?, es simple, hace un tiempo me enviaron una solicitud de amistad, desde un perfil fake, pero como foto de perfil incluía esa imagen.





Nos arrojó varios resultados, elegí solo uno para no entrar en detalles, ya que veremos otro caso.

<https://ra.co/dj/djmiyu>



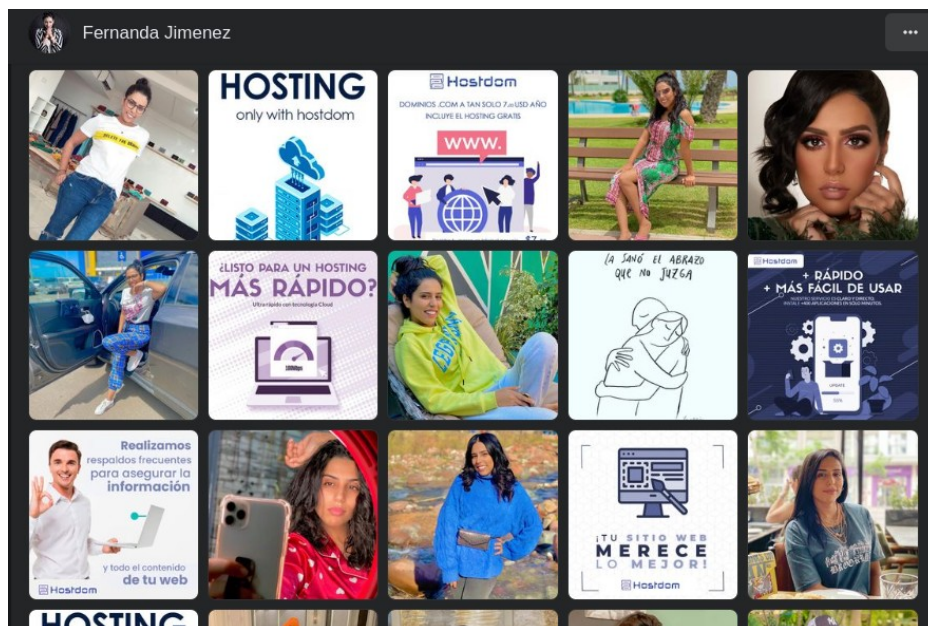
En esa parte están sus redes sociales y pude corroborar que ese usuario estaba suplantando la identidad de esa persona.

Ahora veremos un caso más detallado.

Hace casi 3 años aproximadamente, un usuario de fb, me envió una solicitud de amistad.



Como ven, acepté su solicitud, la verdad que no la conocía, pero bueno quise saber si era fake o real.



Empece a ver sus fotos, parecían muy naturales, así que hice la búsqueda por google imágenes.

Me arrojó esos resultados. Continué con mi búsqueda...

Google

Imágenes

Cerca de 5 resultados (0.36 segundos)

Tamaño de la imagen:
1000 × 837

Buscar esta imagen en otros tamaños:
[Todos los tamaños](#) - [Mediano](#)

Sugerencia: Ingresa una palabra descriptiva en el cuadro de búsqueda.

Páginas con imágenes que coinciden con la búsqueda

aldar.ma
<https://aldar.ma> · Traducir esta página

بالفيديو..رجاء بلميز توجه رسالة إلى جميع الفتيات
الدار/ شيماء أيت عمرات وجهت القناة المغربية رسالتها إلى جمع — 860 × 720 · 16 dic 2019
الفتيات بخصوص موضوع الظهور في مواقع التواصل الإجتماعي بدون ميكاب.

le360.ma
<https://ar.le360.ma/people> · Traducir esta página

رجاء بلميز تدخل المستشفى بسبب أزمة صحية مفاجئة - Le360
1318 × 741 · 16 sept 2019 — انتشرت عبر مواقع التواصل الاجتماعي صورة لرجاء وهي طريحة —
الفراس في المستشفى، الأمر الذي أثار قلق جمهورها. ولكن سرعان ما قامت بلميز بنشر ...

aldar.ma/108101.html

الرئيسية أخبار الدار المواطن ملتيميديا مال وأعمال الرياضة حوادث فن وثقافة صحة الميزيد البرامج ALDAR Français

الرئيسية / فن وثقافة / بالفيديو..رجاء بلميز توجه رسالة إلى جميع الفتيات

بالفيديو..رجاء بلميز توجه رسالة إلى جميع الفتيات

16 ديسمبر، 2019

المعبر الحدودي
الكراتيات

الدار في نظر مواطنيها ومواطنيها من الكركرات
الله الوطن الملك

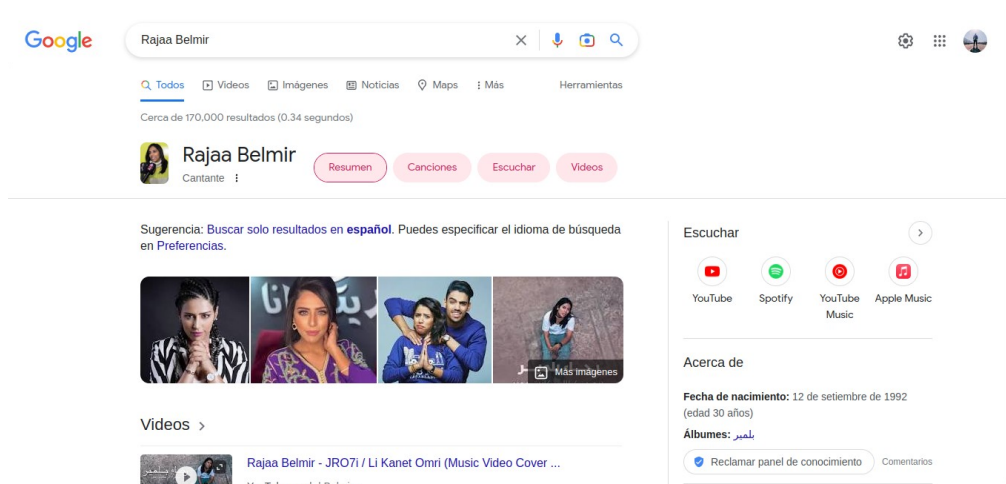
حوادث

أمن مدينة القنيطرة
يوقف مشتببه به في
قراصنة شبكات الاتصالات
الوطنية

26 فبراير، 2023

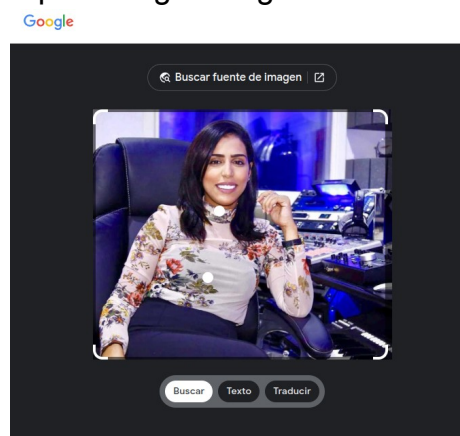


Usé el traductor, ya que está en otro idioma que desconozco.

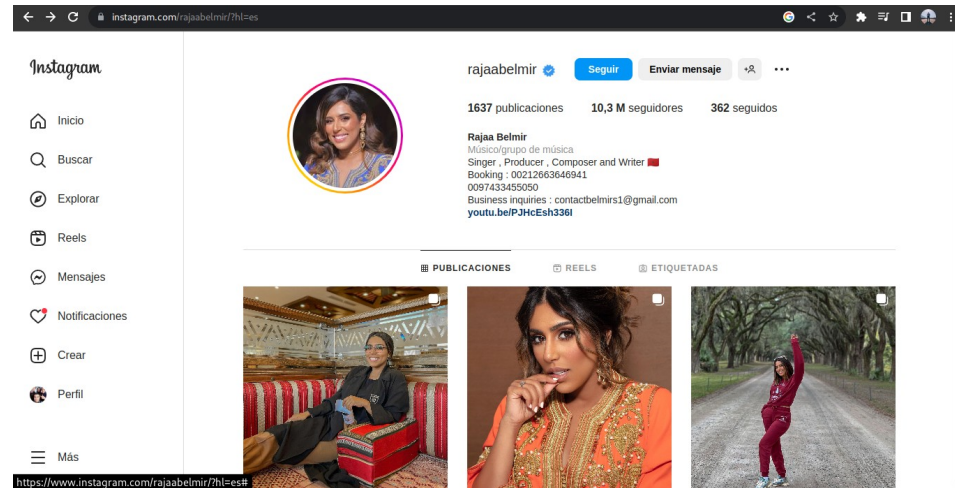


Hice la búsqueda del nombre por Google y me mostró muchos resultados.

También hice la búsqueda por Google imágenes...



Encontre su cuenta de instagram, es una figura pública y cantante, por su emoji de bandera, es de Marruecos.



Hay personas que no saben en absoluto buscar este tipo de información, para corroborar que un perfil es real o fake, ya que muchas veces los cibercriminales crean identidades lo más reales y confiables posibles, para enviar enlaces con phishing, y así poder hacer estafas o robar información confidencial, muchas veces son usados como bot o un perfil espía que propaga malware por redes sociales.

Porque digo esto, estube observando de lejos a este perfil en diversos grupos de WordPress en facebook, y me di con la sorpresa que estaba dando plugins premium, pero de forma gratis, en pocas palabras plugins Nulled (crackeados), que con el tiempo por instalar esos plugins, miles de paginas son infectadas mundialmente. Pero eso ya lo veremos en otro tema.

Lo que quiero decir es que no confien en nadie en redes sociales, ya se ha visto casos que detrás de una pantalla con el perfil creado de una persona, pueden aprovecharse de diferentes maneras. Inclusive puedes estar pensando que estás chateando con una chica hermosa, cuando en realidad es un señor de edad.



Porque digo esto...

He visto muchos casos de perfiles falsos, unos dejan más rastros que otros, pero desde que navegamos en internet se deja al menos la más mínima huella y un descuido puede ser fatal, para alguien que es anónimo, estuve por mucho tiempo en grupos (comunidades) de telegram, gente realmente anónima, que

nadie sabía quién estaba detrás de ese usuario (nick), he sido testigo de cómo a veces por envidia o problemas que se tenían algunos, fueron doxeados, muchas veces de la persona que menos te imaginas, eres traicionado y es por eso que corren el peligro que tu identidad sea descubierta.

Hasta a veces suelen fabricar pruebas falsas, y te acusan con las autoridades, por manchar la reputación, es necesario que tomes cuidado, ya que no solamente tu poder ser expuesto, sino toda tu familia.

Por ejemplo estando por instagram he visto personas que publican su pasaje de avión, su ubicación, incluso su pasaporte y permiso de conducir, entre otros datos personales.

Por ello es importante tomar conciencia de lo que se comparte en redes sociales.



Visualización de datos EXIF:

De forma online:

<https://jimpl.com/>

Esta web, extrae y elimina los metadatos de una imagen o mediante una url.

Visor de datos EXIF en línea

Descubre metadatos ocultos de sus fotos. Encuentra cuándo y dónde se tomó la foto. **Elimine los datos EXIF** de la imagen para proteger su información personal.

★★★★☆ 4.2
Basado en 23016 votos
Para dejar un voto, sube una imagen



Arrastre y suelte una imagen aquí o haga clic para cargar






Hasta 50 MB. Tus cargas son privadas.
Eliminaremos todos los archivos después de 24 horas.

o cargar desde URL

Ejemplo: <https://jimpl.com/og-image.png>



¿Qué son los datos EXIF?

 Información de la cámara	 Propiedades de la imagen	 datos GPS
<ul style="list-style-type: none">◦ Marca y modelo◦ Lente◦ Longitud focal◦ Abertura◦ Exposición◦ Velocidad ISO◦ Destello◦ Número de disparos	<ul style="list-style-type: none">◦ Nombre del archivo◦ Tamaño del archivo◦ Tipo de Mimica◦ Tamaño de la imagen◦ Espacio de color <div> Otros datos</div> <ul style="list-style-type: none">◦ Fecha y hora◦ Miniaturas◦ software de procesamiento◦ ...y muchos más	<ul style="list-style-type: none">◦ Latitud◦ Longitud◦ Altitud◦ dirección y velocidad
<div> información de derechos de autor</div>		

Al agregar la imagen puedes ver toda la Metadata.

📁 UPLOAD ANOTHER IMAGE



Metadata takes **3.11 KB (3.3%)** of this image and may include sensitive info. To protect your privacy, download this image without metadata by clicking the button below.

📁 REMOVE METADATA

📁 Image metadata

Name	google.jpg
File size	95 KB (97300 bytes)
File type	JPEG
MIME type	image/jpeg
Image size	800 x 461 (0.369 megapixels)

PrimaryPlatform	Microsoft Corporation
ProfileCMMType	Linotronic
ProfileClass	Display Device Profile
ProfileConnectionSpace	XYZ
ProfileCopyright	Copyright (c) 1998 Hewlett-Packard Company
ProfileCreator	Hewlett-Packard
ProfileDateTime	1998-02-09 06:49:00 +0000
ProfileDescription	sRGB IEC61966-2.1
ProfileFileSignature	acsp
ProfileID	0
ProfileVersion	2.1.0

FotoForensics:

<https://fotoforensics.com/>

FotoForensics proporciona herramientas y capacitación para el análisis de imágenes digitales, incluido el análisis del nivel de error, metadatos y tutoriales.

Además de ver si una imagen es falsa, por las texturas y opciones que tiene esta herramienta en línea.

Se puede poner una URL, o también seleccionar una imagen desde nuestra computadora, para el respectivo análisis.



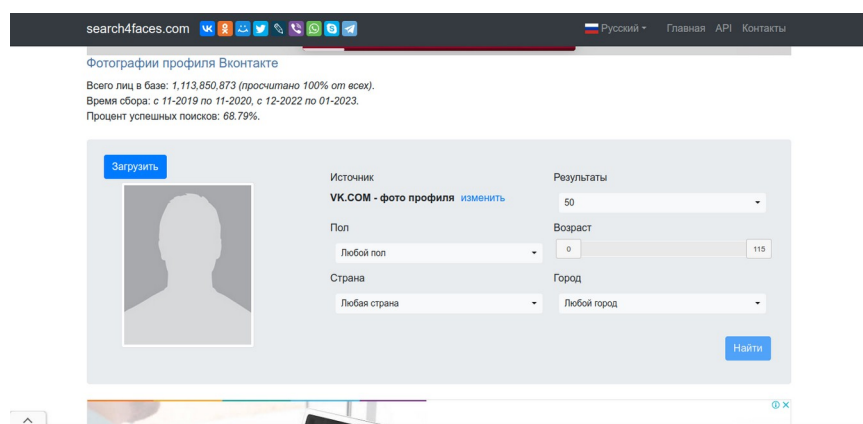
File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Current IPTC Digest	c5cfe4e59c95ded2835e29c49c2614a4
Image Width	720
Image Height	720
Encoding Process	Progressive DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)
JFIF	
JFIF Version	1.01
Resolution Unit	None
X Resolution	1
Y Resolution	1
IPTC	
Job Identifier	_6TaYUGjFJ7RjT7zZJz9
Composite	
Image Size	720x720
Megapixels	0.518

En este caso elegimos los metadatos, para ver la información que oculta la imagen.

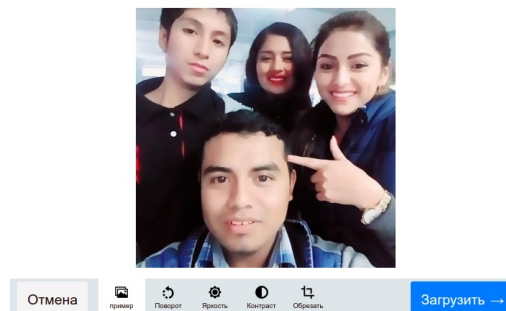
Search4faces:

Esta pagina es buena para encontrar información de la red social VK, con solo poner la foto. Incluso si la foto tiene a varias personas, te los separa y te da a elegir cual quieres buscar.

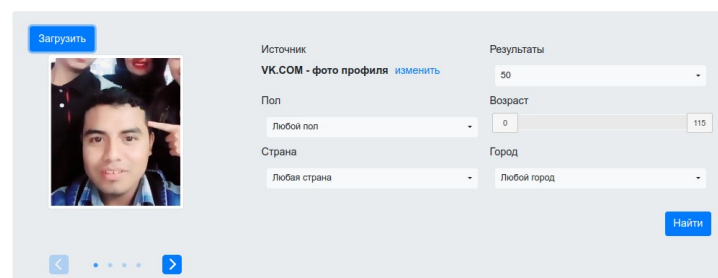
<https://search4faces.com/vk01/index.html>

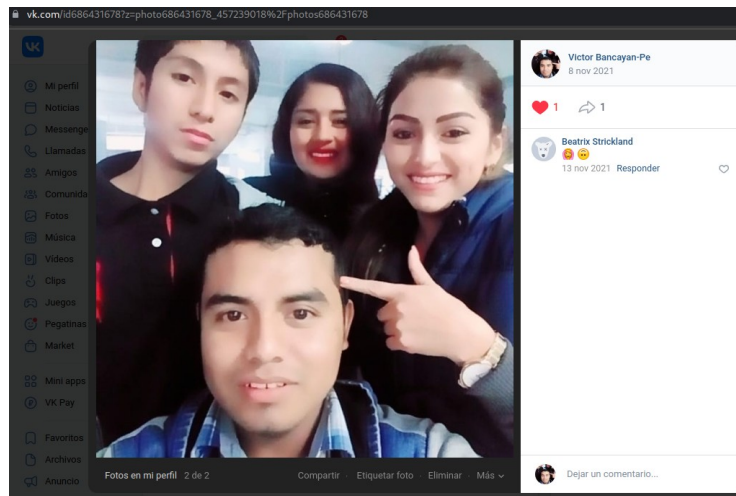


Ahora subiermos la imagen.



Me muestra para seleccionar que imagen deseo buscar, ya que detecta 4 rostros.





Nos muestra información relevante de nuestro objetivo.

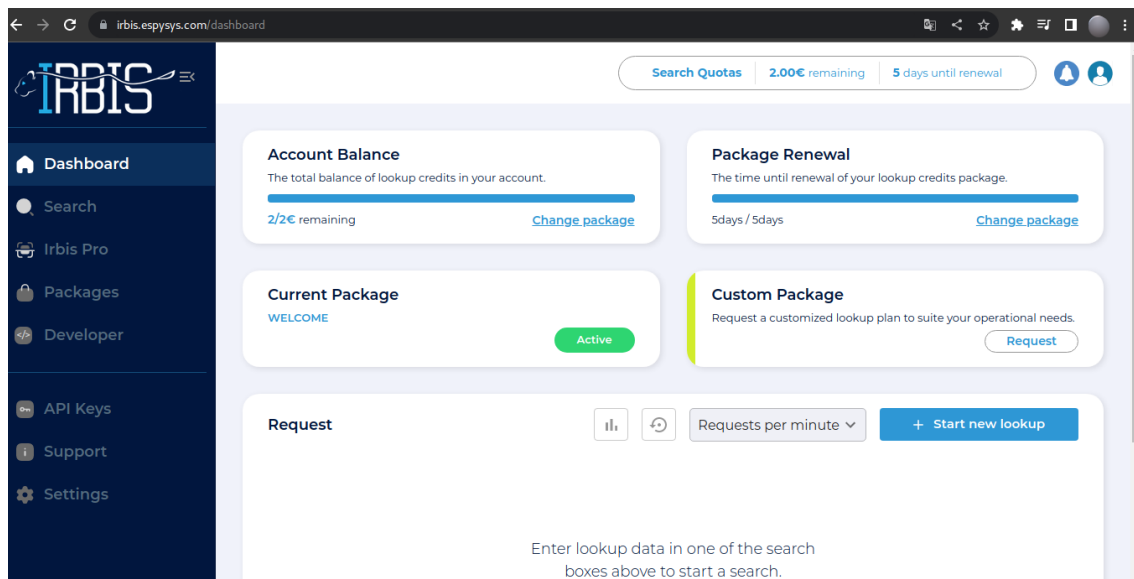
También hay otra herramienta online muy parecida, sólo deben crearse una cuenta y les dará 2 euros en saldo, lo veremos a continuación.

Irbis:

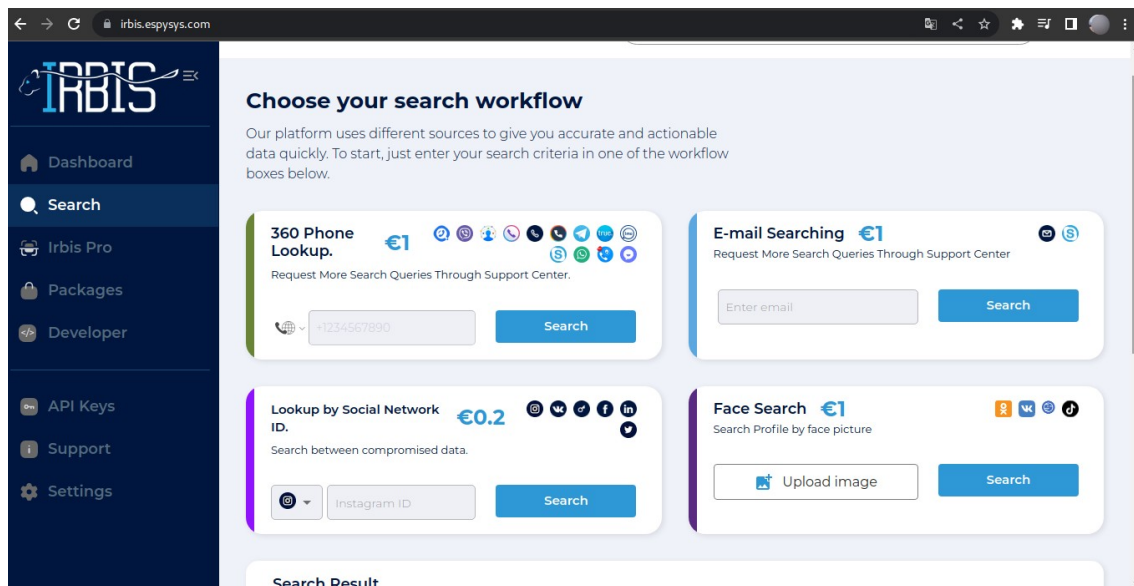
Diseñado para Usuarios que requieren una herramienta para consultar datos de destino en función de su actividad en Redes Sociales.

<https://irbis.espysys.com/>

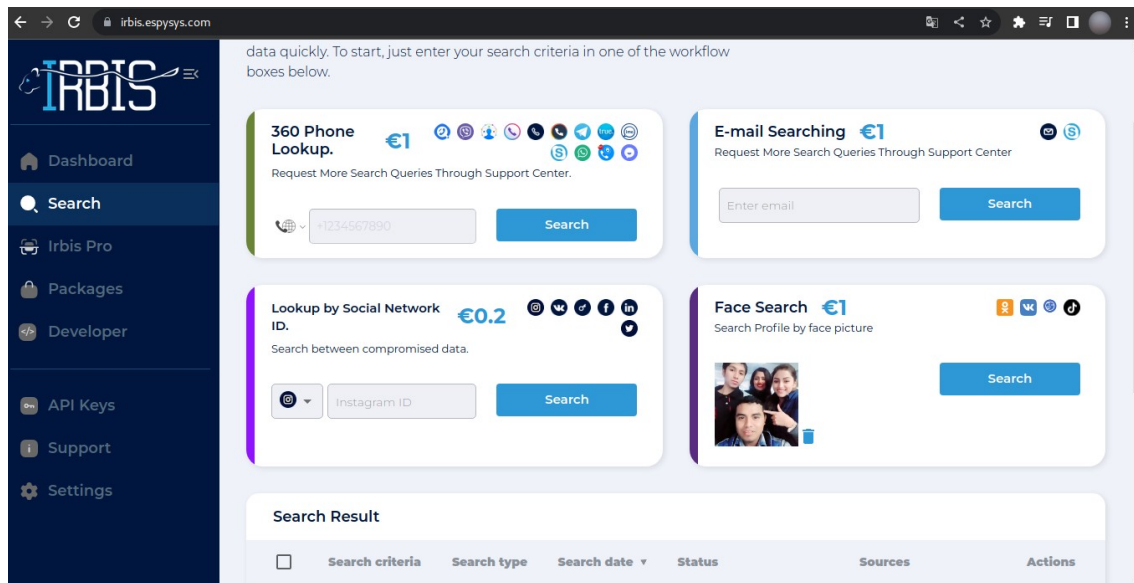




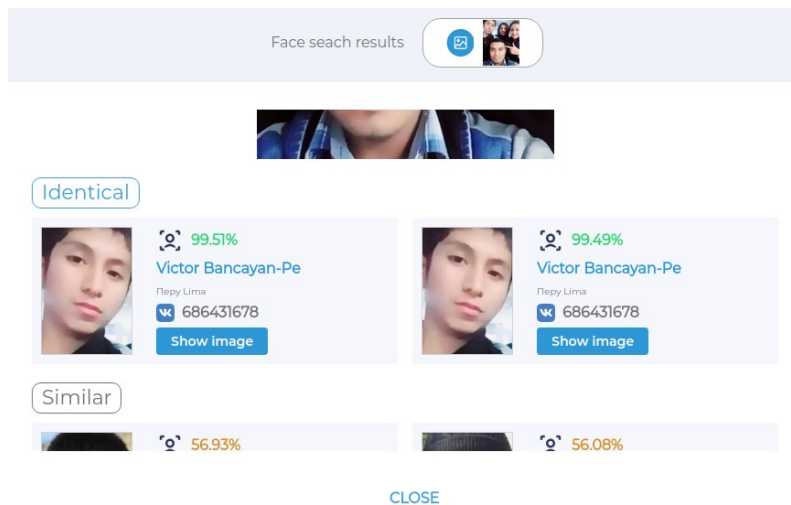
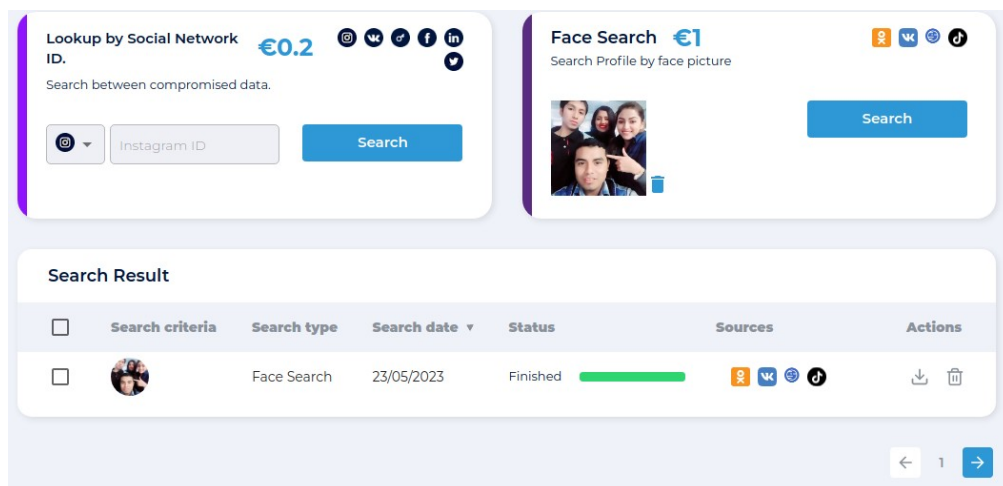
Podemos hacer las siguientes búsquedas, depende a lo que nos sea de más utilidad.

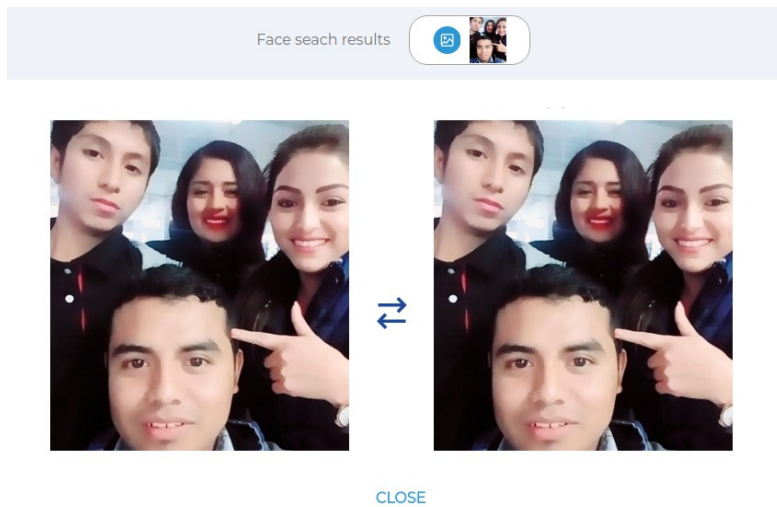


Vemos que nos muestra cuatro tipos de búsquedas, en este ejemplo vamos a usar la opción “**Face Search**”.



Al subir la imagen desde nuestro disco local, le damos clic a “**Search**”.





Vemos en la parte de arriba que nos muestra la cuenta de VK, con el ID.

Por terminal:

ExifTool:

<https://exiftool.org/>

ExifTool es un programa de software gratuito y de código abierto para leer, escribir y manipular metadatos de imágenes, audio, video y PDF. Es independiente de la plataforma, disponible como biblioteca Perl y como aplicación de línea de comandos.

ExifTool by Phil Harvey

Read, Write and Edit Meta Information!

Also available --> [Utility to fix Nikon NEF images corrupted by Nikon software](#)

Note: If exiftool.org goes down, it is because of the crappy DreamHost web hosting which disables an "unlimited traffic" web site if a single bot hammers the site with a moderate load. An alternate ExifTool homepage is available at <http://exiftool.sourceforge.net/>

Installing	Tag Names	Resources	History	Forum	FAQ
Download Version 12.57 (4.9 MB) - Feb. 23, 2023					Features User Comments Supported File Types System Requirements Running ExifTool Example Output Tag Names Explained Tag Groups Writing Information Writer Limitations Known Problems Security Issues Date/Time Shift Renaming Files Performance ExifTool Library Additional Resources New Discoveries Acknowledgements License Donate Contact Me
<p>ExifTool is a platform-independent Perl library plus a command-line application for reading, writing and editing meta information in a wide variety of files. ExifTool supports many different metadata formats including EXIF, GPS, IPTC, XMP, JFIF, GeoTIFF, ICC Profile, Photoshop IRB, FlashPix, AECF and ID3. Lyrics3, as well as the maker notes of many digital cameras by Canon, Casio, Fuji, Fujifilm, GE, GoPro, HP, JVC/Vision, Kodak, Leaf, Minolta/Konica-Minolta, Motorola, Nikon, Nintendo, Olympus/Epson, Panasonic/Leica, Pentax/Asahi, Phase One, Reconyx, Ricoh, Samsung, Sanyo, Sigma/Foveon and Sony.</p> <p>ExifTool is also available as a stand-alone Windows executable and a MacOS package. (Note that these versions contain the executable only, and do not include the HTML documentation or other files of the full distribution above.)</p> <p>Windows Executable: exiftool-12.57.zip (6.6 MB)</p> <p>The stand-alone Windows executable does not require Perl. Just download and un-zip the archive then double-click on "exiftool(-k).exe" to read the application documentation, drag-and-drop files and folders to view meta information, or rename to "exiftool.exe" for command-line use. Runs on all versions of Windows.</p> <p>(Note: Oliver Betz provides an alternate ExifTool Windows installer that avoids some problems of the self-extracting archive version above. Please post here if you have any problems/comments with this version.)</p> <p>MacOS Package: ExifTool-12.57.dmg (3.2 MB)</p> <p>The MacOS package installs the ExifTool command-line application and libraries in /usr/local/bin. After installing, type "exiftool" in a Terminal window to run exiftool and read the application documentation.</p> <p>Read the installation instructions for help installing ExifTool on Windows, MacOS and Unix systems.</p> <p>Click here for the GUI and MPF alternatives to verify these distribution packages</p>					

Lo bueno que es multiplataforma, así que lo podemos usar en diferentes sistemas operativos. Ahora lo usaremos usando Kali Linux, pero ustedes lo pueden hacer prácticamente desde cualquier sistema operativo, teniendo instalado Perl.

<https://www.kali.org/tools/libimage-exiftool-perl/>

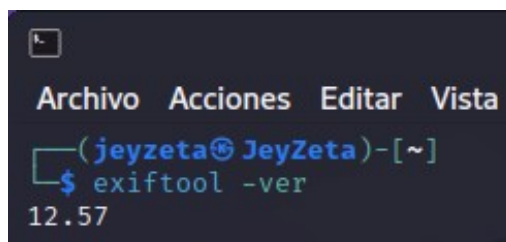
<https://github.com/exiftool/exiftool>

Para instalar, corran este comando desde la terminal.

sudo apt install libimage-exiftool-perl

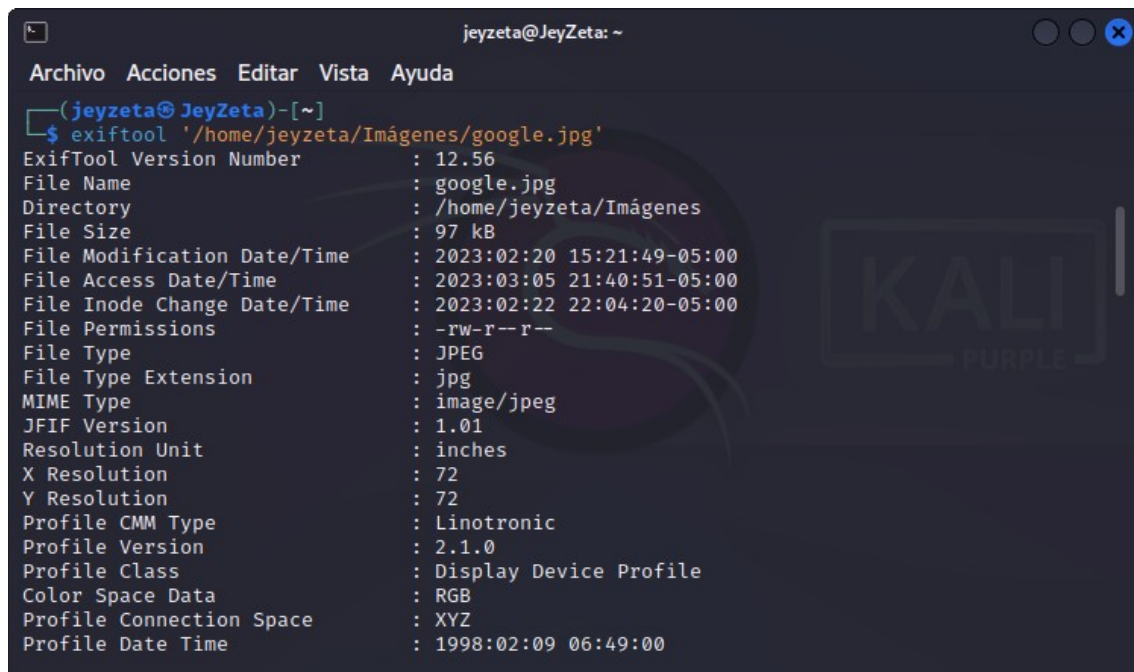
(Para ver la versión) - **exiftool -ver**

Nos debería mostrar como la siguiente imagen.



```
Archivo Acciones Editar Vista
(jeyzeta@JeyZeta)-[~]
$ exiftool -ver
12.57
```

exiftool '/rutadetuimagen.jpg'



```
jeyzeta@JeyZeta: ~
Archivo Acciones Editar Vista Ayuda
(jeyzeta@JeyZeta)-[~]
$ exiftool '/home/jeyzeta/Imágenes/google.jpg'
ExifTool Version Number      : 12.56
File Name                    : google.jpg
Directory                   : /home/jeyzeta/Imágenes
File Size                    : 97 kB
File Modification Date/Time  : 2023:02:20 15:21:49-05:00
File Access Date/Time       : 2023:03:05 21:40:51-05:00
File Inode Change Date/Time  : 2023:02:22 22:04:20-05:00
File Permissions             : -rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : inches
X Resolution                  : 72
Y Resolution                  : 72
Profile CMM Type              : Linotronic
Profile Version               : 2.1.0
Profile Class                 : Display Device Profile
Color Space Data              : RGB
Profile Connection Space     : XYZ
Profile Date Time             : 1998:02:09 06:49:00
```



```
jeyzeta@JeyZeta: ~  
Archivo Acciones Editar Vista Ayuda  
Profile File Signature      : acsp  
Primary Platform           : Microsoft Corporation  
CMM Flags                   : Not Embedded, Independent  
Device Manufacturer        : Hewlett-Packard  
Device Model                : sRGB  
Device Attributes          : Reflective, Glossy, Positive, Color  
Rendering Intent            : Perceptual  
Connection Space Illuminant : 0.9642 1 0.82491  
Profile Creator             : Hewlett-Packard  
Profile ID                  : 0  
Profile Copyright           : Copyright (c) 1998 Hewlett-Packard Company  
Profile Description         : sRGB IEC61966-2.1  
Media White Point           : 0.95045 1 1.08905  
Media Black Point           : 0 0 0  
Red Matrix Column           : 0.43607 0.22249 0.01392  
Green Matrix Column         : 0.38515 0.71687 0.09708  
Blue Matrix Column          : 0.14307 0.06061 0.7141  
Device Mfg Desc             : IEC http://www.iec.ch  
Device Model Desc           : IEC 61966-2.1 Default RGB colour space - sRGB  
Viewing Cond Desc           : Reference Viewing Condition in IEC61966-2.1  
Viewing Cond Illuminant     : 19.6445 20.3718 16.8089  
Viewing Cond Surround       : 3.92889 4.07439 3.36179  
Viewing Cond Illuminant Type : D50
```

```
Luminance                   : 76.03647 80 87.12462  
Measurement Observer        : CIE 1931  
Measurement Backing         : 0 0 0  
Measurement Geometry        : Unknown  
Measurement Flare           : 0.999%  
Measurement Illuminant      : D65  
Technology                  : Cathode Ray Tube Display  
Red Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)  
Green Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)  
Blue Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)  
Image Width                 : 800  
Image Height                 : 461  
Encoding Process             : Progressive DCT, Huffman coding  
Bits Per Sample              : 8  
Color Components             : 3  
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)  
Image Size                   : 800x461  
Megapixels                   : 0.369
```

Hasta le podemos añadir un campo Make, como en la imagen.

```
(jeyzeta@JeyZeta)-[~]  
$ exiftool -make='Hello Hackers' Python.ai  
1 image files updated
```

Lo bueno de exiftool, es que es una herramienta muy rápida y efectiva, usada por analistas forenses.

```
jeyzeta@JeyZeta: ~  
Archivo Acciones Editar Vista Ayuda  
(jeyzeta@JeyZeta)-[~]  
$ exiftool Python.ai  
ExifTool Version Number      : 12.56  
File Name                    : Python.ai  
Directory                    : .  
File Size                    : 1508 kB  
File Modification Date/Time   : 2023:03:07 00:09:14-05:00  
File Access Date/Time        : 2023:03:07 00:09:13-05:00  
File Inode Change Date/Time   : 2023:03:07 00:09:14-05:00  
File Permissions              : -rw-r--r--  
File Type                    : AI  
File Type Extension           : ai  
MIME Type                    : application/vnd.adobe.illustrator  
PDF Version                  : 1.5  
Linearized                   : No  
XMP Toolkit                   : Image::ExifTool 12.56  
Format                       : application/pdf  
Title                        : Python  
Creator Sub Tool              : AIRobin  
Startup Profile               : Print  
Type                         : Document  
Producer                     : Adobe PDF library 15.00  
Make                         : Hello Hackers  
Create Date                   : 2023:01:31 23:31:02-04:00  
Creator Tool                  : Adobe Illustrator 24.0 (Windows)  
Metadata Date                 : 2023:01:31 23:31:15-05:00
```

En mi blog, hice un post con más detalles.

<https://hackingenvivo.blogspot.com/2017/08/extraer-modificar-y-eliminar-los.html>

Hasta el GPS, se podría adulterar (modificar), pero en este caso no cambiaremos las coordenadas.

Búsqueda de archivos

- [Mamont](#)
- [NAPALM FTP Indexer](#)
- [Faganfinder](#)
- [grayhatwarefare](#): Buscar Buckets abiertos de Amazon s3 y su contenido.
- [FileZilla](#)
- [Shodan](#)

Búsqueda por Fagan Finder:

The screenshot shows the Fagan Finder web application. At the top, there's a search bar with the text 'osint' and buttons for 'search' and 'clear'. Below this is a section titled 'options' which contains three columns of radio button selections for file formats, search engines, and other options. The 'File Format' column includes options like Adobe Portable Document Format, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Microsoft Works, Microsoft Write, Rich Text Format, and Corel WordPerfect. The 'Search Engine' column includes Google, Yahoo!, Gigablast, Teoma, Exalead, Scirus, and Sensis. Below the options is an 'information' section with sub-sections: 'About this Tool', 'File Viewing', 'Scirus and Sensis', and 'PDF Searching'. At the bottom, there are 'links' to 'Inside Fagan Finder' and 'Miscellaneous'.

Al buscar algún archivo nos muestra para elegir diferentes formatos, al elegir nos redirige a una búsqueda de google mediante una dork que lo generará dependiendo la extensión que escojas.

The screenshot shows a Google search results page for the query 'osint filetype:pdf'. The search bar at the top contains the text 'osint filetype:pdf'. Below the search bar, there are several search results. The first result is from 'upv.es' and is titled 'Fuentes de Información OSINT para la Clasificación y ... - RiuNet'. The second result is from 'delitosfinancieros.org' and is titled 'OSINT E INVESTIGACIÓN EN REDES SOCIALES'. The third result is from 'cybercamp.es' and is titled 'OSINT/SOCMINT para la detección - CyberCamp'. The fourth result is from 'auditoresintemos.es' and is titled 'OSINT: INTELIGENCIA PARA INVESTIGAR (MEJOR)'. Each result includes a brief description and a link to the document.

Búsqueda por GrayHatWarfare:

The screenshot shows the GrayHatWarfare search interface. At the top, there's a navigation bar with links to 'Buckets', 'Shorteners', 'Pricing', 'FAQ', and 'Contact Us'. Below this is a search bar with a magnifying glass icon and a 'Login/Register' button. The main section is titled 'Search files' and contains a form for searching. The form has a 'Keywords' field with the text 'hacker', a 'Filename Extensions' field with the text 'php, xlsx, docx, pdf', and a 'Search' button. There are also checkboxes for 'Full Path' and 'Treat as regex', and a dropdown menu for 'Additional filters'.

Home Filter Buckets Search Files Docs / API Top Keywords

Results for "hacker" [See corresponding API Call](#)

Ignored Buckets
None

Showing 1 - 20 out of 12453 results

Premium users see 46865 more results. [More info here.](#)

#	Bucket	Filename	Container	Size
1	portel.s3.amazonaws.com	8297/hacker-1944688_640.jpg		92.42kB
2	portel.s3.amazonaws.com	9210/hacker-1944688_640.jpg		92.42kB
3	portel.s3.amazonaws.com	9422/hacker-1944688_640.jpg		92.42kB
4	rs2.ams3.digitaloceanspaces.com	theroms/Acorn Archimedes/Games/Hacker v3.05, The (1993)(DoggySoft).zip		385.33kB
5	rs3.fra1.digitaloceanspaces.com	theroms/Acorn 8 bit/Hackstar v2.2 (1984)(The Hacker).zip		7.31kB

Podrían usar también shodan, para ver ciertos dispositivos de almacenamiento, que se reportó en Netgear.

https://www.shodan.io/search?query=port%3A21+214-ADMIN_LOGIN

Vídeo:

<https://www.youtube.com/watch?v=VrJoyUZxsQo&t=66s>

Noticia:

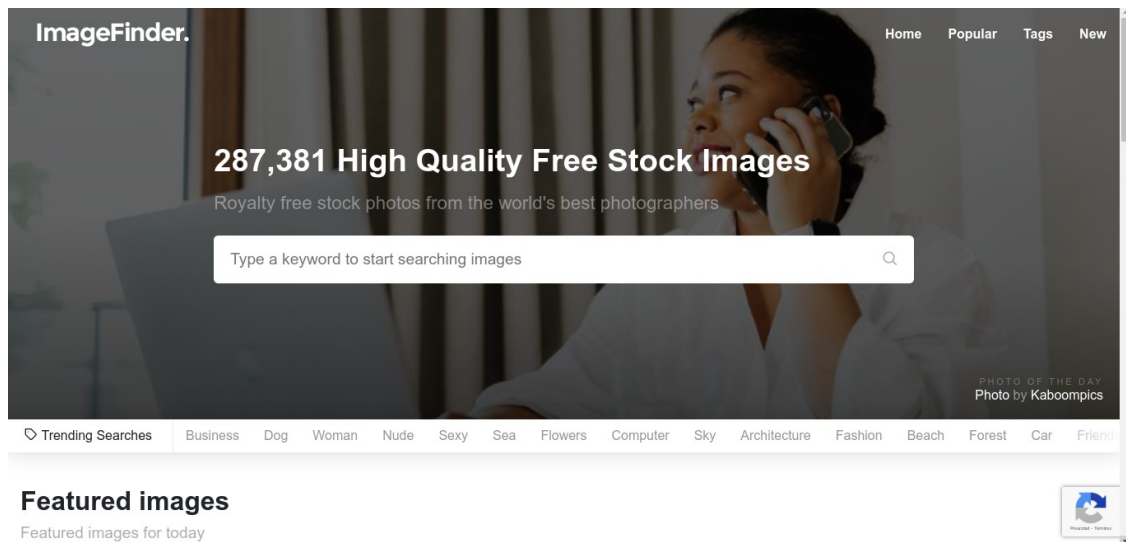
<https://www.sfgate.com/business/article/Netgear-Add-a-password-or-risk-losing-your-data-6811071.php>

Búsqueda de fotos online:

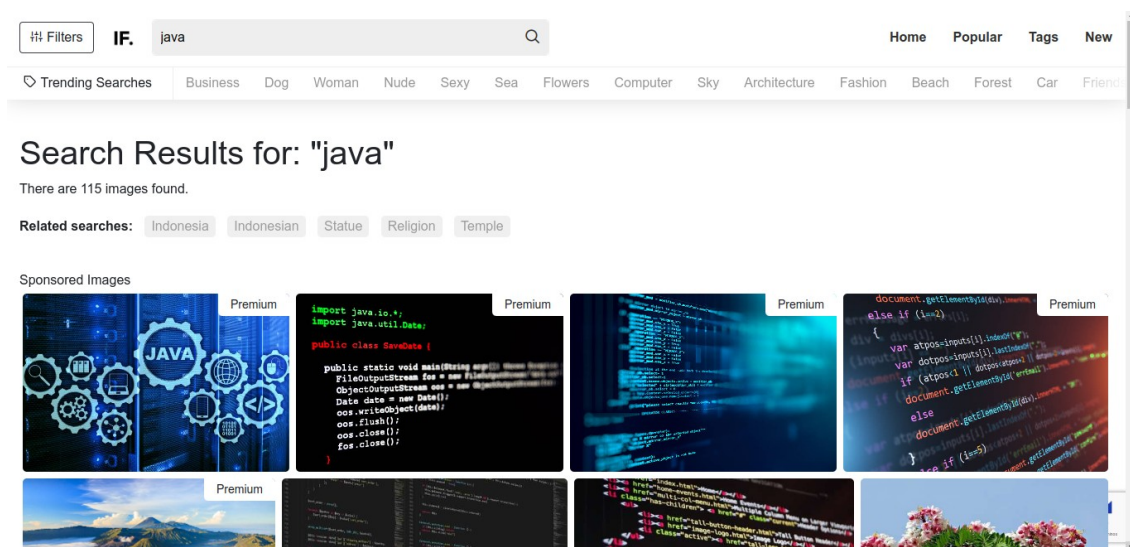
- [ImageFinder](#)
- [istockphoto](#)
- [stocksnap](#)
- [gettyimages](#)
- [shutterstock](#)

- [pikwizard](#)
- [mostphotos](#)
- [photopin](#)

Búsqueda por ImageFinder:



Muchas veces buscamos imágenes por google, pero estas plataformas son más personalizadas a las búsquedas que les brindes.

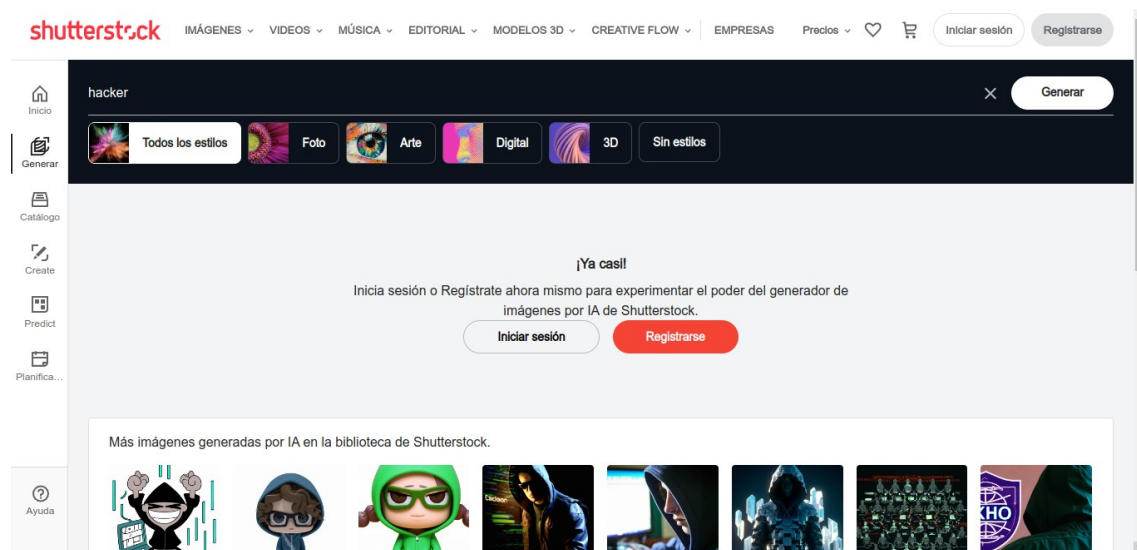


Búsqueda por Shutterstock:

<https://www.shutterstock.com/es>

En esta plataforma de imágenes se puede descargar imágenes y también generar imágenes con IA.

Muchas paginas para usarlas al 100% se debe estar registrado.

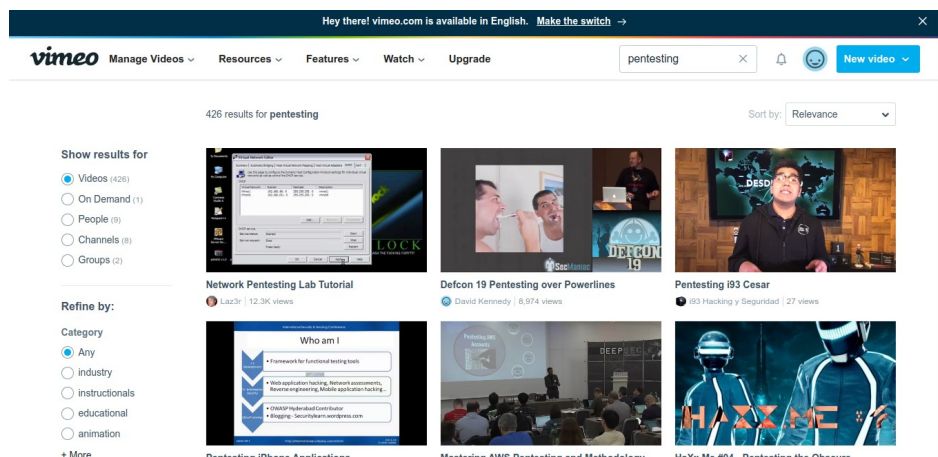


Búsqueda de vídeos:

- [YouTube](#)
- [Google video](#)
- [Yahoo video search](#)
- [Bing videos](#)
- [AOL videos](#)
- [StartPage video search](#)
- [Veoh](#)
- [Vimeo](#)

- [360daily](#)
- [Official Facebook video search](#)
- [Crowd tangle \(Facebook video search\)](#)
- [Internet archive open source movies](#)
- [Live Leak](#)
- [Facebook live video map](#)
- [Meta Tube](#)
- [Geo Search Tool](#): Búsqueda de todas las películas según una consulta específica introducida por el usuario, el conjunto de resultados se filtrará además según la distancia desde una ubicación específica (ciudad, pueblo, intersección) y según un marco temporal específico (última hora, últimas dos o tres horas, etc).
- [Earth Cam](#)
- [Insecam](#)

Búsqueda por Vimeo:

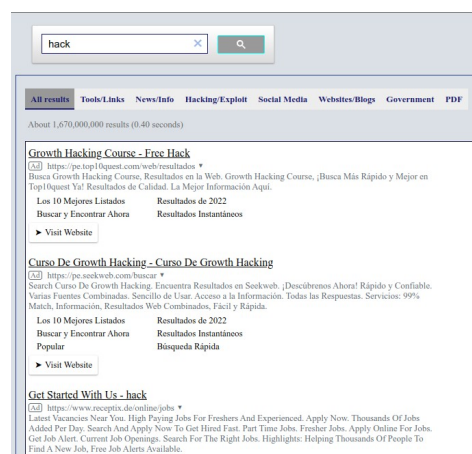


Pueden hacer sus búsquedas en los enlaces que dejé anteriormente.

Motor de búsqueda personalizado:

- [Google Custom Search Engines Finder](#)
- [300+ Social Networking Sites](#)
- [250+ Video Sharing Sites](#)
- [File Sharing Sites Search](#)
- [FTP and File Search Engine](#)
- [Github Awesome Custom Search Engine](#)
- [OSINT Tools, Resources & News Search](#)
- [Torrent Search](#)
- [Social Media Custom Search Engine](#)
- [IFTTT Applet Finder](#)
- [WordPress Content Hacker Search Engine](#)
- [Short URL Search Engine](#)
- [Raw Git Hacker Custom Search Engine](#)

Búsqueda por Engines Finder:



Búsqueda por Torrent Search:

Aproximadamente 1,670,000 resultados (0.46 segundos)

[seguridad informatica - ciberseguridad peru](#)
[Anuncio] <https://lima.newhorizons.com/ciberseguridad>
CEH, CSX, CISSP, CISM, CRISC, CISA, ISO 27032 y más. 25 años de experiencia en capacitaciones. Clases en vivo. 25 años de experiencia. Cursos: Aplicativos, Gestión de Innovación, Gestión Empresarial, Tec. de la Información.
Ethical Hacker ITIL 4
New Horizons CPENT
[Inicio](#)
[► Acceder al sitio web](#)

[Technical Privacy Expertise - ISACA's CDPSE Certification](#)
[Anuncio] <https://www.isaca.org/>
Advance Your Data Science Career with Certified Data Privacy Solutions Engineer (CDPSE) Showcase your expertise in privacy governance, architecture and data lifecycle with CDPSE. Check Events. Register Online. Explore Resources. Highlights: Membership Option Available, Experts Available, Journal Available.
[ISACA CDPSE Prep Manual · What is CDPSE?](#)
[► Acceder al sitio web](#)

[OSCP Exam Dumps, OSCP Practice Test Questions - PrepAway](#)
[Anuncio] <https://www.prepaway.com/>
Unlimited Access Sale Offer 30% Off, Pass Your IT Certification Exams in First Attempt. Pass Your Next IT Certification Exam Easily & Hassle Free. 98.6% Pass Rate. Free & Fast Updates. Pass in First Attempt. Exam Testing Engine. 30 Days Free Fast Updates. Types: Microsoft Exam Questions, Cisco Exam Questions, CompTIA Exam Questions.
[► Acceder al sitio web](#)

[Curso CISSP \(ISC\)2 - Certificación Oficial CISSP](#)

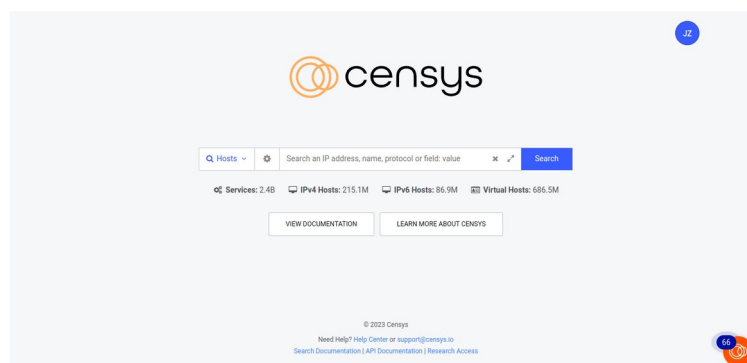
Dedende de la búsqueda que escriban el el buscador, se mostrarán los resultados.

BELFA'S TORRENTS					
name	se	le	size	time	
Wondershare Dr.Fone toolkit for iOS and Android v10.5.0.316 Multi-[WEB]	6	7	0	124.5 MB	2 years ago
Rohos.Logon.Key.v4.6.Multi-[WEB]		9	0	14.3 MB	2 years ago
PORTABLE.FlashBoot.3.2y.Free.ENG.LM		23	0	61.5 MB	2 years ago
Adguard Premium v7.4.3232.0 Multi-[WEB]	3	18	0	25.3 MB	2 years ago
Paragon.Linux.File.Systems.for.Windows.v5.2.1128.Multi-[WEB]	1	15	1	30.1 MB	2 years ago
La.Ragazza.Del.Tempo.Weathering.With.You.2019.ITA.MD.JAPAC3.BDRip.XviD-ISTANCE		9	1	1.9 GB	2 years ago
Microsoft.Office.Select.Edition.2016.VL.v16.0.5005.1000.64Bit.Maggio.2020.ITA.LM		19	6	6.7 GB	2 years ago
PORTABLE.FoneDog.Toolkit.per.Android.2.0.28.ENG.LM		17	0	83.4 MB	2 years ago
Vintage.Reggae.Cafe.COLLECTION.[9CD].2013.2019.[mp3-320kbps]-[WEB]		14	1	954.8 MB	2 years ago
VMware Workstation Pro v15.5.2 Build 15785246 64 Bit ENG [WEB]		8	0	180.6 MB	2 years ago
Claris FileMaker Pro v19.0.1.116 64 Bit Portable Multi-[WEB]	2	7	0	99.2 MB	2 years ago
Microsoft.Windows.e.Office.ISO.Down.Tool.v8.36.ADS.Remover.Portable.Multi-[WEB]	1	15	0	2.6 MB	2 years ago
Microsoft.Office.Professional.Plus.2016.VL.v16.0.5005.1000.Preattivato.64Bit.Mag...		17	6	2.0 GB	2 years ago
Windows Movie Maker 2020 v8.0.7.0 64 Bit Portable Multi [WEB]	1	25	4	310.9 MB	2 years ago
OSCP course - Penetration Testing With Kali Linux PWK 2020 ENG [WEB]	2	17	1	2.4 GB	2 years ago
Active Partition Recovery Ultimate v20.0.1 e Portable ENG [WEB]	4	21	0	983.8 MB	2 years ago

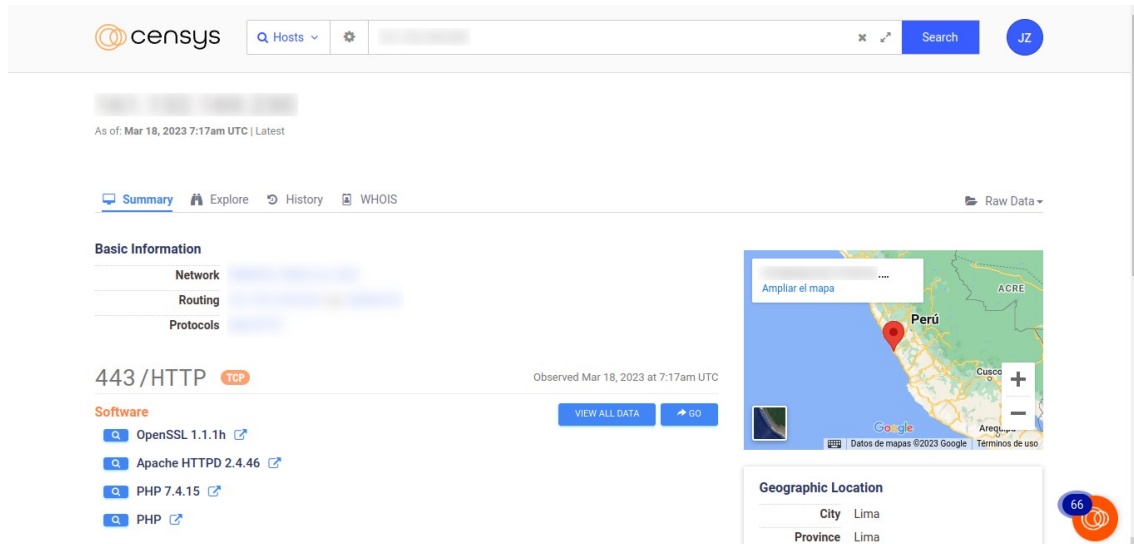
Buscador de dispositivos:

- [Shodan](#): Shodan es el primer motor de búsqueda del mundo para dispositivos conectados a Internet.
- [Airport webcams](#)
- [Insecam](#)
- [Lookr](#)
- [Earthcam](#)
- [Openstreetcam](#)
- [Opentopia](#)
- [Pictimo](#)
- [Thingful](#)
- [Webcam.nl \(NL\)](#)
- [Webcams.travel](#)
- [Worldcam](#)
- [censys](#): Censys es un motor que permite realizar búsquedas que proporciona respuestas a los investigadores sobre los hosts y la red que compone Internet.

Búsqueda por censys:



Usaremos cualquier IP, al azar.



Nos dio la información que vemos en la imagen.

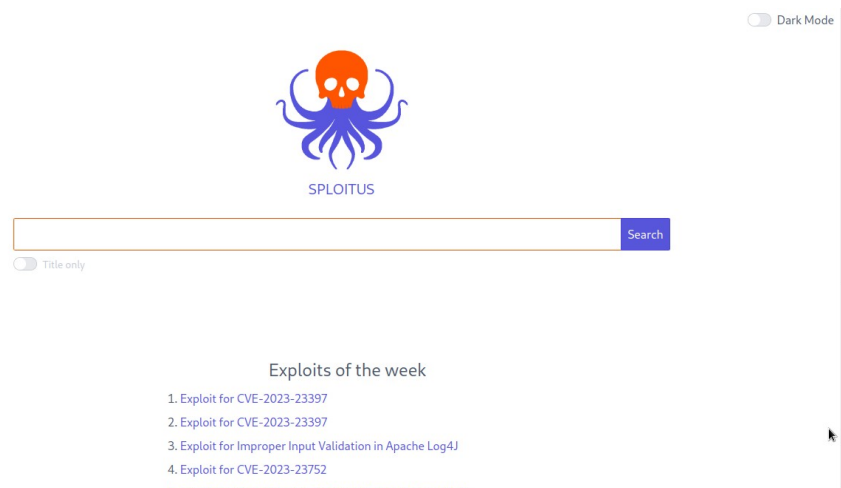
Es recomendable crear una cuenta en Censys, ya que nos servirá para tener la API, y para usarlas con muchas herramientas de OSINT.

Explotar el motor de búsqueda:

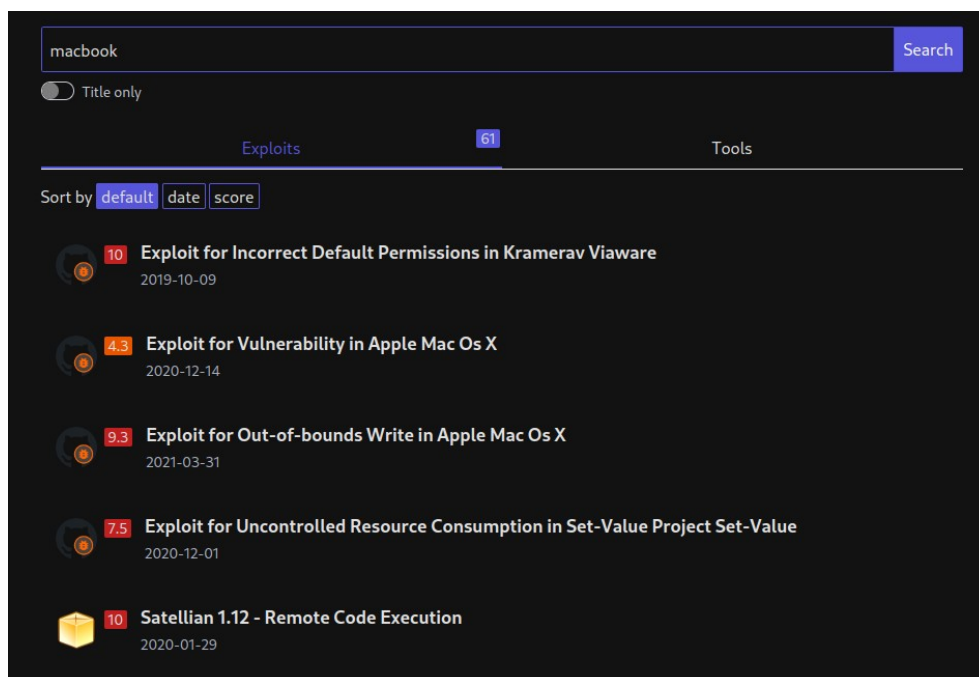
- [sploitus](#): Buscador de exploits y herramientas de seguridad
- [exploit-db](#)
- [Vulnerability Assesment Platform](#)
- [CVE Details](#)
- [nmmapper](#)
- [Vulmon](#)
- [exploits.shodan](#)
- [vulnerability-lab](#)

- 0day.today

Búsqueda por SPLOITUS:



<https://sploit.us/?query=macbook#exploits>

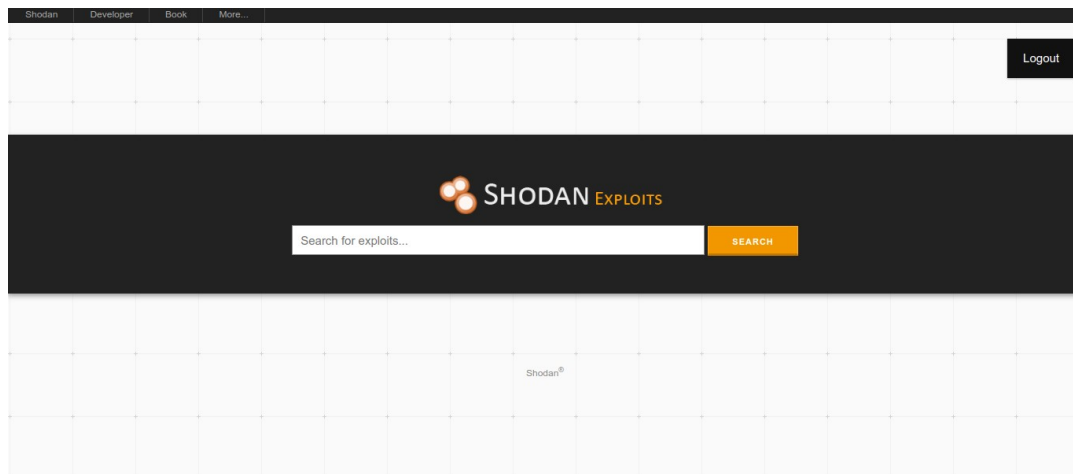


Se puede buscar infinidad de exploits.

Si en el buscador de shodan en el subdominio exploits, buscamos linux.

Búsqueda por Shodan Exploits:

<https://exploits.shodan.io/?q=linux>



Vemos 1.295 resultados para la búsqueda que hicimos, se puede hacer de android, iphone, windows, etc...

TOTAL RESULTS

1,295

SOURCE

exploitdb	1,251
metasploit	44

PLATFORM

linux	644
php	317
multiple	100
hardware	71
windows	39

TYPE

webapps	425
remote	297
dos	274

BibTeX - \'.bib\' File Handling Memory Corruption
Vincent Lafevre
dos
... Bugtraq ID: 34332
Class: Failure to Handle Exceptional Conditions
Published: Apr 01 2009 12:00AM
Updated: Nov 13 2009 03:46PM
Credit: Vincent Lafevre
Vulnerable: RedHat Linux 2.1
RedHat Fedora 9 0
RedHat Fedora 11
RedHat Fedora 10
RedHat Enterprise Linux WS 5
RedHat Enterprise Linux WS ...

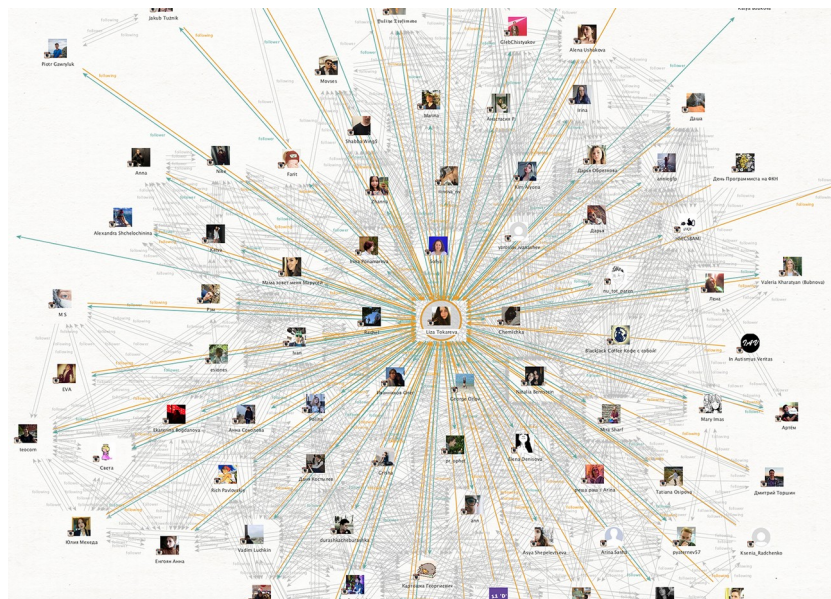
BibTeX - \'.bib\' File Handling Memory Corruption
Vincent Lafevre
dos
... Bugtraq ID: 34332
Class: Failure to Handle Exceptional Conditions
Published: Apr 01 2009 12:00AM
Updated: Nov 13 2009 03:46PM
Credit: Vincent Lafevre

NONBRES DE USUARIOS

En esta sección haremos reconocimiento de la búsqueda de usuarios.

Con herramientas automatizadas, para obtener ciertos datos de un usuario en específico.

Ver en qué redes sociales se encuentra registrado el usuario y otros datos fundamentales para OSINT.



Búsqueda de personas para Investigación:

- Decida cómo organizar / cotejar los datos.
- No incumplir con la ley.
- Identificar nombres formales.
- Identificar títulos y datos.
- Identificar los perfiles de redes sociales del objetivo.
- Identificar los datos de contacto del objetivo.
- Identifique los nombres de usuario del objetivo.
- Identificar la ubicación del objetivo.
- Identificar las afiliaciones del objetivo.

Hay muchas maneras de encontrar las redes sociales de un usuario en específico, vamos a usar plataformas web y herramientas en la terminal, incluso haciendo una búsqueda por google, en este espacio de los usuarios, vamos a detallar con algunas herramientas.

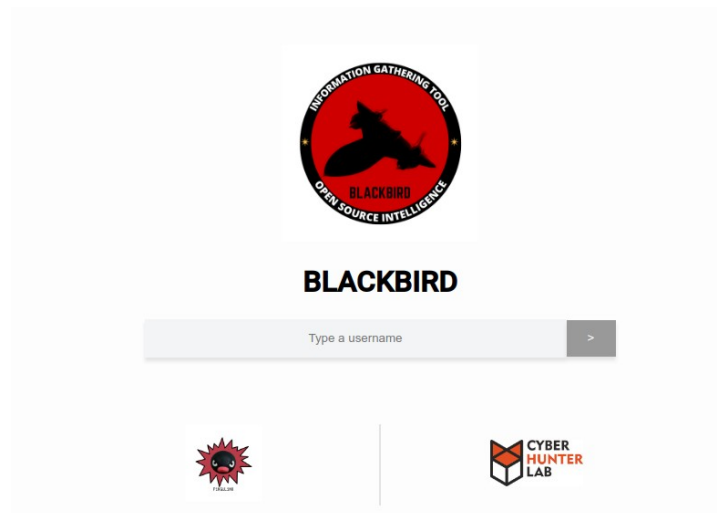
Es importante saber que muchas personas usan el username dependiendo de sus datos personales y muchas otras apodos (nick), ya que las plataformas normalmente al registrarte de piden uno, para que te identifiquen como tal. Así que debemos de tener paciencia ya que lo normal es que nos muestre varios resultados, y tenemos que ir descartando falsos positivos y quedarnos con la información verídica.

Trataré de usar mi username (nick), en casi todas las demostraciones, ya que no quiero afectar a ninguna persona, no es mi intención.

Cómo primer punto usaremos BlackBird.

Búsqueda por BlackBird:

<https://blackbird-osint.herokuapp.com/>



Ponemos el username que queremos buscar.

BLACKBIRD

Search for 'jeyzetaoficial' in 575 sites completed in 10.5 seconds

Filter:

FOUND **NOT FOUND** **ERROR** **ALL**

EXPORT AS ...

200 OK

Facebook

#1

FOUND

200 OK

Twitter

#3

FOUND

200 OK

Instagram

#7

FOUND

200 OK

Twitter Archived

#16

FOUND

Instagram

@jeyzetaoficial

<https://www.picuki.com/profile/jeyzetaoficial>

METADATA

Name Jey Zeta

Bio CYBER SECURITY RESEARCHER ..:

Followers 167

Following 22

Export results

Filename: .pdf

Type:

DOWNLOAD

Como vieron en la imagen de arriba, nos muestra de forma gráfica lo que encontró con nuestro usuario.

Lo pueden exportar como extensión .pdf para tenerlo como un reporte.

```
Results
Found (4)
The searched username was found on the following sites:

Facebook #1
Result: FOUND
URL: https://www.facebook.com/jeyzetaoficial
HTTP STATUS: 200 OK

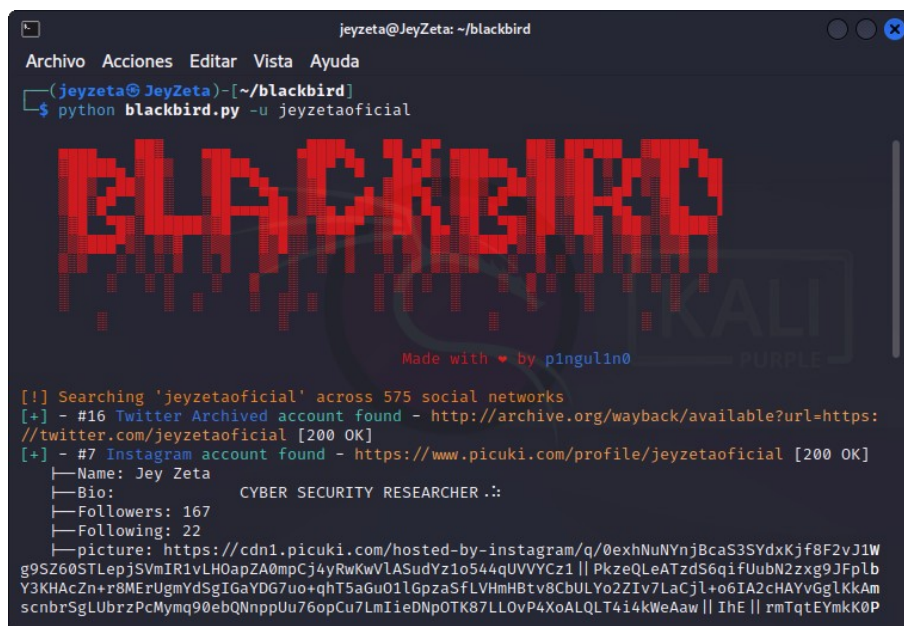
Twitter #3
Result: FOUND
URL: https://nitter.net/jeyzetaoficial
HTTP STATUS: 200 OK
Metadata
  Name: Jey Zeta
  Bio: CYBER SECURITY RESEARCHER 5
  Member since: 5:18 PM - 23 May 2022

Instagram #7
Result: FOUND
URL: https://www.picuki.com/profile/jeyzetaoficial
HTTP STATUS: 200 OK
Metadata
  Name: Jey Zeta
  Bio: CYBER SECURITY RESEARCHER 5
  Followers: 167
  Following: 22
```

Hice un vídeo de la herramienta en mi canal.

<https://www.youtube.com/watch?v=E1YBQB8iG0s&t=8s>

También lo veremos desde la terminal.



```
jeyzeta@JeyZeta: ~/blackbird
Archivo Acciones Editar Vista Ayuda
(jeyzeta@JeyZeta)~[/blackbird]
$ python blackbird.py -u jeyzetaoficial

BLACKBIRD
KALI
Made with ♥ by pingulino

[!] Searching 'jeyzetaoficial' across 575 social networks
[+] - #16 Twitter Archived account found - http://archive.org/wayback/available?url=https://twitter.com/jeyzetaoficial [200 OK]
[+] - #7 Instagram account found - https://www.picuki.com/profile/jeyzetaoficial [200 OK]
  Name: Jey Zeta
  Bio: CYBER SECURITY RESEARCHER .:
  Followers: 167
  Following: 22
  picture: https://cdn1.picuki.com/hosted-by-instagram/q/0exhNuYnjBcaS3SYdxKjf8F2vJ1Wg9SZ60STLepjSVmIR1vLH0apZA0mpCj4yRwKwVlASudYz1o544qUVVYCz1 || PkzeQLeATzdS6q1fUubN2zXg9JFplbY3KHAcZn+r8MERUgmYdSgIGaYDG7uo+qhT5aGu01lGpzaSfLVHmHBtv8CbULYo2ZiV7LaCjL+o6IA2cHAYvGglKkAmscnBrSgLUbrzPcMymq90ebQNppUu76opCu7LmIieDnp0TK87LLOvP4XoALQLT4i4kWeAaw || IhE || rmTqtEYmkK0P
```

Бúsqueda por Snoop:

<https://github.com/snooppr/snoop>

Una herramienta hecho por Rusos, que nos muestra las redes sociales de un objetivo y otros datos como audio.

```
jeyzeta@JeyZeta: ~/snoop
Archivo Acciones Editar Vista Ayuda

(jeyzeta@JeyZeta)~[~/snoop]
$ python snoop.py jeyzetaoficial

v1.3.7b

#Примеры:
cd ~/snoop
python3 snoop.py --help #справка
python3 snoop.py nickname #поиск user-a
python3 snoop.py --module #задействовать плагины

загружена локальная база: 182_Websites
[*] разыскиваем: < jeyzetaoficial >
[-] 1001mem: Увы!
[-] 3dnews: Увы!
[-] 4gameforum: Увы!
[-] About.me: Увы!
[-] Akniga: Увы!
[-] Allods: Увы!
[-] Anarcho-punk: Увы!
[-] Anime-planet: Увы!
```

```
jeyzeta@JeyZeta: ~/snoop
Archivo Acciones Editar Vista Ayuda

[-] Turpravda: Увы!
Twitch: https://www.twitch.tv/jeyzetaoficial
Twitter: https://twitter.com/jeyzetaoficial
[-] Ubisoft: Увы!
[-] VC: Увы!
[-] Vgtimes: Увы!
[-] Vimeo: Увы!
[-] VK: Увы!
[-] Vkrugdruzei: Увы!
[-] W3schools: Увы!
[-] Wikimapia: Увы!
[-] Wikipedia: Увы!
[-] Windowsforum: Увы!
[-] WordPressOrg: Увы!
[-] Wowhead: Увы!
[-] YouTube: Увы!
[-] Zonazakona: Увы!
0:00:17 100%
—Результаты: найдено → 5 url (сессия: 17 сек_8.35Mb)
—Сохранено в: /home/jeyzeta/snoop/nicknames/results/*
—Дата поиска: 19/03/2023_23:30:24

лицензия
demo: snoopproject@protonmail.com до 5/3/2024

(jeyzeta@JeyZeta)~[~/snoop]
$
```


Al finalizar nos muestra un archivo con extensión .html con los resultados.

Бúsqueda por Sherlock:

<https://github.com/sherlock-project/sherlock>

```
jeyzeta@JeyZeta: ~/sherlock
Archivo Acciones Editar Vista Ayuda
(jeyzeta@JeyZeta)~[~/sherlock]
$ python sherlock -h
usage: sherlock [-h] [--version] [--verbose] [--folderoutput FOLDEROUTPUT]
               [--output OUTPUT] [--tor] [--unique-tor] [--csv] [--xlsx]
               [--site SITE_NAME] [--proxy PROXY_URL] [--json JSON_FILE]
               [--timeout TIMEOUT] [--print-all] [--print-found] [--no-color]
               [--browse] [--local] [--nsfw]
               USERNAMES [USERNAMES ...]

Sherlock: Find Usernames Across Social Networks (Version 0.14.3)

positional arguments:
  USERNAMES            One or more usernames to check with social networks. Check
                        similar usernames using {%} (replace to '_', '-', '.').

options:
  -h, --help            show this help message and exit
  --version             Display version information and dependencies.
  --verbose, -v, -d, --debug
                        Display extra debugging information and metrics.
  --folderoutput FOLDEROUTPUT, -fo FOLDEROUTPUT
                        If using multiple usernames, the output of the results will be
                        saved to this folder.
  --output OUTPUT, -o OUTPUT
                        If using single username, the output of the result will be saved
                        to this file.
  --tor, -t            Make requests over Tor; increases runtime; requires Tor to be
                        installed and in system path.
```


Vemos que tiene varias opciones, hasta se podría usar con TOR, pero veremos la forma más básica.

```
(jeyzeta@JeyZeta)-[~/sherlock]
$ python sherlock jeyzetaoficial
[*] Checking username jeyzetaoficial on:

[+] Coil: https://coil.com/u/jeyzetaoficial
[+] Enjin: https://www.enjin.com/profile/jeyzetaoficial
[+] HackerOne: https://hackerone.com/jeyzetaoficial
[+] Instagram: https://www.instagram.com/jeyzetaoficial
[+] Periscope: https://www.periscope.tv/jeyzetaoficial/
[+] Twitch: https://www.twitch.tv/jeyzetaoficial
[+] Twitter: https://twitter.com/jeyzetaoficial

[*] Search completed with 7 results
```

Nos muestra 7 resultados, deben tomar en cuenta que no todas las cuentas pueden pertenecer a la misma persona, ya que hay usuarios que pueden usar antes ese username, o plataformas que no usamos y otras personas pueden haber creado un usuario como el de ustedes, esto es muy importante porque debemos de ir descartando información que no es la del usuario que queremos recopilar información.

Búsqueda por whatsmyname:

<https://whatsmyname.app/>

The screenshot shows the website <https://whatsmyname.app/> with the search results for the username 'jeyzetaoficial'. The interface includes a search bar at the top with the username entered and a search button. Below the search bar, there are filters and a table of results.

Active Filter: ALL

Found: 4 Processed: 629 / 630

Buttons: Show Found, Show False Positives, Show Not Found, Show All

Results Summary:

- Twitter archived: Username: jeyzetaoficial, Category: archived, Account Found
- HackerOne: Username: jeyzetaoficial, Category: tech, Account Found
- YouTube User2: Username: jeyzetaoficial, Category: video, Account Found
- Twitter: Username: jeyzetaoficial, Category: social, Account Found

Filter by Username: jeyzetaoficial

Buttons: Show 50 rows, Copy, CSV, PDF, Search: []

SITE	USERNAME	CATEGORY	LINK
HackerOne	jeyzetaoficial	tech	https://hackerone.com/jeyzetaoficial
Twitter	jeyzetaoficial	social	https://twitter.com/jeyzetaoficial
Twitter archived..	jeyzetaoficial	archived	https://web.archive.org/web/2/https://twitt
YouTube User2	jeyzetaoficial	video	https://www.youtube.com/@jeyzetaoficia

Navigation: Previous, 1, Next

Cada uno muestra diferentes resultados, y es porque algunas herramientas tienen diferentes plataformas añadidas en sus herramientas, por ejemplo si quisieramos hacer una herramienta parecida, podríamos tomar de referencia algunas de las mostradas y añadirle muchas plataformas que faltan.

Por eso es bueno no quedarse con una herramienta, usar varias para obtener diferentes resultados e ir descartando las que no nos sirven.

Búsqueda por UserRecon:

<https://github.com/issamelferkh/userrecon>

```
jeyzeta@JeyZeta: ~/userrecon
Archivo Acciones Editar Vista Ayuda
(jeyzeta@JeyZeta)~[~/userrecon]
$ ./userrecon.sh

UserRecon
v1.0, Author: @issamelferkh

[?] Input Username: jeyzetaoficial

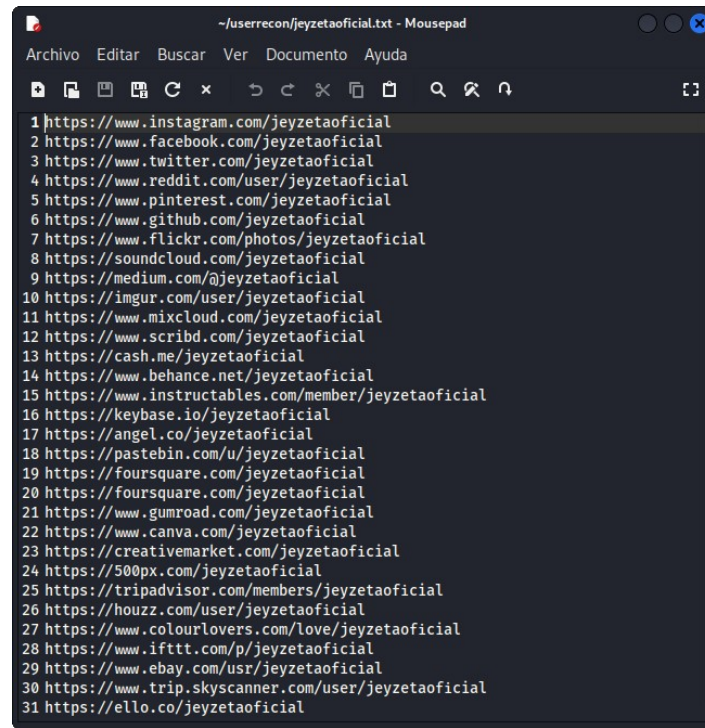
[*] Checking username jeyzetaoficial on:
[+] Instagram: Found! https://www.instagram.com/jeyzetaoficial
[+] Facebook: Found! https://www.facebook.com/jeyzetaoficial
[+] Twitter: Found! https://www.twitter.com/jeyzetaoficial
[+] YouTube: Not Found!
[+] Blogger: Not Found!
[+] GooglePlus: Found! https://plus.google.com/+jeyzetaoficial/posts
[+] Reddit: Found! https://www.reddit.com/user/jeyzetaoficial
[+] Wordpress: Not Found!
[+] Pinterest: Found! https://www.pinterest.com/jeyzetaoficial
[+] Github: Found! https://www.github.com/jeyzetaoficial
[+] Tumblr: Not Found!
[+] Flickr: Found! https://www.flickr.com/photos/jeyzetaoficial
[+] Steam: Not Found!
[+] Vimeo: Not Found!
```

```
jeyzeta@JeyZeta: ~/userrecon
Archivo Acciones Editar Vista Ayuda

[+] Trakt: Not Found!
[+] 500px: Found! https://500px.com/jeyzetaoficial
[+] BuzzFeed: Not Found!
[+] TripAdvisor: Found! https://tripadvisor.com/members/jeyzetaoficial
[+] HubPages: Not Found!
[+] Contently: Not Found!
[+] Houzz: Found! https://houzz.com/user/jeyzetaoficial
[+] blip.fm: Not Found!
[+] Wikipedia: Not Found!
[+] HackerNews: Not Found!
[+] CodeMentor: Not Found!
[+] ReverbNation: Not Found!
[+] Designspiration: Not Found!
[+] Bandcamp: Not Found!
[+] ColourLovers: Found! https://www.colourlovers.com/love/jeyzetaoficial
[+] IFTTT: Found! https://www.ifttt.com/p/jeyzetaoficial
[+] Ebay: Found! https://www.ebay.com/usr/jeyzetaoficial
[+] Slack: Not Found!
[+] OkCupid: Not Found!
[+] Trip: Found! https://www.trip.skyscanner.com/user/jeyzetaoficial
[+] Ello: Found! https://ello.co/jeyzetaoficial
[+] Tracky: Not Found!
[+] Tripit: Not Found!
[+] Basecamp: Not Found!
[*] Saved: jeyzetaoficial.txt

(jeyzeta@JeyZeta)~[~/userrecon]
$
```

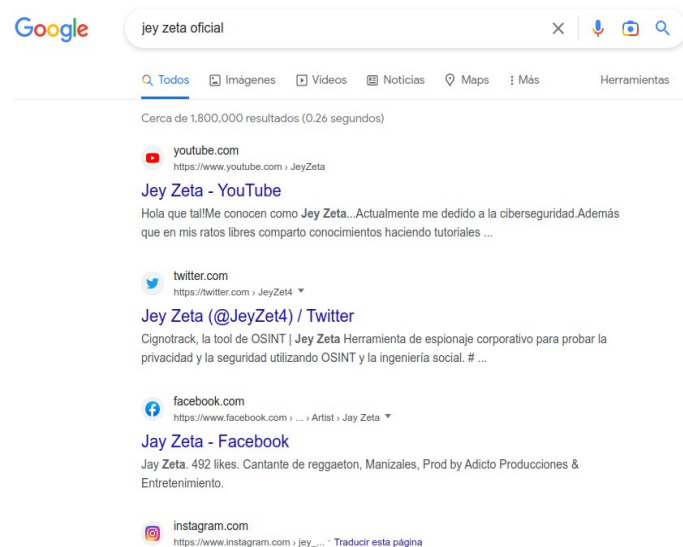
Al finalizar nos guarda en un archivo con extensión .txt todas las url que han sido encontradas con mi nombre de usuario.



```
1 https://www.instagram.com/jeyzetaoficial
2 https://www.facebook.com/jeyzetaoficial
3 https://www.twitter.com/jeyzetaoficial
4 https://www.reddit.com/user/jeyzetaoficial
5 https://www.pinterest.com/jeyzetaoficial
6 https://www.github.com/jeyzetaoficial
7 https://www.flickr.com/photos/jeyzetaoficial
8 https://soundcloud.com/jeyzetaoficial
9 https://medium.com/@jeyzetaoficial
10 https://imgur.com/user/jeyzetaoficial
11 https://www.mixcloud.com/jeyzetaoficial
12 https://www.scribd.com/jeyzetaoficial
13 https://cash.me/jeyzetaoficial
14 https://www.behance.net/jeyzetaoficial
15 https://www.instructables.com/member/jeyzetaoficial
16 https://keybase.io/jeyzetaoficial
17 https://angel.co/jeyzetaoficial
18 https://pastebin.com/u/jeyzetaoficial
19 https://foursquare.com/jeyzetaoficial
20 https://foursquare.com/jeyzetaoficial
21 https://www.gumroad.com/jeyzetaoficial
22 https://www.canva.com/jeyzetaoficial
23 https://creativemarket.com/jeyzetaoficial
24 https://500px.com/jeyzetaoficial
25 https://tripadvisor.com/members/jeyzetaoficial
26 https://houzz.com/user/jeyzetaoficial
27 https://www.colourlovers.com/love/jeyzetaoficial
28 https://www.ifttt.com/p/jeyzetaoficial
29 https://www.ebay.com/usr/jeyzetaoficial
30 https://www.trip.skyscanner.com/user/jeyzetaoficial
31 https://ello.co/jeyzetaoficial
```

Cabe recalcar que no todos esos usuarios me pertenecen.

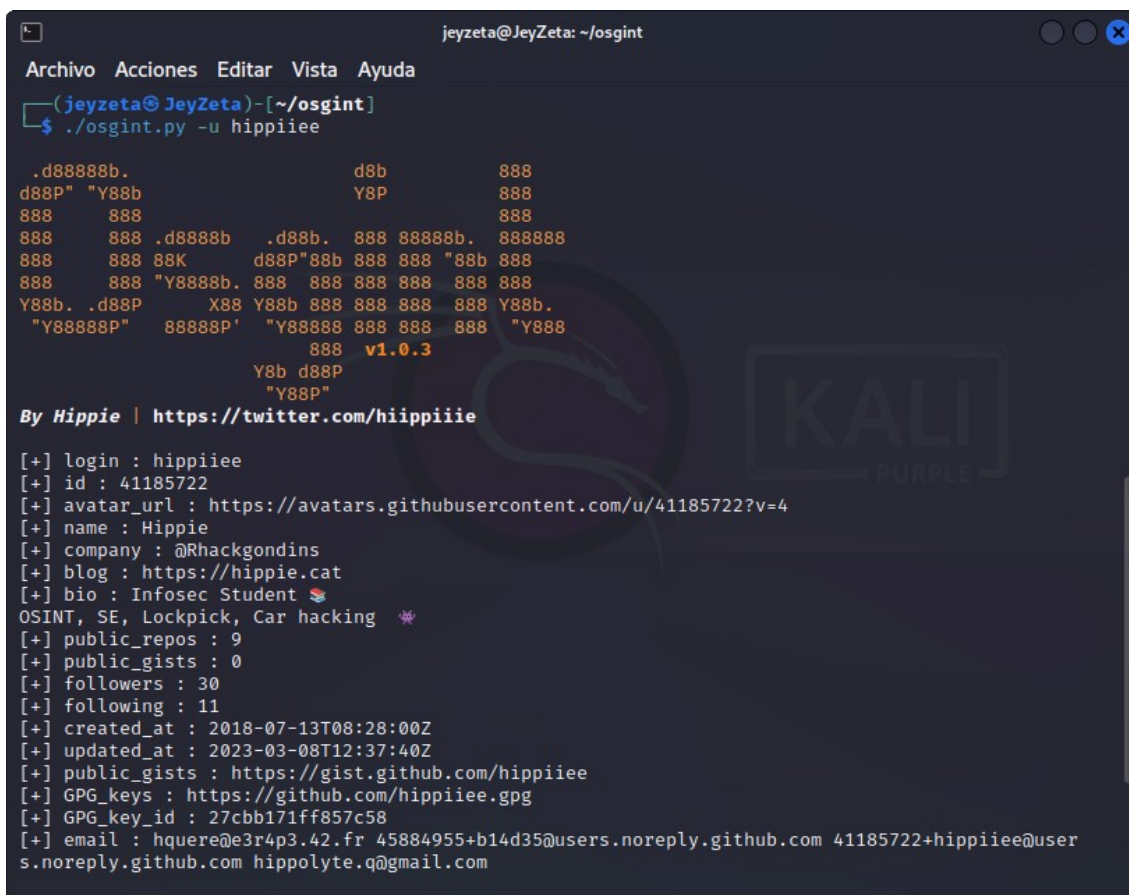
También podemos buscar por los navegadores que hemos visto anteriormente, por ejemplo por Google. (la vieja confiable).



Hace unas semanas usé la herramienta llamada “Osgint”, que es para hacer OSINT, a cualquier usuario de GitHub.

Búsqueda por Osgint:

<https://github.com/hippiiee/osgint>



```
jeyzeta@JeyZeta: ~/osgint
Archivo Acciones Editar Vista Ayuda
(jeyzeta@JeyZeta)~[~/osgint]
$ ./osgint.py -u hippiee

.d88888b.      d8b      888
d88P" "Y88b      Y8P      888
888      888      888
888      888 .d888b .d88b. 888 88888b. 888888
888      888 88K   d88P"88b 888 888 "88b 888
888      888 "Y8888b. 888 888 888 888 888 888
Y88b. .d88P      X88 Y88b 888 888 888 Y88b.
"Y88888P" 88888P' "Y88888 888 888 888 "Y888
              888 v1.0.3
              Y8b d88P
              "Y88P"

By Hippie | https://twitter.com/hiippiie

[+] login : hippiee
[+] id : 41185722
[+] avatar_url : https://avatars.githubusercontent.com/u/41185722?v=4
[+] name : Hippie
[+] company : @Rhackgondins
[+] blog : https://hippie.cat
[+] bio : Infosec Student 🦋
OSINT, SE, Lockpick, Car hacking 🦋
[+] public_repos : 9
[+] public_gists : 0
[+] followers : 30
[+] following : 11
[+] created_at : 2018-07-13T08:28:00Z
[+] updated_at : 2023-03-08T12:37:40Z
[+] public_gists : https://gist.github.com/hippiee
[+] GPG_keys : https://github.com/hippiee.gpg
[+] GPG_key_id : 27cbb171ff857c58
[+] email : hquere@e3r4p3.42.fr 45884955+b14d35@users.noreply.github.com 41185722+hippiee@user
s.noreply.github.com hippolyte.q@gmail.com
```

Vemos que al poner el usuario de cualquier cuenta de GitHub, nos muestra cierta información de la cuenta de GitHub, y además en la parte final nos muestra los correos vinculados a esta cuenta.

Búsqueda por Zen:

<https://github.com/s0md3v/Zen>

Es una herramienta OSINT para encontrar y recopilar correos electrónicos de usuarios de Github.

```
jeyzeta@JeyZeta: ~/Zen
Archivo Acciones Editar Vista Ayuda

(jeyzeta@JeyZeta)-[~/Zen]
$ python zen.py -h
usage: zen.py [-h] [-o OUTPUT] [-u UNAME] [-t THREADS] [--org] [--breach] target

positional arguments:
  target                target

options:
  -h, --help            show this help message and exit
  -o OUTPUT              output file
  -u UNAME               your username
  -t THREADS             number of threads
  --org                 organization
  --breach               check emails for breach

(jeyzeta@JeyZeta)-[~/Zen]
$ python zen.py [redacted]

Z E N v1.0
[redacted] : [redacted]@hotmail.com
```

Búsqueda por Magma OSINT:

<https://github.com/Anonimo501/Magma-OSint>

Script que ayuda a la búsqueda de información sobre una persona, ingresando el nombre y apellido(s) o el nickname, creado por LimerBoy.

```
root@JeyZeta: /home/jeyzeta/Magma-OSint
Archivo Acciones Editar Vista Ayuda

(root@JeyZeta)-[/home/jeyzeta/Magma-OSint]
# python3 osint.py

MAGMA OSINT
Created by LimerBoy

Find > jey zeta
[~] Searching jey zeta

[+] Url detected: https://twitter.com/jeyzet4?lang=en
[?] Title: null

[+] Url detected: https://www.instagram.com/jez_zeta/?hl=en
[?] Title: Jey Zeta (@jez_zeta) • Instagram photos and videos
— No data found

[+] Url detected: https://www.youtube.com/c/JeyZeta
[?] Title: Jey Zeta - YouTube

[+] Url detected: https://www.facebook.com/JeyZetaOficial/
[?] Title: Jey Zeta
— No data found

[+] Url detected: https://www.facebook.com/jey.zeta.10/?locale=es_LA
[?] Title: Jey Zeta
— No data found

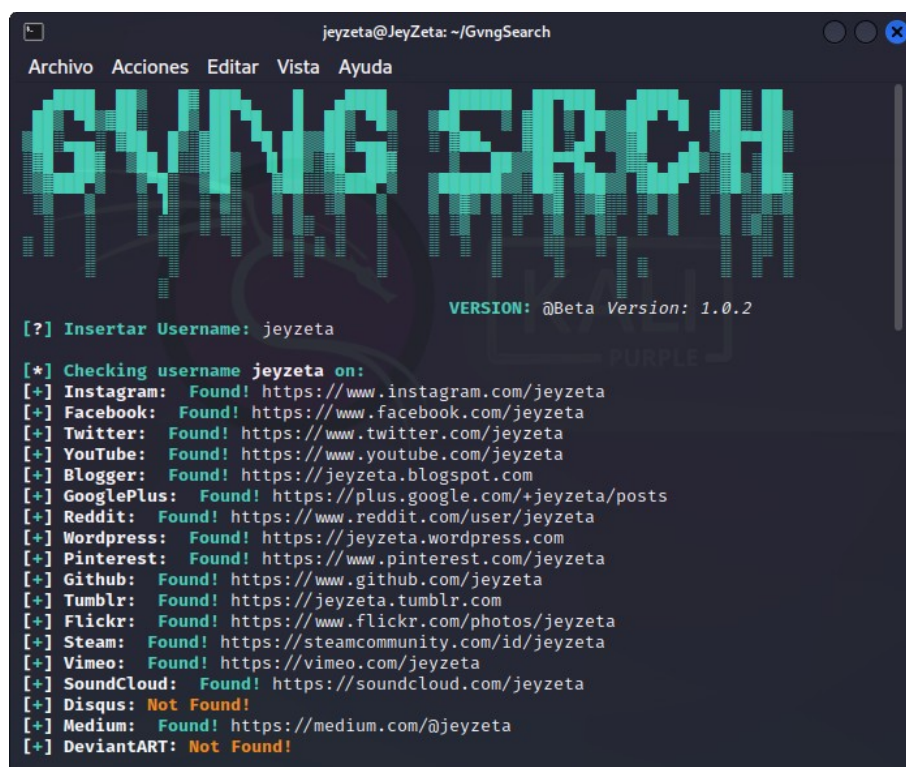
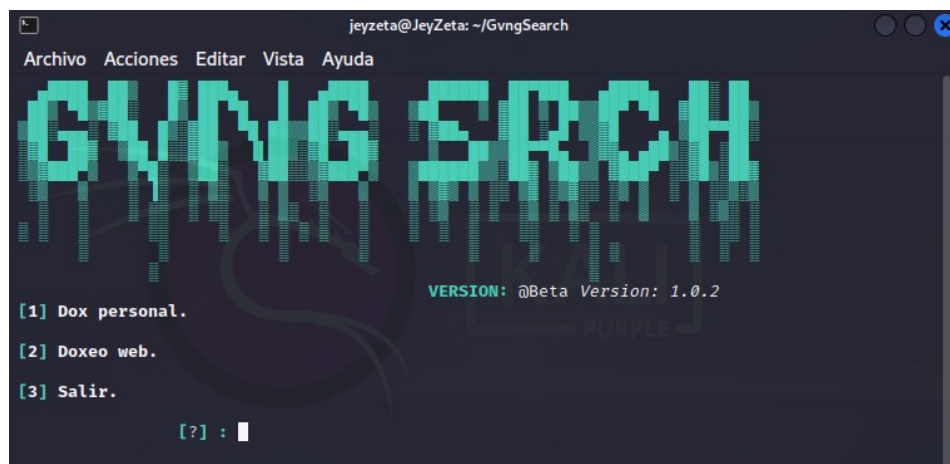
[+] Url detected: https://soundcloud.com/desege3/naicen-jezeta
[?] Title: Stream " Naicen " - Jey.Zeta by DESGRACIA SECTA | Listen online for free on SoundCloud
```


Búsqueda por GvngSearch:

<https://github.com/Tr4cKm4N/GvngSearch>

Es una herramienta Dox, enfocada en dos niveles:

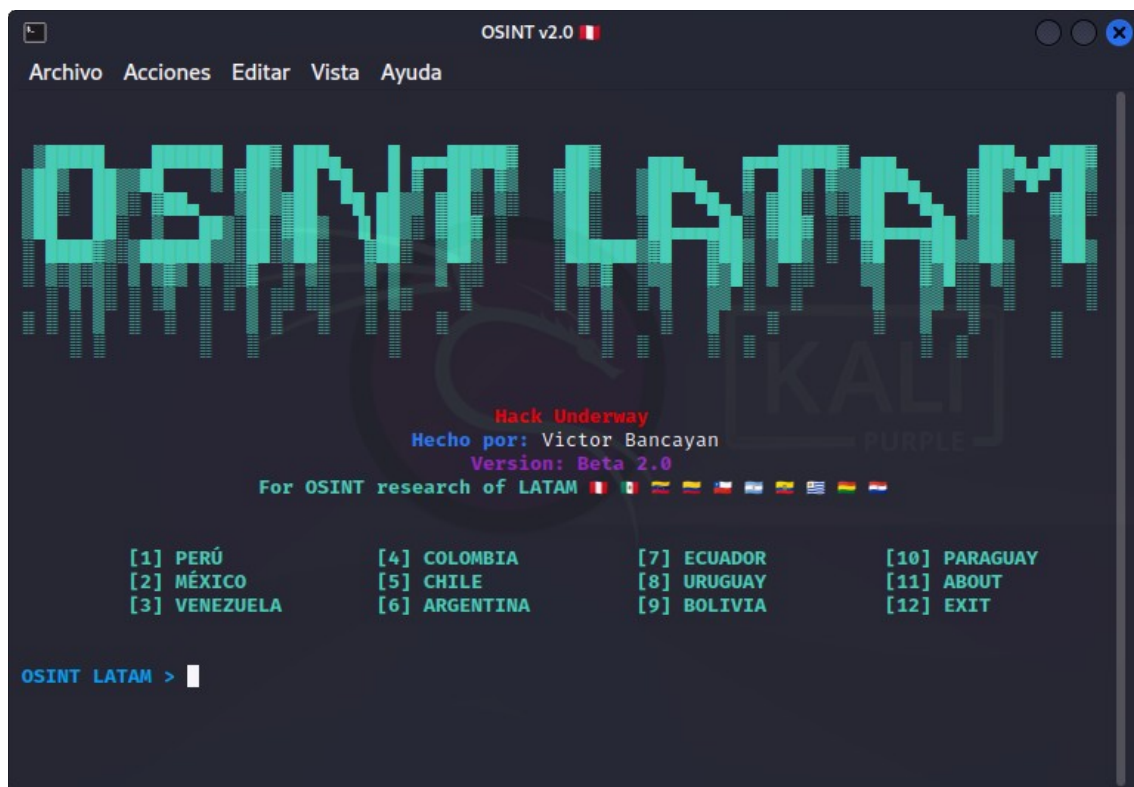
- Dox Personal: Orientado al doxeo de personal o usuario de internet.
- Dox Web: Orientado al doxeo general de una página o servidor web.



PERSONAS Y EMPRESAS

Veremos la herramienta OSINT LATAM, realizada por mi persona, para recopilar cierta información de los 10 países de la lista, nos enfocaremos en las personas, desde saber su balance en su wallet de bitcoin, ver información de su placa de vehículo, gps, dni, cédula, número, familiares, pasatiempos, ubicaciones, etc.

Esta herramienta aún no la he subido a mi repositorio, ya que viene incluido como herramienta al momento de obtener este libro.



Como primer paso tenemos 2 direcciones Bitcoin (BTC), tenemos que ver el balance que tienen ambos.

Para eso usaremos esta pagina web.

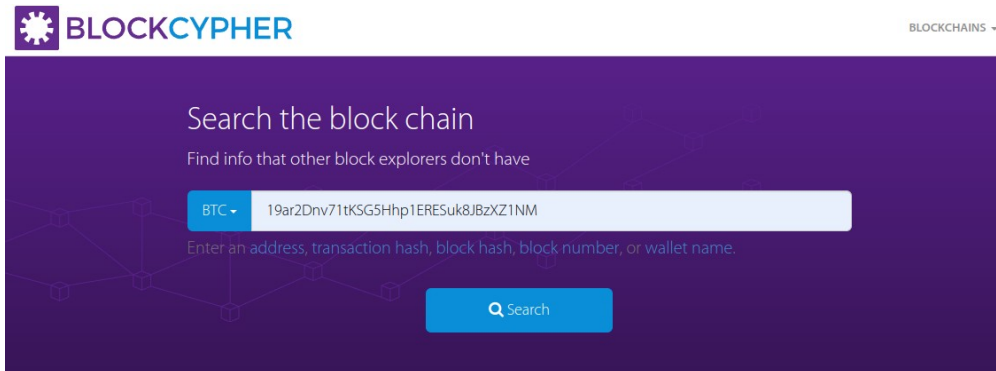
Ver información de Bitcoin (wallet):

<https://live.blockcypher.com/>

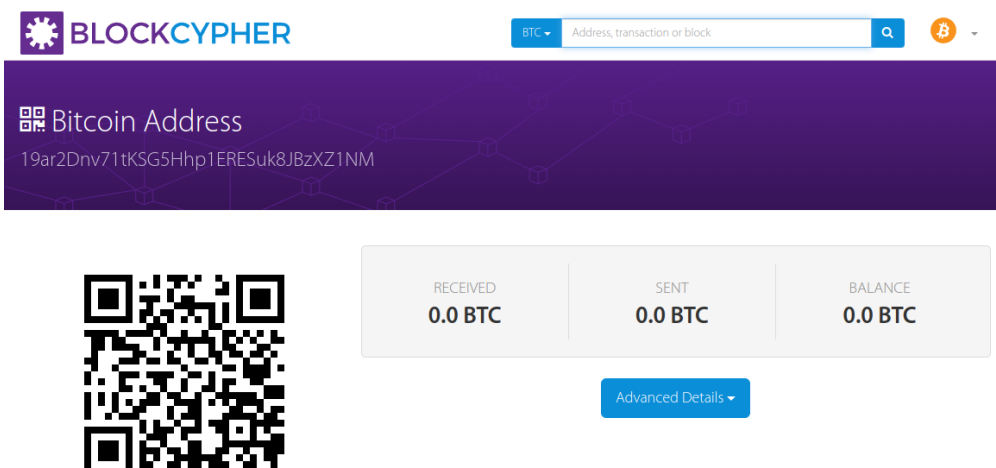
19ar2Dnv71tKSG5Hhp1ERESuk8JBzXZ1NM

3E8ociqZa9mZUSwGdSmAEMAoAxBK3FNDcd

Búsqueda por Block Cypher:

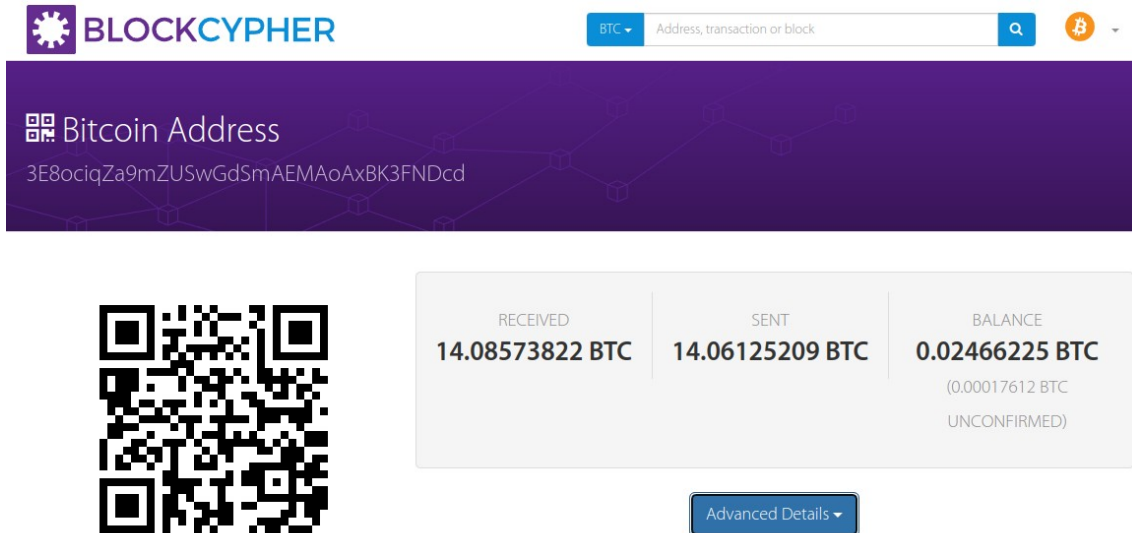
The image shows the BlockCypher search interface. At the top left is the BlockCypher logo. To the right is a dropdown menu labeled 'BLOCKCHAINS'. Below the logo is a search bar with the text 'Search the block chain' and 'Find info that other block explorers don't have'. The search bar has a dropdown menu set to 'BTC' and contains the address '19ar2Dnv71tKSG5Hhp1ERESuk8JBzXZ1NM'. Below the search bar is a button labeled 'Search'. The background of the search bar area is a dark purple with a faint network diagram.

Tenemos que poner la wallet de BTC.

The image shows the BlockCypher Bitcoin Address page. At the top left is the BlockCypher logo. To the right is a dropdown menu set to 'BTC' and a search bar with the text 'Address, transaction or block'. Below the search bar is a Bitcoin icon. The main content area has a dark purple background with a faint network diagram. It displays the text 'Bitcoin Address' and the address '19ar2Dnv71tKSG5Hhp1ERESuk8JBzXZ1NM'. Below the address is a QR code. To the right of the QR code is a table with three columns: 'RECEIVED', 'SENT', and 'BALANCE'. Each column shows a value of '0.0 BTC'. Below the table is a button labeled 'Advanced Details'.

Nos muestra 0 en el balance de la wallet.

Ahora veremos la otra wallet de Btc.

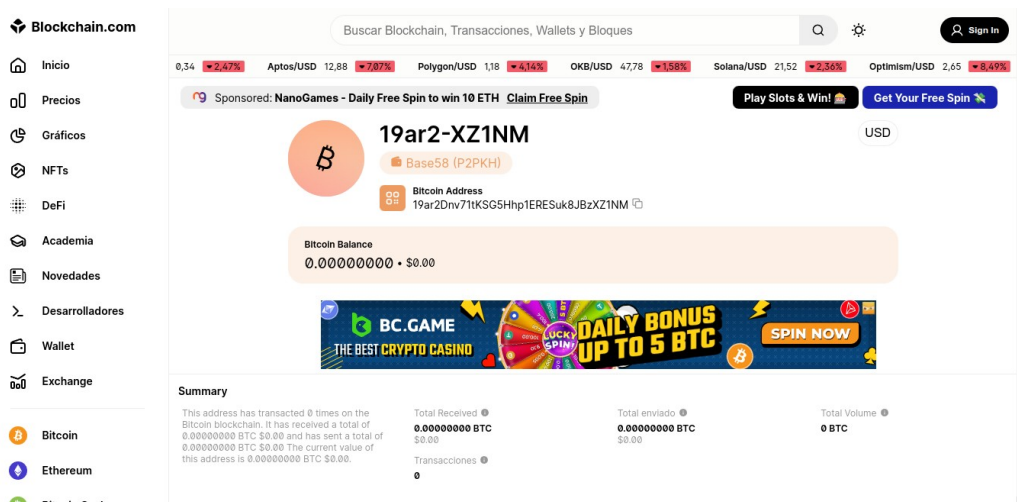


The screenshot shows the BLOCKCYPHER website interface. At the top, there's a navigation bar with the logo, a search bar, and a Bitcoin icon. Below the navigation bar, the main content area displays a Bitcoin address: 3E8ociqZa9mZUSwGdSmAEMaOAxBK3FNDcd. To the left of the address is a QR code. To the right, there's a summary box showing the balance: 0.02466225 BTC (0.00017612 BTC UNCONFIRMED). Below the summary box is a button labeled 'Advanced Details'.

Nos muestra que si tiene balance.

Búsqueda por BlockChain:

Blockchain wallet 1



The screenshot shows the Blockchain.com website interface. At the top, there's a navigation bar with the logo, a search bar, and a 'Sign In' button. Below the navigation bar, the main content area displays a Bitcoin address: 19ar2-XZ1NM. To the left of the address is a Bitcoin icon. To the right, there's a summary box showing the balance: 0.00000000 • \$0.00. Below the summary box is a banner for 'BC.GAME' with a 'DAILY BONUS UP TO 5 BTC' offer. At the bottom, there's a 'Summary' section with details about the address's transaction history.

Mediante la url que nos ofrece blockchain, al final al poner la wallet, nos muestra el balance y transacciones.

Es muy importante saber esto, ya que en una investigación OSINT, te topas con gente realmente anónima que deberás investigarlos para hallar con ellos.

Blockchain wallet 2

Blockchain.com

Inicio

Precios

Gráficos

NFTs

DeFi

Academia

Novedades

Desarrolladores

Wallet

Exchange

Bitcoin

Ethereum

Riotin Cash

Buscar Blockchain, Transacciones, Wallets y Bloques

Cardano/USD 0,38 5,28% Aptos/USD 12,22 1,41% Solana/USD 22,71 1,79% Polygon/USD 1,14 0,44% Optimism/USD 2,64 2,17%

Sponsored: 100 Free Spins in Slots Claim now! Play Slots & Win! Get Your Free Spin

3E8oc-FNDcd

Base58 (P2SH)

Bitcoin Address 3E8ociqZa9mZUSwGdSmAEMAoAxBK3FNDcd

Bitcoin Balance 0.02448613 • \$671,26

Daily Wager Contest

Wallet Gráfico

Summary








This address has transacted 1684 times on the Bitcoin blockchain. It has received a total of 14.08591434 BTC \$386.148 and has sent a total of 14.06125209 BTC \$385.476. The current value of this address is 0.02448613 BTC \$671.26.

Total Received 14.08591434 BTC \$386.148

Total enviado 14.06125209 BTC \$385.476

Total Volume 28.14716643 BTC \$771.624

Vemos el balance y transacciones que se hizo, si estás tratando de rastrear las transacciones se te hará necesario saber estos movimientos.

Transacciones				
	ID: dc61-295c 22/3/2023, 12:44:54	De 3PYR-m6yX Para 2 Outputs	0.00017612 BTC • \$4,83 Comisión 1.0K Sats • \$0,29	▼
	ID: c9f3-d11d 21/3/2023, 20:10:19	De bc1q-484n Para 203 Outputs	0.00031470 BTC • \$8,63 Comisión 180.8K Sats • \$49,57	▼
	ID: f706-e853 21/3/2023, 20:14:21	De 1Gr-NqfR Para 2 Outputs	0.00004476 BTC • \$1,23 Comisión 7.0K Sats • \$1,91	▼
	ID: af66-00b4 21/3/2023, 8:27:42	De bc1q-v5kw Para 199 Outputs	0.00010748 BTC • \$2,95 Comisión 72.5K Sats • \$19,89	▼
	ID: 3ac4-188f 20/3/2023, 17:28:36	De bc1q-9dcf Para 2 Outputs	0.00020000 BTC • \$5,48 Comisión 3.3K Sats • \$0,90	▼
	ID: 94a9-4f00 20/3/2023, 8:14:02	De 3KYE-oPpD Para 3E8o-NDcd	0.00002934 BTC • \$0,80 Comisión 1.7K Sats • \$0,46	▼
	ID: cd7f-8136 20/3/2023, 3:35:25	De bc1q-4x53 Para 68 Outputs	0.00095286 BTC • \$26,12 Comisión 44.1K Sats • \$12,08	▼

118

INVESTIGADOR_Z

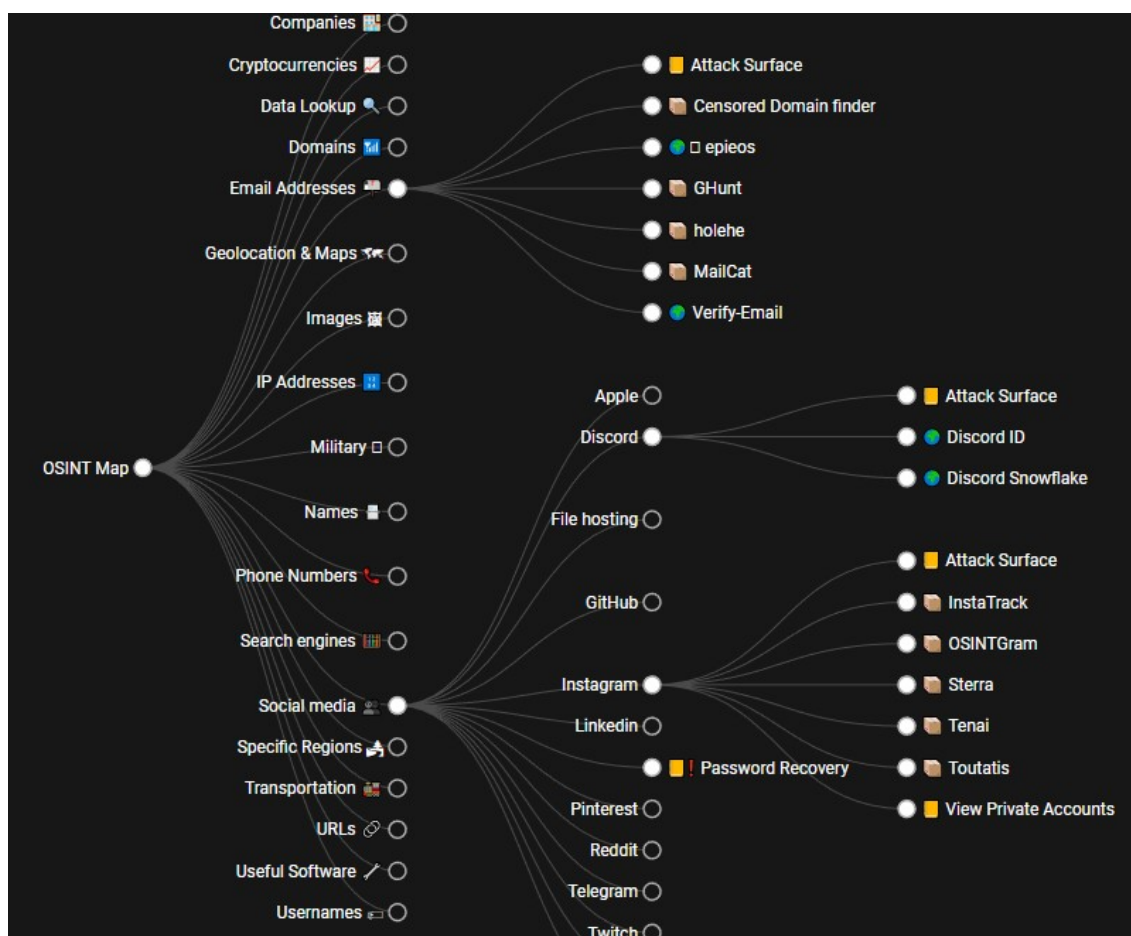
OSINT Framework:

<https://osintframework.com/>

Ya está algo decontinuada, por eso que un usuario de twitter, hizo una réplica con las herramientas más actuales, llamada “Malfrat's OSINT Map”.

Malfrat's OSINT Map:

<https://map.malfrats.industries/>



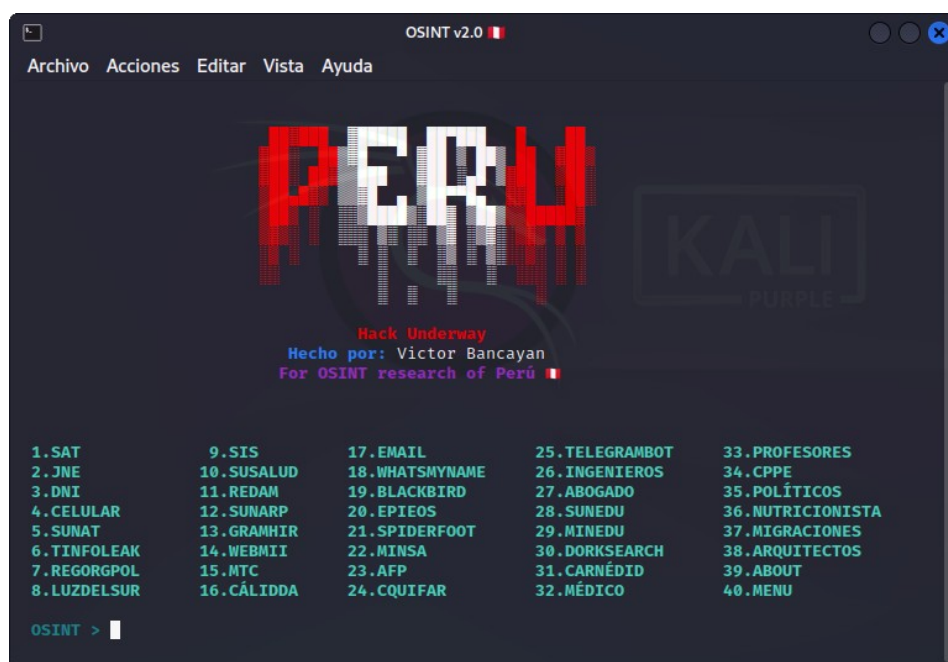
Vemos que está bien organizado para automatizar nuestra búsqueda de OSINT. En este punto en adelante vamos a estar usando la herramienta OSINT LATAM, que servirá como lanzador de varias herramientas seleccionadas por mucho tiempo para llevar las búsquedas más precisas de OSINT, a nivel de global, ya que la mayoría de herramientas que usamos en este libro son

universal, lo hago para que sea factible para todos aquellos que quieran guiarse con las técnicas mostradas en este libro.

OSINT LATAM:

Ahora veremos unos ejemplos de Perú y 1 de cada país de la herramienta OSINT LATAM.

Perú:




Al escoger la opción 2. (Multas Electorales).

The image shows a web form titled "Multas Electorales" with the subtitle "Consulte si tiene multas pendientes:". Below the subtitle, there is a label "Ingrese su DNI" and a text input field with a DNI icon. A checkbox labeled "Términos y Condiciones de uso del sistema." is checked. Below the checkbox is a red button labeled "CONSULTAR". At the bottom, there is a yellow button labeled "Aviso de pagos en línea" with a document icon. The footer contains logos for ONPE, JNE, and RENIEC.

En esta opción debemos poner el número de DNI.

Para ver si se tiene deuda por no botar en las elecciones.



Relación de Multas Electorales

Nombre : DNI :

CÓDIGO	PROCESO ELECTORAL	TIPO OMISIÓN	DEUDA (S/.)	ETAPA DE COBRANZA
54S7	ELECCIONES CONGRESALES EXTRAORDINARIAS 2020	SUFRAGIO		

Ahora escogemos la opción 5. (Ruc).



Consulta RUC

Criterios de la búsqueda

© 1997 - 2023 SUNAT Derechos Reservados

En este caso, ponemos el número de Ruc, de una empresa, es necesario saber este dato para personas que quieran comprobar si una empresa existe, para tener una mayor confianza a querer obtener algún servicio que brinda la empresa.

Consulta RUC

Resultado de la Búsqueda	
Número de RUC:	206 - E.I.R.L.
Tipo Contribuyente:	EMPRESA INDIVIDUAL
Nombre Comercial:	R.
Fecha de Inscripción:	24/08/2020
Fecha de Inicio de Actividades:	01/09/2020
Estado del Contribuyente:	ACTIVO
Condición del Contribuyente:	HABIDO
Domicilio Fiscal:	MARIATEGUIJ LIMA - LIMA - ATE
Sistema Emisión de Comprobante:	COMPUTARIZADO
Actividad Comercio Exterior:	IMPORTADOR
Sistema Contabilidad:	COMPUTARIZADO
Actividad(es) Económica(s):	Principal - 6202 - CONSULTORÍA DE INFORMÁTICA Y GESTIÓN DE INSTALACIONES INFORMÁTICAS

	Secundaria 1 - 6190 - OTRAS ACTIVIDADES DE TELECOMUNICACIONES
	Secundaria 2 - 4741 - VENTA AL POR MENOR DE ORDENADORES, EQUIPO PERIFÉRICO, PROGRAMA DE INFORM. Y EQU. DE TELECOM. EN COMERCIOS ESPECIALIZADOS
Comprobantes de Pago c/aut. de impresión (F. 806 u 816):	NINGUNO
Sistema de Emisión Electrónica:	FACTURA PORTAL DESDE 19/01/2021 BOLETA PORTAL DESDE 23/12/2020 DESDE LOS SISTEMAS DEL CONTRIBUYENTE. AUTORIZ DESDE 30/10/2020
Emisor electrónico desde:	30/10/2020
Comprobantes Electrónicos:	BOLETA (desde 30/10/2020),FACTURA (desde 30/10/2020),GUIA (desde 05/06/2022)
Afiliado al PLE desde:	-
Padrones:	Incorporado al Régimen de Buenos Contribuyentes (Resolución N° 0230050317313) a partir del 01/02/2022
Fecha consulta: 23/03/2023 23:54	

En la parte inferior, podemos ver otras opciones, en este caso queremos saber quién es el representante legal.

Volver

Información Histórica

Deuda Coactiva

Omissiones Tributarias

Cantidad de Trabajadores y/o Prestadores de Servicio

Actas Probatorias

Facturas Fisicas

Reactiva Perú : Deuda en cobranza coactiva

Programa de garantías COVID_19 : Deuda en cobranza coactiva

Representante(s) Legal(es)

Imprimir

Ingresa Email

e-mail

© 1997 - 2023 SUNAT Derechos Reservados

Nos muestra la siguiente información.

REPRESENTANTES LEGALES DE 20

Resultado de la Búsqueda

La información exhibida en esta consulta corresponde a lo declarado por el contribuyente ante la Administración Tributaria.

Documento	Nro. Documento	Nombre	Cargo	Fecha Desde
DNI	106		TITULAR-GERENTE	18/08/2020

Volver

Imprimir

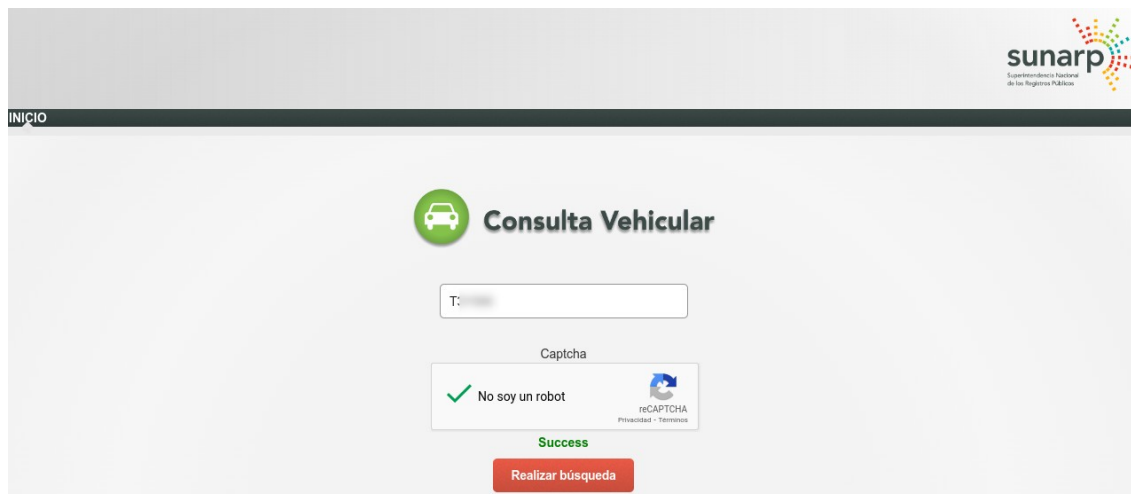
Ingresa Email

e-mail

© 1997 - 2023 SUNAT Derechos Reservados

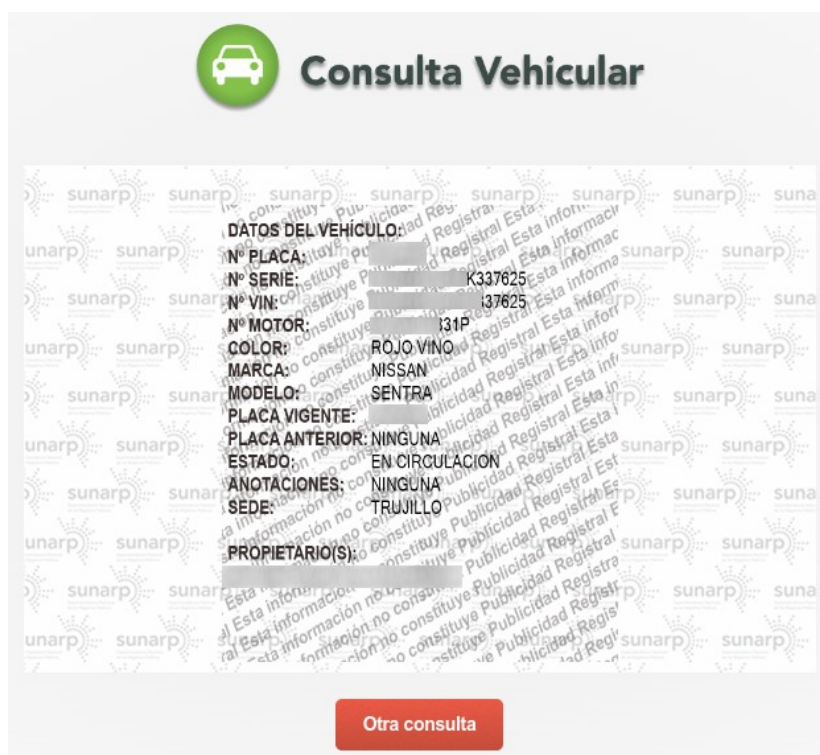
Esta herramienta es esencial al momento de hacer una compra o obtener un servicio, ya que vemos que la empresa está registrada.

Ahora si elegimos la opción 12. (**Consulta Vehicular**).



The screenshot shows the 'Consulta Vehicular' (Vehicle Query) page on the sunarp website. At the top right is the sunarp logo with the text 'Superintendencia Nacional de los Registros Públicos'. Below the logo is a navigation bar with 'INICIO'. The main heading is 'Consulta Vehicular' with a car icon. There is a text input field labeled 'T:' for the license plate. Below it is a 'Captcha' section with a green checkmark and the text 'No soy un robot', and a reCAPTCHA logo. A green 'Success' message is displayed. At the bottom is a red button labeled 'Realizar búsqueda'.

Al poner la placa de un vehículo, nos muestra la siguiente información.



The screenshot shows the results of a vehicle query. The heading is 'Consulta Vehicular' with a car icon. Below it is a table of vehicle data. The table is overlaid with a repeating watermark of the sunarp logo and the text 'Esta información no constituye Publicidad Registral'. At the bottom is a red button labeled 'Otra consulta'.

DATOS DEL VEHICULO:	
N° PLACA:	[REDACTED]
N° SERIE:	K337625
N° VIN:	337625
N° MOTOR:	131P
COLOR:	ROJO VINO
MARCA:	NISSAN
MODELO:	SENTRA
PLACA VIGENTE:	[REDACTED]
PLACA ANTERIOR:	NINGUNA
ESTADO:	EN CIRCULACION
ANOTACIONES:	NINGUNA
SEDE:	TRUJILLO
PROPIETARIO(S):	[REDACTED]

En la siguiente opción veremos la número 26. (**Colegio de Ingenieros**).

Es para obtener datos del colegio de ingenieros del Perú. Cabe recalcar que todo es público, no estamos accediendo a información privada.

#	Ver Detalle	CIP	Apellidos y Nombres	Especialidad	Sede	Estado del Registro
1			[blurred]	CIVIL	ICA	ACTIVO

Nos muestra sus datos y foto. Podemos verificar que realmente está habilitado.

Capítulo	Especialidad	Fecha Reconocimiento CIP
CIVIL	[blurred]	[blurred]

Como última opción para Perú, escogemos la opción 27. (**Abogados**)

Para saber datos de abogados, puede servir para no ser estafados y ver que realmente está inscrito.

BÚSQUEDA POR COLEGIATURA

#Número de colegiatura

Ingresar el código Captcha

420488

Consultar Regresar

Colegio de Abogados de Lima © 2023 Todos los Derechos Reservados

En esta parte se debe saber el REGCAL (en caso sea de lima), varía dependiendo la provincia. Este dato se ve al momento de hacer una firma con su sello el abogado.

BÚSQUEDA DE AGREMIADOS

BÚSQUEDA POR COLEGIATURA

Colegiatura

Apellido Paterno

Apellido Materno

Nombres


Estado
HABILITADO

Está información es **NO OFICIAL**, si Ud. desea una constancia de Habilitación, acérquese a la oficina de caja.

México:



Al escoger la opción 1. (Curp).



GOBIERNO DE
MÉXICO

TrámitesGobierno

RENAPO

Inicio

 >

Consulta tu CURP

Consulta tu CURP

Paso 1
Búsqueda

Paso 2
Descargar CURP

Búsqueda

La consulta puede efectuarse indicando la clave CURP cuando ya la conoce o proporcionando su nombre y datos de nacimiento.


Clave Única de Registro de Población

Datos Personales

Clave Única de Registro de Población (CURP)*:

[¿No conoces tu CURP?](#)

✓ No soy un robot



reCAPTCHA

Privacidad - Términos

* Campos obligatorios

Buscar

Datos del solicitante

CURP:

Nombre(s):

Primer apellido:

Segundo apellido:

Sexo:

Fecha de nacimiento: ⓘ

Nacionalidad:

Entidad de nacimiento:

Documento probatorio:

Datos del documento probatorio

Año registro:

Número de acta:

Entidad de registro:

Municipio de registro:

Descargar pdf

Al poner el CURP, nos muestra toda la información de una persona de México, incluso nos deja descargar en PDF.

ESTADOS UNIDOS MEXICANOS
CONSTANCIA DE LA CLAVE ÚNICA
DE REGISTRO DE POBLACIÓN

SECRETARÍA DE GOBERNACIÓN
DIRECCIÓN GENERAL DEL
REGISTRO NACIONAL DE POBLACIÓN
E IDENTIDAD

Clave: [REDACTED]
Nombre: [REDACTED]
Fecha de inscripción: [REDACTED] Folio: [REDACTED] Entidad de registro: [REDACTED]

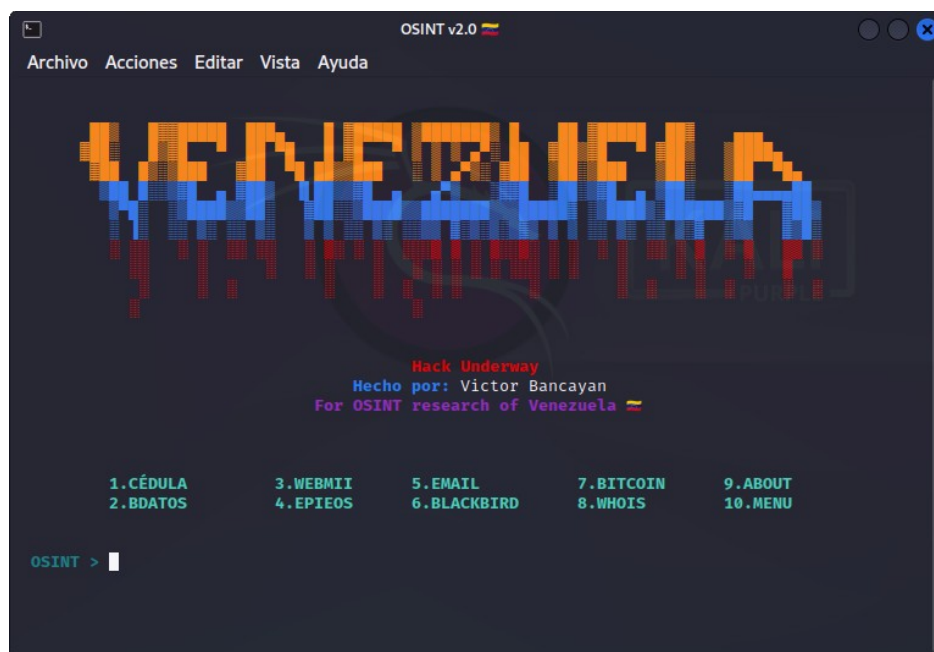
Soy México

CURP Certificada: verificada con el Registro Civil

PRESENTE

El derecho a la identidad está consagrado en nuestra Constitución. En la Secretaría de Gobernación trabajamos todos los días para garantizar que las y los mexicanos gocen de este derecho plenamente; y de esta forma puedan acceder de manera más sencilla a trámites y servicios.

Venezuela:



Escogemos la opción 1. (Registro Electoral).

Al poner el número de cédula, nos muestra la siguiente información.

REGISTRO ELECTORAL - CONSULTA DE DATOS	
DATOS DEL ELECTOR	
Cédula:	V- [REDACTED]
Nombre:	[REDACTED]
Estado:	EDO. LA GUAIRA
Municipio:	MP. VARGAS
Parroquia:	PQ. [REDACTED]
Centro:	[REDACTED]
Dirección:	[REDACTED]
Planilla General de Reclamos Imprimir Cerrar	

Es importante usar esta información con el mayor cuidado posible, y no estar divulgando la información de personas, a menos que sea un estafador y tenga las pruebas pertinentes, ya que publicar datos de personas podría ser un delito, dependiendo el país donde se encuentre.

Colombia:



Al momento de escoger la opción 4. (**Sena**).

Certificado Digital SENA

Para descargar su certificado

Debe diligenciar el Número de Registro que le han suministrado en su Centro de Formación. En caso de no conocerlo puede digitar el tipo y número de su documento de identificación.

Esta opción le permite obtener una lista de los certificados que tiene disponibles para descarga. Utilice el botón Consultar que se halla en la sección correspondiente para obtener el certificado.

Importante! Para visualizar los certificados se requiere la herramienta **Adobe Reader**, la cual puede descargar desde la siguiente [URL](#).


Seleccione opción de búsqueda

Consultar por: Documento ▼

Tipo de Documento: CEDULA DE CIUDADANIA ▼

Número de Documento:

Ingrese el texto que ve en la imagen:



Con esta opción al poner el número de cédula, nos sale una lista de los cursos que el usuario ha realizado y podemos descargar los certificados.

Registro	Título	Tipo	Programa	Certificación	Firma Certificado	
						Descargar
						Descargar
						Descargar
						Descargar
						Descargar
						Descargar
						Descargar
						Descargar



Libertad y orden
REPÚBLICA DE COLOMBIA

El Servicio Nacional de Aprendizaje SENA

En cumplimiento de la Ley 119 de 1994

Hace constar que

Con Cédula de Ciudadanía No. [REDACTED]

Cursó y aprobó la acción de Formación

con una duración de 40 horas

En testimonio de lo anterior, se firma el presente en Ibagué, al primer(1) día del mes de agosto de dos mil veintidos (2022)

Firmado Digitalmente por

[Firma digital]

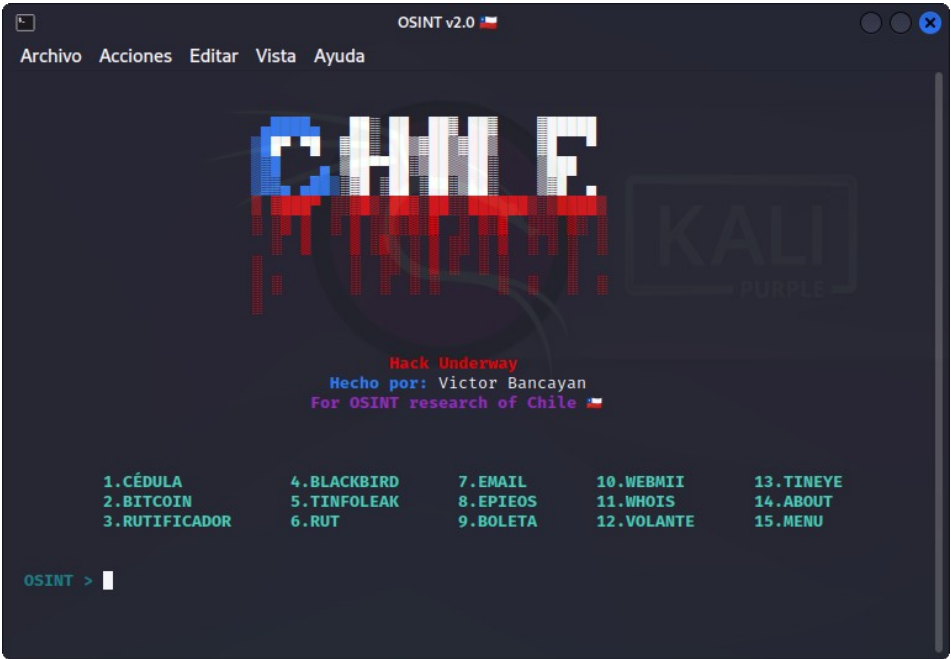
Subdirectora (E)
CENTRO DE INDUSTRIA Y CONSTRUCCION
REGIONAL TOLIMA

FECHA REGISTRO

La autenticidad de este documento puede ser verificada en el registro electrónico que se encuentra en la página web <http://certificados.sena.edu.co>, bajo el número [REDACTED].

Como pueden apreciar, nos muestra el certificado y demás detalles, como la firma electrónica, y otros datos.

Chile:



Al escoger la opción 1. (Cédula).

Quiero saber acerca de... Cambiar país Chile

Buscador de Personas por Nombre o Cédula Boletines Oficiales

Busca información pública sobre cualquier persona en Chile

Ingresar Apellidos y Nombres o Número de Cédula

[Accede al Buscador de Personas en Chile](#)

La información que estás buscando sobre cualquier persona en Chile con sólo ingresar un nombre completo o número de cédula.

Nombre	Cédula o RUN	
[Blurred Name]	[Blurred ID]	<input type="button" value="Ver Más"/>
[Blurred Name]	[Blurred ID]	<input type="button" value="Ver Más"/>
[Blurred Name]	[Blurred ID]	<input type="button" value="Ver Más"/>
[Blurred Name]	[Blurred ID]	<input type="button" value="Ver Más"/>
[Blurred Name]	[Blurred ID]	<input type="button" value="Ver Más"/>
[Blurred Name]	[Blurred ID]	<input type="button" value="Ver Más"/>
[Blurred Name]	[Blurred ID]	<input type="button" value="Ver Más"/>
[Blurred Name]	[Blurred ID]	<input type="button" value="Ver Más"/>
[Blurred Name]	[Blurred ID]	<input type="button" value="Ver Más"/>

Nos muestra varios resultados, para una búsqueda precisa es con la cédula.

Argentina:



Escogemos la opción 4. (**Constancia CUIT**).

CUIT del Contribuyente:

Código de seguridad:

En este caso, tenemos que colocar el CUIT, y rellenar el recaptcha, para que detecte que somos personas, lo hacen para que no usen ilegalmente las consultas, aunque hay métodos de saltarse, pero en nuestro caso sólo haremos 1 consulta como ejemplo, para que aprecien la información que nos brinda.

VOLVER

IMPRIMIR PANTALLA



CONSTANCIA DE OPCIÓN

Régimen Simplificado para Pequeños Contribuyentes

CUIT:

BAHIA BLANCA
8000-BUENOS AIRES

020 - MONOTRIBUTO

CATEGORIA

A

MONOTRIBUTO SOCIAL LOCACION

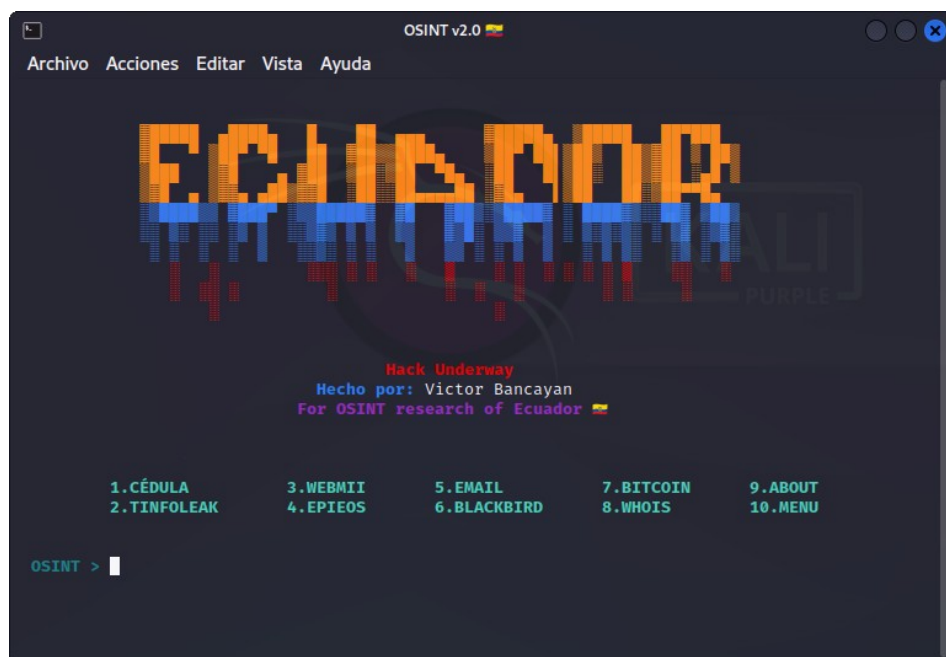
FECHA DE INICIO: 01-09-2019

5095 - REGIMEN SIMPLIFICADO IMPUESTO SOBRE INGRESOS BRUTOS ARBA

NA

Nos muestra datos de la cédula consultada.

Ecuador:



Escogemos la opción 1. (Cédula).

Para hacer este ejemplo hice algunas búsquedas en google, y me mostró legalmente muchas cédulas de Ecuador.

Dirección General de Registro Civil, Identificación y Cedulación

CONSULTA EL
ESTADO DE TU TRÁMITE

Búsqueda

Seleccione: ☐ Por NUT ☒ Por CÉDULA

Digite el número de cédula:

[Generar números nuevos](#)

Digite los números mostrados:

932512

Consultar

Notas:
- NUT: Número Único de Trámite
* Campos obligatorios

BIENVENIDO

La Dirección General del Registro Civil, Identificación y Cedulación pone a disposición de los usuarios la consulta en línea del estado de su trámite, previa a la obtención de su cédula de identidad.

La única institución que está presente
a lo largo de su vida

Para el correcto funcionamiento de la aplicación se recomienda usar: Mozilla Firefox versión 15, Microsoft Internet Explorer 9, MAC Safari 5, Google Chrome 35, o las versiones superiores de estos navegadores.

Al poner la cédula y los números del recaptcha. Nos muestra la siguiente información.

Resultados

Fecha trámite:

NUT:

Cédula solicitante:

Nombres solicitante:

Cédula trámite:

Nombres trámite:

Estado:

1 de 2

Resultados

Fecha trámite:

NUT:

Cédula solicitante:

Nombres solicitante:

Cédula trámite:

Nombres trámite:

Estado:

2 de 2

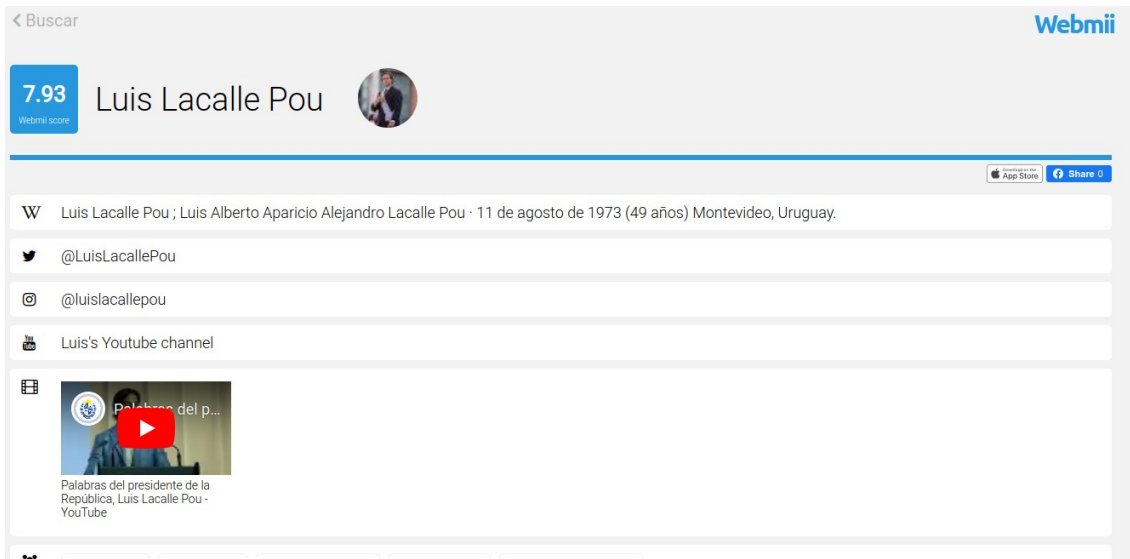
Uruguay:



Escogemos la opción 3. (**Webmii**).

Para ver información pública.






Bolivia:



Elegimos la opción 3. (Email con Epieos).

 Google account finder will show you if the requested email is linked to a Google account and/or if the person left reviews on Google Maps.

Query

Photo

Name

Id

Last Update

Services

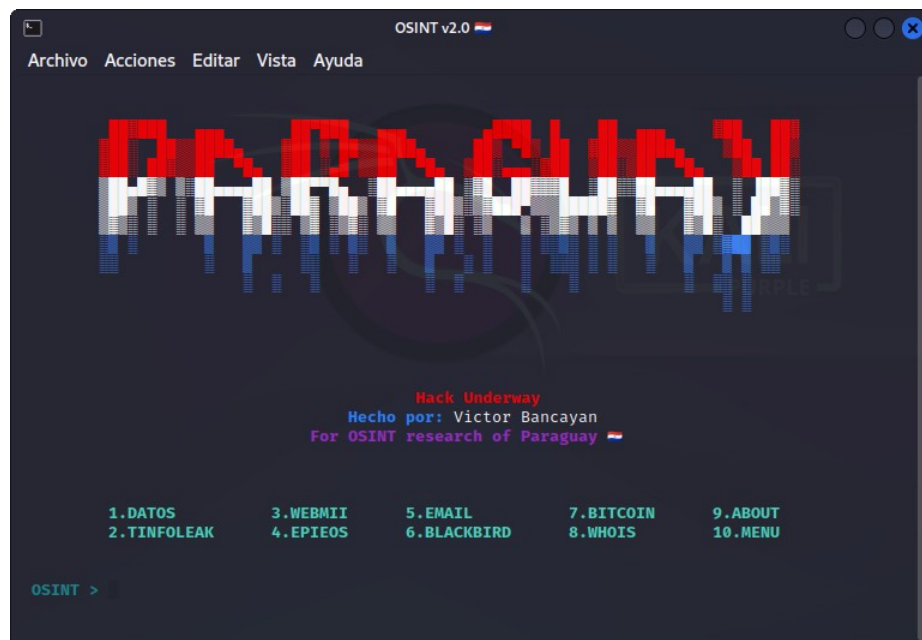
Google Maps

Google Calendar

Google Plus Archive

Nos muestra información de un correo corporativo de mozilla Bolivia.

Paraguay:

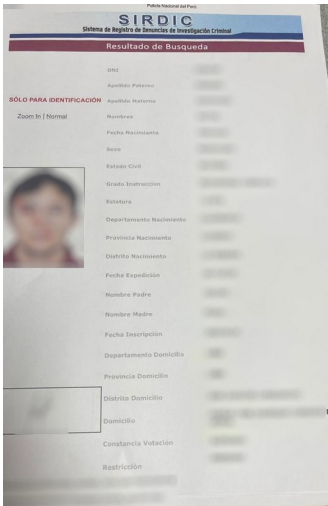


Escogemos la opción 1. (**Datos**).

Vemos en la imagen anterior una brecha de seguridad que sufrió Twitter hace unos meses, al tener acceso a ciertas bases de datos nos brindan la posibilidad de hacer OSINT, de una manera más rápida y precisa, estas bases de datos son ofrecidas en la dark web e incluso en grupos de telegram y otros.

Me enteré de un caso que un grupo de hackers tuvieron una discusión con un usuario en un foro que se usa para vender e intercambiar db, al tener varias bases de datos, estos usuarios hicieron pública la información de su objetivo, ya que prácticamente lo tenían todo a la mano.

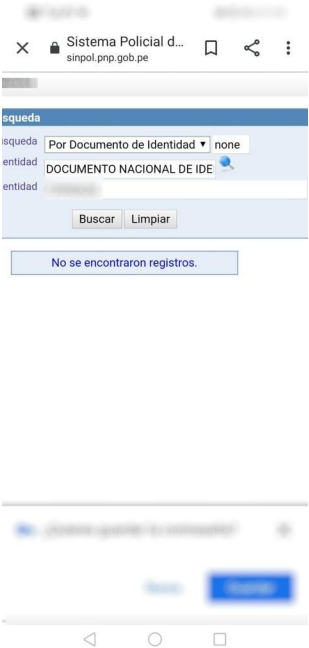
Los policías tiene acceso a la información de la siguiente imagen.




Salen todos sus datos personales, foto, firma, huella, etc...



También los policías tienen acceso a ver si una persona tiene orden de captura (RQ).



En realidad a las personas que tienen cargos en el gobierno, tienen mucho acceso a información privada y se les hace mucho más fácil acceder a información para hacer OSINT, es la ventaja que tienen las autoridades, aparte de no meterse en problemas ya que ellos tienen cierta autorización a esos datos, siendo ellos la autoridad.

	CEDULA:
	NOMBRE:
	CONDICION DE CIUDADANO:
	FECHA DE NACIMIENTO:
	LUGAR DE NACIMIENTO:
	NACIONALIDAD:
	ESTADO CIVIL:
	CONYUGE:
	NOMBRE PADRE:
	NACIONALIDAD PADRE:
	NOMBRE DE LA MADRE:
	NACIONALIDAD MADRE:
	DOMICILIO:
	CALLES DE DOMICILIO:
	NUMERO DE CASA:
FECHA DE MATRIMONIO:	
LUGAR DE MATRIMONIO:	
FECHA DEFUNCION:	
FECHA INSCRIPCION DEFUNCION:	
SEXO:	
GENERO:	

Cuando trabajas para el gobierno, podrías obtener datos legales de cualquier persona dentro del territorio autorizado.

Se imaginan a cuánta información tienen acceso organizaciones como la CIA, FBI, NSA, NASA, etc.

NUMERORUC:	REGISTROS
PERSONASOCIEDAD: PNL	
RAZONSOCIAL:	
OBLIGADO: N	
FECHAINICIOACTIVIDADES:	
FECHAACTUALIZACION:	VALOR
	VALOR
	VALOR
ACTIVIDADECONOMICAPRINCIPAL:	
ESTADOPERSONANATURAL: ACTIVO	
	VALOR
TIPOCONTRIBUYENTE: PERSONAS NATURALES	
CLASECONTRIBUYENTE: OTROS	
	DETALLE
	ITEMS
	REGISTROS
NUMERORUC:	
NUMEROESTABLECIMIENTO: 1	
	VALOR
ESTADOESTABLECIMIENTO: ABIERTO	
CALLE:	
INTERSECCION:	
NUMERO:	
TIPOESTABLECIMIENTO: MATRIZ	
	REGISTROS
NUMERORUC:	
MARCALISTABLANCA: S	
	REGISTROS
	VALOR
S: S	

Podríamos poner mucha más información, pero se que se aclararon varias dudas y que se quedan con la base a la hora de buscar información para OSINT.

CORREOS ELECTRÓNICOS

Veremos cómo obtener información de correos electrónicos.

Tener información, a qué cuentas está asociada correos electrónicos.

Además de ver si tiene brechas de seguridad, entre otros temas.



Motor de búsqueda de fugas de datos:

- [Leak.sx](#)
- [dehashed](#)
- [Cryptome](#)
- [Intelligence X](#)
- [GlobaLeaks](#): Es un programa informático gratuito y de código abierto destinado a facilitar iniciativas de denuncia seguras y anónimas.
- [leak-lookup](#)
- [Al Jazeera's Investigative Unit](#)
- [leakcheck](#)
- [ghostproject](#)
- [nuclearleaks](#)
- [spycloud](#)
- [leakpeek](#)
- [BreachForums](#)
- [haveibeenpwned](#): Compruebe si su correo electrónico o su teléfono se encuentran en una fuga de datos
- [snusbase](#)
- [Have I Been Sold?](#)
- [leakhispano](#)
- [Fasterbroadband](#)
- [WikiLeaks](#)

- [F-Secure Identity Theft Checker](#)
- [Joe Black Security](#)
- [Firefox Monitor](#)
- [Black Kite](#)
- [Amibreached](#)
- [scatteredsecrets](#)
- [inoitsu](#)
- [Password Checkup by Google](#)
- [Identity Leak Checker](#)
- [Personal Data Leak Checker](#)

have i been pwned:


<https://haveibeenpwned.com/>

Nos muestra brechas de seguridad, mediante un correo electrónico.

Quiero decir, si el correo al cuál te has registrado en una plataforma que ha sufrido de un hackeo de su base de datos, y esta se ha expuesto en internet, aparecerán en esta plataforma, y te avisará cuál ha sido comprometida, para que tengas en cuenta mediante OSINT, en cuales está registrado un objetivo, en caso no lo encuentre es que el correo no ha sido comprometido en las fugas de información recientes.


Oh no — pwned!

Pwned in 9 data breaches and found no pastes (subscribe to search sensitive breaches)




3 Steps to better security


[Start using 1Password.com](https://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.

Why 1Password?







[Donate](#)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.


Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.




Canva: In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Email addresses, Geographic locations, Names, Passwords, Usernames



Cit0day (unverified): In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Passwords



Covve: In February 2020, a massive trove of personal information referred to as "db8151dd" was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. Later identified as originating from the Covve contacts app, the exposed data included extensive personal information and interactions between Covve users and their contacts. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Job titles, Names, Phone numbers, Physical addresses, Social media profiles



Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles



Gravatar: In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars. 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, Gravatar release an FAQ detailing the incident.

Compromised data: Email addresses, Names, Usernames



LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords



LinkedIn Scraped Data: During the first half of 2021, LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on [An update on report of scraped data](#).

Compromised data: Education levels, Email addresses, Genders, Geographic locations, Job titles, Names, Social media profiles



ShareThis: In July 2018, the social bookmarking and sharing service ShareThis suffered a data breach. The incident exposed 41 million unique email addresses alongside names and in some cases, dates of birth and password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by dehashed.com.

Compromised data: Dates of birth, Email addresses, Names, Passwords



Stratfor: In December 2011, "Anonymous" attacked the global intelligence company known as "Stratfor" and consequently disclosed a veritable treasure trove of data including hundreds of gigabytes of email and tens of thousands of credit card details which were promptly used by the attackers to make charitable donations (among other uses). The breach also included 860,000 user accounts complete with email address, time zone, some internal system data and MD5 hashed passwords with no salt.

Compromised data: Credit cards, Email addresses, Names, Passwords, Phone numbers, Physical addresses, Usernames

El correo que pusimos, tiene 9 brechas de seguridad, ya que se ha registrado en 9 plataformas, de los cuales han sufrido hackeos, por ello es recomendable actualizar las contraseñas de esas plataformas, que ha sido comprometidas, siempre es bueno estar al tanto de las brechas, ya que en el OSINT, se usa este método para tener toda la información comprometida, arriba dejé varios enlaces, pueden ir probando, la que más les sea útil.

Si probara todas la herramientas y sitios web, no terminaría nunca este libro, ya que hay miles de sitios y herramientas, donde se puede obtener información.

Investigación de búsqueda de correo electrónico:

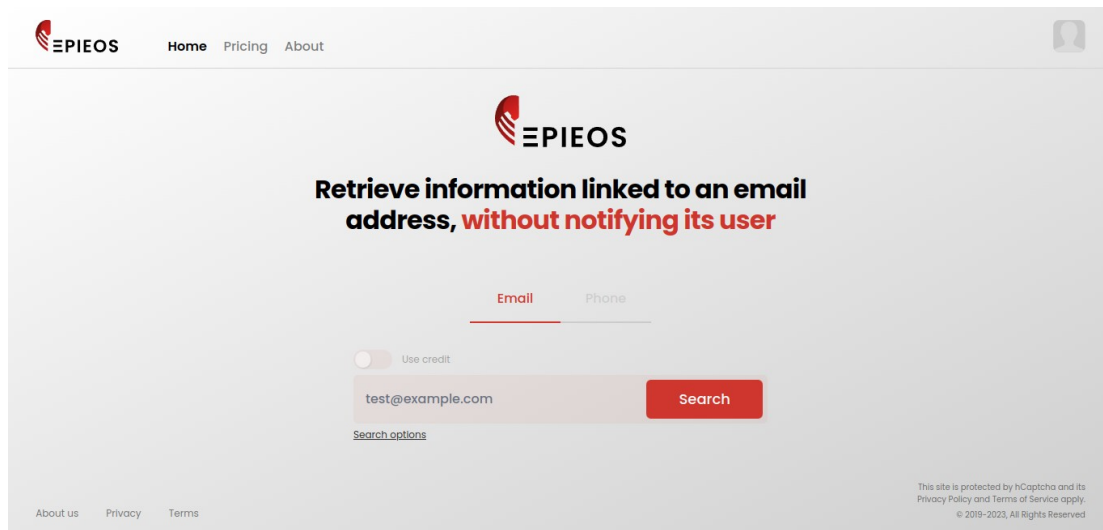
- Los nombres de usuario suelen asociarse a correos electrónicos
- Realice consultas en Google / configure alertas de Google
- Compruebe los datos filtrados (<https://haveibeenpwned.com>)
- Encontrar una dirección de correo electrónico privada (construcciones y suposiciones, socmint)
- Buscar direcciones de correo electrónico profesionales (www.hunter.io)
- Ejecutar el validador de correo electrónico (www.email-validator.net)
- Comprobación inversa del correo electrónico (www.pipl.com)
- Comprobar el proveedor de correo electrónico para los correos electrónicos comerciales (www.mxtoolbox.com)
- Comprobar listas negras (www.mxtoolbox.com)
- <https://github.com/thewhiteh4t/pwnedOrNot>
- <https://github.com/khast3x/h8mail>

Como lo vimos anteriormente en la sección de Data Breach, usaremos correos para obtener cierta información.

Epieos:

<https://epieos.com/>

Recuperar información vinculada a una dirección de correo electrónico, sin avisar a su usuario.



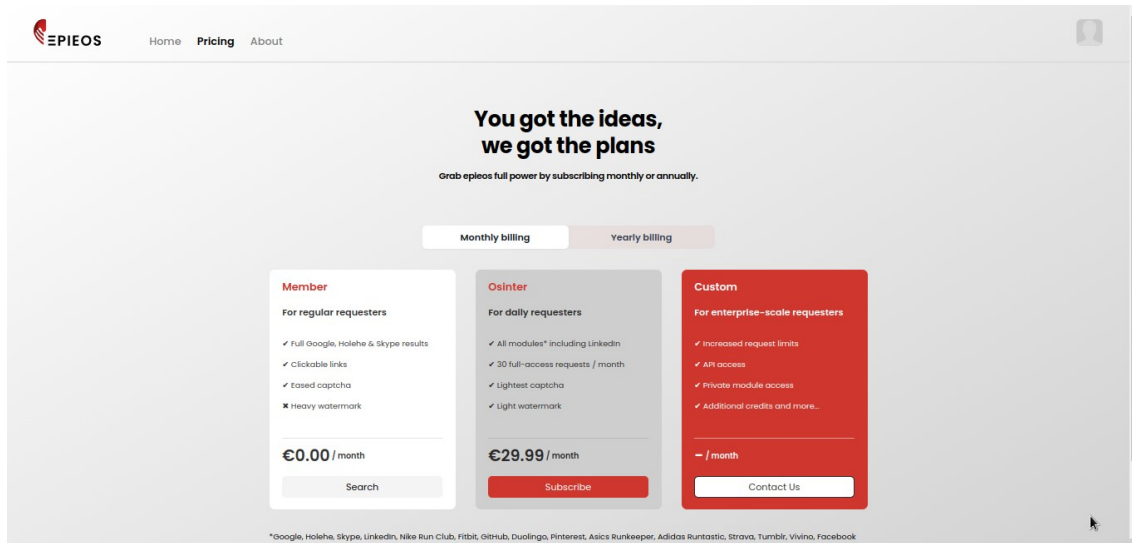
The screenshot shows the Epieos website interface. At the top, there is a navigation bar with the Epieos logo and links for Home, Pricing, and About. Below the navigation bar, the main heading reads "Retrieve information linked to an email address, without notifying its user". There are two input fields: "Email" and "Phone". The "Email" field is active and contains the text "test@example.com". Below the input fields, there is a toggle switch labeled "Use credit" which is currently turned off. A red "Search" button is positioned to the right of the input fields. Below the search button, there is a link for "Search options". At the bottom of the page, there are links for "About us", "Privacy", and "Terms". A small disclaimer at the bottom right states: "This site is protected by hCaptcha and its Privacy Policy and Terms of Service apply. © 2019-2023, All Rights Reserved".

Brinda información de: Google, Holehe, Skype, LinkedIn, Nike Run Club, Fitbit, GitHub, Duolingo, Pinterest, Asics Runkeeper, Adidas Runtastic, Strava, Tumblr, Vivino, Facebook...

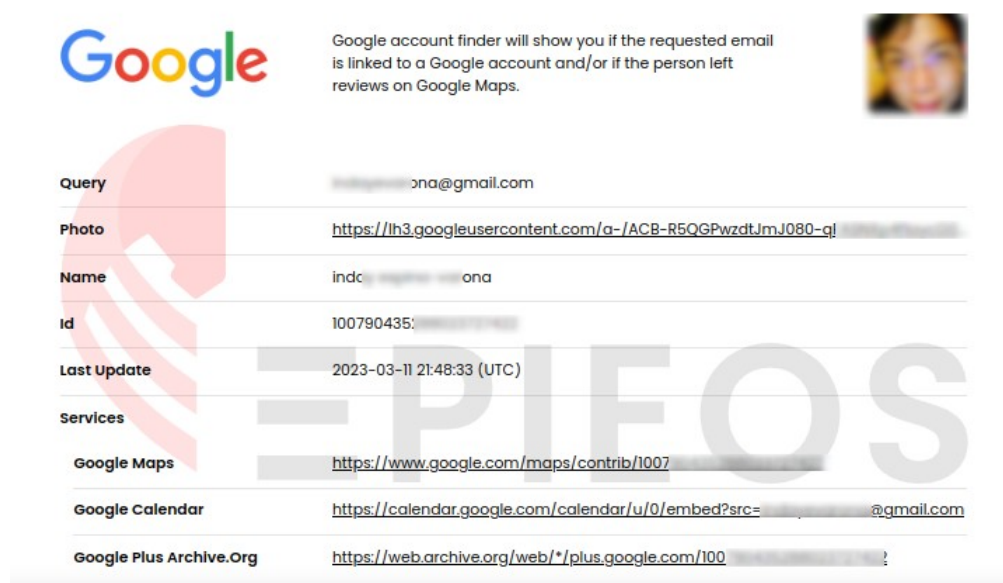
Registrarse es gratis, pero también tiene opciones premium.

<https://epieos.com/pricing>

Hay planes en esta plataforma, ya que hay información que no es visible al consultarlo, para eso debemos de tener una suscripción premium, por si quiere usar esta herramienta al 100%.




Haremos 2 búsquedas con correos diferentes para ver los resultados de ambos.




Nos muestra datos de su cuenta de Google, como foto, id, calendario, etc.


Eso muestra porque al momento de configurar su cuenta de gmail puso algunos datos en público.



This tool allows you to find the skype user linked to an email address.



Query	xxxxxxxxx@gmail.com
Photo	https://avatar.skype.com/v1/avatars/livxxxxxxxxx/public
Accounts	
Photo	https://avatar.skype.com/v1/avatars/livexxxxxxxxx/public
Name	xxxxxx
Id	xxxxxxxxxxxxxx
Contact Type	Skype4Consumer
Photo	https://avatar.skype.com/v1/avatars/xxxxxxxxx/public
Name	xxxxxxxxna
Id	xxxxxxxxxxna
Country	Philippines
City	Bacolod
Contact Type	Skype4Consumer




This tool allows you to check if an email address is used on several social networks or websites.


Query	xxxxxxxxx@gmail.com
Websites	spotify.com










Nos muestra información de Skype y también nos arroja que desde ese correo están usando una cuenta de Spotify.

Ahora veremos otro ejemplo, pero con otro correo.



This tool allows you to find a duolingo account linked to an email address.




Query	xxxxxxxxx@gmail.com
Photo	https://profile.picture.guy  Subscribe
Login	xxxxxxxxxxxxxxxx  Subscribe
Name	xxxxxx xxxxx xxxxxxx  Subscribe
Id	xxxxxxxxxxxxxxxx  Subscribe
Creation Date	2017-04-01  Subscribe
Learning Language	xxxxxx xxxxxxx xxxxx  Subscribe
From Language	xxxxxxxxxxxx  Subscribe
Activity 15 Days	xxxxxxxxxxxxxxxx  Subscribe
Profile	https://duolingo.com/profile/xxxxxxxxx  Subscribe

Para ver esa información completa nos pide una suscripción, ya que esta en privado.

También nos dio la información de Linkedin, vinculado a un correo.

Spokeo:


SPOKEO

[ABOUT](#)
[LOGIN](#)
[SIGN UP](#)

Reverse Email Lookup






NAMEEMAILPHONEADDRESS

SEARCH NOW


Lookup any email to see who owns it and to search for more information on the owner

- ✓ Uncover owner identity and location
- ✓ Lookup pics and social media profiles
- ✓ Search confidentially for instant results

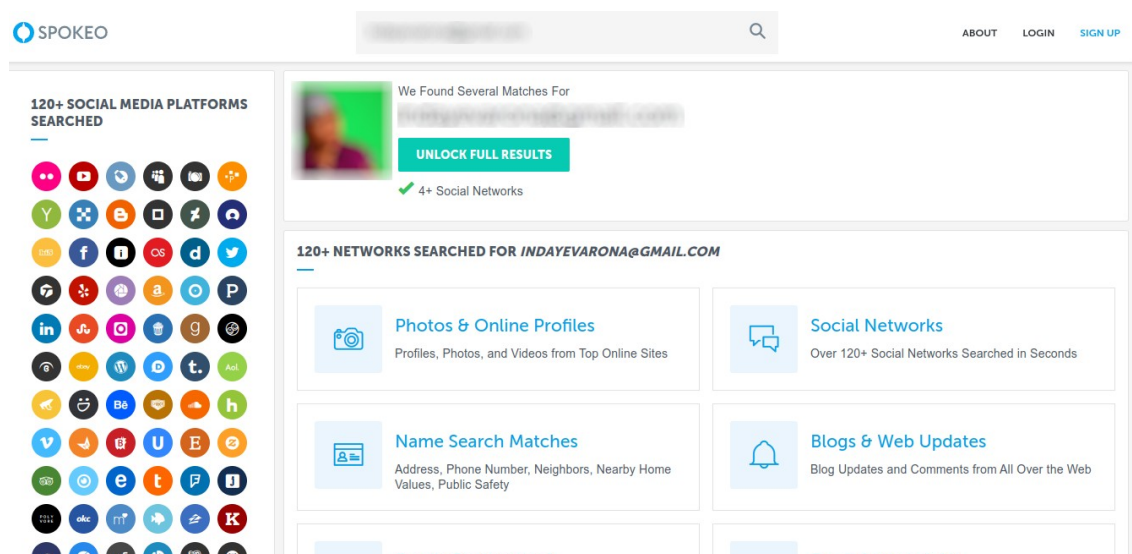
SPOKEO HAS BEEN FEATURED ON

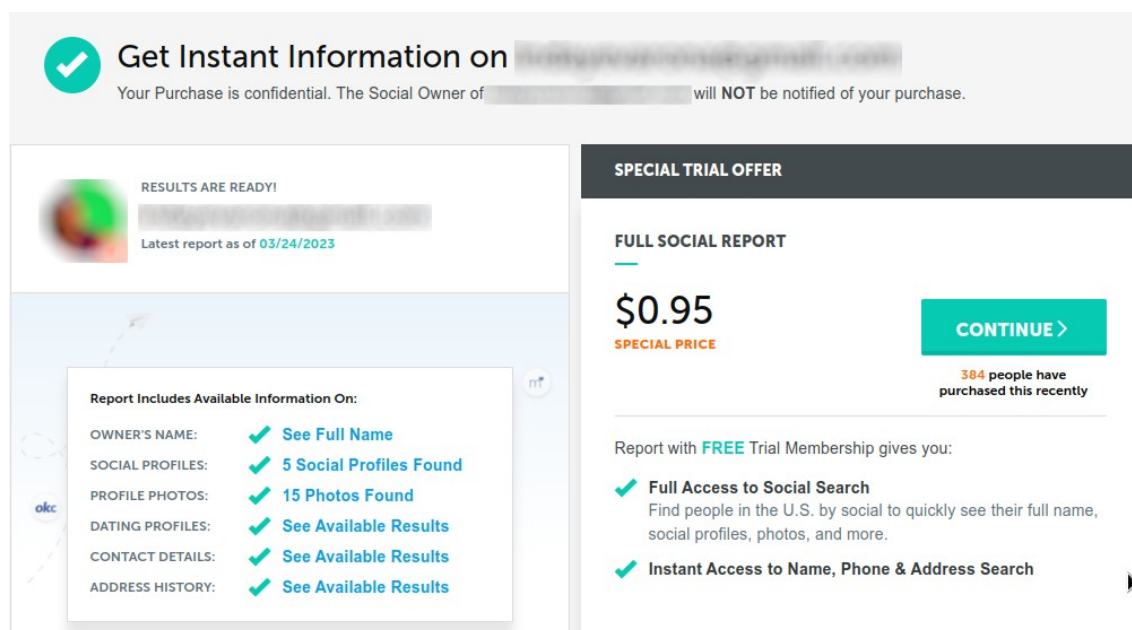
Disclaimer: Reference to these media organizations should not be construed to imply an endorsement of Spokeo or its products.



Con spokeo podemos hacer varias búsquedas, entre ellas lo que es el email.



Encontró 4 redes vinculadas al correo que pusimos.

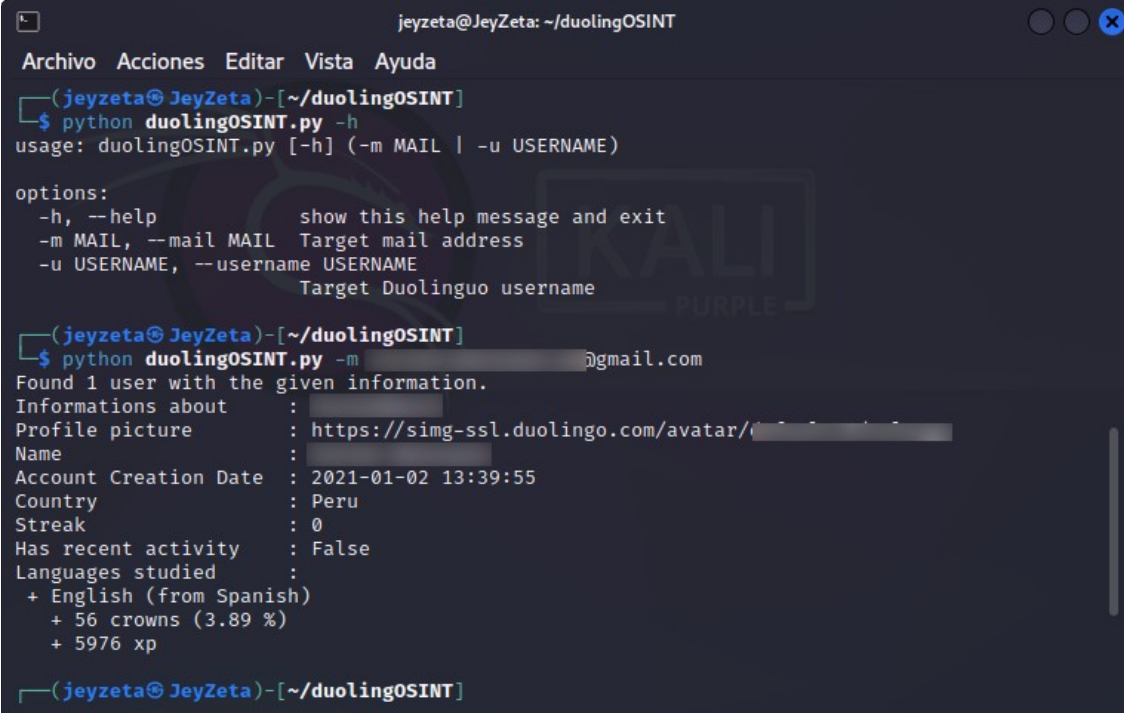


El precio es casi 1 dólar que cobra para acceder a la información encontrada, es muy cómodo desde mi punto de vista, así que recomiendo que lo prueben con sus correos para ver que tan efectivo es la búsqueda con esta herramienta online.

DuolingOSINT:

Es una herramienta para recopilar información sobre un usuario de Duolingo.

<https://github.com/ajuelosemmanuel/duolingOSINT>



```
jeyzeta@JeyZeta: ~/duolingOSINT
Archivo Acciones Editar Vista Ayuda
(jeyzeta@JeyZeta)-[~/duolingOSINT]
$ python duolingOSINT.py -h
usage: duolingOSINT.py [-h] (-m MAIL | -u USERNAME)

options:
  -h, --help            show this help message and exit
  -m MAIL, --mail MAIL  Target mail address
  -u USERNAME, --username USERNAME
                        Target Duolingo username

(jeyzeta@JeyZeta)-[~/duolingOSINT]
$ python duolingOSINT.py -m @gmail.com
Found 1 user with the given information.
Informations about : 
Profile picture    : https://img-ssl.duolingo.com/avatar/
Name               : 
Account Creation Date : 2021-01-02 13:39:55
Country            : Peru
Streak              : 0
Has recent activity : False
Languages studied  : 
+ English (from Spanish)
+ 56 crowns (3.89 %)
+ 5976 xp

(jeyzeta@JeyZeta)-[~/duolingOSINT]
```

Prot1ntelligence:

Es un script desarrollado en Python, le ayudará a obtener información sobre cuentas y usuarios de ProtonMail, direcciones IP de ProtonVPN, claves PGP de usuarios de ProtonMail, huellas digitales dejadas por el usuario de ProtonMail en la surface web y darkweb.

<https://github.com/C3n7ral051nt4g3ncy/Prot1ntelligence>


```
root@JeyZeta: /home/jeyzeta/ProtIntelligence
Archivo Acciones Editar Vista Ayuda
Input CAPITAL LETTER from each option to make choice!
A | B | C | D | E
Input choice: B

Checking server status

<Response [200]>
Status: Success!

Enter Target Email in quotation marks!(Example:"admin@protonmail.com"): darkmatterproject@protonmail.com

Processing request ...

https://onionlandsearchengine.com/search?q=dark4s5k7jw5zjgkm5wzo3zbvwpwvzi7gqo5kpzvzfggtcnze
xdu7gsyd.onion
https://www.thedarkmatterproject.org/
https://github.com/C3n7ral051nt4g3ncy/ProtIntelligence/blob/master/protintel.py
https://darkweb.wiki/scam-list/
https://www.gadgetgyani.com/top-best-onion-deep-web-sites/
https://codebeautify.org/jsonviewer/y239b5774
https://indico.cern.ch/event/686555/book-of-abstracts.pdf
https://softpanorama.org/Windows/windows_security.shtml
https://softpanorama.org/Windows/index.shtml
https://med.nyu.edu/research/boeke-lab/research/dark-matter-project

Continue [Y] or [N]: Y
Input CAPITAL LETTER from each option to make choice!
A | B | C | D | E
```

Esta herramienta tiene muchas más funciones (A, B, C, D, E)

Dependiendo lo que quieran encontrar ponen la letra en mayúscula, en el repositorio están los detalles de esta herramienta.

Maryan:

Es un Framework de código abierto basado en OSINT y recopilación de datos. Está diseñado para proporcionar un entorno robusto para recopilar datos de fuentes abiertas y motores de búsqueda de forma rápida y exhaustiva.

<https://github.com/saeeddhqan/Maryam>


```
root@JeyZeta: /home/jeyzeta/Maryam
Archivo Acciones Editar Vista Ayuda

yahoo
metacrawler
baidu
startpage
qwant
duckduckgo
hunter
gigablast
github
keyserver

Examples:
email_search -q microsoft.com -e bing --output
email_search -q owasp.org -e google,bing,yahoo -l 20 -t 3 --output
[maryam][default] > email_search -q gmail.com -e bing,google,yahoo --output
[*] [BING] Searching in 1 page ...
[*] [GOOGLE] Searching in 1 page ...
[*] [GOOGLE] Searching in 2 page ...
[*] [YAHOO] Searching in 1 page ...
[*] [GOOGLE] Searching in 3 page ...
[*] [YAHOO] Searching in 2 page ...
[*] [YAHOO] Searching in 3 page ...
[*] EMAILS
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
[*]
```

Nos muestra correos obtenidos por google, bing, yahoo, pueden buscar de dsitintos buscadores, depende de lo que deseen encontrar personalizaran el comando para que la herramienta haga la búsqueda y muestre los resultados.

Holehe:

Permite comprobar si el correo se utiliza en diferentes sitios como twitter, instagram y recuperará información sobre los sitios con la función de contraseña olvidada.

Anteriormente vimos en epieos algo parecido, pero en este caso lo haremos con esta herramienta, desde nuestra terminal.

<https://github.com/megadose/holehe>

The screenshot displays the Leak-Lookup web application. The top navigation bar includes a search icon and social media links. The left sidebar contains a menu with options: Dashboard, Search, Databases, API, Pricing, Documentation, Support, Account, Settings, and Sign out. The main dashboard area shows four key metrics: Total Records (25,095,223,249), Total Breaches (3,961), Breaches Indexed (0), and Available Credits (0). Below these is a Search History section with a search bar and a table of queries. The Results section shows a list of search results for the query 'collection-1'. The results are displayed in a grid format, showing the date indexed, total records, and the number of records found and columns for each result.

Dashboard Metrics:

- Total Records: 25,095,223,249
- Total Breaches: 3,961
- Breaches Indexed: 0
- Available Credits: 0

Search History:

Query	Type	Results	Date	Options
No data available in table				

Results:

Results found: 6/6

Filter Results:

Columns	Count
email_address	6
password	5
userid	1
secret	1
fullname	1
address	1

Search Results:

- collection-1**
Date Indexed: 2019-01-24
Total Records: 2,147,483,647
1 Record found, 2 Columns
- collection-4-eu**
Date Indexed: 2019-03-13
Total Records: 2,147,483,519
1 Record found, 2 Columns
- collection-4-u**
Date Indexed: 2019-04-03
Total Records: 2,010,963,743
1 Record found, 2 Columns
- gonitro.com**
Date Indexed: 2021-04-20
Total Records: 77,173,015
1 Record found, 4 Columns
- linkedin.com**
Date Indexed: 2017-02-20
Total Records: 250,778,227
1 Record found, 2 Columns
- peopledatalabs**
Date Indexed: 2020-12-16
Total Records: 416,726,546
1 Record found, 3 Columns

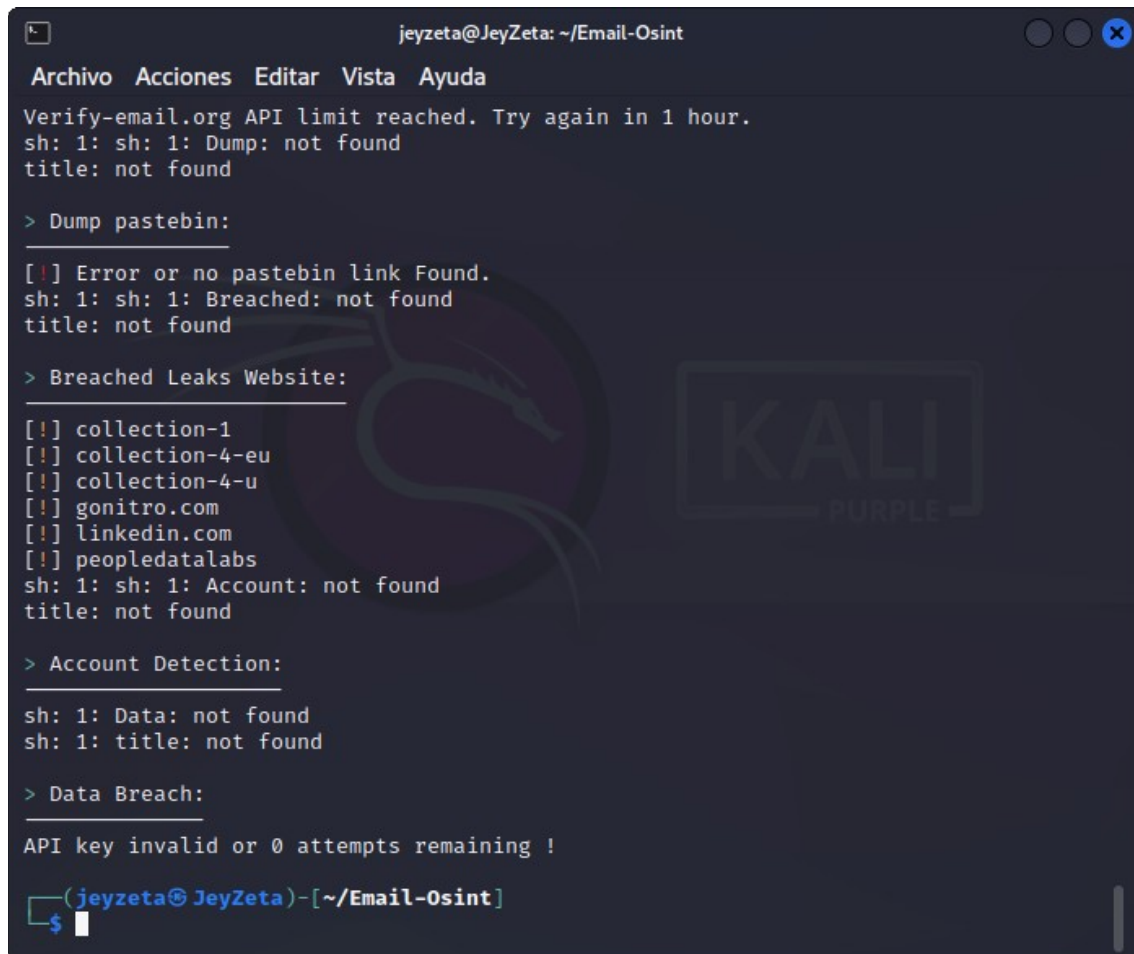
Al buscar un correo, nos muestra que el correo ha sido comprometido en 6 plataformas.

En caso quieran más detalles esta plataforma ofrece una suscripción premium, con más características.

Email OSINT:

Es una herramienta OSINT para correos electrónicos. Le ayuda a recopilar información sobre el correo electrónico de destino.

<https://github.com/KanekiWeb/Email-OSint>



```
jeyzeta@JeyZeta: ~/Email-OSint
Archivo Acciones Editar Vista Ayuda
Verify-email.org API limit reached. Try again in 1 hour.
sh: 1: sh: 1: Dump: not found
title: not found

> Dump pastebin:
[!] Error or no pastebin link Found.
sh: 1: sh: 1: Breached: not found
title: not found

> Breached Leaks Website:
[!] collection-1
[!] collection-4-eu
[!] collection-4-u
[!] gonitro.com
[!] linkedin.com
[!] peopledatalabs
sh: 1: sh: 1: Account: not found
title: not found

> Account Detection:
sh: 1: Data: not found
sh: 1: title: not found

> Data Breach:
API key invalid or 0 attempts remaining !

(jeyzeta@JeyZeta)-[~/Email-OSint]
```

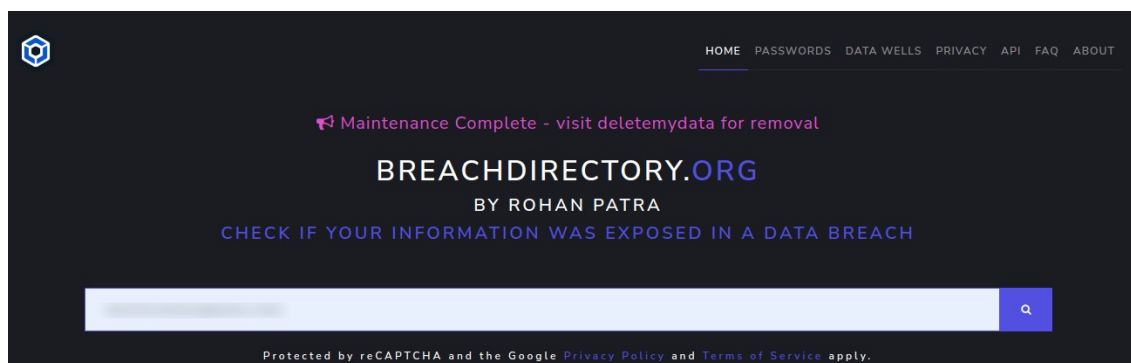
Esta herramienta nos muestra en forma de terminal, las fugas del correo electrónico.

Ahora veremos otra que es una plataforma parecida a la que vimos anteriormente.

Breachdirectory:

Es una web, para ver si ha sufrido una fuga de datos por medio del username, email y phone.

<https://breachdirectory.org/>



Mosint:

Es la herramienta OSINT más rápida para correos electrónicos. Le ayuda a recopilar información sobre el correo electrónico de destino.

<https://github.com/alpkeskin/mosint>

```
jeyzeta@JeyZeta: ~/mosint
Archivo Acciones Editar Vista Ayuda

(jeyzeta@JeyZeta)-[~/mosint]
$ go run main.go -h

mosint

v2.3
https://github.com/alpkeskin/
Now: Wednesday, 10 May 2023
0% |
An automated e-mail OSINT tool

Usage:
mosint [email] [flags]

Flags:
-h, --help  help for mosint
```

Para usar esta herramienta al 100%, deben tener cuenta las siguientes plataformas, ya que requiere API KEY.

Services (APIs):

Service	Function	Status
ipapi.co - Public	More Information About Domain	✓
hunter.io - Public	Related Emails	✓ 🔑
emailrep.io - Public	Breached Sites Names	✓ 🔑
scylla.so - Public	Database Leaks	⚠️
psbtmp.ws - Public	Pastebin Dumps	✓ 🔑
Intelligence X	Password Leaks	✓ 🔑
BreachDirectory	Password Leaks	✓ 🔑

Antes de seguir, dejare un texto sobre la API KEY.

API KEY:

La clave de API es un identificador único que se utiliza para autenticar solicitudes asociadas a tu proyecto con fines de uso y facturación.

[https://developers.google.com/maps/documentation/javascript/get-api-key?
hl=es](https://developers.google.com/maps/documentation/javascript/get-api-key?hl=es)

Si te dedicas al OSINT, programación, ciberseguridad y otras áreas, es necesario saber estos términos y tener cuentas en diferentes plataformas para buscar la información que nos sea útil, en este caso para temas de investigación OSINT.

REQUIREMENTS:

Existe una forma mucho más conveniente para descargar e instalar los paquetes necesarios para un proyecto Python. Involucra utilizar un archivo de texto (llamado `requirements.txt`), en el cual se anotan los paquetes para que pip se encargue de instalarlos de forma automática.

El archivo *requirements.txt* permite automatizar la instalación de paquetes.

Por ejemplo si el proyecto subido a GitHub, tiene varios paquetes que son necesarios para su funcionamiento.

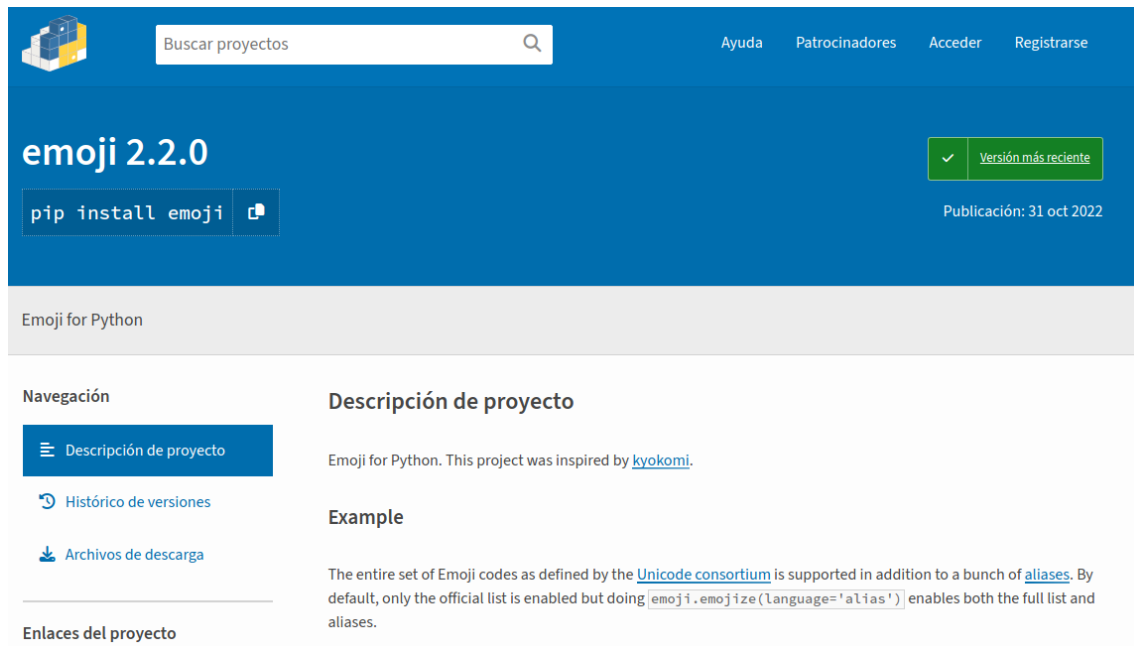
<https://pypi.org/project/emoji/>

No vamos a estar ejecutando cada paquete para instalarlo individualmente.

```
pip install emoji
```

```
pip install colorama
```

```
pip install shodan
```

The screenshot shows the PyPI project page for 'emoji 2.2.0'. At the top, there's a search bar and navigation links like 'Ayuda', 'Patrocinadores', 'Acceder', and 'Registrarse'. The main header features the package name 'emoji 2.2.0' and a 'pip install emoji' button. A green badge indicates it's the 'Versión más reciente' (latest version), and the release date is '31 oct 2022'. Below the header, the description states 'Emoji for Python'. The left sidebar contains navigation links: 'Descripción de proyecto' (selected), 'Histórico de versiones', and 'Archivos de descarga'. The main content area shows the project description, an example of using the emoji module with aliases, and a list of project links.

Para automatizar el proceso de la instalación de paquetes, se crea un archivo requirements.txt

- *Para instalar una versión específica.*

package==version

- *Para instalar una versión igual o superior.*

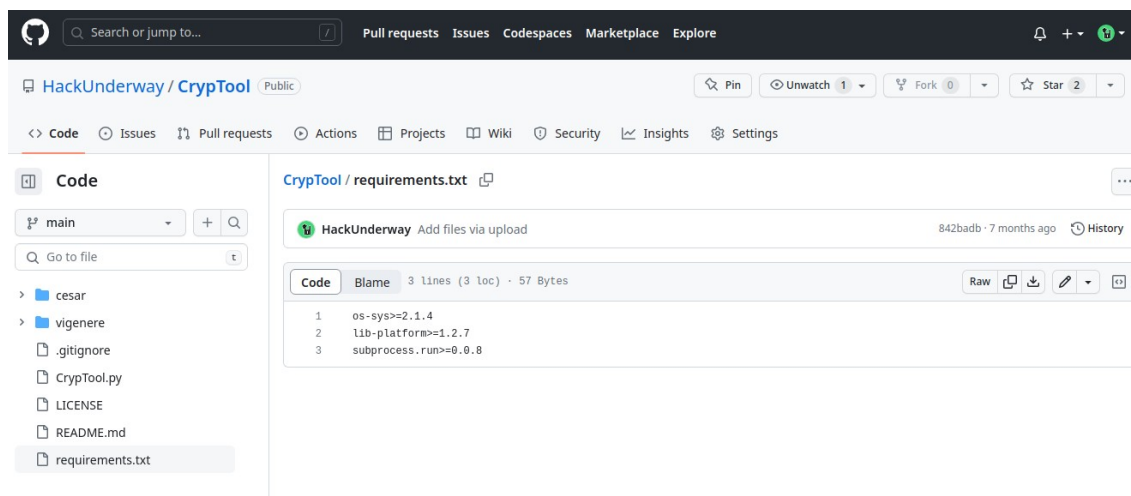
package>=version

- *Para instalar la versión más reciente.*

package

Por eso, cuando clonan un repositorio en GitHub, normalmente ven un archivo txt con los requerimientos, y se instala dependiendo la versión de pip instalada.

Ejemplo: pip3 install -r requirements.txt



<https://rukbottoland.com/blog/como-instalar-paquetes-python-con-requirements.txt/>

<https://www.delftstack.com/es/howto/python/python-create-requirements.txt/>

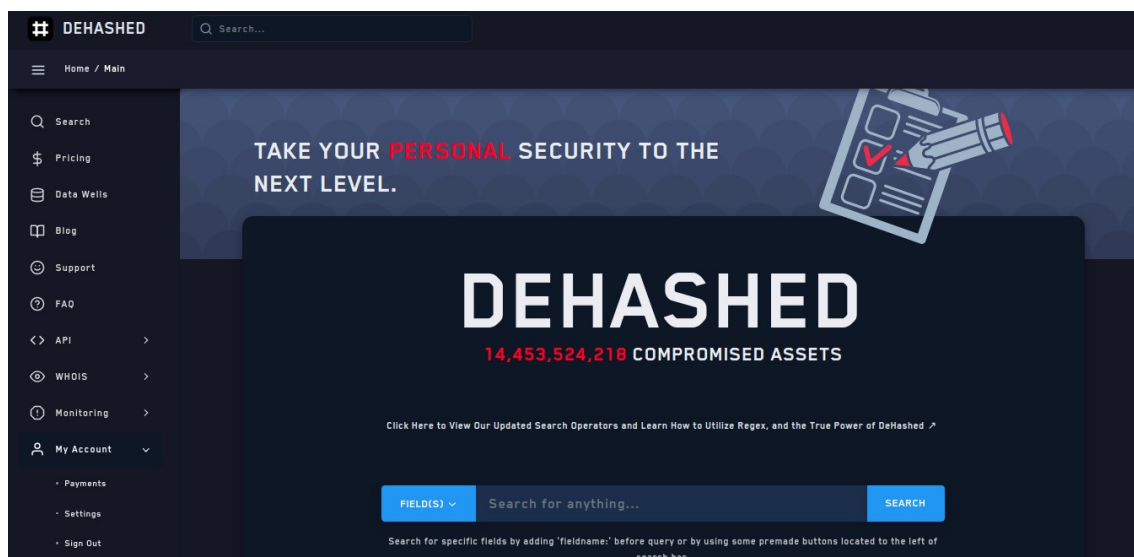
Espero que les hallan podido despejar algunas dudas y disculpen por la interrupción, ahora sigamos.

DeHashed:

Proporciona escaneos gratuitos de la Deep Web (web profunda) y protección contra fugas de credenciales. Un moderno motor de búsqueda de activos personales creado para analistas de seguridad, periodistas, empresas de seguridad y gente corriente para ayudar a proteger cuentas y proporcionar información sobre activos comprometidos. Alertas y notificaciones de infracciones gratuitas.

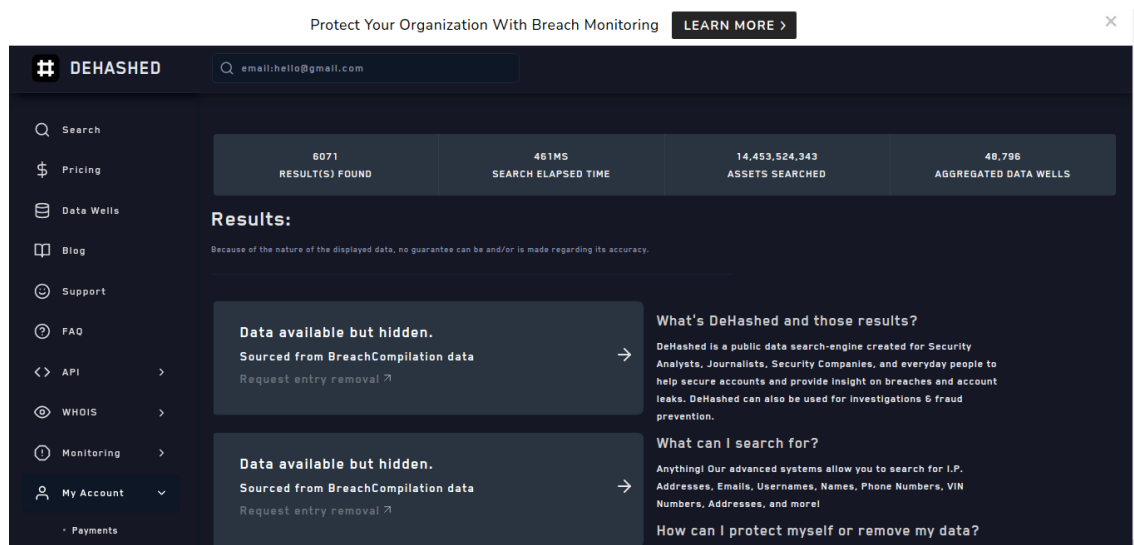
Tiene opción free y premium, es una buena opción nuestras investigaciones OSINT.

<https://dehashed.com/>



En este caso sólo daré un ejemplo de la opción free. En caso se dediquen profesionalmente a OSINT, podrían obtener los planes dependiendo a sus necesidades.





GHunt:

Es una herramienta OSINT modulable diseñada para evolucionar a lo largo de los años e incorpora muchas técnicas para investigar cuentas u objetos de Google.

Actualmente se centra en OSINT, pero cualquier uso relacionado con Google es posible.

<https://github.com/mxrch/GHunt>

¿Qué puede encontrar GHunt?

- Nombre del propietario
- Gaia ID
- Última vez que se editó el perfil
- Imagen de perfil (+ detectar imagen personalizada)
- Si la cuenta es un Hangouts Bot
- Servicios de Google activados (YouTube, Fotos, Mapas, News360, Hangouts, etc.)

166

- Posible canal de YouTube
- Posibles otros nombres de usuario
- Reseñas de Google Maps
- Posible ubicación física
- Eventos de Google Calendar
- Organizaciones (trabajo y educación)
- Correos electrónicos de contacto
- Teléfonos de contacto
- Direcciones

https://www.youtube.com/watch?v=XGE_uQe9IRQ

https://www.youtube.com/watch?v=05TrA_sJmis

```

root@JeyZeta: /home/jeyzeta/GHunt
Archivo Acciones Editar Vista Ayuda
(root@JeyZeta)-[/home/jeyzeta/GHunt]
# pipx run ghunt email @gmail.com --json user_data2.json

.d8888b. 888 888 888
d88P Y88b 888 888
888 888 888 888
888 8888888888 888 888 88888b. 888888
888 88888 888 888 888 888 "88b 888
888 888 888 888 888 888 888 888
Y88b d88P 888 888 Y88b 888 888 Y88b.
"Y8888P88 888 888 "Y8888 888 888 "Y888 v2

By: mxrch (🐦 @mxrchreborn)
Support my work on GitHub Sponsors ! ❤️

[+] Authenticated !
👤 Google Account data
Name : 
[+] Custom profile picture !
⇒ 
👤 
[-] Default cover picture
Last profile edit : 

```

Enlaces externos de OSINT DOJO:

[CentralOPS Email Tool](#)

[Defastra Email Search](#)

[Dehashed](#)

[Email OSINT Attack Surface](#)

[OSINT Email Methodology: Part 1](#)

[OSINT Email Methodology: Part 2](#)

[Epieos Email Tool](#)

[HaveIBeenPwned](#)

[Holehe](#)

[MXToolbox Blacklist Check](#)

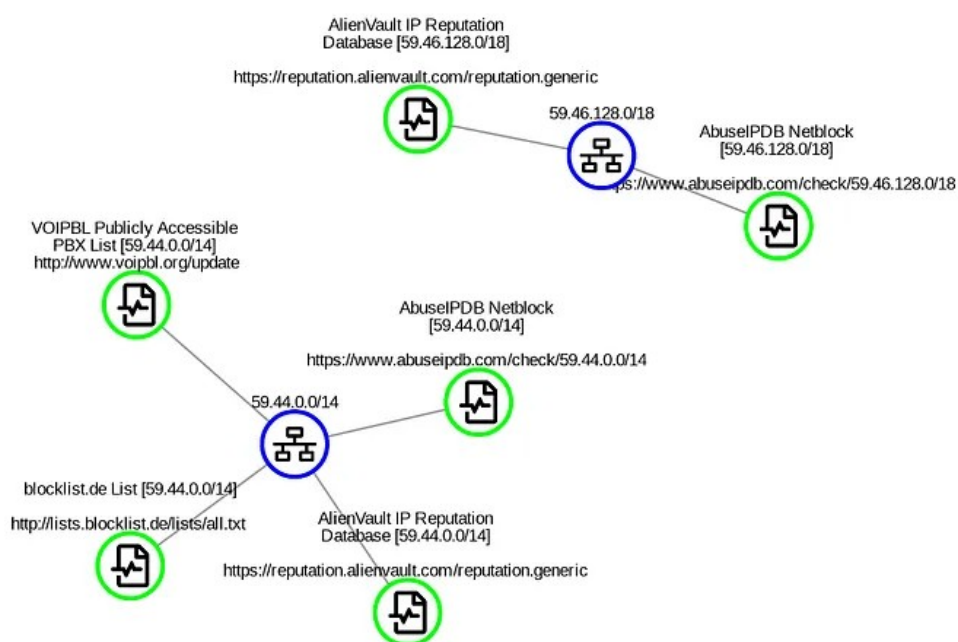
[MXToolbox Email Headers Tool](#)

[ThatsThem Email Lookup](#)

DIRECCIÓN IP

Haremos reconocimiento de IP, para ver información cómo la geolocalización, información de dispositivos.

Obtener datos relevantes de direcciones IP, con herramientas, API, tools desde la terminal.



OSINT para la investigación de direcciones IP:

- maxmind (<https://www.maxmind.com/en/geoip2-precision-demo>) (GeoIP)
- sypexgeo (<https://sypexgeo.net/ru/demo/>) (GeoIP)
- ipinfo (<https://ipinfo.io/map>) (GeoIP)
- domaintools (<https://whois.domaintools.com/>) (WHOIS)
- virustotal (<https://www.virustotal.com/>) (Virus Check)
- dnsdumpster (<https://dnsdumpster.com/>) (DNS)
- ptrarchive (http://ptrarchive.com/tools/lookup2.htm?ip=IP_HERE) (DNS)
- dnslytics (<https://dnslytics.com/reverse-ip/>) (DNS)
- viewdns (<https://viewdns.info/reverseip/>) (DNS)
- intelx (<https://intelx.io/>) (Leaks)
- leakix (<https://leakix.net/>) (Leaks)
- cyberhubarchive (<https://github.com/1x019/CyberHub-Archive>) (Skype Leaks)
- webresolver (<https://webresolver.nl/tools/ip2skype>) (Skype Leaks)
- talosintelligence (https://talosintelligence.com/reputation_center/lookup) (IP Quality)
- ipqualityscore (<https://www.ipqualityscore.com/>) (IP Quality)
- censys (<https://censys.io/ipv4>) (IoT)
- zoomeye (<https://www.zoomeye.org/>) (IoT)
- shodan (<https://www.shodan.io/>) (IoT)
- alienvault (<https://otx.alienvault.com/>) (Framework)
- spiderfoot (<https://www.spiderfoot.net/>) (Framework)
- robtex (<https://www.robtex.com/>) (Framework)

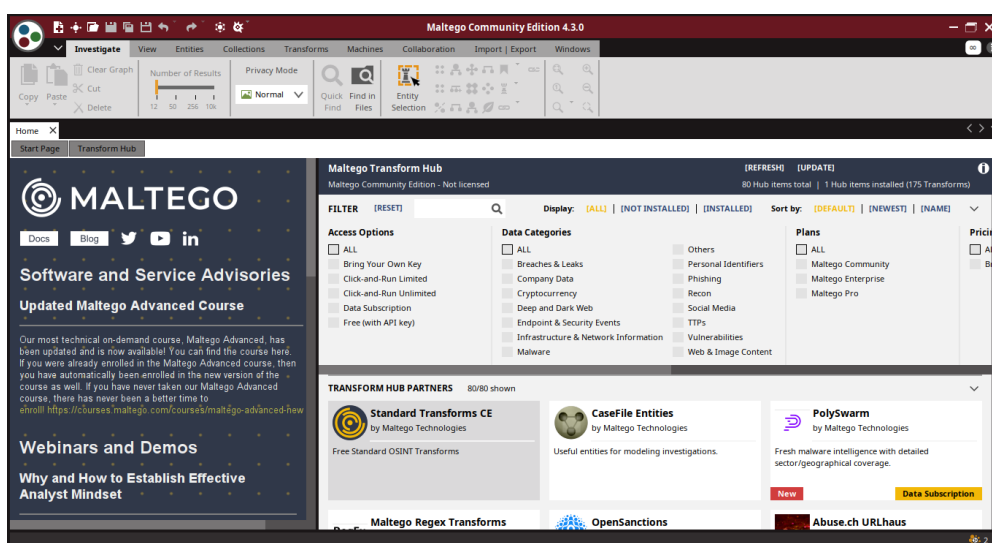
- threatcrowd (<https://www.threatcrowd.org/>) (Visualization)
- canarytokens (<http://canarytokens.org/generate>) (Logger IP)
- grabify (<https://grabify.link/>) (Logger IP)
- iplogger (<https://iplogger.ru/location-tracker/>) (Logger IP)
- iknowwhatyoudownload (<https://iknowwhatyoudownload.com/en/peer/>) (Torrents)

A lo largo de este libro vamos a ver que las herramientas muchas veces tienen varias funciones, por ejemplo hay paginas que puedes poner una ip, dominio, usuario, coordenadas, etc.

En muchos casos las herramientas privadas tienen ciertas funciones a destacar, por ejemplo Maltego que es muy popular al hacer OSINT, tiene su versión premium (de paga), que es recomendable su uso ya que tiene funciones avanzadas.

Maltego:

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



Obtener IP de usuarios:

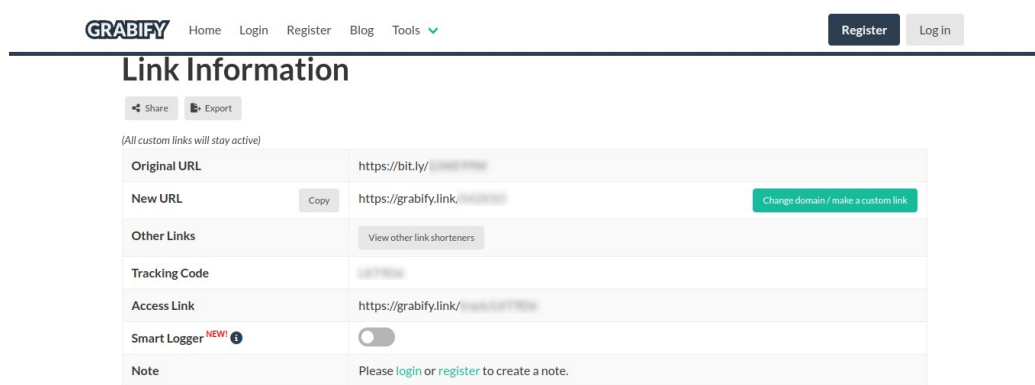
Grabify:

<https://grabify.link/>

Con esta herramienta online generamos una enlace, para que el que abra el enlace podamos saber su ubicación y otros detalles.



Nos debe generar como la siguiente imagen la nueva url y el acceso a la url, para ver los resultados.



Ahora vamos a acortar el enlace para que enmascararlo y no vean la url original.

<https://bitly.com/>





Ya está acortada la url, en este caso yo abriré ese enlace desde telegram.

Results: 3

Note: If you have posted your link on Facebook, Twitter, or in a URL shortener, you may see results from various "bots" (BitlyBot, FacebookBot, etc.)

Hide your IP! - Click here to hide your IP from Grabify and stay anonymous online.

☒ Hide Bots

Date/Time	IP/Provider	Country	User Agent	Referring URL	More
2020-08-21 17:28:45UTC	190.100.100.100	Peru Lima	Mozilla/5.0 (Linux; Android 10; Moto G (9) AppleWebKit/537.36 Chrome/85.0.4183.101)	android-app://org.telegram.messenger/	More Info

Nos muestra el resultado del dispositivo que abrió el enlace, en este caso desde Android, y me muestra más detalles a continuación.

Advanced Log	
Date/Time	2020-08-21 17:28:45UTC
IP Address	190.100.100.100
Country	Peru, Lima
Browser	Chrome Mobile (110.0.0.0)
Operating System	Android
Device	Motorola Moto G (9) 5G
User Agent	Mozilla/5.0 (Linux; Android 10; Moto G (9) AppleWebKit/537.36 Chrome/85.0.4183.101)
Referring URL	android-app://org.telegram.messenger/
Host Name	190.100.100.100
ISP	Telefonos del Peru S.A.S.

Close

Ahora veremos otra herramienta, parecida, pero esta nos muestra otros detalles.

IpLogger:

<https://iplogger.org/>

El mismo procedimiento, generamos la url, lo ocultamos con el acortador, se lo mandamos a la target, en este caso yo estoy poniendome de ejemplo, ya que no quiero perjudicar a nadie.

all data

Show bots

Unique only

Visitors

Analytics

2 clicks (unique)

2 clicks (total)

1

Datetime

IP/Provider

Country/City

Device

Referring pages

Device identificator

More info

Peru

Breña

Android

Chrome

https://iplogge

Smart data

Accuracy: ip

Extended data

copy

X

San Juan de Lurigancho

Rimac

El Agustino

Lima

Santa Beatriz

Lince

San Luis

San Borja

San Isidro

Magdalena

Pueblo Libre

San Miguel

La Perla

Carmen de la Legua-Reynoso

Independencia

accelerometer

Yes

adblock

Not

applepay

Not

googlepay

Supported

audiodevices

audioinput audioinput audioinput
videoinput videoinput audiooutput

battery

39%

screen

760 x 360 x 24

colorgamut

srgb

network

wifi

RTT

100 ms

hdr

Not

platform

Android

downlink

1.2 Mbps

incognito

Not

plugins

ECT

Yes

indexeddb

Yes

reducedmotion

Not

contrast

Not

language

es-419

sessionstorage

Yes

cookiesenabled

Yes

languages

es-419

timezone

America/Lima

darkmode

Not

localStorage

Yes

touchsupport

5 points

RAM

8 GB

monochrome

Not

vendor

Google Inc.

forcedcolors

Not

offset

-05:00

datetime

Tue Mar 21 2023 12:11:36 GMT-0500 (hora estándar de Perú)

gyroscope

Yes

opendatabase

Yes

date

Tue Mar 21 2023 12:11:36 GMT-0500 (hora estándar de Perú)

CPU Threads

8

pixelratio

2

browser

Chrome

isp

ISP

useragent

Mozilla/5.0 (Linux; Android 10; Redmi 9 5G) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.120 Mobile Safari/537.36

latitude

12.096111111111111

ip

196.206.10.146

longitude

-77.03611111111111

country

Peru

accuracy

ip

city

Breña

fingerprint

2a111111111111111111111111111111

state

Lima region

referer

https://iplogger.com

bot

Not

Nos muestra datos interesantes como que sistema operativo usa, cuanta ram tiene, el porcentaje de la batería, que navegador usa, coordenadas, etc.

Cabe recalcar que no es la ubicación exacta, para ello si tendrías que contratar servicios premium.

Canary tokens:

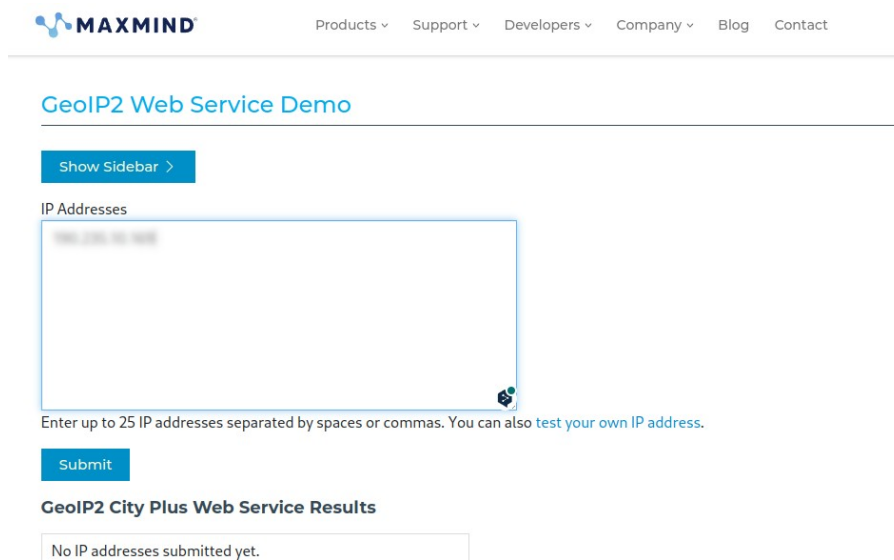
<https://canarytokens.org/generate>

Canary tokens es una web parecida a las que hemos visto, solo que esta trae otras alternativas interesantes, siempre es bueno usar varias alternativas e ir separando la información que necesitamos.

Obtener datos geográficos de una IP:

Maxmind:

<https://www.maxmind.com/en/geop2-precision-demo>

The screenshot shows the MaxMind website's GeolIP2 Web Service Demo page. At the top, there's a navigation bar with the MaxMind logo and links for Products, Support, Developers, Company, Blog, and Contact. Below the navigation bar, the page title "GeolIP2 Web Service Demo" is displayed. A "Show Sidebar >" button is visible. The main section is titled "IP Addresses" and contains a large text input field. Below the input field, there's a note: "Enter up to 25 IP addresses separated by spaces or commas. You can also [test your own IP address](#)." A "Submit" button is located below the input field. At the bottom, the section "GeolIP2 City Plus Web Service Results" shows a message: "No IP addresses submitted yet."

Al poner la IP, nos muestra ciertos resultados.

<div>Submit</div>									
GeolIP2 City Plus Web Service Results									
IP Address	Country Code	Location	Network	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain
192.168.1.1	PE	Lima, Lima, Peru, South America	192.168.1.1		12.0464, -77.0428	5	Telefonos del Peru	Telefonos del Peru	

Sypexgeo:

IPGeolocation:

```
root@JeyZeta: /home/jeyzeta/IPGeoLocation
Archivo Acciones Editar Vista Ayuda
root@JeyZeta:~# python ipgeolocation.py -t [REDACTED]
IPGeolocation 2.0.4

--[ Retrieve IP Geolocation information from ip-api.com
--[ Copyright (c) 2015-2016 maldevel (@maldevel)
--[ ip-api.com service will automatically ban any IP addresses doing over 150 requests per
  minute.

Target: [REDACTED]
IP: [REDACTED]
ASN: [REDACTED]
City: Lima
Country: Peru
Country Code: PE
ISP: [REDACTED]
Latitude: -[REDACTED]
Longitude: [REDACTED]
Organization: [REDACTED]
Region Code: LMA
Region Name: Lima
Timezone: America/Lima
Zip Code: [REDACTED]
Google Maps: http://www.google.com/[REDACTED]
```


Nos muestra datos de la IP, desde la terminal, con diferentes datos como coordenadas, ASN, país, etc.

IpGeo:

<https://github.com/z4l4mi/IpGeo>

IpGeo es una herramienta hecha en python para extraer direcciones IP de archivos de tráfico de red capturados (pcap/pcapng) y generar informes csv que contengan detalles sobre la geolocalización de cada ip en los paquetes. Previamente capturados con Wireshark.

H.I.V.E:

Es una multiherramienta OSINT (Open Source Intelligence) automatizada que permite la recopilación eficaz de datos de diversas fuentes mediante la utilización de una única plataforma unificada.

<https://github.com/Shad0w-ops/H.I.V.E>

GhostTrack:

Herramienta útil para rastrear la ubicación de una dirección IP o número de teléfono, por lo que esta herramienta se usa para OSINT a IP y números, cabe resaltar que se debe corroborar la información brindada con diferentes medios e ir seleccionando la información comprobada y verídica, para nuestras investigaciones OSINT. Ya que esta y otras herramientas arrojan resultados diferentes.

<https://github.com/HunxByts/GhostTrack>

Otras herramientas:

<https://github.com/AmdAdam/IP-Locator>

<https://github.com/shaikhsajid1111/ip-locator>

Servicio Whois:

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

<https://who.is/>

The screenshot shows the DomainTools website interface. At the top, there's a navigation bar with links: PROFILE, CONNECT, MONITOR, and SUPPORT. A search bar labeled 'Whois Lookup' is on the right. The main heading is 'IP Information for 167.132.147.108'. Below this, there's a 'Quick Stats' section with a table of key information:

IP Location	Peru Lima
ASN	PE (registered Feb 15, 2018)
Whois Server	whois.lacnic.net
IP Address	167.132.147.108
Reverse IP	1 website uses this address.

Below the table is a detailed 'inetnum' block from a whois database:

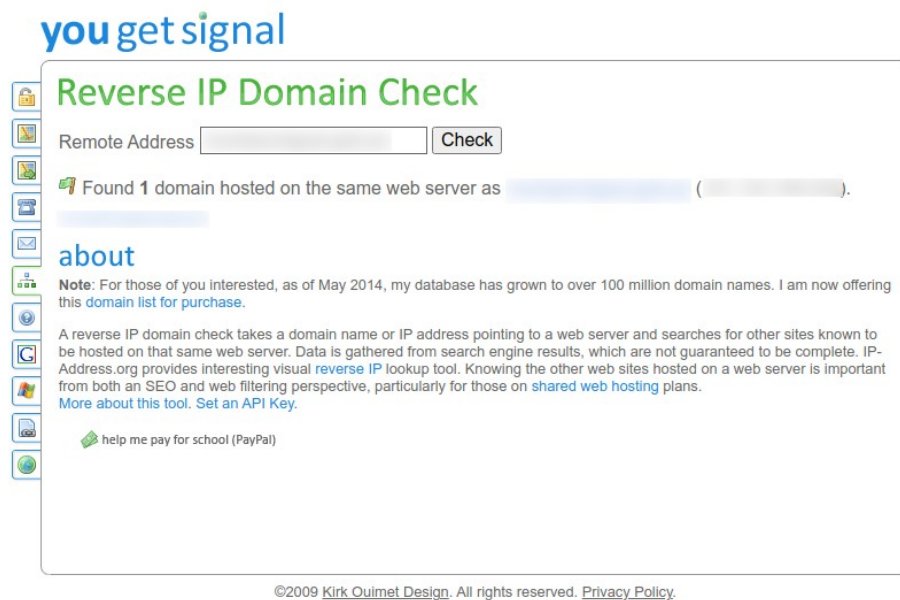
```
inetnum: 167.132.147.108
status: assigned
aut-num: N/A
owner: Rion Gonzales Prada
ownerid: PE 167132147108
responsible: Ruben Rodriguez
address: Jiron Gonzales Prada, 108
address: L2 - Lima
country: PE
phone: +51 1 7888108
owner-c: RUB4
tech-c: RUB4
abuse-c: RUB4
inetrev: 167.132.147.108
nserver: IC47 477 487 48
nsstat: 20190118 00
nslastaa: 20190118
nserver: NS 477 487 48
nsstat: 20190118 00
nslastaa: 20190118
created: 19100000
changed: 20190118

nic-hdl: RUR4
person: Ruben Rodriguez
e-mail: rodriguez@rur4.net
address: Jiron Gonzales Prada, 108
address: 47 - Lima, Surquillo - Lima
country: PE
phone: +51 1 7888108 [0000]
created: 20090722
changed: 20220329
```

Exploración DNS, IP inversa:

Reverse IP domain check

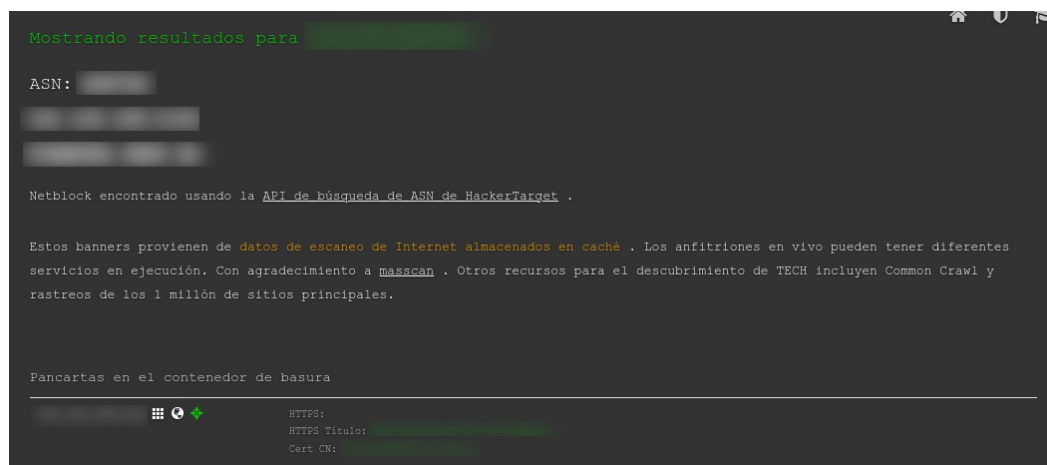
<https://www.yougetsignal.com/tools/web-sites-on-web-server/>



Ahora veremos que pasa si ponemos la IP, real de una pagina web, en dnsdumpster.

DNSdumpster:

<https://dnsdumpster.com/>



DNSlytics:

<https://dnslytics.com/reverse-ip>

Reverse IP

Find domains sharing the same IP address or subnet.

Go

Enter domain name, IP address (IPv4 and IPv6) or subnet.

Reverse IP lookup for:

Found **one** domain hosted on IP address

#	Domain	Tools
1	<input type="text"/>	Search Typos History Whois
DomainRank: 2/10		
Name servers: <input type="text"/> (used by 50,475 domains) <input type="text"/> (used by 50,441 domains)		
Mail servers: <input type="text"/> (used by 1 domain)		
IPv4: <input type="text"/> (used by 1 domain)		
<input type="text"/> (found 4 exact matched domains on different TLDs)		

También lo podemos poner con una IP personal.

Viewdns:

<https://viewdns.info/reverseip/>

Viewdns.info

[Tools](#) [API](#) [Research](#) [Data](#)

[ViewDNS.info](#) > [Tools](#) > **Reverse IP Lookup**

Takes a domain or IP address and does a reverse lookup to quickly shows all other domains hosted from the same server. Useful for finding phishing sites or identifying other sites on the same shared hosting server.

Domain / IP: [GO](#)

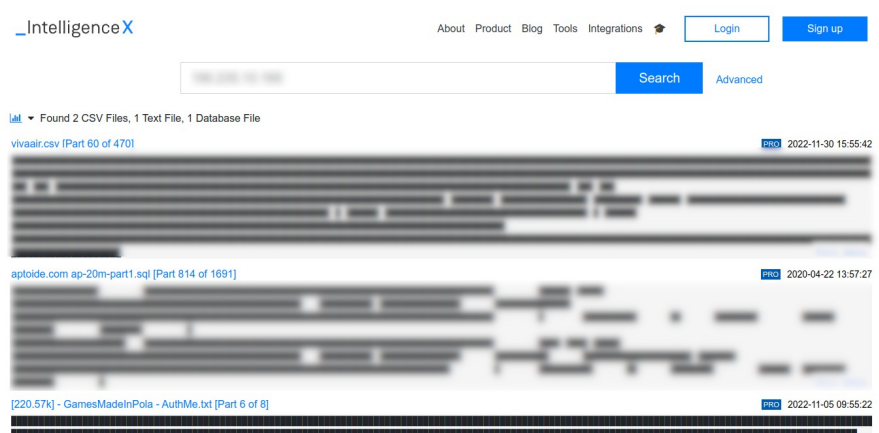
Reverse IP results for

=====

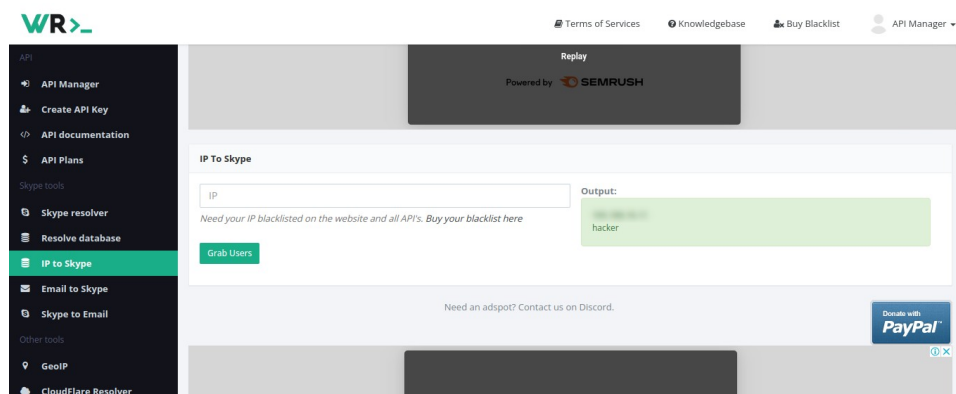
There are 1 domains hosted on this server.
The complete listing of these is below:

Domain	Last Resolved Date
<input type="text"/>	<input type="text"/>

Fugas de datos por dirección IP:



<https://webresolver.nl/tools/ip2skype>



<https://leakix.net/>

<https://www.cibertip.com/tutoriales/como-usar-leakix-el-nuevo-motor-de-busqueda-para-profesionales-de-la-ciberseguridad-que-facilita-la-deteccion-de-dispositivos-vulnerables/>

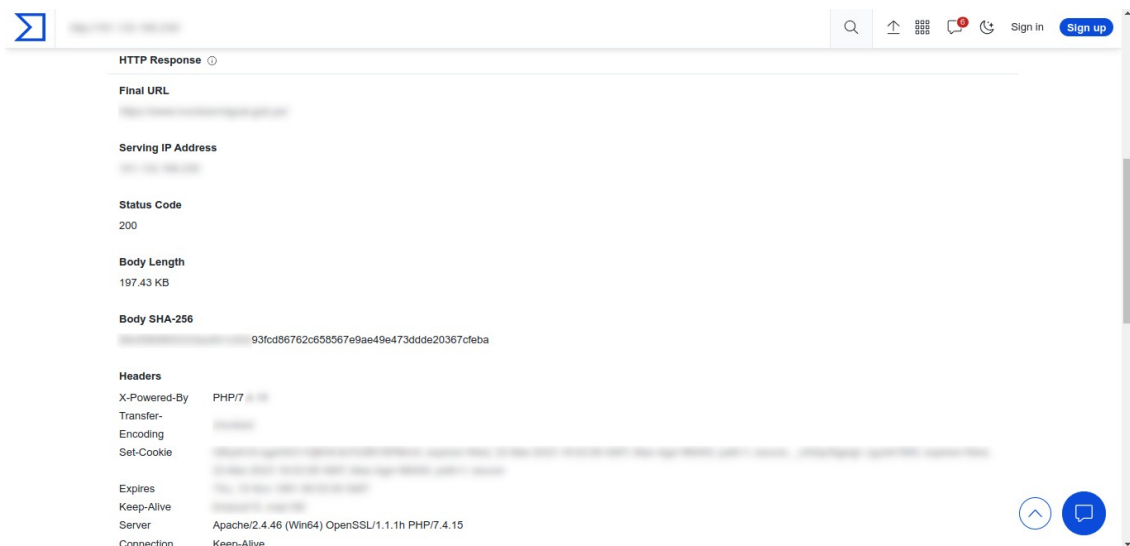
Control de calidad de virus e IP:

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

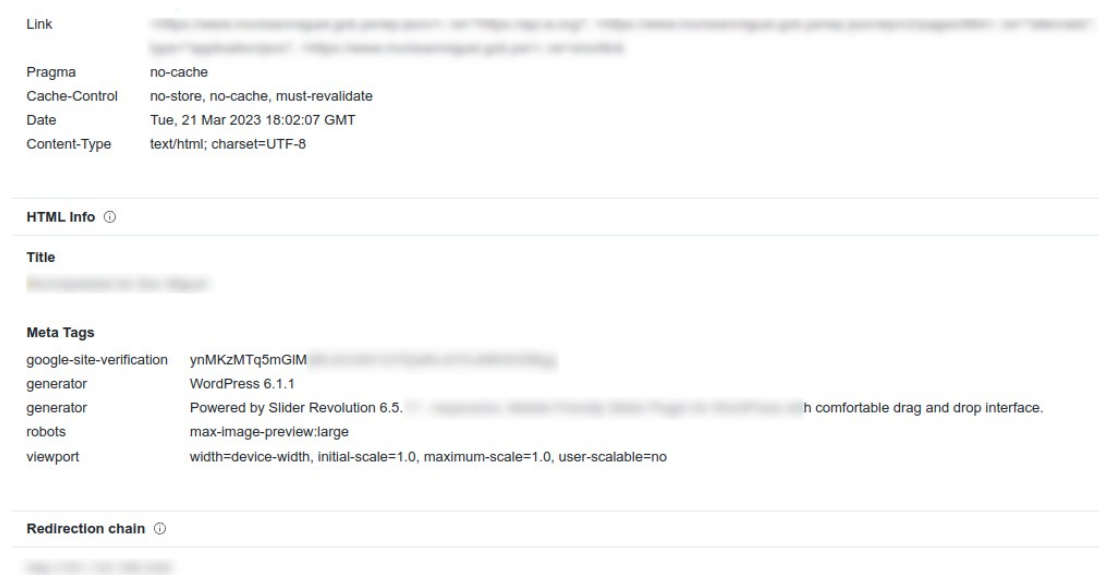
https://talosintelligence.com/reputation_center/lookup

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

VirusTotal:




Nos muestra información sobre la url puesta. Lo uso mucho al momento que me envían enlaces por correo.



Internet de las cosas (IoT):

Censys:

https://censys.io/ipv4



Hosts

Search

Register
Log In

Summary

Explore

History

WHOIS

Raw Data

Basic Information

Network

Routing

Protocols

443 / HTTP

TCP

Observed Mar 20, 2023 at 3:45am UTC

VIEW ALL DATA

GO

Software

OpenSSL 1.1.1h

Apache HTTPD 2.4.46

PHP 7.4.15

PHP

Details

Request

Protocol

Status Code

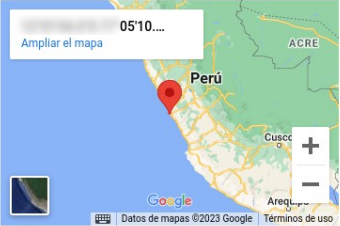
GET /

HTTP/1.1

301

0510...

Ampliar el mapa



Geographic Location

City

Province

Country

Coordinates

Timezone

San Martin de Porras

Lima region

Peru (PE)

America/Lima

Status Reason Moved Permanently

TLS

Fingerprint

JARM 2ad2ad16d2ad2ad22c42d42

JA3S aaffa2addb1036

Handshake

Version Selected TLSv

Cipher Selected TLS_

Leaf Certificate

c549b1bc4972043c66b04e39f

CN=

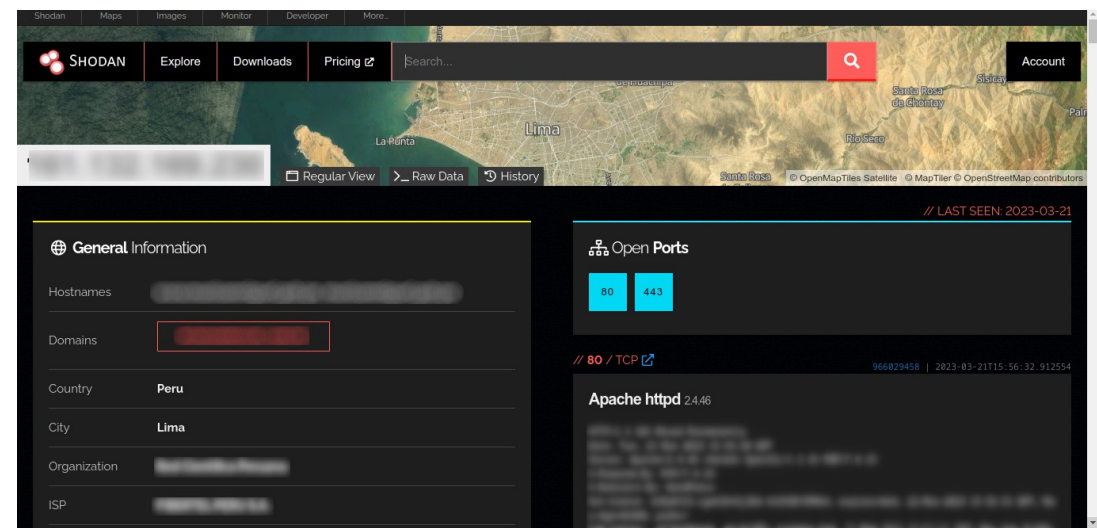
C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA

184

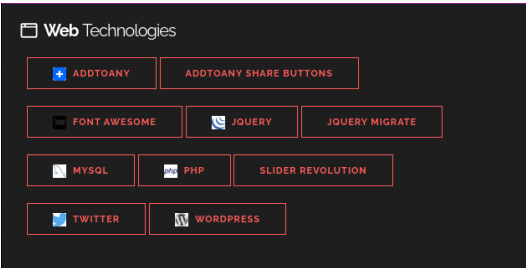
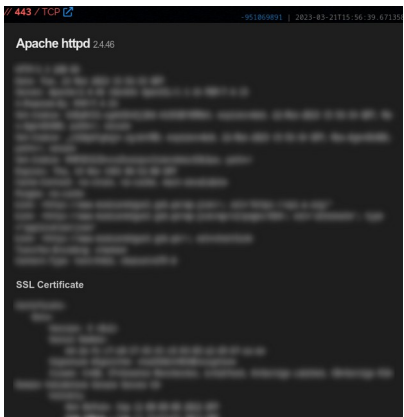
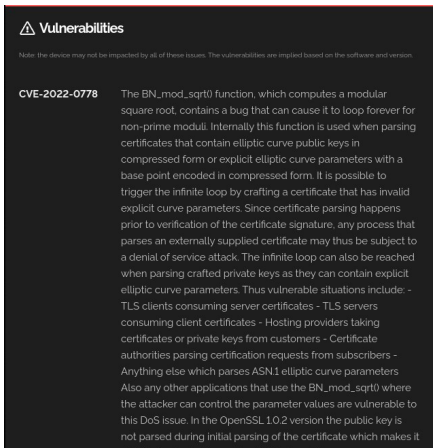
INVESTIGADOR_Z

Shodan:

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



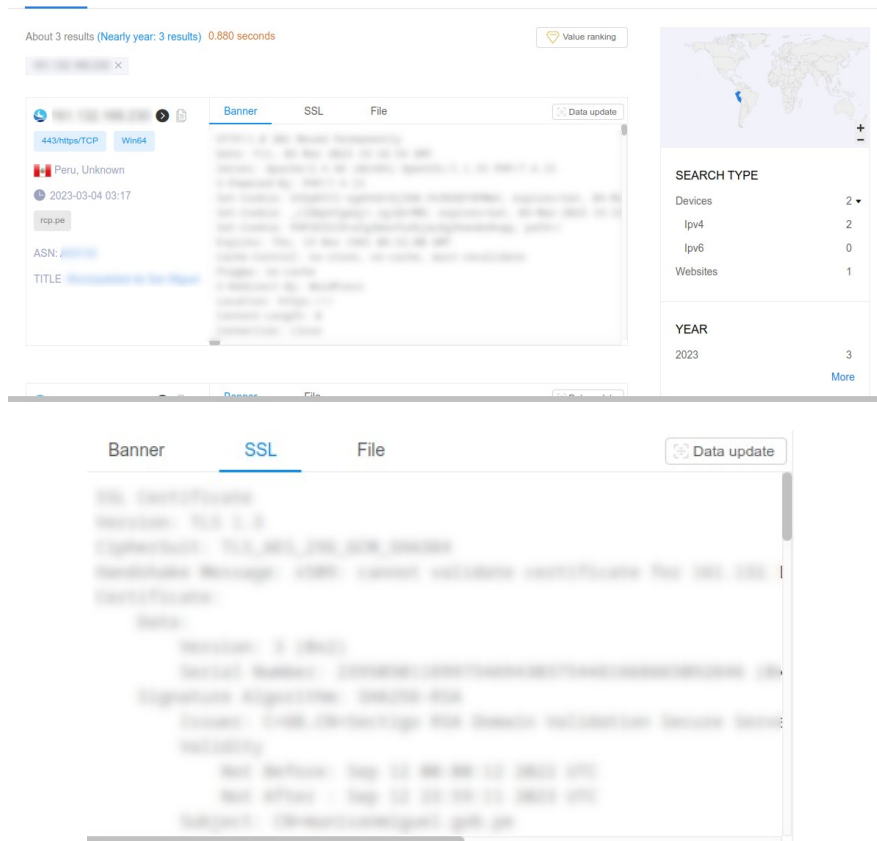
Nos muestra cierta información y tecnologías que usa.



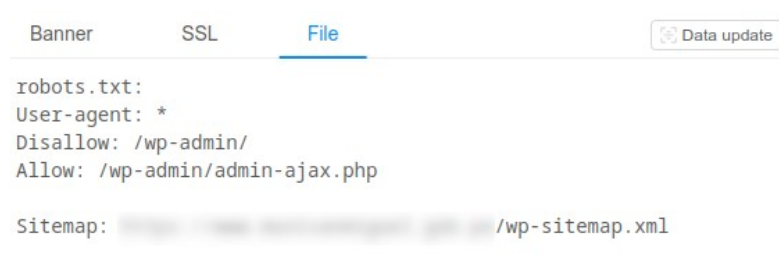
Otros enlaces: [Shodan Dorks](#) / [Shodan Eye](#) / [Shonda Hat](#)

Zoomeye:

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



Hay paginas que no configuran el wpadmin, que viene por defecto al instalar wordpress.



Nos muestra información relevante de la dirección IP que pusimos.

Related vulnerability data is provided by [SeeBug](#) for reference only

Vul Search



http

99561	2022-08-18	high	muhtpd Web 服务器 未授权任意文件读取漏洞 (CVE-2022-31793)
99364	2021-10-08	high	Apache HTTPd 多个路径穿越与命令执行漏洞 (CVE-2021-41773 CVE-2021-42013) ...
97900	2019-04-10	high	CVE-2019-0211 Apache Root Privilege Escalation
97633	2018-10-30	high	ACME Mini_httpd组件任意文件读取漏洞(CVE-2018-18778)
96556	2017-09-20	high	Apps industrial OT over Server: Anti-Web Local File Incl...

openssl

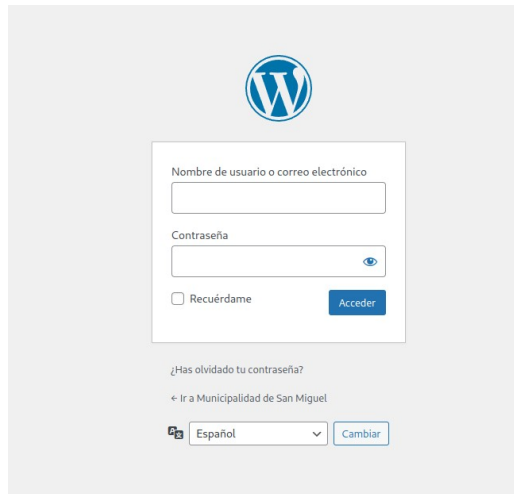
99601	2022-11-03	high	OpenSSL 缓冲区溢出漏洞 (CVE-2022-3602)
99496	2022-04-15	high	OPENSSL拒绝服务漏洞(CVE-2022-0778)
99170	2021-03-29	high	OpenSSL 拒绝服务攻击 (CVE-2021-3449)
97082	2018-01-15	high	An Analysis of the OpenSSL SSL Handshake Error State Secu...
92577	2016-12-20	middle	OpenSSL SSL/TLS MITM 漏洞 (CVE-2014-0224)

wordpress

99530	2022-06-22	high	Wordpress 存储型XSS漏洞 (CVE-2022-21662)
99516	2022-05-20	high	Wordpress 插件Tatsu builder 未授权RCE漏洞 (CVE-2021-25094)
99431	2022-01-10	high	wordpress SQL注入漏洞 (CVE-2022-21661)
99304	2021-07-19	high	woocommerce 插件 SQL注入漏洞
99235	2021-04-28	high	wordpress 5.7 授权XXE漏洞 (CVE-2021-29447)

apache httpd

99364	2021-10-08	high	Apache HTTPd 多个路径穿越与命令执行漏洞 (CVE-2021-41773 CVE-2021-42013) ...
97900	2019-04-10	high	CVE-2019-0211 Apache Root Privilege Escalation



Lo bueno que automatiza la búsqueda de información.

Marcos para explorar las direcciones IP:

<http://3.233.242.75:8080/>

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

Usamos spiderfoot, se puede usar de forma online y también desde la terminal, en este caso lo usaremos de las 2 maneras.

Spiderfoot:

New Scan

Scan Name
The name of this scan.

Scan Target
The target of your scan.

Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:

- Domain Name: e.g. example.com
- IPv4 Address: e.g. 1.2.3.4
- IPv6 Address: e.g. 2608:4700:4700::1111
- Hostname/Sub-domain: e.g. abc.example.com
- Subnet: e.g. 1.2.3.0/24
- Bitcoin Address: e.g. 1HesYJSP1QqcyPEjrQ9vzBL1wujruNGe7R
- E-mail address: e.g. bob@example.com
- Phone Number: e.g. +12345678901 (E.164 format)
- Human Name: e.g. "John Smith" (must be in quotes)
- Username: e.g. "jsmith2000" (must be in quotes)
- Network ASN: e.g. 1234

By Use Case | By Required Data | By Module

☒ **All** **Get anything and everything about the target.**
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

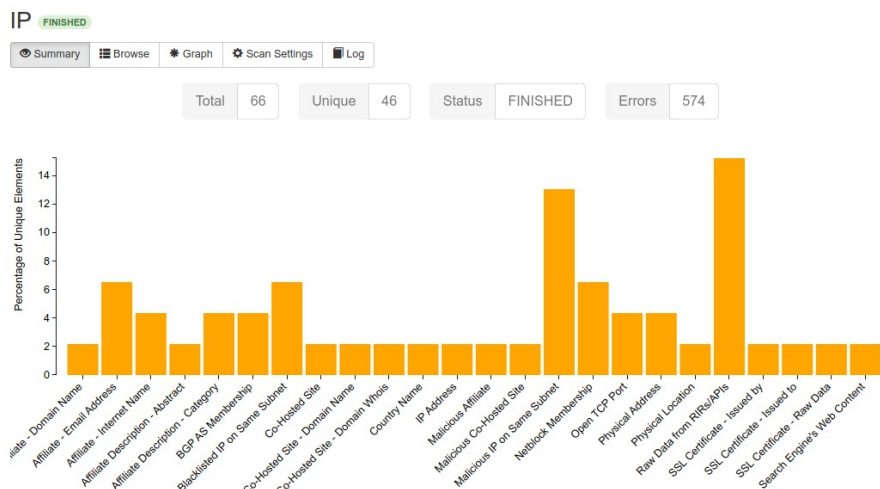
☐ **Footprint** **Understand what information this target exposes to the Internet.**
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

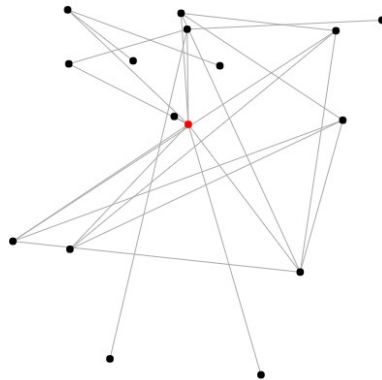
☐ **Investigate** **Best for when you suspect the target to be malicious but need more information.**
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

spiderfoot			
New Scan Scans Settings			
Summary Browse Graph Scan Settings Log			
Search...			
Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Email Address	3	6	2023-03-22 04:49:46
BGP AS Membership	2	5	2023-03-22 04:49:27
Blacklisted IP on Same Subnet	3	3	2023-03-22 04:48:46
Co-Hosted Site	1	2	2023-03-22 04:49:57
Co-Hosted Site - Domain Name	1	1	2023-03-22 04:49:45
Co-Hosted Site - Domain Whois	1	1	2023-03-22 04:49:46
Country Name	1	1	2023-03-22 04:49:45
IP Address	1	1	2023-03-22 04:45:47
Malicious Co-Hosted Site	1	1	2023-03-22 04:49:37
Malicious IP on Same Subnet	6	6	2023-03-22 04:49:22
Netblock Membership	3	3	2023-03-22 04:49:19
Open TCP Port	2	5	2023-03-22 04:50:37
Physical Address	2	5	2023-03-22 04:49:21
Physical Location	1	4	2023-03-22 04:49:53
Raw Data from RIRs/APIs	7	7	2023-03-22 04:49:53

IP RUNNING			
Summary Browse Graph Scan Settings Log			
Browse / Affiliate - Email Address			
Data Element	Source Data Element	Source Module	Identified
		sfp_email	2023-03-22 04:49:46

Lo bueno que es bien detallado.





Scans

Filter: None

<input type="checkbox"/>	Name	Target	Started	Finished	Status	Elements	Action
<input checked="" type="checkbox"/>	[Redacted]	[Redacted]	2023-03-22 04:45:40	2023-03-22 04:51:58	FINISHED	66	[Icons]
<input type="checkbox"/>	[Redacted]	[Redacted]	2022-10-20 02:19:40	2022-10-20 20:01:49	FINISHED	3907	[Icons]
<input type="checkbox"/>	[Redacted]	[Redacted]	2022-03-14 06:51:49	2022-03-14 06:52:14	FINISHED	44	[Icons]
<input type="checkbox"/>	[Redacted]	[Redacted]	2021-10-03 01:11:11	2021-10-03 01:57:10	FINISHED	120	[Icons]

Scans 1 - 4 / 4 (4)

Vemos que nos muestra información útil, ahora lo usaremos desde la terminal, se habilitará de modo local. También lo podemos exportar.

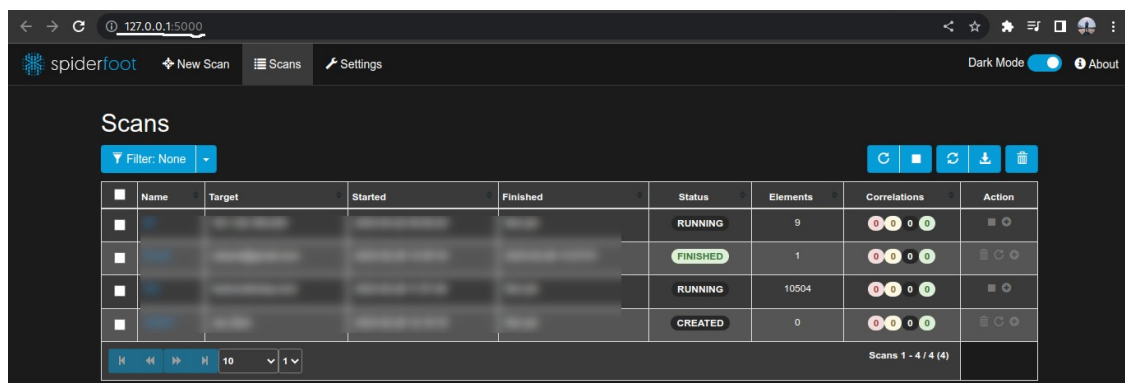
```

jeyzeta@JeyZeta: ~
Archivo Acciones Editar Vista Ayuda
(jeyzeta@JeyZeta)-[~]
$ spiderfoot -l 0.0.0.0:5000
2023-03-21 23:59:32,116 [INFO] sf : Starting web server at 0.0.0.0:5000 ...

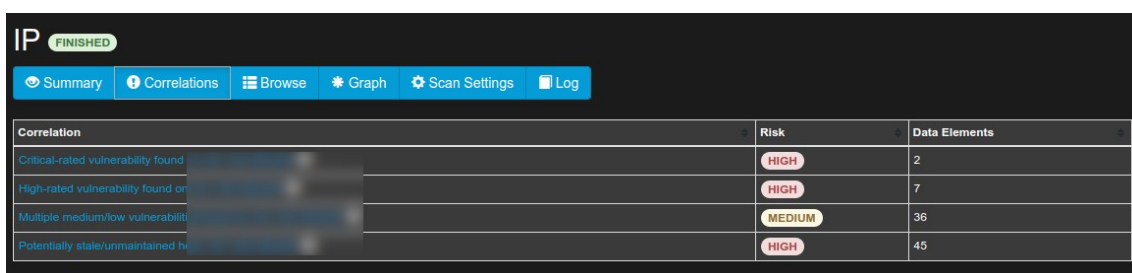
*****
Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:5000
*****

2023-03-21 23:59:32,148 [WARNING] sf :
*****
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
*****

2023-03-22 00:00:23,159 [INFO] sfwebui : Waiting for the scan to initialize...
2023-03-22 00:00:23,331 [INFO] sflib : Downloading configuration data from: https://public
suffix.org/list/effective_tld_names.dat
2023-03-22 00:00:23,888 [INFO] sflib : Scan [06012539] for '[Redacted]' initiated.
2023-03-22 00:00:23,915 [INFO] sflib : sfp_stor_db module loaded.
2023-03-22 00:00:23,950 [INFO] sflib : sfp_abstractapi module loaded.
2023-03-22 00:00:23,979 [INFO] sflib : sfp_abusech module loaded.
  
```

Ahora estamos desde el localhost, que nos creo spiderfoot.



Nos muestra ciertas vulnerabilidades.

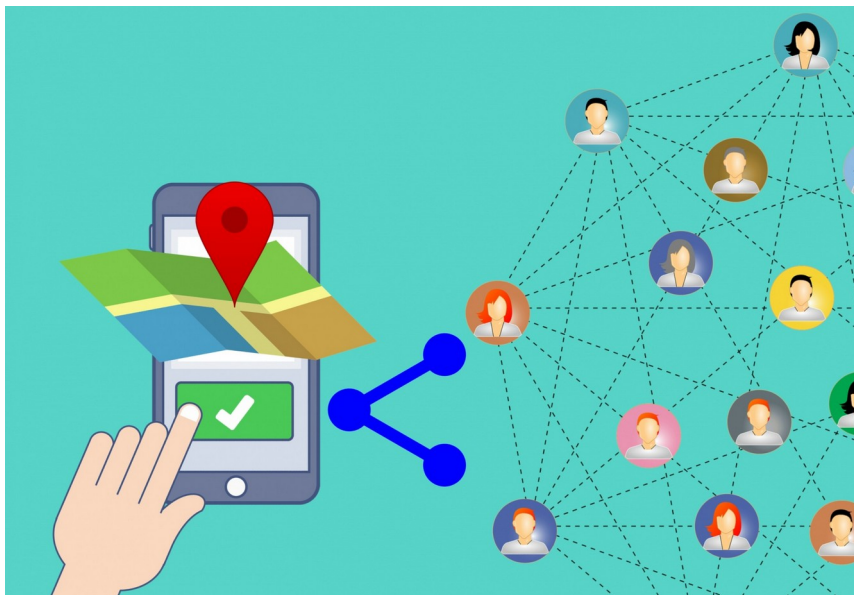
<https://www.kali.org/tools/spiderfoot/>

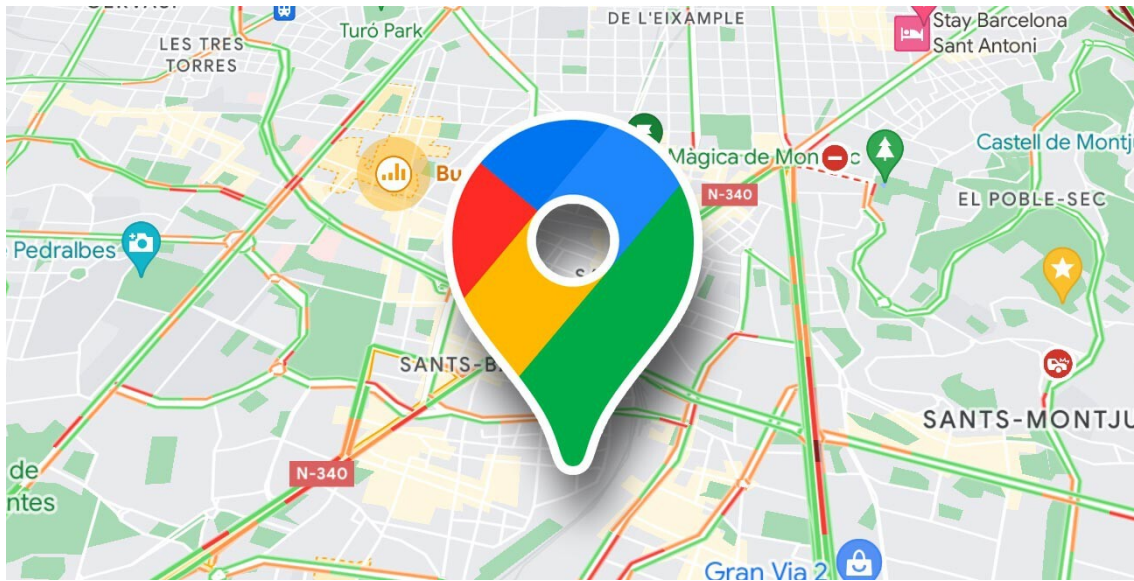
https://medium.com/@ibederov_en/ip-address-osint-49234840e133

GEOLOCALIZACIÓN / MAPAS

Veremos diferentes medios de búsqueda en ubicaciones GPS, direcciones, coordenadas.

Usando herramientas desde el navegador y desde la terminal.





Google Maps:

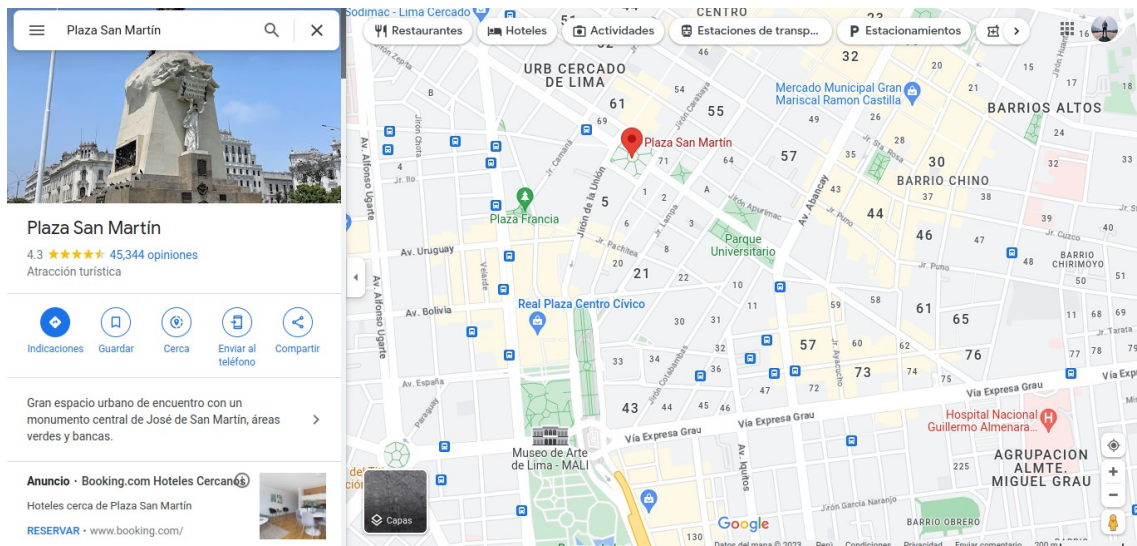
<https://maps.google.com/>

Google Maps: Es un servidor de aplicaciones de mapas en la [web](#) que pertenece a [Alphabet Inc.](#) Ofrece imágenes de [mapas](#) desplazables, así como [fotografías](#) por [satélite](#) del [mundo](#) e incluso la ruta entre diferentes ubicaciones o imágenes a pie de calle con [Google Street View](#), condiciones de tráfico en tiempo real (Google Traffic) y un [calculador de rutas](#) a pie, en coche, bicicleta (beta) y transporte público y un [navegador GPS](#), Google Maps Go.

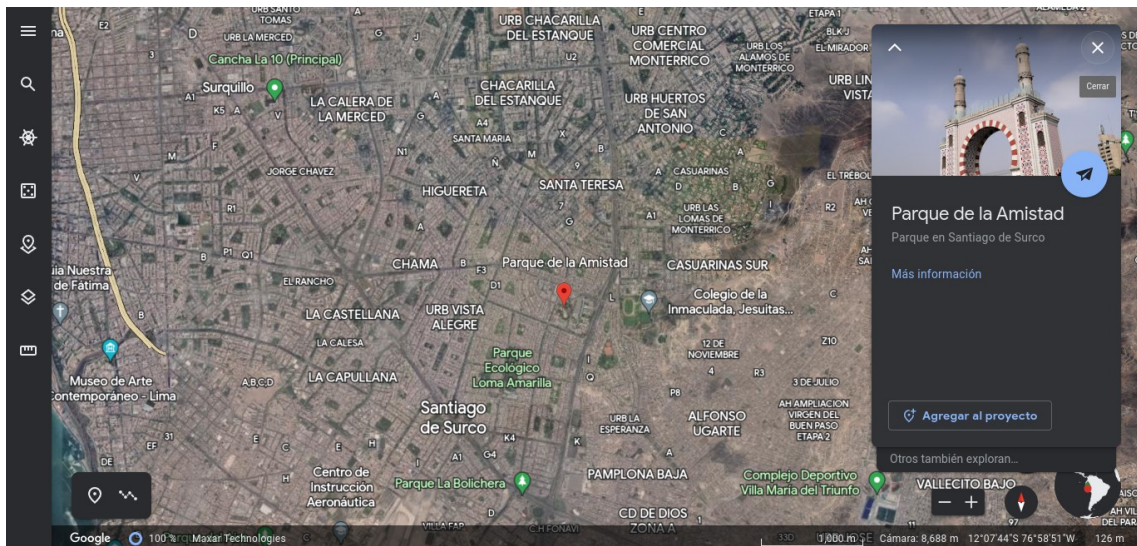
Por ejemplo si busco una ubicación por coordenadas o dirección o incluso si estas algo perdido y quieres guiarte hacia una dirección, puedes usar Google Maps, Waze, etc.

Se puede hacer búsquedas avanzadas con google maps, ya que hoy en día hay demasiada información y recursos para la globalización.

https://www.google.com/maps/place/Plaza+San+Mart%C3%ADn/@-12.0551462,-77.0363236,15.82z/data=!4m6!3m5!1s0x9105c8c80c682de3:0x17152161175cbcd!8m2!3d-12.0516797!4d-77.034641!16s%2Fm%2F0534_w9



Si vemos otra ubicación y desde otro modo.



Al usar Google maps podemos ver ubicaciones a nivel mundial, conocer lugares a nivel mundial.

Cabe recalcar que se van actualizando la vista cada vez que pasa el tiempo, ya que he buscado lugares, que la grafica sigue siendo de años.

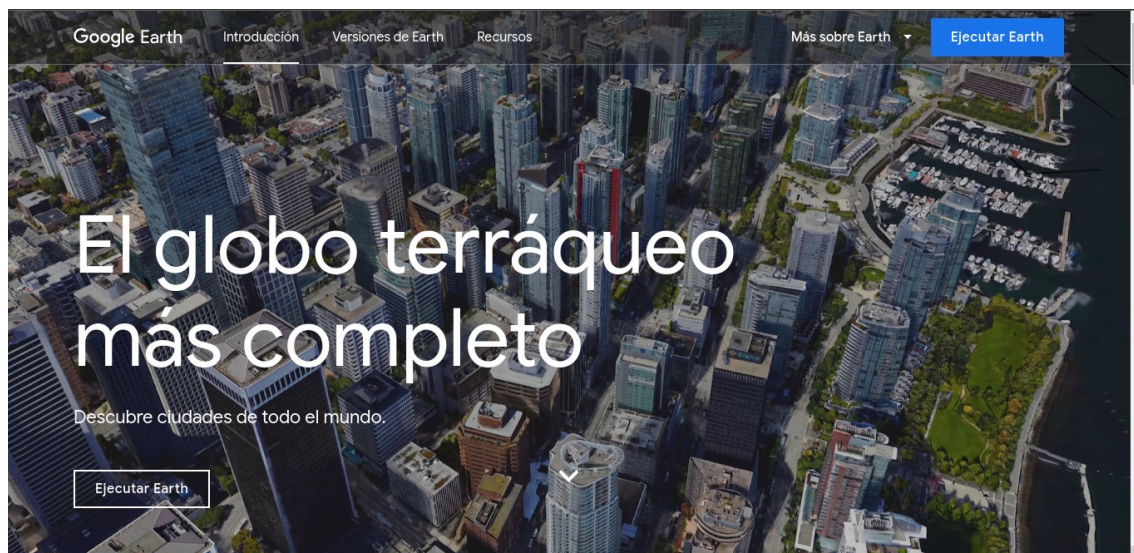
Por ejemplo busqué una ubicación y me seguía saliendo la imagen como de 10 años atrás, cuando en la actualidad ese lugar está más urbanizado.

Muchas personas usan para llegar a cierto lugar, ya que quizás no conocen ciertos lugares y con Google Maps, podemos llegar y conocer ubicaciones.

Google Earth:

<https://www.google.es/intl/es/earth/index.html>

Google Earth: Es un sistema de información geográfica que muestra un globo terráqueo virtual que permite visualizar múltiple cartografía, basado en imágenes satelitales y además permite la creación de entidades de puntos líneas y polígonos, contando también con la posibilidad de crear mapas.

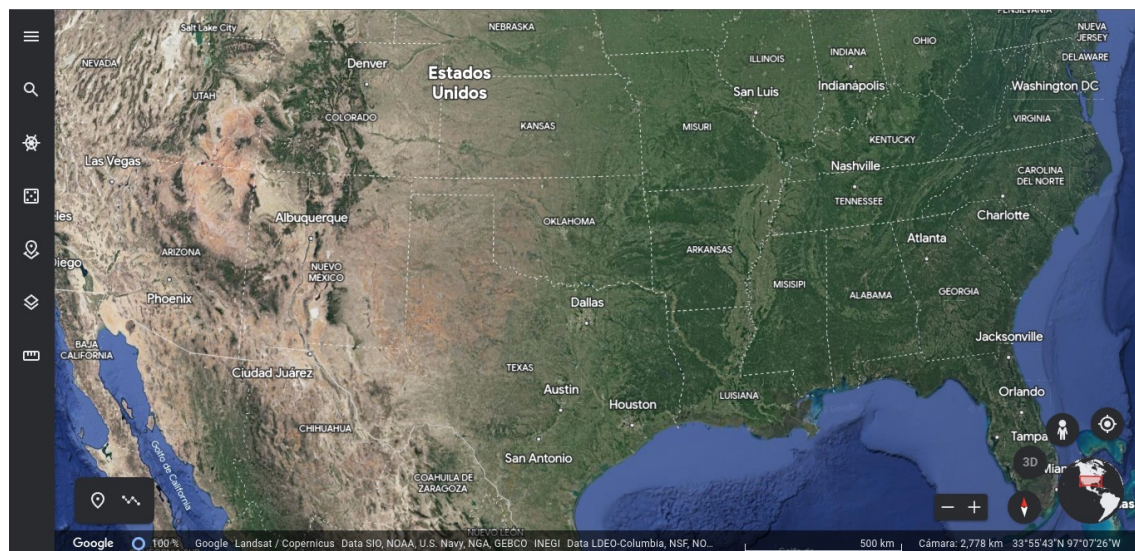


Al ejecutar Earth, no redirige a la siguiente URL.

<https://earth.google.com/web/>



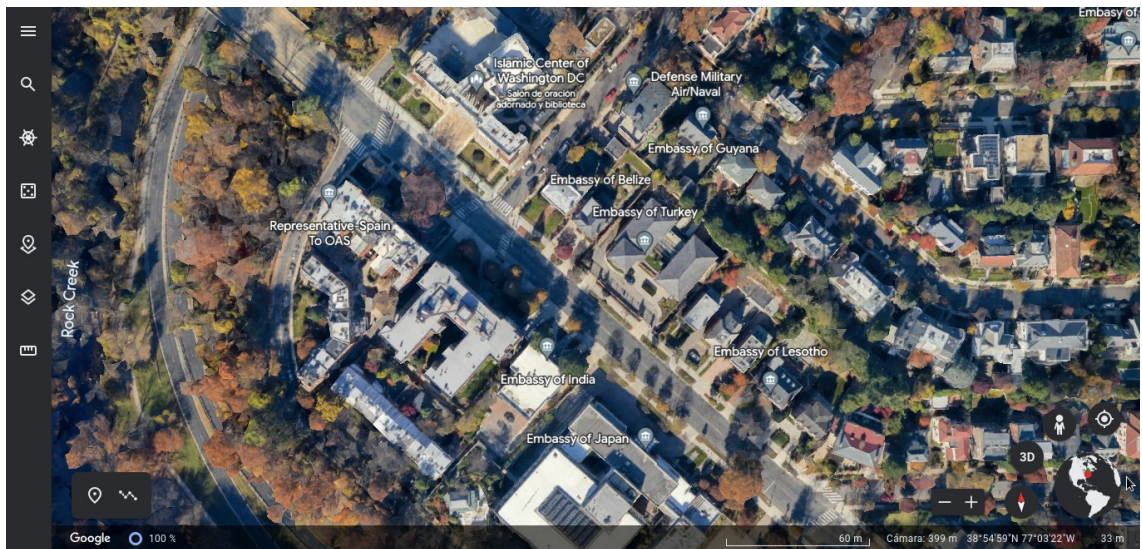
No podemos ir a estados unidos y ver ubicaciones.



Podemos ver por ejemplo las embajadas.

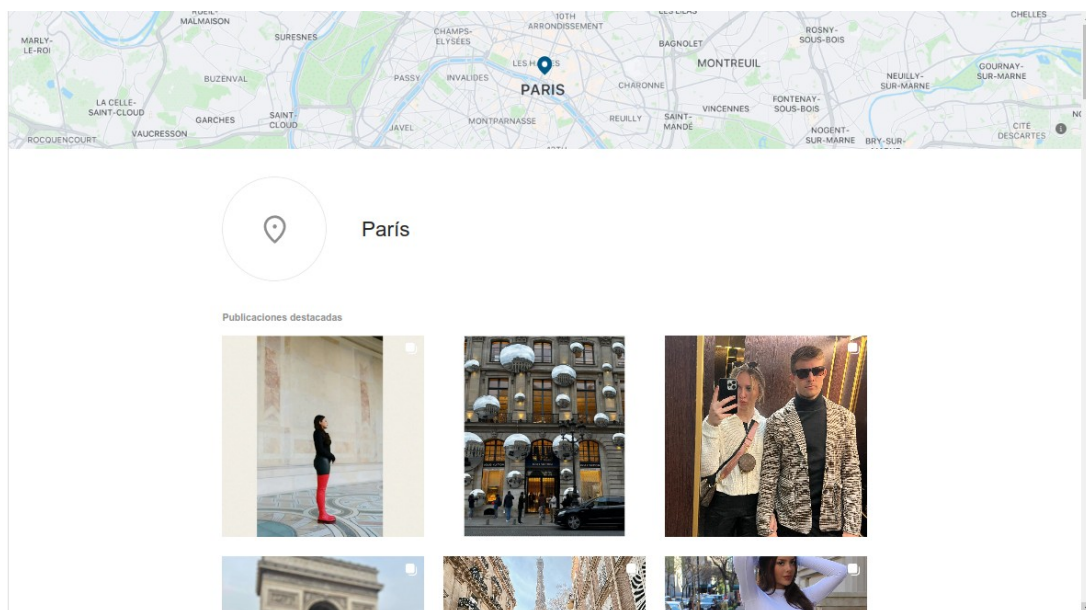
[https://earth.google.com/web/@38.91640901,-](https://earth.google.com/web/@38.91640901,-77.05635424,32.66593183a,365.95447704d,35y,1.42227153h,0t,0r)

[77.05635424,32.66593183a,365.95447704d,35y,1.42227153h,0t,0r](https://earth.google.com/web/@38.91640901,-77.05635424,32.66593183a,365.95447704d,35y,1.42227153h,0t,0r)



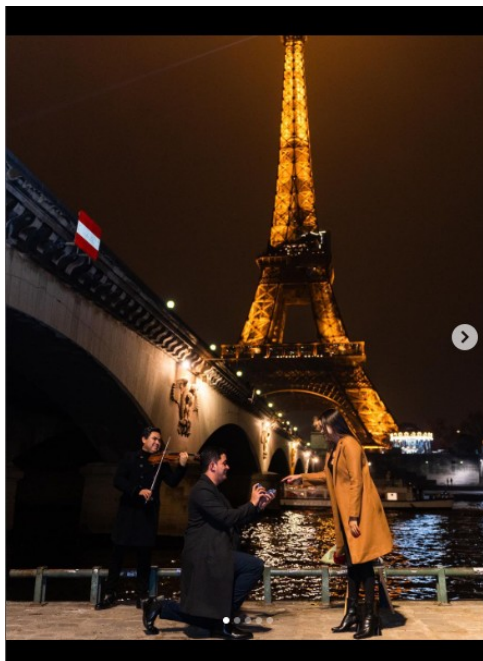
Otro dato, podemos usar Waze para ver ubicaciones, hay muchos programadores que utilizan las apis, de Google maps para hacer sus aplicaciones, por ejemplo, uber tiene sus propias apis, para automatizar la geolocalización de sus clientes y trabajadores.

Como otro ejemplo hace unas semanas usé DiDi, para llegar a un lugar, y lo grandioso es que desde su aplicación me mostraba la geolocalización en tiempo real del conductor, sus datos y en cuanto tiempo llegaría a mi ubicación.



Instagram se ha convertido en oro para personas que buscan información de un objetivo, ya que por lo general las personas comparten información, en este caso buscaremos algo al azar.

Escogimos Paris – Francia, sin dudarlo si alguien va a la torre a dicho país y lugares turísticos como la Torre Eiffel, vemos a una pareja de novios que están en un momento privado en su vida, pero muchas veces se comparten ciertas cosas para mostrar la felicidad a nuestros conocidos.

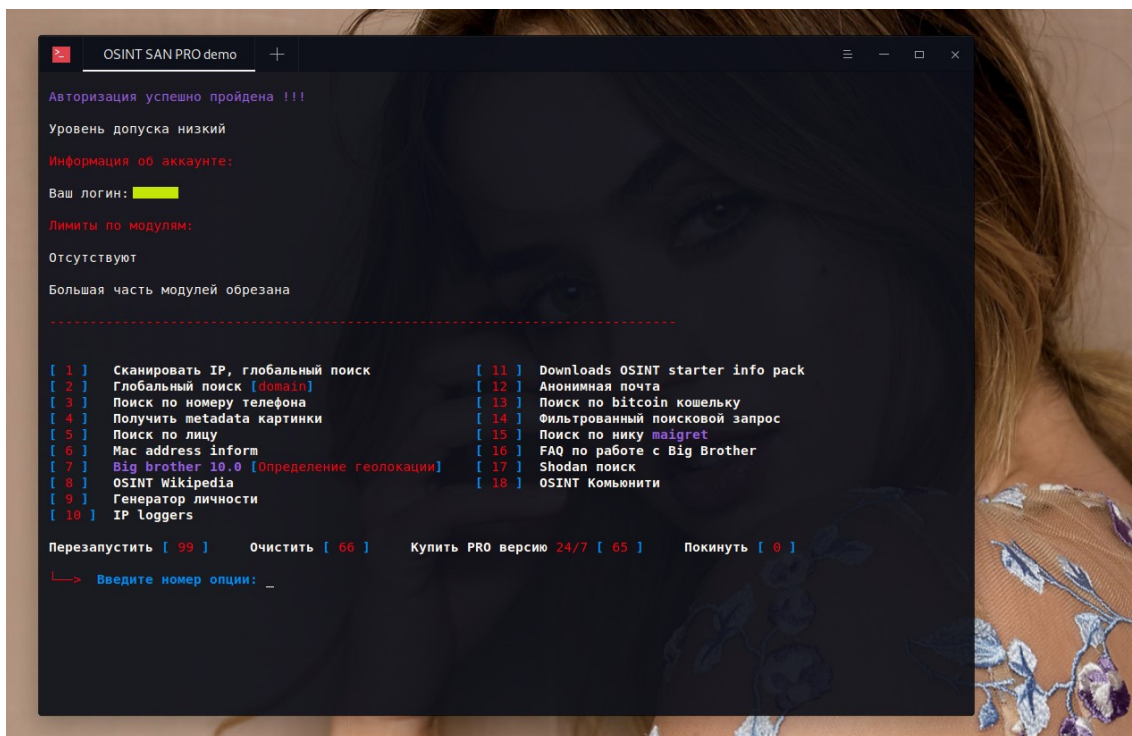


OSINT-SAN:

<https://github.com/Bafomet666/OSINT-SAN>

OSINT-SAN: Framework permite encontrar rápidamente información y desanonimizar usuarios de Internet. El software es un marco con 25 funciones para encontrar información o desanonimizar usuarios. este software, puede recopilar información sobre usuarios en Internet, de forma anónima y sin conocimientos especiales.

Tiene su opción free y de paga. (https://t.me/osint_san_framework)



Tiene buenas funciones, scripts, lanzador de enlaces.

Les dejo la demo que el autor de esta herramienta hizo como tutorial.

<https://cloud.mail.ru/public/xCk1/UGcdm61nM>

Como está en idioma Ruso, deben usar el traductor para ciertas palabras, pero es muy buena esta herramienta.

Una muestra de su Map

<https://osintsan.ru/cam.html>

Hablando de Rusos, recuerdo un anécdota de un conocido de nick Hiro Maxwell que se enamoró de una chica Rusa, y comenzó a buscar información de ella.

Hasta encontró su pasaporte y demás datos personales de la chica.

Es cierto que cuando el objetivo es una persona o empresa de otro país que desconoces su idioma es dificultoso encontrar información rápidamente, por el idioma, paginas de ese país que no conoces, etc.

Lo cierto es que si eres una persona con paciencia y dedicada, vas a poder usar el OSINT, a nivel profesional y no habrá límites para llegar a tu objetivo.



Hiro Maxwell

Así se doxea, se pentestea, y se relaja, hermanos y hermanas 😊

[~]Hacking

[~]Doxing

[~]нежность :3~

Me gusta · Comentar · Compartir · 27 de junio

Álbum: Fotos de la biografía

Foto compartida con:

Amigos

Etiquetar esta foto

En el post de mi colega Omar, lo pueden ver más a detalle en la parte final.

<https://backtrack-omar.blogspot.com/2015/10/aprendiendo-el-arte-del-doxing.html>

Mapa de cables submarinos:

El Mapa de cables submarinos es un recurso gratuito que se actualiza periódicamente.

<https://www.submarinecablemap.com/landing-point/mersin-turkey>

Geolocation for IP 104.21.33.251

[Hide IP with VPN](#)

IP Location Finder

IPv4, IPv6 or Domain Name

IP Lookup


Here are the results from a few Geolocation providers. Is the data shown below not accurate enough? Please read geolocation accuracy info to learn why.



Do you have a problem with IP location lookup? Report a problem.

You've entered a domain name. We've found an IP address from the domain name you've entered. Your translated IP address is 104.21.33.251


Geolocation data from IP2Location (Product: DB6, 2023-3-1)


 **DOMAIN NAME:** hackunderway.com


 **ISP:** CloudFlare Inc.


 **COUNTRY:** United States 

 **ORGANIZATION:** Not available

 **REGION:** California

 **LATITUDE:** 37.7757

 **CITY:** San Francisco



 **LONGITUDE:** -122.3952


Nos muestra varios resultados.

Geolocation data from ipinfo.io (Product: API, real-time)


 **DOMAIN NAME:** hackunderway.com


 **ISP:** Cloudflare, Inc.

 **COUNTRY:** United States 

 **ORGANIZATION:** Cloudflare, Inc. (cloudflare.com)

 **REGION:** California


 **LATITUDE:** 37.7621

 **CITY:** San Francisco


 **LONGITUDE:** -122.3971

Geolocation data from DB-IP (Product: API, real-time)


 **DOMAIN NAME:** hackunderway.com

 **ISP:** Cloudflare, Inc.

 **COUNTRY:** Canada 










 **ORGANIZATION:** Cloudflare, Inc










 **REGION:** Ontario










 **LATITUDE:** 43.6532









 **CITY:** Toronto

 **LONGITUDE:** -79.3832

Geolocation data from IPRegistry.co (Product: API, real-time)			
 IP ADDRESS: 104.21.33.251	 ISP: Cloudflare, Inc.		
 COUNTRY: United States 	 ORGANIZATION: Cloudflare, Inc. (cloudflare.com)		
 REGION: California	 LATITUDE: 37.77571		
 CITY: San Francisco	 LONGITUDE: -122.39525		

Geolocation data from IPGeolocation.io (Product: API, real-time)			
 DOMAIN NAME: hackunderway.com	 ISP: Cloudflare, Inc.		
 COUNTRY: United States 	 ORGANIZATION: Cloudflare, Inc.		
 REGION: California	 LATITUDE: 37.78035		
 CITY: San Francisco	 LONGITUDE: -122.39059		

Geolocation data from IPapi.co (Product: API, real-time)			
 IP ADDRESS: 104.21.33.251	 ISP: CLOUDFLARENET		
 COUNTRY: Canada 	 ORGANIZATION: CLOUDFLARENET		
 REGION: Ontario	 LATITUDE: 43.6752		
 CITY: Toronto	 LONGITUDE: -79.3472		

Geolocation data from criminalip.io (Product: API, real-time)			
 DOMAIN NAME: hackunderway.com	 ISP: CLOUDFLARENET		
 COUNTRY: Not available	 ORGANIZATION: Cloudflare		
 REGION: Not available	 LATITUDE: Not available		
 CITY: Not available	 LONGITUDE: Not available		

Vemos cierta información de mi dominio, en diferentes fuentes que ofrece esta pagina web.

Más adelante veremos también sobre unos ejemplos usando Termux, desde el celular, y que también puedes usar el celular para hacer OSINT, sólo que desde mi punto de vista me siento más cómodo usando una computadora.

Pero les daré unos ejemplos. (OSINT SPY y Metasploit).

```
README.md osint-spy.py
~/OSINT-SPY $ python osint-spy.py

      @@@@@@@@@@ @@@@@@@@@@ | @ @ 88888|88
888  @@@@@@@@@@ @@@@@@@@@@ | @ @  e
      | 8 @ | @ @  e
      @@@@@@@@@@ | @ @  e
      | 8 @ | @ @  e
888888888888 | @ @  e
---- | @@@@@@@@@@ @@@@@@@@@@ | @ @  e
      @@@@@@@@@@ | @ @  e
      | 8 @ | @ @  e
888888888888 | @ @  e
      @@@@@@@@@@ | @ @  e
      | 8 @ | @ @  e
      @@@@@@@@@@ | @ @  e

OSINT Search using
Website: https://
/docs.osint-spy.io

Usage: osint-spy.py [options]
Options:
-h, --help show
this help message and exit Get l
--btc_block Get b
atest bitcoin block info Get b
--btc_date Get b
itcoin block info by date, example - 20190614 Get i
--btc_address Get i
nfo of any bitcoin wallet address List
--ssl_cipher List
out supported SSL ciphers used by any domain Check
--ssl_bleed Check
whether server is vulnerable to heart bleed or not Do do
--domain Do do
main recon Do em
--email Do em
ail recon Do em
--device Explo
re the Internet of Things. Example - opensips,asterisk
,juniper,windows10 WHOIS
--ip WHOIS
IP Lookup Send
--malware Send
files to VirusTotal for malware analysis

ESC  CTRL ALT - ↓ ↑
```

```
ARE.se--MMjMs 'MjM--WE
S.CITY's--' +-KANSAS
ERS-./.' J-HAKC
q!:' .esc:W
H' +++AT

=[ metasploit v5.0.95-dev
+ --==[ 2038 exploits - 1103 auxiliary - 344 post
+ --==[ 562 payloads - 45 encoders - 10 nops
+ --==[ 7 evasion

Metasploit tip: Display the Framework log using the lo
g command, learn more with help log

msf5 > banner
IIIIII dTb.dTb
II 4' v B
II 6. P
II 'T: ;P'
II 'T: ;P'
IIIIII 'YvP'

I love shells --egypt

=[ metasploit v5.0.95-dev
+ --==[ 2038 exploits - 1103 auxiliary - 344 post
+ --==[ 562 payloads - 45 encoders - 10 nops
+ --==[ 7 evasion

Metasploit tip: Use the edit command to open the curre
ntly active module in your editor

msf5 >
```

IPGeolocation:

<https://github.com/maldevel/IPGeoLocation>

```
~/IPGeoLocation $ python ipgeolocation.py -t

IPGeolocation 2.0.4

--[ Retrieve IP Geolocation information from ip-api.co
m
--[ Copyright (c) 2015-2016 maldevel (@maldevel)
--[ ip-api.com service will automatically ban any IP a
ddresses doing over 150 requests per minute.

Target:
IP:
ASN:
City:
Country:
County:
ISP:
Latitude:
Longitude:
Organization:
Registrar:
Registration:
Timezone:
Zip:
Google:
,-7

~/IPGeoLocation $
```


Seeker:

Localización precisa de teléfonos inteligentes mediante ingeniería social, lo bueno que es multiplataforma, lo pueden usar en la mayoría de sistemas operativos, aparte de tener templates de Drive, WhatsApp, Telegram, Zoom.

Se usa con ngrok, para montar un enlace.

<https://github.com/thewhiteh4t/seeker>

<https://www.youtube.com/watch?v=Q91cTFwlvLc&t=5s>

<https://www.elcursodelhacker.com/seeker/>



ngrok:

Es una entrada como servicio simplificada basada en API que añade conectividad, seguridad y capacidad de observación a sus aplicaciones en una sola línea.

Nos permite crear nuestro servidor local en un subdominio para poder visualizarlo fuera de la LAN, a través de internet; por ejemplo, para realizar

pruebas de intrusión necesitamos de un túnel donde recibiremos las conexiones, un método que puede sustituir el uso de Ngrok es el “PortForwarding”, sin embargo, este método es más laborioso, a comparación de Ngrok.

<https://ngrok.com/>

<https://www.elcursodelhacker.com/ngrok/>

Enlaces sobre Termux:

<https://termux.dev/en/>

<https://github.com/termux/termux-app>

[https://play.google.com/store/apps/details?
id=com.termux&hl=es_PE&gl=US&pli=1](https://play.google.com/store/apps/details?id=com.termux&hl=es_PE&gl=US&pli=1)

Otros recursos extras:

[All Area Codes](#)

[A Very Particular Set of Skills](#)

[Descartes Labs](#)

[EarthCam](#)

[Emporis Buildings Database](#)

[Flags of the World](#)

[Geoguesser](#)

[Geolocating photo's with OSM overpass API](#)

[Google Maps and Streetview](#)

[Google Streetview Coverage](#)

[IEC World Electrical Plugs](#)

[Insecam](#)

[Left vs Right Driving Countries](#)

[MoonCalc](#)

[N2YO Satellite Tracker](#)

[Open Street Map Search Engines](#)

[Overpass Turbo](#)

[Redfin](#)

[Shadow Calculator](#)

[SunCalc](#)

[Trulia](#)

[Wikimapia](#)

[WorldCam](#)

[Zillow](#)

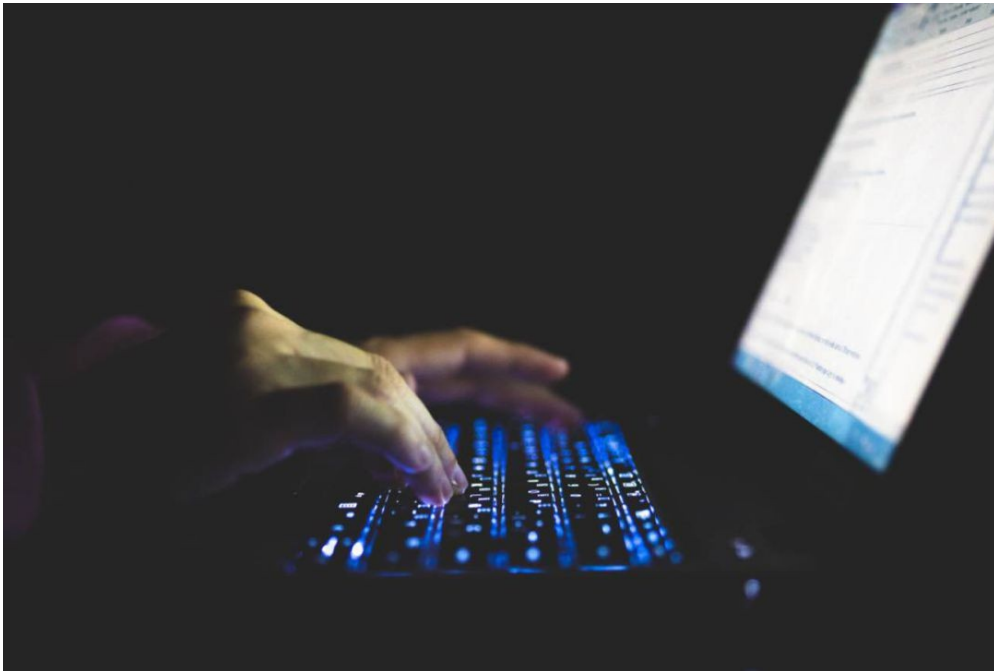
Recursos OSINT DOJO:

<https://www.osintdojo.com/resources/#geolocation>

INTELIGENCIA Y RECONOCIMIENTO WEB

Encontrar información de sitio web, mediante una serie de procesos, para encontrar información dns, tecnología, etc.

Veremos algunos recursos para hacer OSINT a paginas web, shop, plataformas.



Algunos recursos:

<https://sitecheck.sucuri.net/>

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

<https://centralops.net/co/>

<https://dnslytics.com/>

<https://spyonweb.com/>

<https://www.virustotal.com/gui/home/url>

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

<https://viewdns.info/>

<https://dnschecker.org/>

<https://www.nslookup.io/>

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

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

<https://subdomainfinder.c99.nl/>

<https://seranking.com/free-tools/subdomain-finder.html>

<https://osint.sh/subdomain/>

<https://subdomainfinder.c99.nl/scans/2020-04-02/spyse.com>

<https://crt.sh/>

<https://archive.org/>

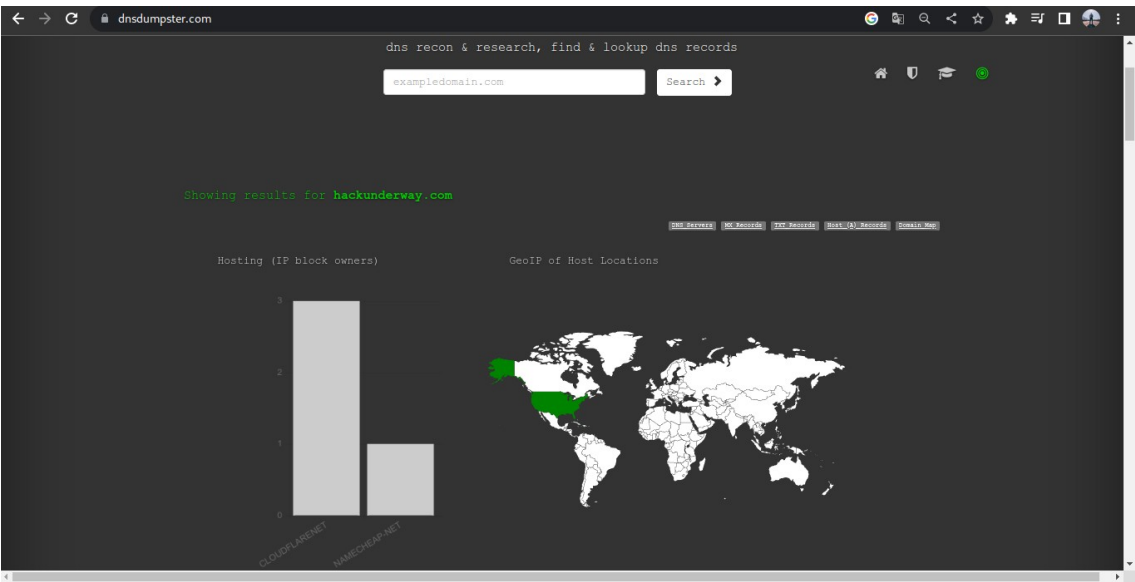
<https://www.isitwp.com/>

<https://www.domain.com/whois/whois/>

<https://whatwpthemeisthat.com/>

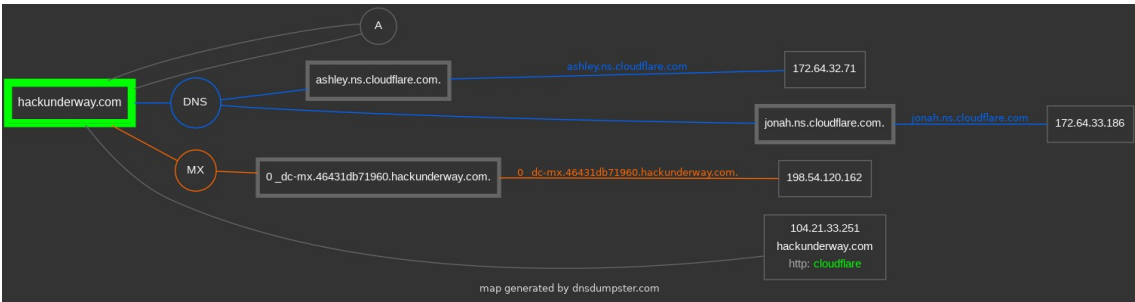
DNSdumpster: <https://dnsdumpster.com/>

dns recon & research, encontrar y buscar registros dns



Se podría exportar el resultado en un archivo .xlsx

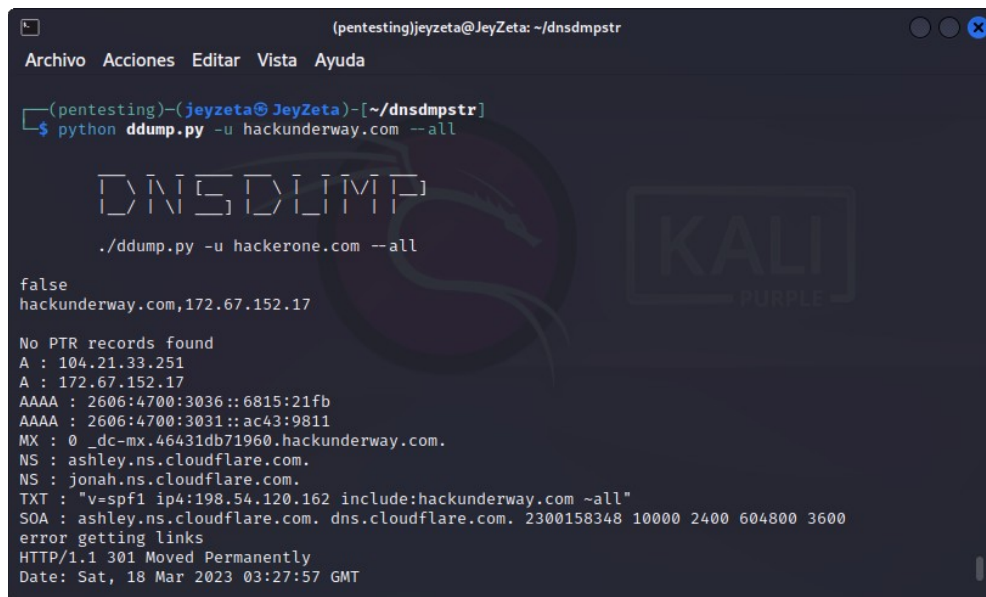
DNS Servers			
ashley.ns.cloudflare.com.	172.64.32.71	CLOUDFLARENET	
	ashley.ns.cloudflare.com	United States	
jonah.ns.cloudflare.com.	172.64.33.186	CLOUDFLARENET	
	jonah.ns.cloudflare.com	United States	
MX Records ** This is where email for the domain goes...			
0 _dc-mx.46431db71960.hackunderway.com.	198.54.120.162	NAMECHEAP-NET	
	premium65-4.web-hosting.com	United States	
TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations			
"v=spf1 ip4:198.54.120.162 include:hackunderway.com ~all"			
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)			
hackunderway.com	104.21.33.251	CLOUDFLARENET	
		unknown	
HTTP: cloudflare			



Lo que vimos arriba en la web, podemos también usarlo desde la terminal con una herramienta que veremos a continuación.

Dnsdmpstr: API y cliente no oficiales para las herramientas DNS Dumpster y HackerTarget.com IP.

<https://github.com/zeropwn/dnsdmpstr>



```
(pentesting)jeyzeta@JeyZeta: ~/dnsdmpstr
Archivo Acciones Editar Vista Ayuda

(pentesting)-(jeyzeta@JeyZeta)-[~/dnsdmpstr]
$ python ddump.py -u hackunderway.com --all

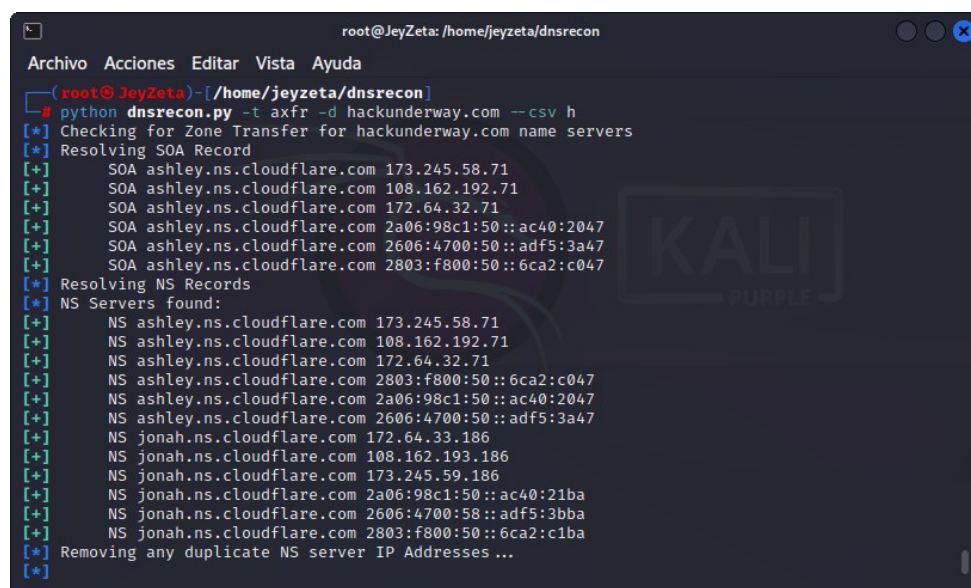
DNSDMP
./ddump.py -u hackerone.com --all

false
hackunderway.com,172.67.152.17

No PTR records found
A : 104.21.33.251
A : 172.67.152.17
AAAA : 2606:4700:3036::6815:21fb
AAAA : 2606:4700:3031::ac43:9811
MX : 0 _dc-mx.46431db71960.hackunderway.com.
NS : ashley.ns.cloudflare.com.
NS : jonah.ns.cloudflare.com.
TXT : "v=spf1 ip4:198.54.120.162 include:hackunderway.com ~all"
SOA : ashley.ns.cloudflare.com. dns.cloudflare.com. 2300158348 10000 2400 604800 3600
error getting links
HTTP/1.1 301 Moved Permanently
Date: Sat, 18 Mar 2023 03:27:57 GMT
```

DNSRecon: Para ver los registros DNS.

<https://github.com/darkoperator/dnsrecon>

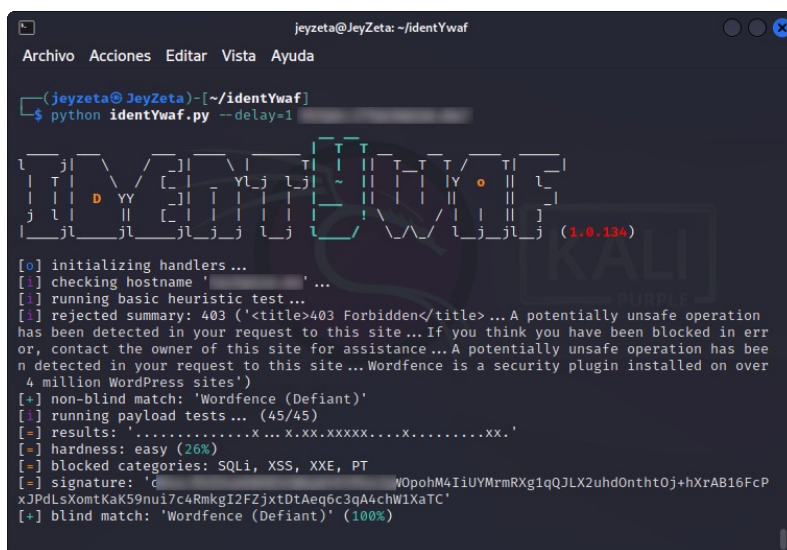


```
root@JeyZeta: /home/jeyzeta/dnsrecon
Archivo Acciones Editar Vista Ayuda

(root@JeyZeta)-[/home/jeyzeta/dnsrecon]
$ python dnsrecon.py -t axfr -d hackunderway.com --csv h
[*] Checking for Zone Transfer for hackunderway.com name servers
[*] Resolving SOA Record
[+] SOA ashley.ns.cloudflare.com 173.245.58.71
[+] SOA ashley.ns.cloudflare.com 108.162.192.71
[+] SOA ashley.ns.cloudflare.com 172.64.32.71
[+] SOA ashley.ns.cloudflare.com 2a06:98c1:50::ac40:2047
[+] SOA ashley.ns.cloudflare.com 2606:4700:50::adf5:3a47
[+] SOA ashley.ns.cloudflare.com 2803:f800:50::6ca2:c047
[*] Resolving NS Records
[*] NS Servers found:
[+] NS ashley.ns.cloudflare.com 173.245.58.71
[+] NS ashley.ns.cloudflare.com 108.162.192.71
[+] NS ashley.ns.cloudflare.com 172.64.32.71
[+] NS ashley.ns.cloudflare.com 2803:f800:50::6ca2:c047
[+] NS ashley.ns.cloudflare.com 2a06:98c1:50::ac40:2047
[+] NS ashley.ns.cloudflare.com 2606:4700:50::adf5:3a47
[+] NS jonah.ns.cloudflare.com 172.64.33.186
[+] NS jonah.ns.cloudflare.com 108.162.193.186
[+] NS jonah.ns.cloudflare.com 173.245.59.186
[+] NS jonah.ns.cloudflare.com 2a06:98c1:50::ac40:21ba
[+] NS jonah.ns.cloudflare.com 2606:4700:58::adf5:3bba
[+] NS jonah.ns.cloudflare.com 2803:f800:50::6ca2:c1ba
[*] Removing any duplicate NS server IP Addresses ...
[*]
```


IdentYwaf: <https://github.com/stamparm/identYwaf>

identYwaf es una herramienta de identificación que puede reconocer el tipo de protección web (es decir, WAF) basándose en la inferencia ciega. La inferencia ciega se realiza inspeccionando las respuestas provocadas por un conjunto de cargas útiles ofensivas (no destructivas) predefinidas, que se utilizan únicamente para activar el sistema de protección web intermedio.



```
jeyzeta@JeyZeta: ~/identYwaf
Archivo Acciones Editar Vista Ayuda

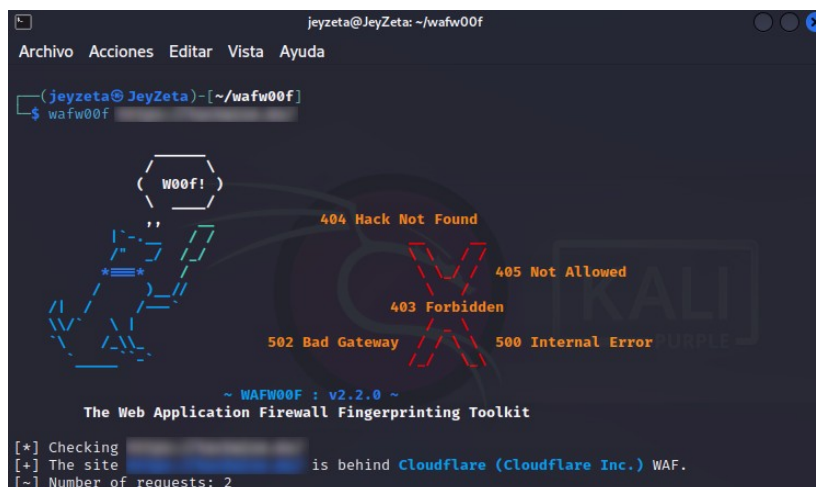
(jeyzeta@JeyZeta)-[~/identYwaf]
$ python identYwaf.py --delay=1

IDENTIFYWAF (1.0.134)

[0] initializing handlers...
[1] checking hostname '...'
[1] running basic heuristic test...
[1] rejected summary: 403 ('<title>403 Forbidden</title> ... A potentially unsafe operation
has been detected in your request to this site ... If you think you have been blocked in err
or, contact the owner of this site for assistance ... A potentially unsafe operation has bee
n detected in your request to this site ... Wordfence is a security plugin installed on over
4 million WordPress sites')
[+] non-blind match: 'Wordfence (Defiant)'
[1] running payload tests ... (45/45)
[+] results: '.....X...X.XX.XXXXX...X.....XX.'
[+] hardness: easy (26%)
[+] blocked categories: SQLi, XSS, XXE, PT
[+] signature: 'c...WOpohM4IiUYMrmRXg1qQLX2uhdOntht0j+hXrAB16FcP
xJPdLsXomtKaK59nui7c4RmkgI2FZjxtDtAeq6c3qA4chW1XaTc'
[+] blind match: 'Wordfence (Defiant)' (100%)
```

WAFW00F: <https://github.com/EnableSecurity/wafw00f>

WAFW00F es una herramienta muy parecida a la que vimos anteriormente, permite identificar y tomar huellas dactilares de los productos Web Application Firewall (WAF) que protegen un sitio web.



```
jeyzeta@JeyZeta: ~/wafw00f
Archivo Acciones Editar Vista Ayuda

(jeyzeta@JeyZeta)-[~/wafw00f]
$ wafw00f

W00f!

404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error

~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking ...
[+] The site ... is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

```
(jeyzeta@JeyZeta)-[~/wafw00f]
$ wafw00f [redacted]

      ( Woof! )
    (  )  (  )
   (  )  (  )
  (  )  (  )
 (  )  (  )
(  )  (  )

~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking [redacted]
[+] The site [redacted] is behind CacheWall (Varnish) WAF.
[~] Number of requests: 2
```

Vemos 2 ejemplos con diferentes url, y cada una dio diferentes resultados, porque están protegidos por diferentes WAF.

Para saber la Ip, real de un sitio web, hay varios métodos, como usando Shodan, CloudFail, etc.

<https://medium.com/@hengky.kaiqi/finding-the-real-ip-address-of-a-website-behind-cloud-flare-c2115be8d163>

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

```
root@JeyZeta: /home/jeyzeta/Descargas
Archivo Acciones Editar Vista Ayuda

(root@JeyZeta)-[/home/jeyzeta/Descargas]
# theHarvester -d [redacted] -l 500 -b bing
*****
*
* [redacted]
*
*
* theHarvester 4.2.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[*] Target: [redacted]
    Searching 0 results.
[*] Searching Bing.
[*] No IPs found.
[*] Emails found: 4
[redacted]
```

```
root@JeyZeta: /home/jeyzeta/Descargas
[*] Emails found: 4
[*] Hosts found: 18
(root@JeyZeta)-[/home/jeyzeta/Descargas]
```

Sublist3r: <https://github.com/about3la/Sublist3r>

```
(pentesting)root@JeyZeta: /home/jeyzeta/Sublist3r
# python sublist3r.py -d [redacted]

Sublist3r
# Coded By Ahmed Aboul-Ela - @about3la

[-] Enumerating subdomains now for [redacted]
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..

[-] Total Unique Subdomains Found: 18

(pentesting)-(root@JeyZeta)-[/home/jeyzeta/Sublist3r]
```

Scilla: <https://github.com/edoardottt/scilla>

```
(jeyzeta@JeyZeta)~[/scilla]
$ scilla subdomain -target [redacted]

  Scilla  v1.2.6

> github.com/edoardottt/scilla
> edoardoottavianelli.it

=====
target: [redacted]
===== SCANNING SUBDOMAINS =====
[+]FOUND: [redacted]
[+]FOUND: [redacted]
[+]FOUND: [redacted]
[+]FOUND: [redacted]
```

GoSFinder: Es una herramienta con fines educativos, para la búsqueda del panel de administrador (admin finder) de sitios web, hecho para investigadores de seguridad.

<https://github.com/HackingEnVivo/GoSFinder>

```
jeyzeta@JeyZeta: ~/GoSFinder
Archivo Acciones Editar Vista Ayuda

(jeyzeta@JeyZeta)~[/GoSFinder]
$ python2 GoSFinder.py -n "Hack Underway"
Buena suerte con tu escaneo. Hack Underway

  KALI  PURPLE

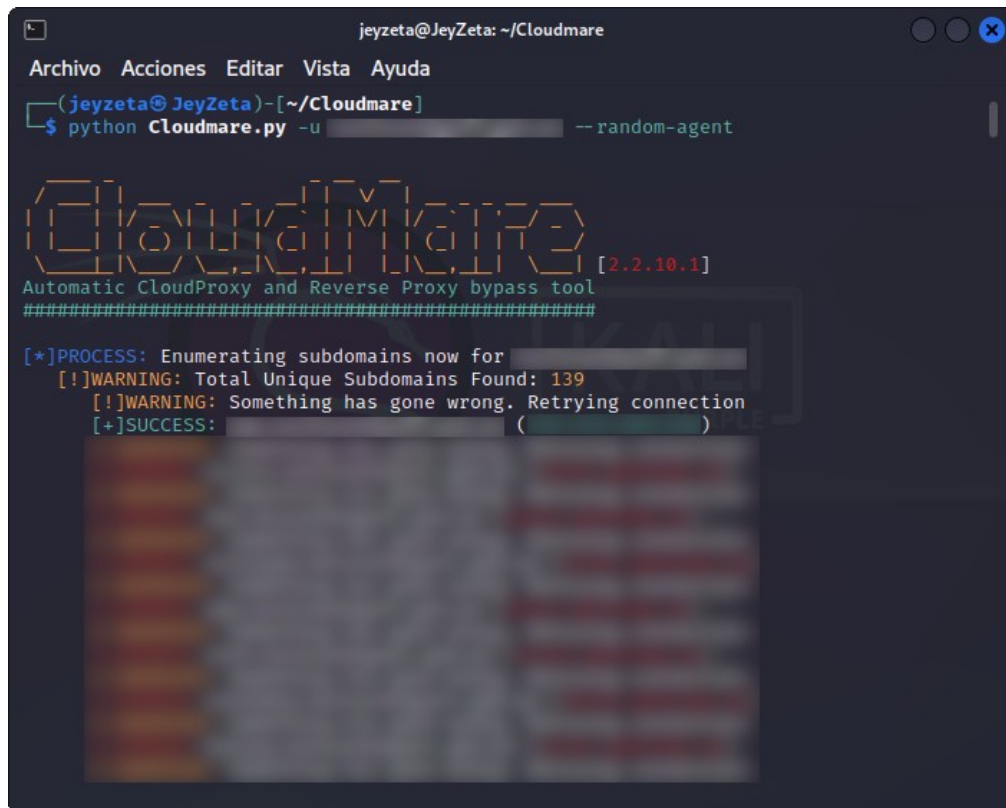
> SITIO PARA SCANEAR: [redacted]

admin/
administrator/
admin1/
cms/
admin2/
admin3/
admin4/
admin5/
usuarios/
usuario/
administrator/

[+]FOUND[+]
[-]ERROR[-]
[-]ERROR[-]
[-]ERROR[-]
[-]ERROR[-]
[-]ERROR[-]
[-]ERROR[-]
[-]ERROR[-]
[-]ERROR[-]
[-]ERROR[-]
[-]ERROR[-]
```

CloudMare: Es una sencilla herramienta para encontrar los servidores de origen de sitios web protegidos por Cloudflare, Sucuri, o Incapsula con un DNS mal configurado.

<https://github.com/mrh0wl/Cloudmare>



```
jeyzeta@JeyZeta: ~/Cloudmare
Archivo Acciones Editar Vista Ayuda
(jeyzeta@JeyZeta)-[~/Cloudmare]
$ python Cloudmare.py -u [redacted] --random-agent

[2.2.10.1]
Automatic CloudProxy and Reverse Proxy bypass tool
#####

[*]PROCESS: Enumerating subdomains now for [redacted]
[!]WARNING: Total Unique Subdomains Found: 139
[!]WARNING: Something has gone wrong. Retrying connection
[+]SUCCESS: [redacted] ( [redacted] )
```

Cignotrack: Herramienta de espionaje empresarial para comprobar la privacidad y la seguridad mediante OSINT e ingeniería social.

Cignotrack tiene estas características:

- Extraer y analizar los metadatos de imágenes y documentos objetivo.
- Descubrir información relacionada con whois, IP y tecnologías.
- Búsqueda de correos electrónicos y seguimiento de redes sociales.
- Buscar archivos sensibles.
- Rastrear la búsqueda en Internet del objetivo (DNS cache snooping).

- <https://github.com/Cignoraptor-ita/cignotrack>

WhatWeb: Identifica sitios web, reconoce tecnologías web como sistemas de gestión de contenidos (CMS), plataformas de blogs, paquetes estadísticos/analíticos, bibliotecas JavaScript, servidores web y dispositivos integrados.

217

WPSeku: Escáner de seguridad de Wordpress.

<https://github.com/andripwn/WPSeku>

```
jeyzeta@JeyZeta: ~/WPSeku
```

```
Archivo Acciones Editar Vista Ayuda
```

```
python3 wpseku.py --url http://[REDACTED] / --verbose
```

```
[REDACTED]
```

```
v0.4.0
```

```
WPSeku - Wordpress Security Scanner  
by Momo Outaadi (m4ll0k)
```

```
[ + ] Target: http://[REDACTED]/  
[ + ] Starting: 21:46:33
```

```
[ + ] Server: LiteSpeed  
[ + ] Uncommon header "content-type" found, with contents: text/html; charset=UTF-8  
[ + ] Uncommon header "link" found, with contents: <https://[REDACTED]/wp-json/>; rel="https://api.w.org/", <https://[REDACTED]/wp-json/wp/v2/pages/5008>; rel="alternate"; type="application/json", <https://[REDACTED]>; rel=shortlink  
[ + ] Uncommon header "transfer-encoding" found, with contents: chunked  
[ + ] Uncommon header "content-encoding" found, with contents: br  
[ + ] Uncommon header "vary" found, with contents: Accept-Encoding,User-Agent  
[ + ] Uncommon header "date" found, with contents: Tue, 18 Apr 2023 02:46:36 GMT  
[ + ] Uncommon header "server" found, with contents: LiteSpeed  
[ + ] Uncommon header "alt-svc" found, with contents: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"  
[ i ] Checking Full Path Disclosure...  
[ i ] Checking wp-config backup file...  
[ + ] wp-config.php available at: http://[REDACTED]/wp-config.php  
[ i ] Checking common files...  
[ + ] robots.txt file was found at: http://[REDACTED]/robots.txt
```

WPScan: Es un escáner de seguridad para WordPress.

<https://wpscan.com/wordpress-security-scanner>

```

jeyzeta@JeyZeta: ~
Archivo Acciones Editar Vista Ayuda

(jeyzeta@JeyZeta)-[~]
$ wpscan --url [redacted] --enumerate u --random-user-agent

WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: [redacted]
[+] Started: [redacted]

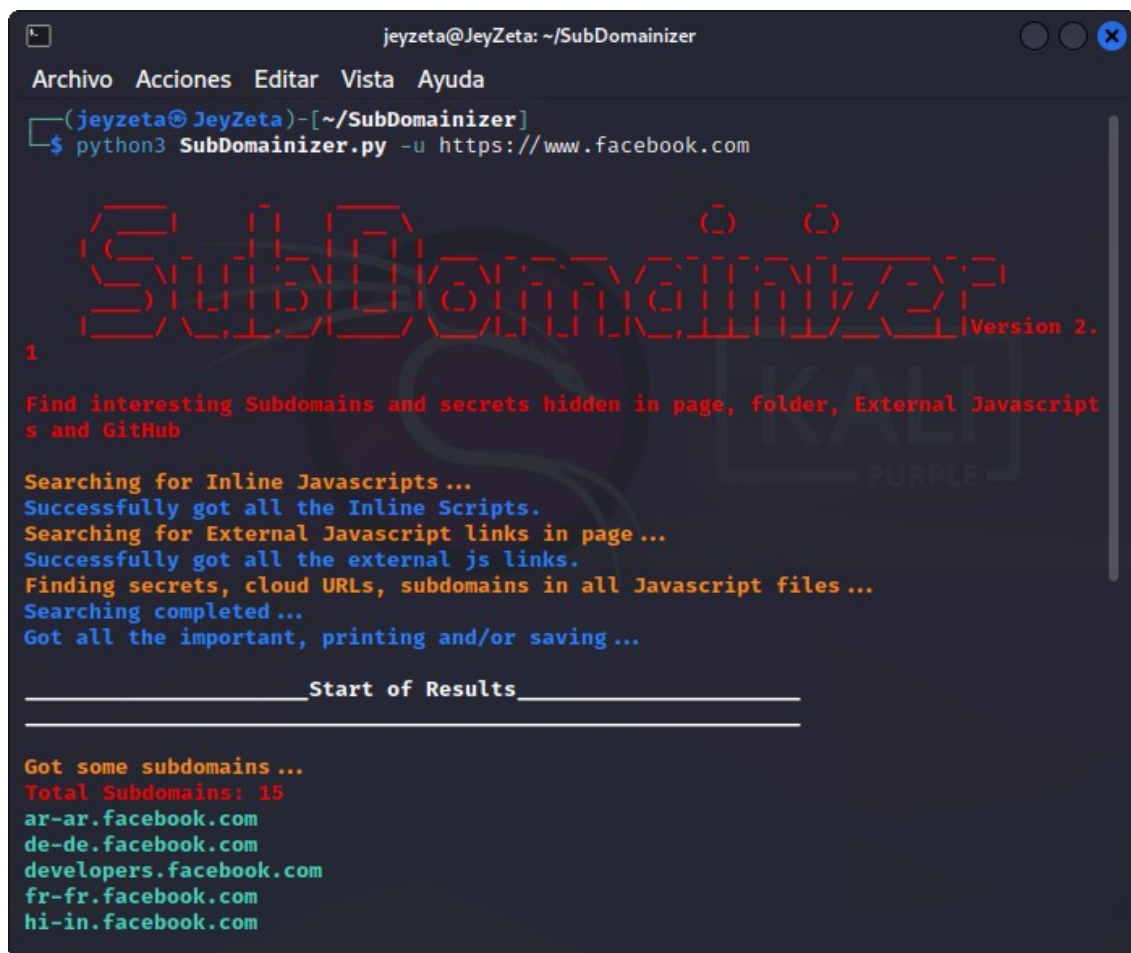
Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - Server: Apache
| - X-Powered-By: PHP/7.4.33
| Found By: Headers (Passive Detection)

```


SubDomainizer: es una herramienta diseñada para encontrar subdominios ocultos y secretos presentes ya sea página web, Github, y javascripts externos presentes en la URL dada. Esta herramienta también encuentra cubos de S3, URL de cloudfront y más de esos archivos JS que podrían ser interesantes como cubo de S3 está abierto a lectura/escritura, o toma de subdominio y caso similar para cloudfront. También escanea dentro de la carpeta dada que contiene sus archivos.

<https://github.com/nsonaniya2010/SubDomainizer>



```
jeyzeta@JeyZeta: ~/SubDomainizer
Archivo Acciones Editar Vista Ayuda
(jeyzeta@JeyZeta)-[~/SubDomainizer]
$ python3 SubDomainizer.py -u https://www.facebook.com

SubDomainizer Version 2.
1

Find interesting Subdomains and secrets hidden in page, folder, External Javascripts and GitHub

Searching for Inline Javascripts ...
Successfully got all the Inline Scripts.
Searching for External Javascript links in page ...
Successfully got all the external js links.
Finding secrets, cloud URLs, subdomains in all Javascript files ...
Searching completed ...
Got all the important, printing and/or saving ...

_____Start of Results_____

Got some subdomains ...
Total Subdomains: 15
ar-ar.facebook.com
de-de.facebook.com
developers.facebook.com
fr-fr.facebook.com
hi-in.facebook.com
```

URLextractor: Recopilación de información y reconocimiento de sitios web.

<https://github.com/eschultze/URLextractor>

```
jeyzeta@JeyZeta: ~/URLextractor
Archivo Acciones Editar Vista Ayuda
#####
# URLextractor #
# Information Gathering & Website Reconnaissance #
# coded by eschultze #
# https://phishstats.info/ #
# version - 0.2.0 #
#####
[INFO] Date: 18/04/23 | Time: 22:12:53
[INFO] _____TARGET info_____
[*] TARGET: https://[REDACTED]/
[*] TARGET IP: [REDACTED]
[ALERT] [REDACTED] has a load balancer for IPv4 with the following IPs:
[*] [REDACTED]
[*] [REDACTED]
[*] [REDACTED]
[*] [REDACTED]
[*] [REDACTED]
[*] DNS servers: c.ns.buddyns.com.
[*] TARGET server:
[*] CC: FR
[*] Country: France
[*] RegionCode: HDF
[*] RegionName: Hauts-de-France
[*] City: Roubaix
[*] ASN: [REDACTED]
[*] BGP_PREFIX: [REDACTED]/16
[*] ISP: OVH OVH SAS, FR
[INFO] SSL/HTTPS certificate detected
[*] Issuer: issuer=C = GR, O = Hellenic Academic and Research Institutions CA, CN = HARICA
DV TLS RSA
[*] Subject: subject=CN = [REDACTED]rewxee3vyu6ex37ukyvdw6jm66npakiyd.onion
[INFO] DNS enumeration:
```

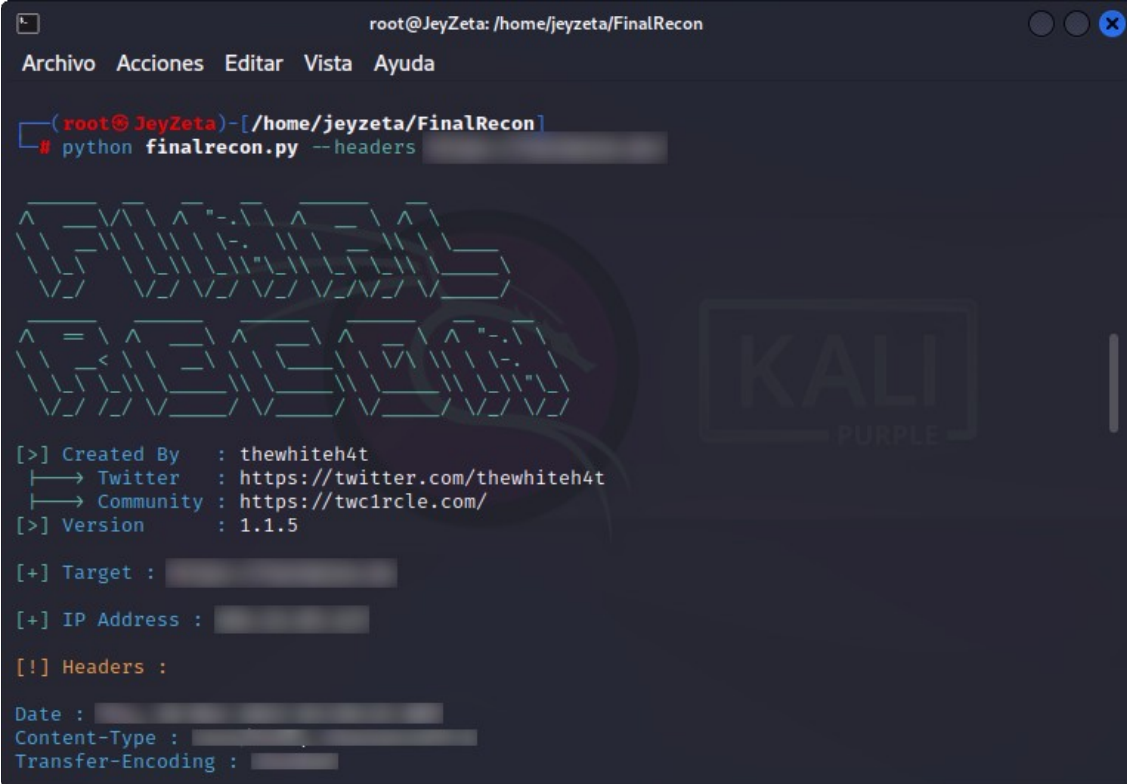
FinalRecon: Es una herramienta automática de reconocimiento web escrita en python. El objetivo de FinalRecon es proporcionar una visión general del objetivo en poco tiempo manteniendo la precisión de los resultados. En lugar de ejecutar varias herramientas una tras otra puede proporcionar resultados similares manteniendo las dependencias pequeñas y simples.

FinalRecon proporciona información detallada como :

- Header Information
- Whois
- SSL Certificate Information
- Crawler
- DNS Enumeration

- Subdomain Enumeration
- Directory Searching
- Wayback Machine
- Port Scan
- Export

<https://github.com/thewhiteh4t/FinalRecon>



```

root@JeyZeta: /home/jeyzeta/FinalRecon
Archivo Acciones Editar Vista Ayuda

(root@JeyZeta)-[/home/jeyzeta/FinalRecon]
# python finalrecon.py --headers

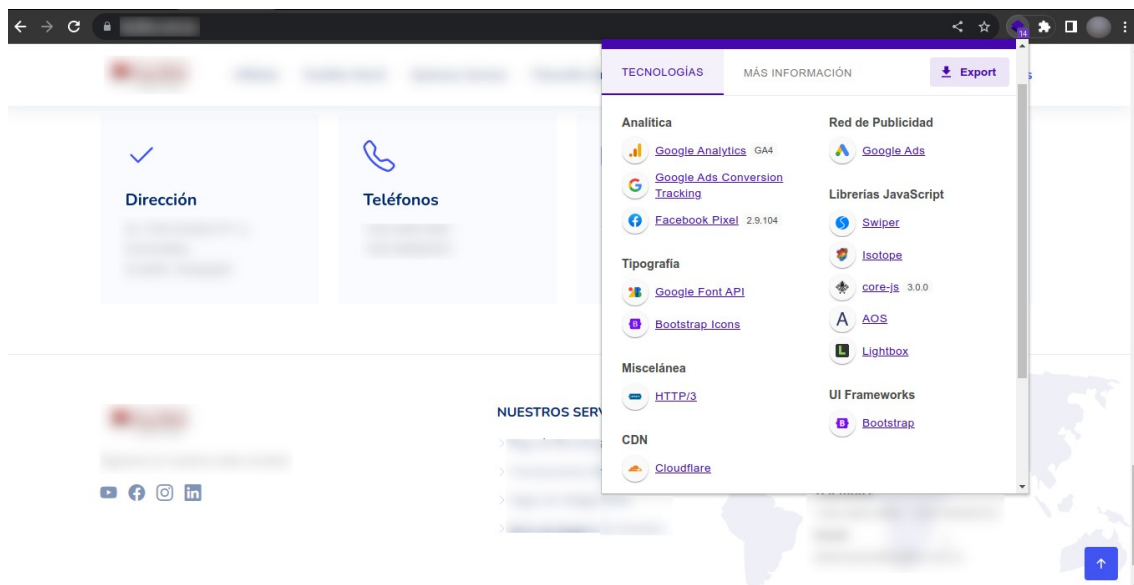
[>] Created By : thewhiteh4t
    |→ Twitter : https://twitter.com/thewhiteh4t
    |→ Community : https://twcircle.com/
[>] Version : 1.1.5

[+] Target : 
[+] IP Address : 
[!] Headers :
Date : 
Content-Type : 
Transfer-Encoding :
  
```

Wappalyzer: Es una herramienta online para Identificar tecnologías en los sitios web, para hacer las consultas debe crearse una cuenta free o también puede instalar la extensión para su navegador.

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

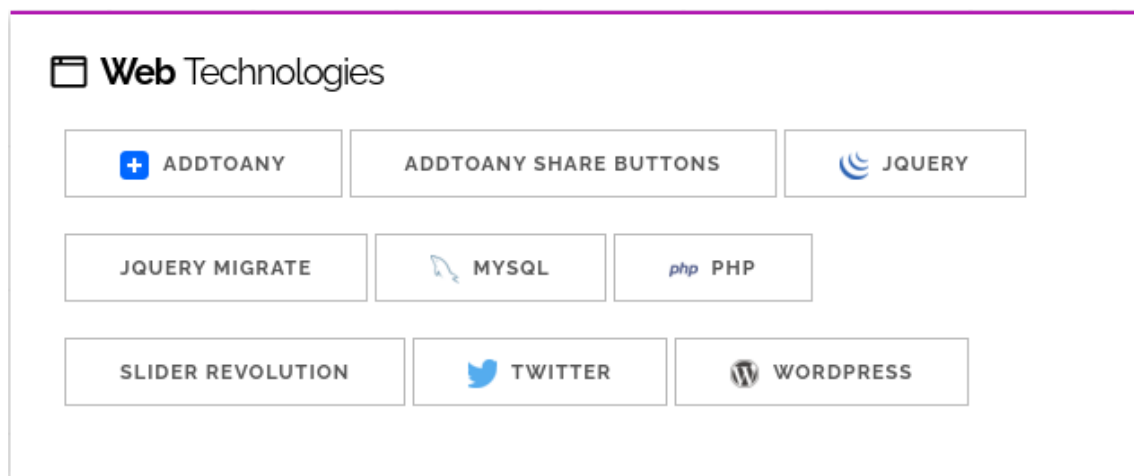
<https://chrome.google.com/webstore/detail/wappalyzer-technology-pro/gppongmhjkpfnbhagpmjfkannfbllamg?hl=es>



Shodan:

Si estaríamos viendo los host de shodan mediante una IP

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



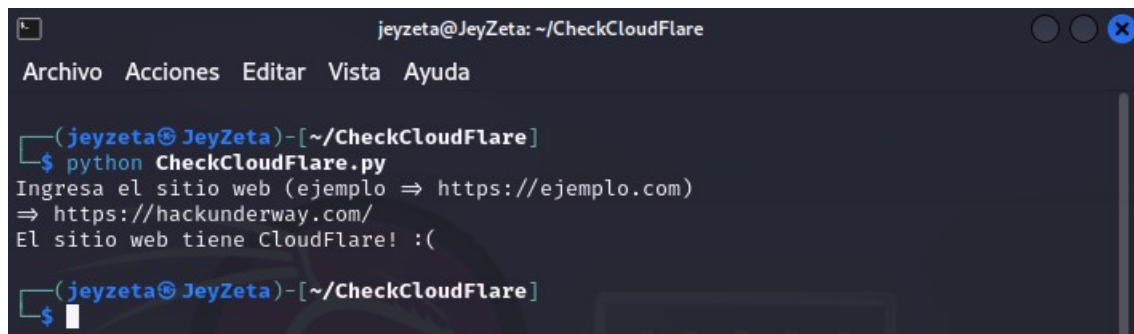
También nos muestra la tecnología que usa la IP o url de un sitio web.

Para terminar esta sección, les mostraré una herramienta simple y útil, que subí hace unos meses a mi repositorio de GitHub.

CheckCloudFlare:

Verificar si un sitio web tiene CLOUDFLARE

<https://github.com/HackUnderway/CheckCloudFlare>



```
jeyzeta@JeyZeta: ~/CheckCloudFlare
Archivo Acciones Editar Vista Ayuda

(jeyzeta@JeyZeta)~[~/CheckCloudFlare]
$ python CheckCloudFlare.py
Ingresa el sitio web (ejemplo => https://ejemplo.com)
=> https://hackunderway.com/
El sitio web tiene CloudFlare! :(

(jeyzeta@JeyZeta)~[~/CheckCloudFlare]
$
```

Otras herramientas:

<https://github.com/m0rtem/CloudFail>

<https://github.com/HackingEnVivo/ShellFinder>

<https://github.com/hash3liZer/Subrake>

<https://github.com/mlcHyAmRaNe/okadminfinder3>

<https://github.com/s0md3v/photon>

<https://github.com/InitRoot/fransRecon>

<https://github.com/evyatarmeged/Raccoon>

<https://github.com/bahatiphill/BillCipher>

Hay muchas más herramientas, pero esos temas de auditorias o web pentesting, lo veremos en otro manual de web pentesting y bug bounty.

REDES SOCIALES

OSINT a redes sociales como facebook, instagram, twitter, twith, tiktok, vk, youtube, vimeo, etc.

Usaremos herramientas online y desde la terminal para automatizar los procesos de recolección de información.



Youtube:

[Youtube Lookup](#)

[DownSub](#)

[video-information-of-youtube](#)

[SaveSubs](#)

[Youtube DL](#)

[Youtube Metadata](#)

Twitter:

[Foller.me](#)

[Nitter](#)

[Tinfoleak](#)

[Tweet Beaver](#)

[Tweetdeck](#)

[Twitter OSINT Attack Surface](#)

[Spoonbill](#)

[Trendsmap](#)

[TweeterID](#)

TikTok:

[OSINT Investigations on TikTok](#)

[TikTok OSINT Bookmarklet Tools](#)

[Vidnice](#)

[Avatares](#)

Tumblr:

[Tumblr OSINT Bookmarklet Tools](#)

[Tumblr OSINT Techniques](#)

Snapchat:

[Snap Map](#)

Skype:

[Skype Resolver](#)

[Skypli](#)

Reddit:

[Rdddeck](#)

[Reddit OSINT Bookmarklet Tools](#)

[Reddit OSINT Techniques](#)

[Uddit](#)

Pinterest:

[OSINT Investigation on Pinterest](#)

LinkedIn:

[Epieos LinkedIn Tool](#)

[How to conduct OSINT on LinkedIn](#)

[LinkedIn OSINT Bookmarklet Tools](#)

[LinkedIn OSINT Techniques: Part I](#)

[LinkedIn OSINT Techniques: Part II](#)

[New LinkedIn Search Features](#)

Instagram:

[Gramho](#)

[Identifying Followers of a Private Instagram Profile](#)

[Picuki](#)

[Stories Down](#)

[Osintgram](#)

[osi.ig](#)

[instaloader](#)

[osgint](#)

GitHub:

[Github URL Hacks](#)

[Gitrecon](#)

[OctoSuite](#)

[Osgint](#)

[Zen](#)

Discord:

[DiscordBee](#)

[DiscordHub User Search](#)

[DiscordServers Search](#)

[Discord Snowflake to Timestamp Converter](#)

[Dutch OSINT Guy Discord Resources](#)

Facebook:

[Facebook ID](#)

[Facebook Graph Searcher](#)

[Tips](#)

Telegram:

[Awesome Telegram OSINT](#)

[Telegram Analytics](#)

[Telegram Database](#)

[Tools](#)

Recursos:

<https://www.osintdojo.com/resources/>

<https://map.malfrats.industries/>

<https://github.com/Malfrats/OSINT-Map>

WhatsApp:

<https://github.com/jasperan/whatsapp-osint>

Ejemplos del mundo real:

Ahora veremos algunos ejemplos de herramientas.

Investigación OSINT en Facebook:

En el verano de 2019, Facebook redujo drásticamente su función Graph Search, que había permitido a los usuarios desenterrar grandes cantidades de información. Varias herramientas en línea gratuitas que habían hecho uso de la función dejaron de funcionar. Lo que siguió ha sido un juego del gato y el ratón, ya que los creadores de las herramientas hicieron cambios para eludir los cambios realizados por Facebook, que a su vez ajustó las cosas de nuevo para cerrar y el ciclo continuó. El resultado es que algunas herramientas han desaparecido probablemente de forma permanente y otras funcionan de forma intermitente.

Si bien estos cambios fueron una bendición para los defensores de la privacidad, ya que los datos estaban un poco más seguros y era más difícil acceder a ellos, los investigadores de OSINT y las fuerzas del orden tuvieron algunos problemas enormes, ya que los datos que habían estado recopilando durante años desaparecieron de la noche a la mañana. Meses más tarde, muchos investigadores habían descubierto métodos para buscar algunos de los mismos contenidos que antes, pero Facebook no hizo una transferencia uno por uno de las características de la búsqueda gráfica anterior a la actual. Muchas de las búsquedas en las que confiábamos para descubrir relaciones y ubicaciones de personas en Facebook simplemente ya no están disponibles.

Detalles del perfil de Facebook:

Facebook asigna a cada usuario un número de usuario único, a cada página un número de página y a cada grupo un número de grupo. Este número lo utiliza el sitio para anotar las actividades (historias que publican, fotos que comentan, vídeos en los que están etiquetados, etc.) de ese objeto (usuario, página o grupo). Este número es un identificador único que nos permitirá buscar información de Facebook que de otro modo quedaría oculta. Para realizar las siguientes búsquedas avanzadas para obtener contenido sobre nuestros objetivos, debes conocer el número de usuario de tu objetivo.

Para encontrar el ID de usuario podemos hacerlo manualmente o por medio de una herramienta online.

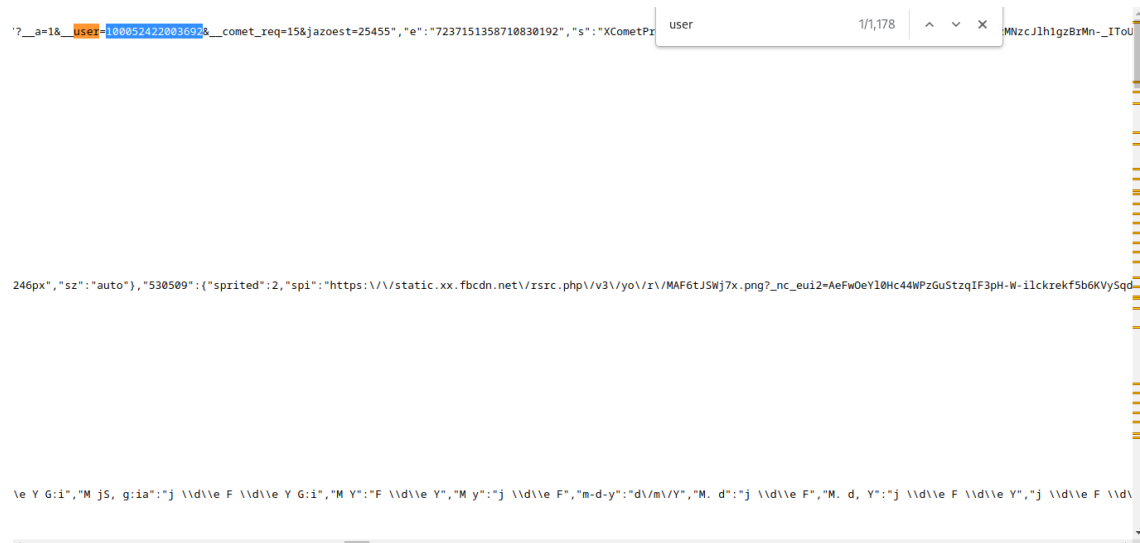
User ID de forma manual:

La forma más potente de hacerlo es ver el código fuente del perfil de Facebook de tu usuario objetivo. El proceso varía según el navegador. En Firefox y Chrome, puedes hacer lo siguiente:

Haz clic con el botón derecho del ratón en la página del perfil de Facebook de tu objetivo y selecciona "Ver fuente de la página".

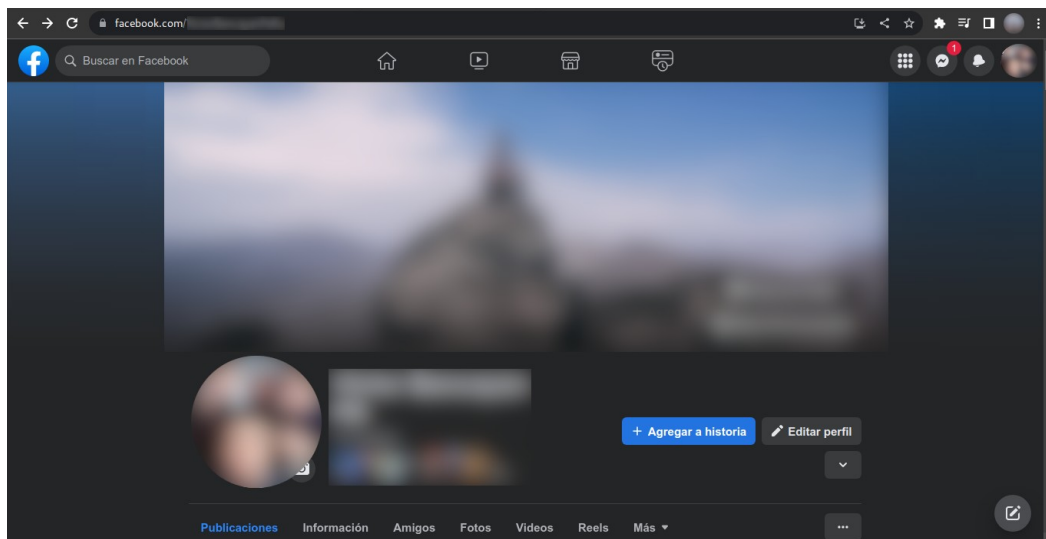
Escribe Ctrl + U.

Asegúrate de no pasar el ratón sobre ningún hipervínculo mientras haces clic con el botón derecho. Se abrirá una nueva pestaña con una vista de sólo texto del código fuente de ese perfil. En el navegador, busque "user" en esta página. Esto identificará una parte del código dentro de esta página que contiene ese término específico.



Al poner facebook.com/100052422003692

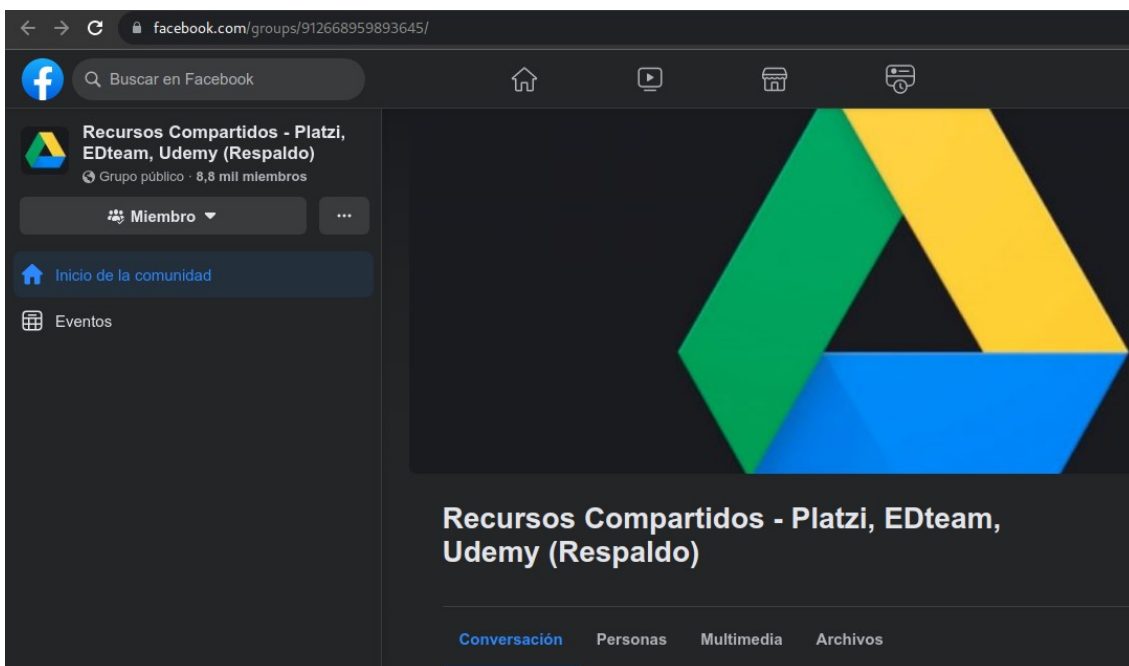
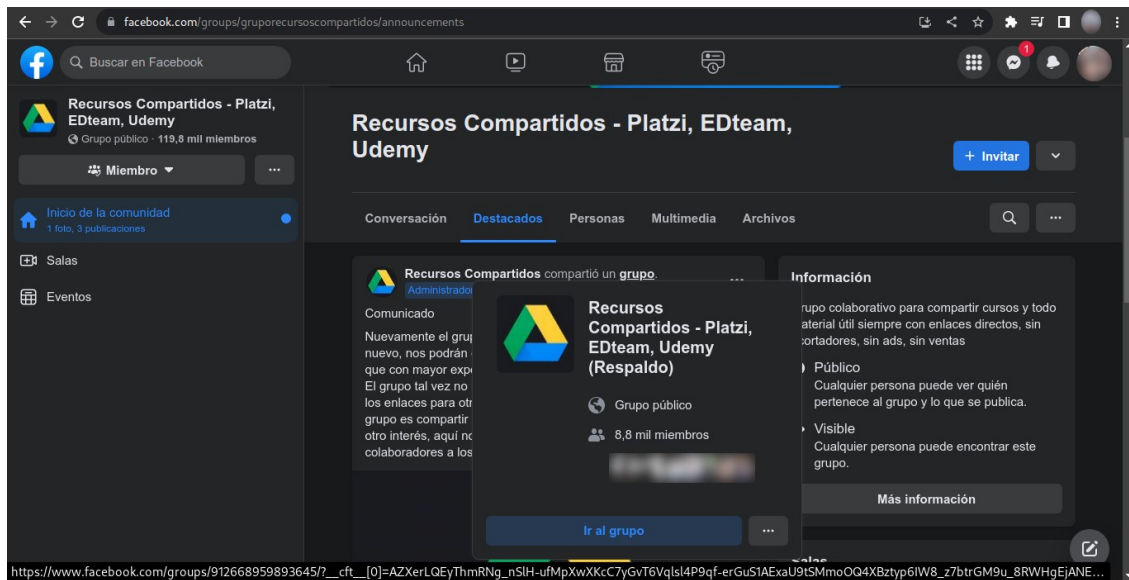
Nos debería redirigir al perfil de facebook.



Buscar el identificador único de un grupo de Facebook es un proceso más sencillo.

Localiza un grupo de Facebook:

En este caso nos iremos a la sección destacados, seleccionamos con el mouse la parte que dice “grupo”, en la parte de abajo sale una previsualización de la URL, abrimos otra pestaña.

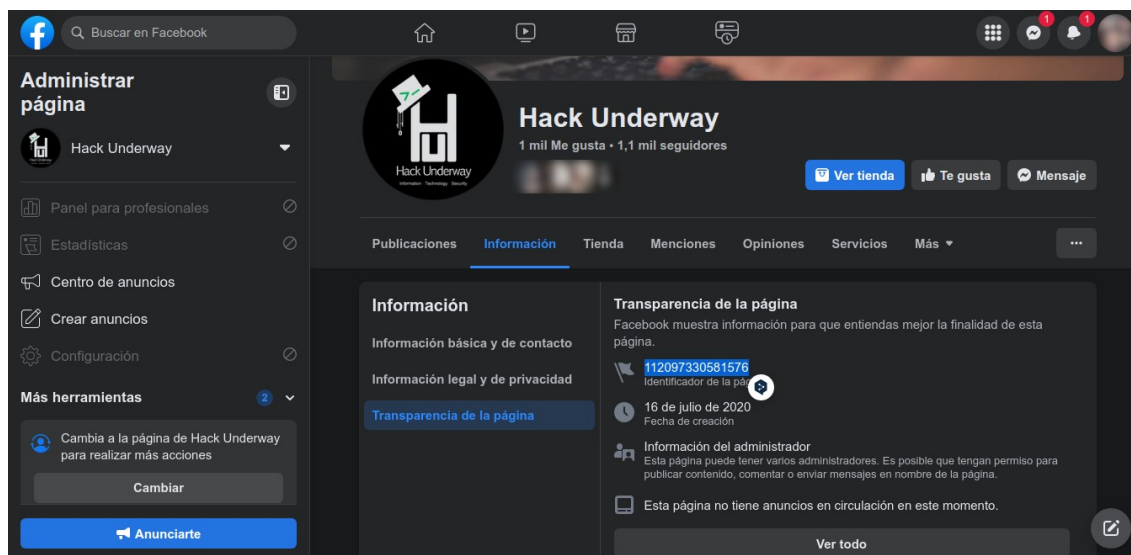


Localizar ID de Fanpage:

https://www.facebook.com/HackUnderway/about_profile_transparency

En este caso nos hemos dirigido a la pestaña “Información”, y a la sub pestaña “Transparencia de la página”.

Encontramos el Identificador de la página.



Fecha de creación del ID de Facebook:

El investigador de OSINT [Josh Huff](#) se dio cuenta de que los ID de perfil de Facebook eran números y que las cuentas más nuevas tenían números más grandes que las más antiguas. Emprendió un proyecto de investigación de un año de duración para rastrear perfiles nuevos y antiguos de Facebook y determinar cuándo se habían creado.

Los resultados de Josh pueden verse en su entrada del blog y en la 8ª edición del libro de Michael Bazzell Open Source Intelligence Techniques (página 237).

Facebook pasó de números de 32 bits, como 554432, a números de 64 bits que empiezan por 100000 entre abril y diciembre de 2009. Por lo tanto, si el número de tu objetivo es inferior a 1000000000000000, es probable que la cuenta se creara antes de abril de 2009. Una cuenta con un número de identificación de 15 dígitos se habría creado después de diciembre de 2009. Podemos desglosar los números por año. Las siguientes son estimaciones

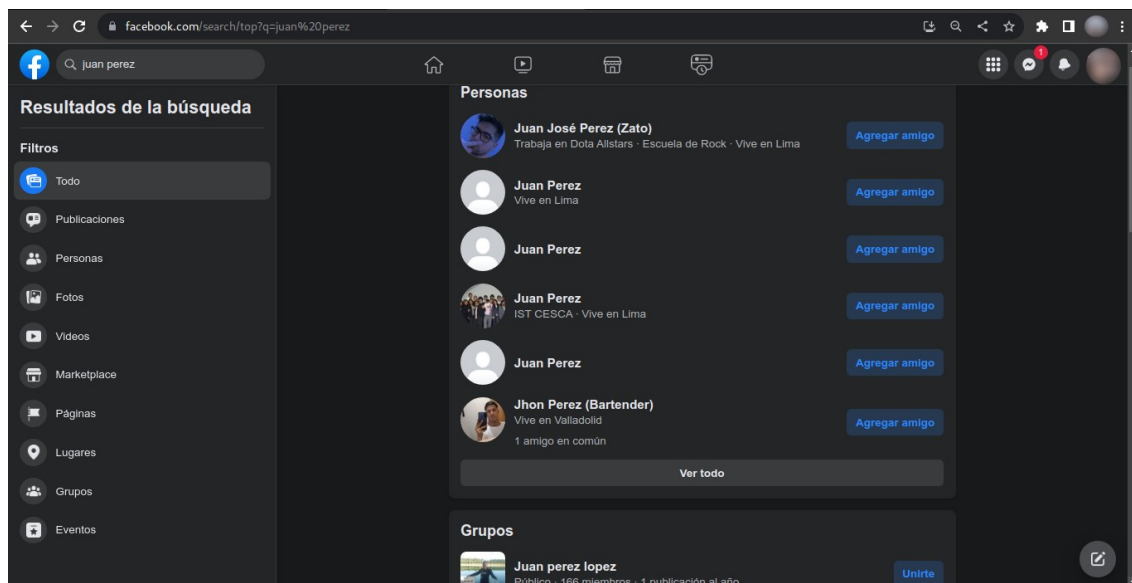
aproximadas que sólo deben utilizarse como orientación general. Facebook parece haber empezado a emitir números aleatorios en 2018.

Año de creación de la cuenta	Rangos de ID de Facebook
2006	Números inferiores a 600400000
2007	600400000 - 1000000000
2008	1000000000 - 1140000000
2009	1140000000- 100000628000000
2010	100000629000000 - 100001610000000
2011	100001 611000000 - 100003302000000
2012	100003303000000 - 100004977000000
2013	100004978000000 - 100007376000000
2014	100007377000000 - 100008760000000
2015	100008761000000 - 100010925000000
2016	100010926000000 - 100014946000000
2017	100014947000000 - 100023810000000
2018	100023811000000 -

Opciones de búsqueda en Facebook:

La función de búsqueda integrada en Facebook es la barra de búsqueda situada en la parte superior izquierda de la mayoría de las pantallas. Si escribes el nombre real de un objetivo, es posible que aparezcan resultados, muchos de los cuales no están relacionados con tu investigación. Para llegar a tu objetivo, es posible que tengas que dar pasos adicionales. Al buscar el nombre (Juan Perez,... por ejemplo), pueden aparecer varias categorías/opciones en los resultados. Obviamente, hay más Joseph Smiths en Facebook que los que aparecen aquí. En la parte inferior de esta lista hay una

opción para "Ver todos" los perfiles con el nombre buscado. Esta lista tampoco es exhaustiva. Al desplazarse hacia abajo deberían aparecer automáticamente más perfiles. Podría echar un vistazo y esperar identificar a su objetivo basándose en la foto, la ubicación o la información adicional que aparece en esta vista. En su lugar, puede refinar su búsqueda incluyendo filtros en el menú de la izquierda.



Por defecto, la búsqueda en Facebook comienza con la categoría "top". También podemos verlo en la URL anterior ("/search/top/").

Cabe recalcar que hay perfiles de Fb, que son privados y facebook en esa parte les brinda una protección extra, ya que han habilitado esa opción que actualmente está habilitado sólo para algunos países.

Esa opción les brinda un plus de privacidad a algunos países, lastimosamente para los países de latinoamerica no está disponible esa opción.

¿Qué es Profile Picture Guard?

Conocida como Profile Picture Guard, se trata de una característica de seguridad de la red social. Nos damos cuenta de que una foto de perfil se encuentra protegida porque aparecerá un icono en forma de escudo debajo de la misma. Gracias a esta característica podemos evitar que alguien copie, comparta, descarga o tome una captura de pantalla de la foto.

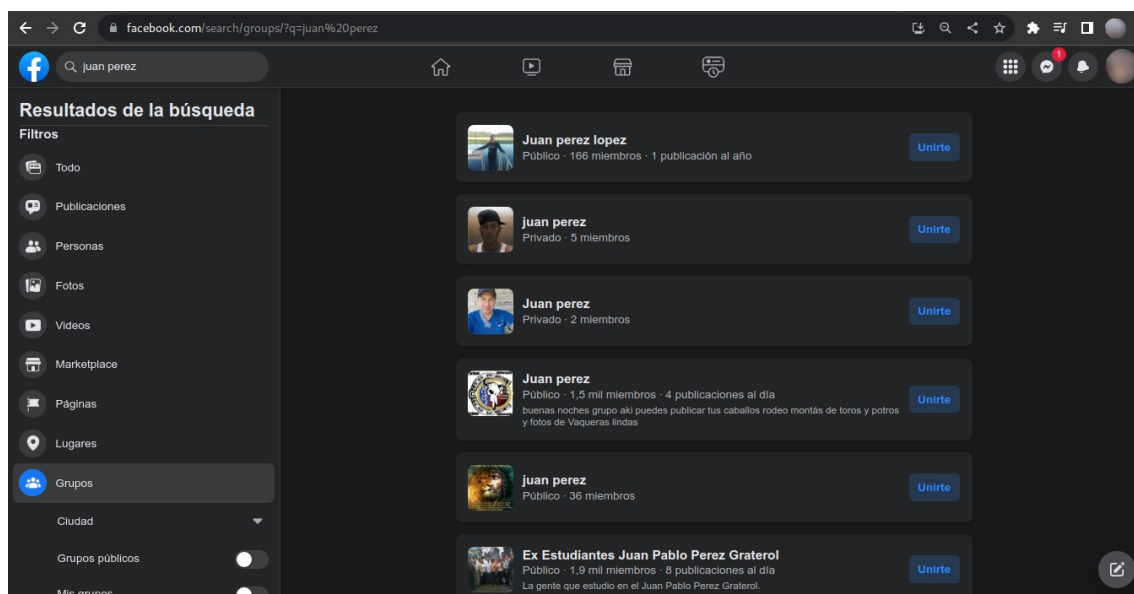
Cuando se activa la protección, únicamente nosotros y nuestros amigos pueden etiquetar la fotografía e incluso comentarla. Es una especie de escudo para la misma.

<https://www.facebook.com/help/756130824560105>

Ahora continuemos con la búsqueda de información en facebook.

<https://www.facebook.com/search/top?q=juan%20perez>

Al elegir una nueva categoría, la URL cambiará como se ve en la siguiente imagen.

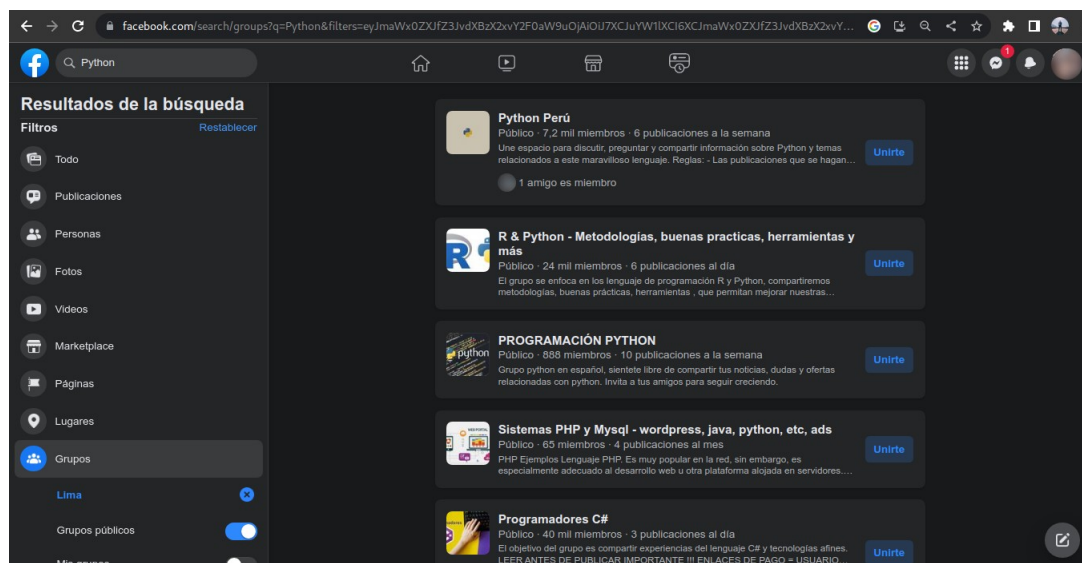


<https://www.facebook.com/search/groups/?q=juan%20perez>

Al cambiar los filtros también se modifica la URL y se afinan los resultados de nuestra búsqueda. La siguiente figura muestra el resultado de mi búsqueda de "Python", que la ubicación es de Lima, y son grupos públicos. Esto localizó varios resultados. Los filtros me ayudaron a pasar de miles de objetivos, a unos cuantos.

Por eso es importante antes de hacer la búsqueda por el filtro de facebook, tener información confiable de nuestro objetivo, en todo caso se tardaría mucho más haciendo la búsqueda manualmente, descartando falsos positivos.

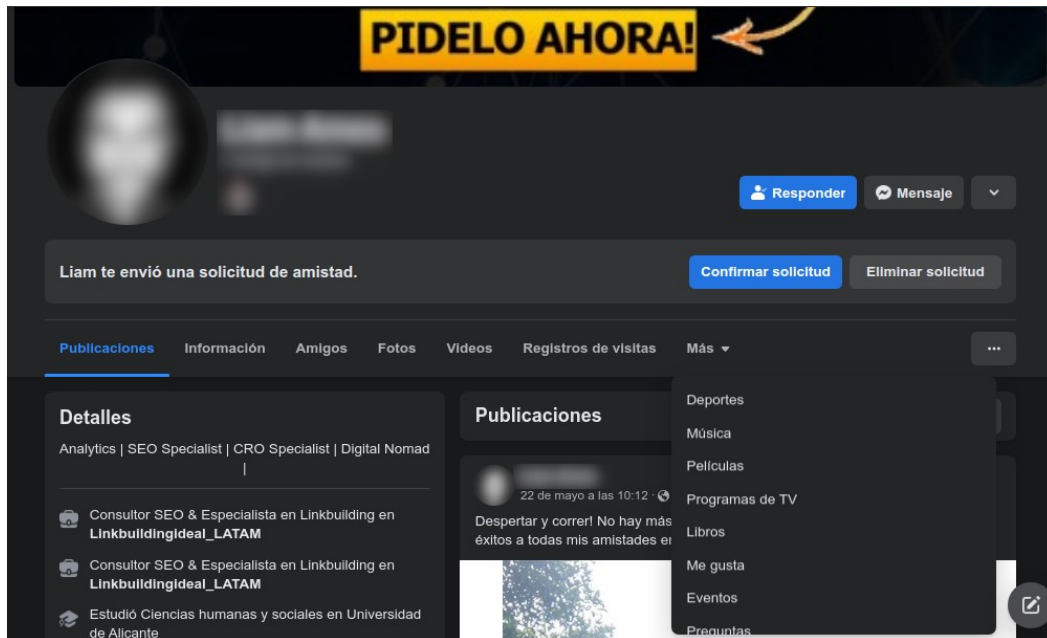
<https://www.facebook.com/search/groups?q=Python&filters=eyJmaWx0ZXJfZ3JvdXBzX2xvY2F0aW9uOjAiOiJ7XCJuYW1IXCI6XCJmaWx0ZXJfZ3JvdXBzX2xvY2F0aW9uXCIsXCJhcmdzXCI6XCIXMDg0NDY3MzI1MjA0NTZcln0iLCJwdWJsaWNfZ3JvdXBzOjAiOiJ7XCJuYW1IXCI6XCJwdWJsaWNfZ3JvdXBzXCIsXCJhcmdzXCI6XCJcIn0ifQ%3D%3D>



Una vez localizado el perfil de un objetivo, la vista por defecto tiene el aspecto que se muestra en la figura siguiente. Al hacer clic en cada uno de estos enlaces se pueden descubrir pruebas valiosas.

Ahora veremos un perfil específico de facebook, y dependiendo de la privacidad en información que comparte el perfil, recolectaremos cierta

información, como las páginas que sigue, grupos, deportes, Libros, etc.



Observe la URL del perfil en la imagen superior. El valor numérico es el ID del perfil del objetivo.

<https://www.facebook.com/profile.php?id=100011556644317>

Debe tenerse en cuenta que cualquier cadena después de facebook.com/ es un identificador único del perfil del objetivo, ya que podría estar en cualquier formato. A continuación se ofrecen algunos ejemplos de identificadores de perfil:

<https://www.facebook.com/mark.hayes.75470316>

<https://www.facebook.com/moronwi.joseph>

Hacer clic en cada uno de estos enlaces en la página de perfil del objetivo, puede descubrir pruebas valiosas. Pero es mejor buscar a través de una URL directa, como se muestra a continuación:

About

<https://www.facebook.com/profile-name/about>

<https://www.facebook.com/profile.php?id=insert-profile-id&sk=about>

Friends

<https://www.facebook.com/profile-name/friends>

<https://www.facebook.com/profile.php?id=insert-profile-id&sk=friends>

Photos

<https://www.facebook.com/profile-name/photos>

<https://www.facebook.com/profile.php?id=insert-profile-id&sk=photos>

Videos

<https://www.facebook.com/profile-name/videos>

<https://www.facebook.com/profile.php?id=insert-profile-id&sk=videos>

Check-ins

<https://www.facebook.com/profile-name/map>

<https://www.facebook.com/profile.php?id=insert-profile-id&sk=map>

Sports

<https://www.facebook.com/profile-name/sports>

<https://www.facebook.com/profile.php?id=insert-profile-id&sk=sports>

Music

<https://www.facebook.com/profile-name/music>

<https://www.facebook.com/profile.php?id=insert-profile-id&sk=music>

Movies

<https://www.facebook.com/profile-name/movies>

<https://www.facebook.com/profile.php?id=insert-profile-id&sk=movies>

TV Shows

<https://www.facebook.com/profile-name/tv>

<https://www.facebook.com/profile.php?id=insert-profile-id&sk=tv>

Books

<https://www.facebook.com/profile-name/books>

<https://www.facebook.com/profile.php?id=insert-profile-id&sk=books>

Likes

<https://www.facebook.com/profile-name/likes>

<https://www.facebook.com/profile.php?id=insert-profile-id&sk=likes>

Events

<https://www.facebook.com/profile-name/likes>

<https://www.facebook.com/profile.php?id=insert-profile-id&sk=likes>

Questions

https://www.facebook.com/profile-name/did_you_know

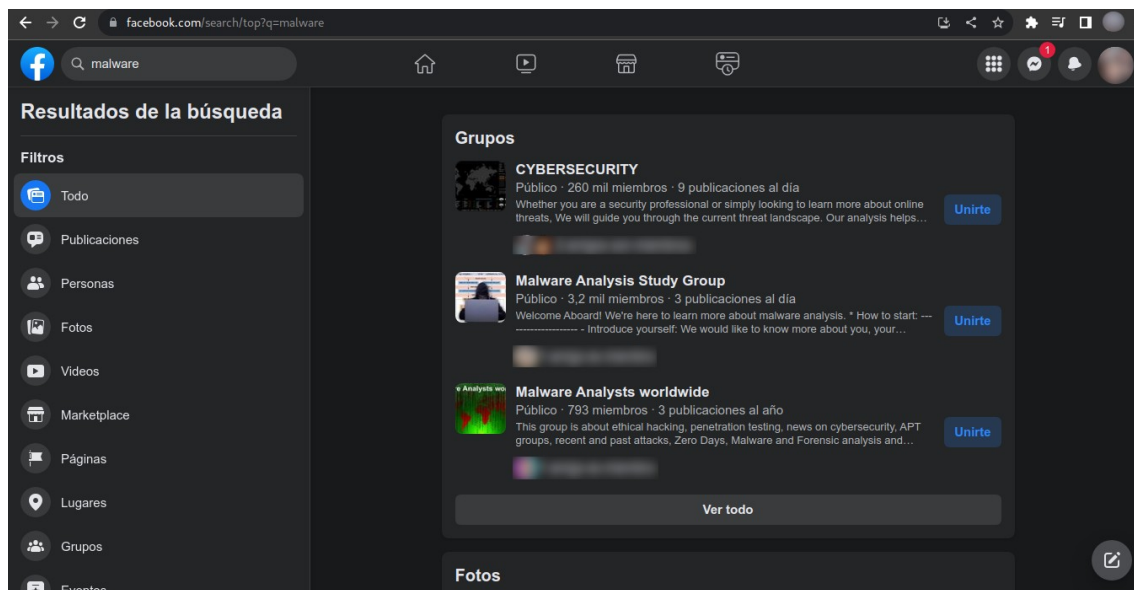
https://www.facebook.com/profile.php?id=insert-profile-id&sk=did_you_know

Reviews Given

https://www.facebook.com/profile-name/reviews_given

https://www.facebook.com/profile.php?id=insert-profile-id&sk=reviews_given

También puedes realizar una búsqueda genérica de palabras clave en Facebook. Supongamos que queremos encontrar cualquier publicación que incluya el término “malware”. Esto nos presenta una página de resultados similares, en la que hemos buscado el nombre de nuestro objetivo, como se muestra a continuación.



En la parte inferior de cada categoría también hay una opción para "Ver todos" los perfiles con la palabra clave de destino. Todos los filtros básicos de Facebook pueden aplicarse mediante URL directas, como se indica a continuación.

All: [https://www.facebook.com/search/top/?](https://www.facebook.com/search/top/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

[q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB](https://www.facebook.com/search/top/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

Posts: [https://www.facebook.com/search/posts/?](https://www.facebook.com/search/posts/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

[q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB](https://www.facebook.com/search/posts/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

People: [https://www.facebook.com/search/people/?](https://www.facebook.com/search/people/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

[q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB](https://www.facebook.com/search/people/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

Photos: [https://www.facebook.com/search/photos/?](https://www.facebook.com/search/photos/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

[q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB](https://www.facebook.com/search/photos/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

Videos: [https://www.facebook.com/search/videos/?](https://www.facebook.com/search/videos/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

[q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB](https://www.facebook.com/search/videos/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

Market Place: <https://www.facebook.com/marketplace/search/?query=malware>

Pages: [https://www.facebook.com/search/pages/?](https://www.facebook.com/search/pages/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

[q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB](https://www.facebook.com/search/pages/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

Places: [https://www.facebook.com/search/places/?](https://www.facebook.com/search/places/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

[q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB](https://www.facebook.com/search/places/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

Groups: [https://www.facebook.com/search/groups/?](https://www.facebook.com/search/groups/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

[q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB](https://www.facebook.com/search/groups/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

Events: [https://www.facebook.com/events/people/?](https://www.facebook.com/events/people/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

[q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB](https://www.facebook.com/events/people/?q=malware&_epa_=SERP_TAB&_eps_=SERP_TOP_TAB)

Codificación Base64 de Facebook:

Después de junio de 2019, Facebook cambió el formato en el que se muestran las URL de los filtros, pasando del formato sencillo a uno más difícil como el que se ve a continuación:

<https://www.facebook.com/search/posts?>

[q=Drugs&filters](https://www.facebook.com/search/posts?q=Drugs&filters)

[=eyJycF9hdXRob3I6MCI6Intclm5hbWVcljpcImF1dGhvcmlwiLFwiYXJnc1wiOlwiMTAwMDE1MTE0OTM2Mzk5XCJ9IiwicnBfY3JIYXRpb25fdGltZTowljoie1wibmFtZVwiOlwiY3JIYXRpb25fdGltZVwiLFwiYXJnc1wiOlwie1xcXCJzdGFydF95ZWVyXFxcljpcXFwiMjAyM1xcXCIsXFxclnN0YXJ0X21vbnRoXFxcljpcXFwiMjAyMy0xXFxclixcXFwiZW5kX3IiYXJcXFwiOlxcXClyMDIzXFxclixcXFwiZW5kX21vbnRoXFxcljpcXFwiMjAyMy0xMlxcXCIsXFxclnN0YXJ0X2RheVxcXCI6XFxcljIwMjMtMS0xXFxclixcXFwiZW5kX2RheVxcXCI6XFxcljIwMjMtMTItMzF0XFwifVwifSJ9](https://www.facebook.com/search/posts?q=Drugs&filters)

Los filtros de Facebook son cadenas JSON que luego se codifican en Base64 y se colocan en la URL. Facebook codifica ese contenido JSON en Base64 para que cualquier carácter especial que pudiera romper una URL (como "&" y "?")

se transforme de forma segura. La codificación Base64 no es una encriptación y se puede invertir o descodificar fácilmente.

El desglose de la URL anterior es el siguiente:

<https://www.facebook.com/> - El dominio de Facebook

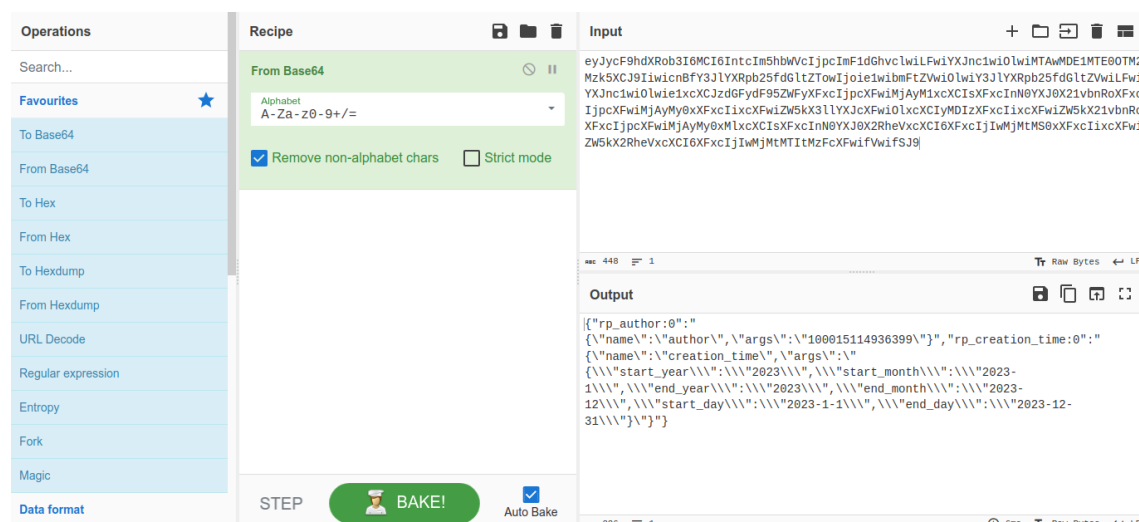
search/ - Indica a Facebook que realice una búsqueda

posts - Especifica el tipo de información deseada

q=Drogas - Busca cualquier publicación que contenga la palabra clave "Drogas".

&filters= - Termina la URL con una demanda de filtro.

Existen herramientas en línea que permiten descodificar cadenas codificadas en Base64. Para decodificar la cadena Base64 anterior, utilizaré Cyberchef. La aplicación [CyberChef](#) ó [Base64Decode](#), nos permite hacer esta transformación y mucho más. Visite el sitio web, copie su cadena codificada en Base64 y péguela en el cuadro como se muestra a continuación.



Si usamos la otra pagina que dejé arriba, también nos muestra el mismo resultado.

Decode from Base64 format

Simply enter your data then push the decode button.

```
eyJycF9hdXRob3I6MCI6Intclm5hbWVvcjpcImF1dGhvcmlwiLFwiYXJnc1wiOlwiMTAwMDE1MTE0OTM2Mzk5XCJ9IiwicnBfY3JIYXRpb25fdGltZTowIjoie1wibmFtZVwiOlwiY3JIYXRpb25fdGltZVwiLFwiYXJnc1wiOlwie1xcXCJzdGFydF95ZWFiYXFcclJpcXFwiMjAyM1xcXClsXFxcInN0YXJ0X21vbnRoXFxclJpcXFwiMjAyMy0xXFxclxcXFwiZW5kX3IiYXJcXFwiOlxcXClyMDIzXFxclxcXFwiZW5kX21vbnRoXFxclJpcXFwiMjAyMy0xMxcXClsXFxcInN0YXJ0X2RheVxcXCi6XFxclJwMjMtMS0xXFxclxcXFwiZW5kX2RheVxcXCi6XFxclJwMjMtMTItMzFcXFwiVwifSJ9
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8

Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF

Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE >

Decodes your data into the area below.

```
{"rp_author:0":{"name":"author","args":"100015114936399"},"rp_creation_time:0":{"name":"creation_time","args":{"start_year":"2023","start_month":"2023-1","end_year":"2023","end_month":"2023-12","start_day":"2023-1-1","end_day":"2023-12-31"}}}
```

```
{"rp_author:0":{"name":"author","args":"100015114936399"},"rp_creation_time:0":{"name":"creation_time","args":{"start_year":"2023","start_month":"2023-1","end_year":"2023","end_month":"2023-12","start_day":"2023-1-1","end_day":"2023-12-31"}}}
```

Interpretar la cadena decodificada:

```
{"rp_author:0":{"name":"author","args":"100015114936399"}}
```

Este es el nombre de perfil del objetivo representado por su ID de perfil (resaltado en rojo más arriba). Por lo tanto, el nombre del objetivo puede determinarse realizando la búsqueda.

<https://www.facebook.com/100015114936399>

```
{\"rp_creation_time\":0\":{\"name\":\"creation_time\",\"args\":{\"start_year\":\"2023\",\"start_month\":\"2023-1\",\"end_year\":\"2023\",\"end_month\":\"2023-12\",\"start_day\":\"2023-1-1\",\"end_day\":\"2023-12-31\"}}}
```

Esta es la fecha de creación de la(s) entrada(s). El año inicial es 2023, el mes inicial es 2023-1, el año final es 2023, el mes final es 2023-12, el día inicial es 2023-1-1 y el día final es 2023-12-31.

Por lo tanto, la URL

[https://www.facebook.com/search/posts?](https://www.facebook.com/search/posts?q=Drugs&filters=eyJycF9hdXRob3I6MCI6Intclm5hbWVcljpcImF1dGhvcmlwLWwiYXJnc1wiOlwiMTAwMDE1MTE0OTM2Mzk5XCJ9liwicnBfY3JIYXRpb25fdGltZTowljoie1wibmFtZVwiOlwiY3JIYXRpb25fdGltZVwiLWwiYXJnc1wiOlwie1xcXCJzdGFydF95ZWFiYXFccljpcXFwiMjAyM1xcXCIsXFxclnN0YXJ0X21vbnRoXFxcljpcXFwiMjAyMy0xXFxclixcXFwiZW5kX3IiYXJcXFwiOlxcXClyMDIzXFxclixcXFwiZW5kX21vbnRoXFxcljpcXFwiMjAyMy0xMlxcXCIsXFxclnN0YXJ0X2RheVxcXCi6XFxcljwMjMtMS0xXFxclixcXFwiZW5kX2RheVxcXCi6XFxcljwMjMtMTItMzFcXWwifVwifSJ9)

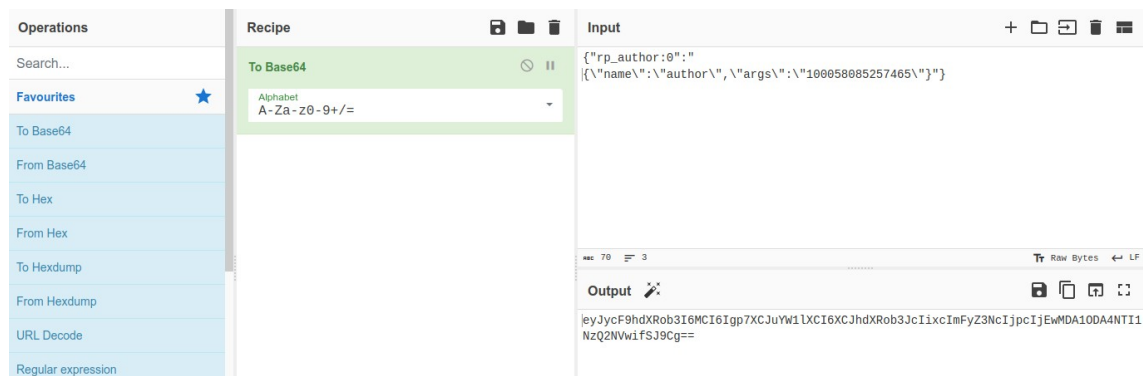
[q=Drugs&filters=eyJycF9hdXRob3I6MCI6Intclm5hbWVcljpcImF1dGhvcmlwLWwiYXJnc1wiOlwiMTAwMDE1MTE0OTM2Mzk5XCJ9liwicnBfY3JIYXRpb25fdGltZTowljoie1wibmFtZVwiOlwiY3JIYXRpb25fdGltZVwiLWwiYXJnc1wiOlwie1xcXCJzdGFydF95ZWFiYXFccljpcXFwiMjAyM1xcXCIsXFxclnN0YXJ0X21vbnRoXFxcljpcXFwiMjAyMy0xXFxclixcXFwiZW5kX3IiYXJcXFwiOlxcXClyMDIzXFxclixcXFwiZW5kX21vbnRoXFxcljpcXFwiMjAyMy0xMlxcXCIsXFxclnN0YXJ0X2RheVxcXCi6XFxcljwMjMtMS0xXFxclixcXFwiZW5kX2RheVxcXCi6XFxcljwMjMtMTItMzFcXWwifVwifSJ9](https://www.facebook.com/search/posts?q=Drugs&filters=eyJycF9hdXRob3I6MCI6Intclm5hbWVcljpcImF1dGhvcmlwLWwiYXJnc1wiOlwiMTAwMDE1MTE0OTM2Mzk5XCJ9liwicnBfY3JIYXRpb25fdGltZTowljoie1wibmFtZVwiOlwiY3JIYXRpb25fdGltZVwiLWwiYXJnc1wiOlwie1xcXCJzdGFydF95ZWFiYXFccljpcXFwiMjAyM1xcXCIsXFxclnN0YXJ0X21vbnRoXFxcljpcXFwiMjAyMy0xXFxclixcXFwiZW5kX3IiYXJcXFwiOlxcXClyMDIzXFxclixcXFwiZW5kX21vbnRoXFxcljpcXFwiMjAyMy0xMlxcXCIsXFxclnN0YXJ0X2RheVxcXCi6XFxcljwMjMtMS0xXFxclixcXFwiZW5kX2RheVxcXCi6XFxcljwMjMtMTItMzFcXWwifVwifSJ9)

Se interpreta como "Buscar en Facebook las publicaciones del usuario 100015114936399 para la palabra clave Drogas del 1 de enero de 2023 al 31 de diciembre de 2023".

Reconocer las cadenas Base64 te hará más poderoso en tu trabajo, ya que podrás revelar lo que está codificado. En los filtros de Facebook, no solo podemos descifrar el Base64, ¡sino que también podemos manipularlo!.

Supongamos que un investigador quiere buscar información de un perfil específico (autor) cuyo ID de perfil es 100058085257465, dada nuestra cadena Base64 decodificada anteriormente, podemos modificar el ID de perfil con el ID de perfil de nuestro nuevo objetivo como se muestra a continuación:

```
{"rp_author:0":{"name\\":\\"author\\",\\"args\\":\\"100058085257465\\"}}
```



A continuación se muestra el resultado:

```
eyJycF9hdXRob3I6MCI6Igp7XCJuYW1lXCI6XCJhdXRob3JclixclmFyZ3NcljpcIjEwMDA1ODA4NTI1NzQ2NVwifSJ9Cg==
```

Supongamos que queremos identificar las publicaciones en ChatGPT creadas por este usuario, combinaremos la URL

<https://www.facebook.com/search/posts?q=ChatGPT&filters=> con la cadena codificada en Base64 anterior.

```
https://www.facebook.com/search/posts?q=ChatGPT&filters=eyJycF9hdXRob3I6MCI6Intclm5hbWVcljpcImF1dGhvclwiLWwiYXJnc1wiOlwiMTAwMDU4MDg1MjU3NDY1XCJ9In0=
```

Directorios de Facebook:

Otro método para descubrir datos en Facebook es navegar por él. Facebook tiene páginas de directorios que muestran un determinado tipo de entrada, como páginas. De este modo, puedes navegar y hacer clic para ir de una amplia gama de páginas o personas a páginas o cuentas específicas. Facebook mantiene estos directorios para muchos tipos diferentes de entidades en su sitio, y el gurú en OSINT [Kirby Plessas](#) mantiene una lista de los diferentes directorios que están disponibles. La mayoría de las páginas de

estos directorios son accesibles sin autenticarse en Facebook. Por supuesto, esas entidades pueden no aparecer en las páginas del directorio de cuentas privadas y grupos ocultos. También enumera fórmulas para buscar en Facebook utilizando la búsqueda nativa de Facebook y [técnicas/herramientas](#) avanzadas.

Extracción de amigos de Facebook:

En primer lugar, identifica la página de tu objetivo, por ejemplo, <https://facebook.com/moronwi.joseph/friends>. Resalta toda la lista de amigos haciendo clic en "Ctrl" + "A" o haciendo clic directamente encima de la parte izquierda del primer amigo y mantén pulsado hasta la zona inferior derecha del último amigo. Ahora, abre Microsoft Excel. Haz clic en la "B" de la columna B para resaltar toda la columna. Pega el contenido con "Ctrl" + "V" (o haz clic con el botón derecho del ratón > pegar). Esto parecerá desorganizado, pero los datos están ahí. Las imágenes estarán encima de los datos del usuario, lo que no funcionará para un informe final.

Utilice F5 para lanzar el menú "Ir a" y seleccione "Especial" en la parte inferior izquierda. Seleccione "Objetos" y haga clic en OK. Esto seleccionará todas esas imágenes. Pulsa la tecla Supr para eliminarlas. Ahora sólo verás los datos de texto (con hipervínculos). Ahora haz clic en la "A" de la columna A y pega de nuevo el contenido amigo con "Ctrl" + "V" (o haz clic con el botón derecho del ratón > pegar). Haz clic con el botón derecho en cualquier celda de esta columna y selecciona "Borrar contenido". Esto eliminará cualquier texto, pero mantendrá las imágenes.

Coloca el ratón entre las columnas A y B y cambia el tamaño de la columna A para que sea un poco más grande que una de las imágenes. Haz lo mismo con la columna B para que quepa todo el texto. Usa la función "Buscar y reemplazar" para encontrar cada instancia de "Añadir amigo" y reemplázala por nada. Esto eliminará las entradas innecesarias. En el menú "Inicio", elija "Formato" y luego "Autoajustar Alto de Fila". Esto eliminará los espacios

innecesarios. Selecciona la columna B y justifica el texto a la izquierda. El resultado final será una hoja de cálculo limpia con todas las imágenes, nombres y enlaces activos de la página de "amigos" de Facebook de tu objetivo.

Las investigaciones en Facebook son siempre un objetivo en movimiento. Afortunadamente, cualquier cambio siempre trae nuevas oportunidades de investigación. Cuando perdimos Graph search en 2019, ganamos métodos Base64. Cuando perdamos las estrategias actuales, algo más estará disponible. Al igual que con todas las técnicas OSINT, la práctica diaria y la comprensión de los recursos son más vitales que la pepita de datos ocasional que aparece en nuestras pantallas. Por último, debes ser muy autodidacta si te quieres dedicar al OSINT de manera profesional.

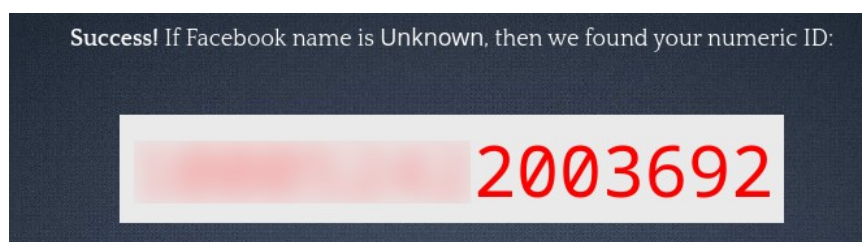
<https://digitalinvestigator.blogspot.com/2023/05/facebook-osint-investigation.html>

User ID, usando LookupID:

<https://lookup-id.com/>

The screenshot shows the homepage of Lookup-ID.com. The header is dark blue with the site name 'Lookup-ID.com' on the left and navigation links 'Facebook ID', 'Unscramble Word', 'Directory', 'Resources', and 'Tools' on the right. The main content area is dark blue with white text that reads 'Looking for your Facebook profile ID / Group ID / Page ID ...'. Below this is a prompt 'Type your Facebook profile URL' followed by a text input field containing 'https://m.facebook.com/username' and a yellow 'Lookup' button.

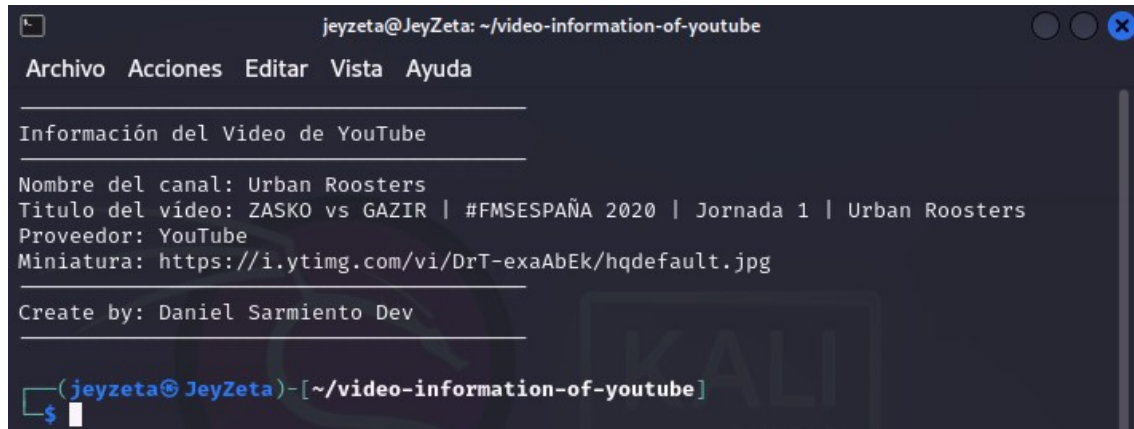
Al poner la url del usuario de fb, nos muestra lo siguiente.



OSINT a Youtube:

Video information of youtube: Una herramienta hecha en python para recolección básica de información de videos de youtube.

<https://github.com/backsoul/video-information-of-youtube>



```
jeyzeta@JeyZeta: ~/video-information-of-youtube
Archivo Acciones Editar Vista Ayuda

Información del Video de YouTube

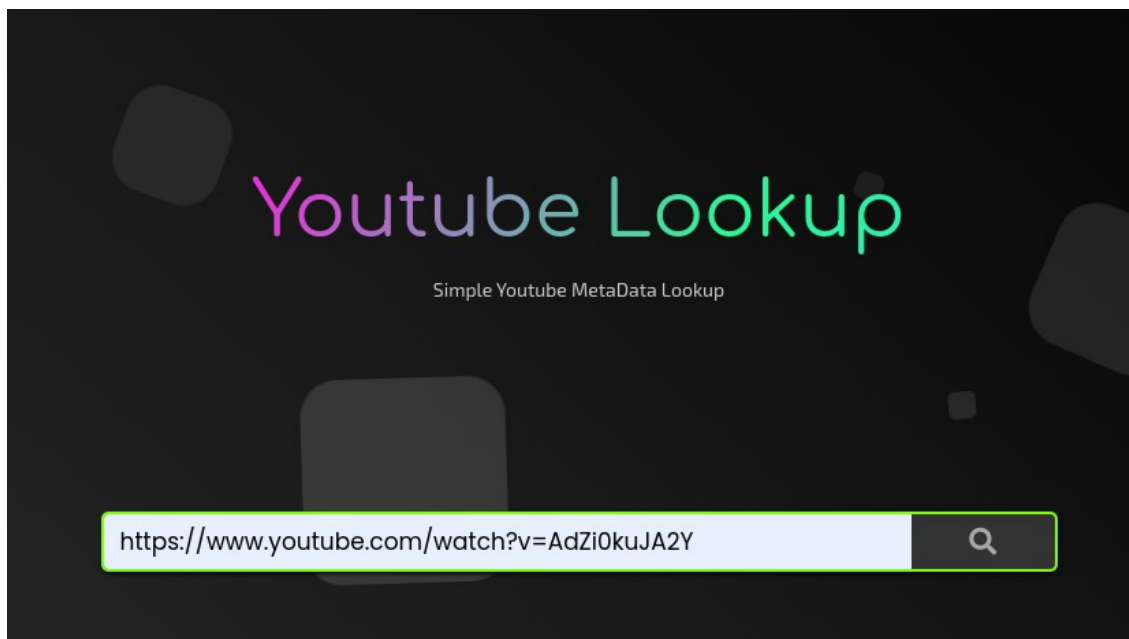
Nombre del canal: Urban Roosters
Titulo del video: ZASKO vs GAZIR | #FMSESPAÑA 2020 | Jornada 1 | Urban Roosters
Proveedor: YouTube
Miniatura: https://i.ytimg.com/vi/DrT-exaAbEk/hqdefault.jpg

Create by: Daniel Sarmiento Dev

(jeyzeta@JeyZeta)-[~/video-information-of-youtube]
```

Youtube Lookup: Una herramienta online, que brinda información detallada de cualquier video de youtube.

<https://youtube-lookup.vercel.app/>



Al poner la url de cualquier vídeo de youtube, nos muestra la siguiente información.

Snippet Details :

Video Title: PERÚ ENLOQUECIÓ con los RESPUESTONES del MENOR! 🇵🇪 🤖
Video Published At: 2022-09-06T21:00:04Z
Channel Name: Willyamet
Channel ID: UCYGUYgQ8aVXTMNyspbAS1A

Statistics Details :

Video viewCount: 422564
Video likeCount: 10648
Video favoriteCount: 0
Video commentCount: 534

Status Details :


Video embeddable: true
Video license: youtube
Video madeForKids:
Video privacyStatus: public
Video publicStatsViewable: true
Video uploadStatus: processed

Content Details :

Video caption: false
Video definition: hd
Video dimension: 2d
Video duration: 2:51
Video licensedContent: true
Video projection: rectangular

Geolocation Details:


Thumbnails :




Topic Details :

- https://en.wikipedia.org/wiki/Hip_hop_music
- <https://en.wikipedia.org/wiki/Music>

Export & Share :

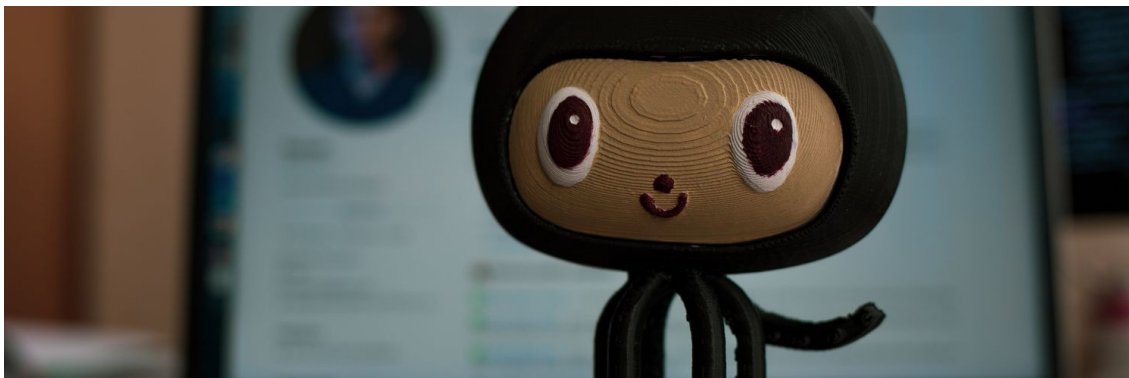
 Export

Share this Result :

<https://youtube-lookup.vercel.app/?id=...> 

OSINT a GitHub:

GitHub URL Hacks:

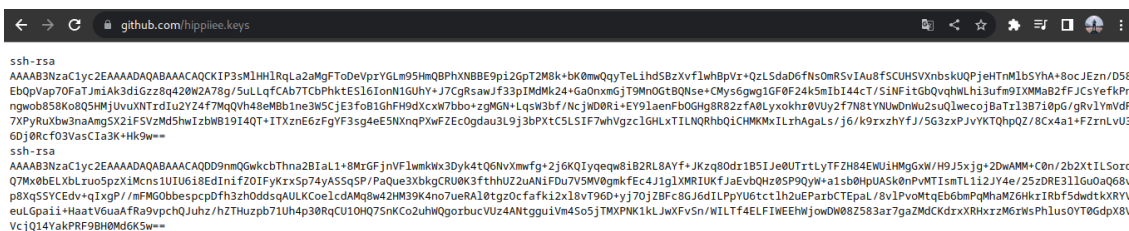


La interfaz de GitHub ha mejorado mucho a lo largo de los años, pero a veces necesitas un acceso rápido sin hacer clic. Aquí tienes algunos consejos sobre la URL de GitHub para obtener los datos que quieres más rápido. Una cosa interesante es que todos estos consejos dan salida de texto sin formato por lo que funcionan muy bien con curl y otras herramientas CLI.

Public SSH keys:

Si quieres obtener las claves ssh públicas de un usuario puedes añadir .keys al final de la URL de su perfil de usuario. Aquí está un ejemplo.

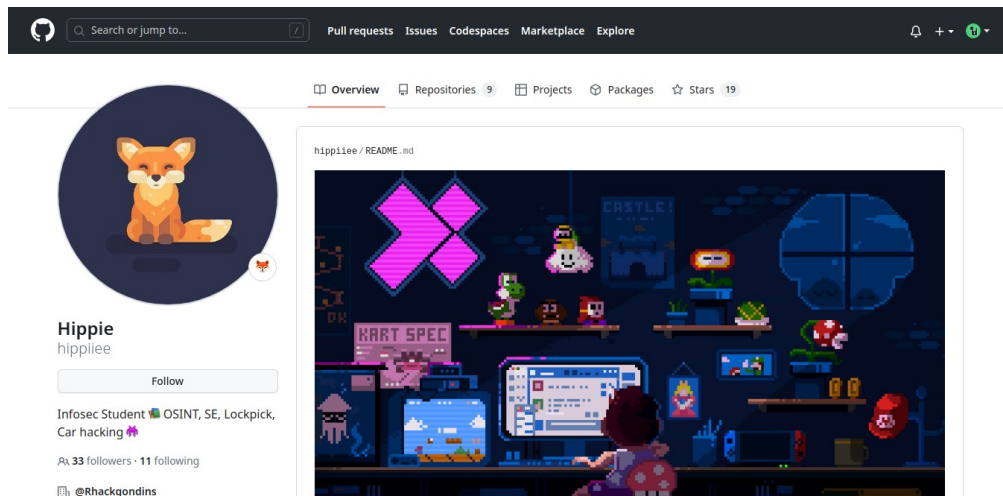
<https://github.com/hippiiee.keys>



Profile imagen:

Si quieres obtener la foto de perfil de un usuario puedes añadir .png al final de la URL de su perfil de usuario.

Por ejemplo, quiero ver la foto completa de este repositorio.

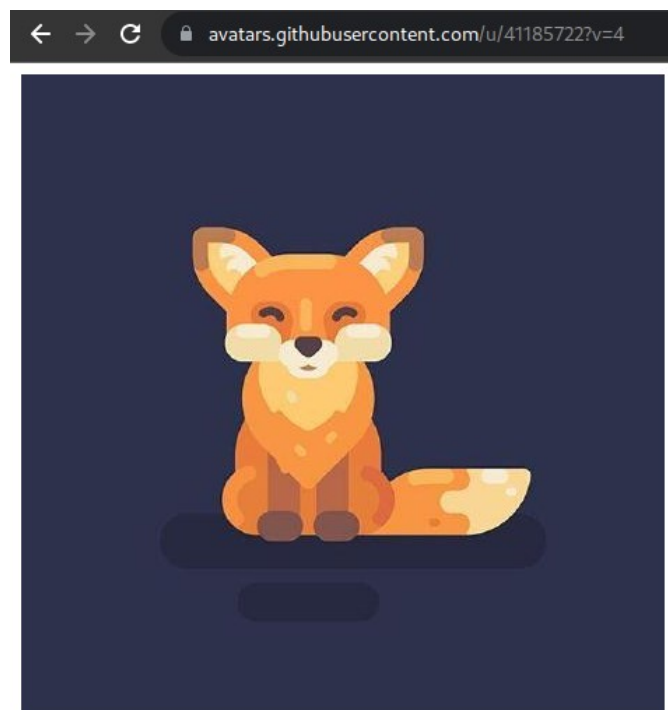


Podría darle clic a la imagen y se me redirige a la fuente original de la imagen, o simplemente en la URL principal del repositorio le agrego el .PNG

<https://github.com/hippiee.png>

Al hacerlo me redirecciona a la siguiente URL.

<https://avatars.githubusercontent.com/u/41185722?v=4>



Public GPG keys:

Si quieres obtener claves públicas gpg puedes añadir .gpg al final de la URL de su perfil de usuario. En realidad no tengo ninguna clave gpg así que puedes ver cómo se ve si un usuario no las tiene con el siguiente perfil.

<https://github.com/s0md3v.gpg>

```
← → ↻ 🔒 github.com/s0md3v.gpg

-----BEGIN PGP PUBLIC KEY BLOCK-----
Note: This user hasn't uploaded any GPG keys.

=twTO
-----END PGP PUBLIC KEY BLOCK-----
```

RSS feeds:

Hay muchos feeds a los que puedes suscribirte.

Repo commits:

[https://github.com/\\$USER/\\$REPO/commits.atom](https://github.com/$USER/$REPO/commits.atom)

```
← → ↻ 🔒 github.com/s0md3v/Zen/commits.atom

<?xml version="1.0" encoding="UTF-8"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:media="http://search.yahoo.com/mrss/" xml:lang="en-US">
  <id>tag:github.com,2008:/s0md3v/Zen/commits/master</id>
  <link type="text/html" rel="alternate" href="https://github.com/s0md3v/Zen/commits/master"/>
  <link type="application/atom+xml" rel="self" href="https://github.com/s0md3v/Zen/commits/master.atom"/>
  <title>Recent Commits to Zen:master</title>
  <updated>2019-05-05T15:49:59Z</updated>
  <entry>
    <id>tag:github.com,2008:Grit::Commit/b9018b4b74eb0cb64d5a61ff0cdd413cf5d7733</id>
    <link type="text/html" rel="alternate" href="https://github.com/s0md3v/Zen/commit/b9018b4b74eb0cb64d5a61ff0cdd413cf5d7733"/>
    <title>
      Initial WhiteSource configuration file
    </title>
    <updated>2019-05-05T15:49:59Z</updated>
    <media:thumbnail height="30" width="30" url="https://0.gravatar.com/avatar/e9b6fa205b78615f0edd20fe9282c1347d=https%3A%2F%2Fgithub.githubassets.com%2Fimages%2Fgravatars%2Fgravatar-user-420.png&amp;r=g&amp;s=30"/>
    <author>
      <name></name>
      <email>whitesource-bolt-for-github[bot]@users.noreply.github.com</email>
    </author>
    <content type="html">
      &lt;pre style=&#39;white-space:pre-wrap;width:81ex&#39;&gt;Initial WhiteSource configuration file&lt;/pre&gt;
    </content>
  </entry>
  <entry>
    <id>tag:github.com,2008:Grit::Commit/2b6c66f5f595518a2d7a4cdd0b90ab5bcfe6ae5e</id>
    <link type="text/html" rel="alternate" href="https://github.com/s0md3v/Zen/commit/2b6c66f5f595518a2d7a4cdd0b90ab5bcfe6ae5e"/>
    <title>
      Merge pull request #12 from abhijithvijayan/master
    </title>
    <updated>2019-01-04T12:00:59Z</updated>
    <media:thumbnail height="30" width="30" url="https://avatars.githubusercontent.com/u/26716802?s=30&amp;v=4"/>
    <author>
      <name>s0md3v</name>
      <uri>https://github.com/s0md3v</uri>
    </author>
```


Repo releases:

[https://github.com/\\$USER/\\$REPO/releases.atom](https://github.com/$USER/$REPO/releases.atom)

```
← → ↻ github.com/s0md3v/Zen/releases.atom

<?xml version="1.0" encoding="UTF-8"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:media="http://search.yahoo.com/mrss/" xml:lang="en-US">
  <id>tag:github.com,2008:https://github.com/s0md3v/Zen/releases</id>
  <link type="text/html" rel="alternate" href="https://github.com/s0md3v/Zen/releases"/>
  <link type="application/atom+xml" rel="self" href="https://github.com/s0md3v/Zen/releases.atom"/>
  <title>Release notes from Zen</title>
  <updated>2018-10-17T11:13:13-05:00</updated>
  <entry>
    <id>tag:github.com,2008:Repository/153084655/v1.1</id>
    <updated>2018-10-17T11:15:04-05:00</updated>
    <link rel="alternate" type="text/html" href="https://github.com/s0md3v/Zen/releases/tag/v1.1"/>
    <title>v1.1</title>
    <content type="html">&lt;ul&gt;
      &lt;li&gt;Bug fixes&lt;/li&gt;
      &lt;li&gt;Multithreading&lt;/li&gt;
      &lt;li&gt;Increased rate limit&lt;/li&gt;
      &lt;li&gt;haveibeenpwned.com API integration&lt;/li&gt;
    &lt;/ul&gt;</content>
    <author>
      <name>s0md3v</name>
    </author>
    <media:thumbnail height="30" width="30" url="https://avatars.githubusercontent.com/u/26716802?s=60&v=4"/>
  </entry>
  <entry>
    <id>tag:github.com,2008:Repository/153084655/v1.0</id>
    <updated>2018-10-15T04:22:44-05:00</updated>
    <link rel="alternate" type="text/html" href="https://github.com/s0md3v/Zen/releases/tag/v1.0"/>
    <title>v1.0</title>
    <content>No content.</content>
    <author>
      <name>s0md3v</name>
    </author>
    <media:thumbnail height="30" width="30" url="https://avatars.githubusercontent.com/u/26716802?s=60&v=4"/>
  </entry>
</feed>
```

Repo tags:

[https://github.com/\\$USER/\\$REPO/tags.atom](https://github.com/$USER/$REPO/tags.atom)

```
← → ↻ github.com/s0md3v/Zen/tags.atom

<?xml version="1.0" encoding="UTF-8"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:media="http://search.yahoo.com/mrss/" xml:lang="en-US">
  <id>tag:github.com,2008:https://github.com/s0md3v/Zen/releases</id>
  <link type="text/html" rel="alternate" href="https://github.com/s0md3v/Zen/releases"/>
  <link type="application/atom+xml" rel="self" href="https://github.com/s0md3v/Zen/releases.atom"/>
  <title>Tags from Zen</title>
  <updated>2018-10-17T11:13:13-05:00</updated>
  <entry>
    <id>tag:github.com,2008:Repository/153084655/v1.1</id>
    <updated>2018-10-17T11:15:04-05:00</updated>
    <link rel="alternate" type="text/html" href="https://github.com/s0md3v/Zen/releases/tag/v1.1"/>
    <title>v1.1</title>
    <content></content>
    <author>
      <name>s0md3v</name>
    </author>
    <media:thumbnail height="30" width="30" url="https://avatars.githubusercontent.com/u/26716802?s=60&v=4"/>
  </entry>
  <entry>
    <id>tag:github.com,2008:Repository/153084655/v1.0</id>
    <updated>2018-10-15T04:22:44-05:00</updated>
    <link rel="alternate" type="text/html" href="https://github.com/s0md3v/Zen/releases/tag/v1.0"/>
    <title>v1.0</title>
    <content></content>
    <author>
      <name>s0md3v</name>
    </author>
    <media:thumbnail height="30" width="30" url="https://avatars.githubusercontent.com/u/26716802?s=60&v=4"/>
  </entry>
</feed>
```

User feeds:

El canal RSS público mostrará la actividad pública de los usuarios. Repo stars, releases, etc.

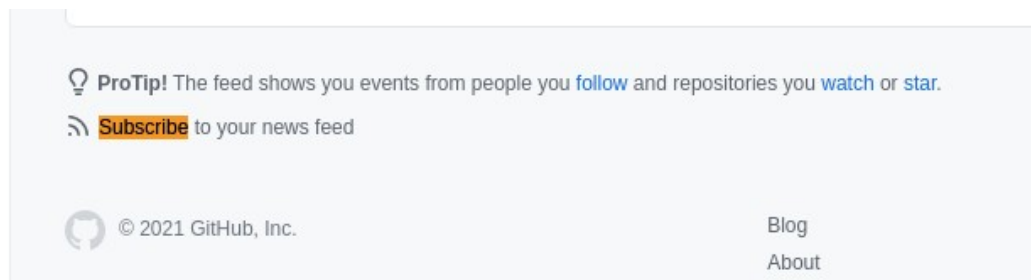
<https://github.com/s0md3v.atom>

```
<?xml version="1.0" encoding="UTF-8"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:media="http://search.yahoo.com/mrss/" xml:lang="en-US">
  <id>tag:github.com,2008:/s0md3v</id>
  <link type="text/html" rel="alternate" href="https://github.com/s0md3v"/>
  <link type="application/atom+xml" rel="self" href="https://github.com/s0md3v.atom"/>
  <title>GitHub Public Timeline Feed</title>
  <updated>2023-05-24T14:55:12Z</updated>
  <entry>
    <id>tag:github.com,2008:PushEvent/29287659753</id>
    <published>2023-05-24T14:55:12Z</published>
    <updated>2023-05-24T14:55:12Z</updated>
    <link type="text/html" rel="alternate" href="https://github.com/s0md3v/uro/compare/68311ccab6...fa649f052e"/>
    <title type="html">s0md3v pushed to main in s0md3v/uro</title>
    <author>
      <name>s0md3v</name>
      <email>s0md3v@gmail.com</email>
      <uri>https://github.com/s0md3v</uri>
    </author>
    <media:thumbnail height="30" width="30" url="https://avatars.githubusercontent.com/u/26716802?s=30&v=4"/>
    <content type="html">&lt;div class="push js-feed-item-view" data-hydro-view="
      (&quot;event_type&quot;:&quot;news_feed.event.view&quot;,&quot;payload&quot;:&quot;{&quot;event&quot;:&quot;
      (&quot;repo_id&quot;:&quot;401081140,&quot;actor_id&quot;:&quot;26716802,&quot;public&quot;:&quot;true,&quot;type&quot;:&quot;PushEvent&quot;,&quot;
      ot,target_id&quot;:&quot;null,&quot;id&quot;:&quot;29287659753,&quot;additional_details_shown&quot;:&quot;false,&quot;grouped&quot;:&quot;false,&quot;event_group&
      &quot;:&quot;null,&quot;org_id&quot;:&quot;null,&quot;target_type&quot;:&quot;,&quot;event&quot;:&quot;,&quot;user_id&quot;:&quot;null,&quot;feed_card&quot;:&quot;
      (&quot;card_retrieved_id&quot;:&quot;,&quot;originating_url&quot;:&quot;https://github.com/s0md3v.atom&quot;)}&quot;,&quot;data-hydro-view-
      hmac&quot;:&quot;7a8c65d03d02fa4f26ed9456841eb0a78481bf325c07962ddc8d56ba3450a1798&quot;,&quot;div class="body&quot;,&quot;
      &lt;!-- push --&gt;
      &lt;div class="d-flex flex-items-baseline py-4&quot;,&quot;
      &lt;div class="d-flex flex-column width-full&quot;,&quot;
      &lt;div class="color-fg-muted&quot;,&quot;
      &lt;span class="mr-2&quot;,&lt;a class="d-inline-block&quot; href="/s0md3v&quot; rel="noreferrer&quot;,&lt;img class="avatar avatar-
      user&quot; src="https://avatars.githubusercontent.com/u/26716802?s=64&v=4&quot; width="32&quot; height="32&quot;
      alt="s0md3v&quot;,&lt;/a&quot;,&lt;/span&quot;
      &lt;a class="Link--primary no-underline wb-break-all&quot; href="/s0md3v&quot; rel="noreferrer&quot;,&quot;s0md3v&lt;/a&quot;
```

También hay un feed de usuario privado que es genial si no te conectas a GitHub a menudo.

Requiere que hagas clic en la interfaz de usuario, pero a mí me sigue pareciendo increíblemente útil. Accede a tu cuenta y en tu panel de control desplázate hasta el final y haz clic en "Suscribirse a tu feed de noticias". Esto generará un token privado automáticamente y te enviará a [https://github.com/\\$USER.private.atom?token=...](https://github.com/$USER.private.atom?token=...)

Puedes conectar esto directamente a un lector RSS e incluirá todo lo que normalmente aparece en tu feed privado. Repos y usuarios que sigues, lanzamientos de proyectos y más.



Security advisories:

Este es un canal RSS público para los avisos de seguridad de GitHub.

<https://github.com/security-advisories.atom>

Global timeline:

<https://github.com/timeline>

Diffs:

Puede diferenciar ramas en un repositorio añadiendo `/compare/[fork-user:]$BRANCH...$BRANCH` al final de la url de un repositorio.

Si quieres comparar una rama de desarrollo con la rama principal de mi bashScheduler puedes comprobarlo.

<https://github.com/rothgar/bashScheduler/compare/main...dev>

Si tuvieras un fork del repo podrías añadir tu nombre de usuario antes de main así.

[https://github.com/rothgar/bashScheduler/compare/\\$USER:main...dev](https://github.com/rothgar/bashScheduler/compare/$USER:main...dev)

Lo bueno es que puedes obtener un parche en bruto o una salida diff usando la misma url y añadiendo `.patch` y `.diff` al final.

<https://github.com/rothgar/bashScheduler/compare/main...dev.patch>

<https://github.com/rothgar/bashScheduler/compare/main...dev.diff>

Puedes encontrar más trucos en el siguiente repositorio.

<https://github.com/tiimgreen/github-cheat-sheet>

<https://justingarrison.com/blog/2021-07-11-github-url-hacks/>

Osgint:

<https://github.com/hippiee/osgint>

Nos muestra información de un usuario de GitHub. Desde su id, fecha de creación, descripción, email, etc.

```
jeyzeta@JeyZeta: ~/osgint
Archivo Acciones Editar Vista Ayuda
(jeyzeta@JeyZeta)-[~/osgint]
$ ./osgint.py -u HackUnderway

.d888888b.      d8b      888
d88P" "Y88b      Y8P      888
888      888      888
888      888 .d8888b .d88b. 888 888888b. 888888
888      888 88K    d88P"88b 888 888 "88b 888
888      888 "Y8888b. 888 888 888 888 888 888
Y88b. .d88P      X88 Y88b 888 888 888 888 Y88b.
"Y88888P" 88888P' "Y88888 888 888 888 "Y888
              888 v1.0.3
              Y8b d88P
              "Y88P"

By Hippie | https://twitter.com/hiippiie

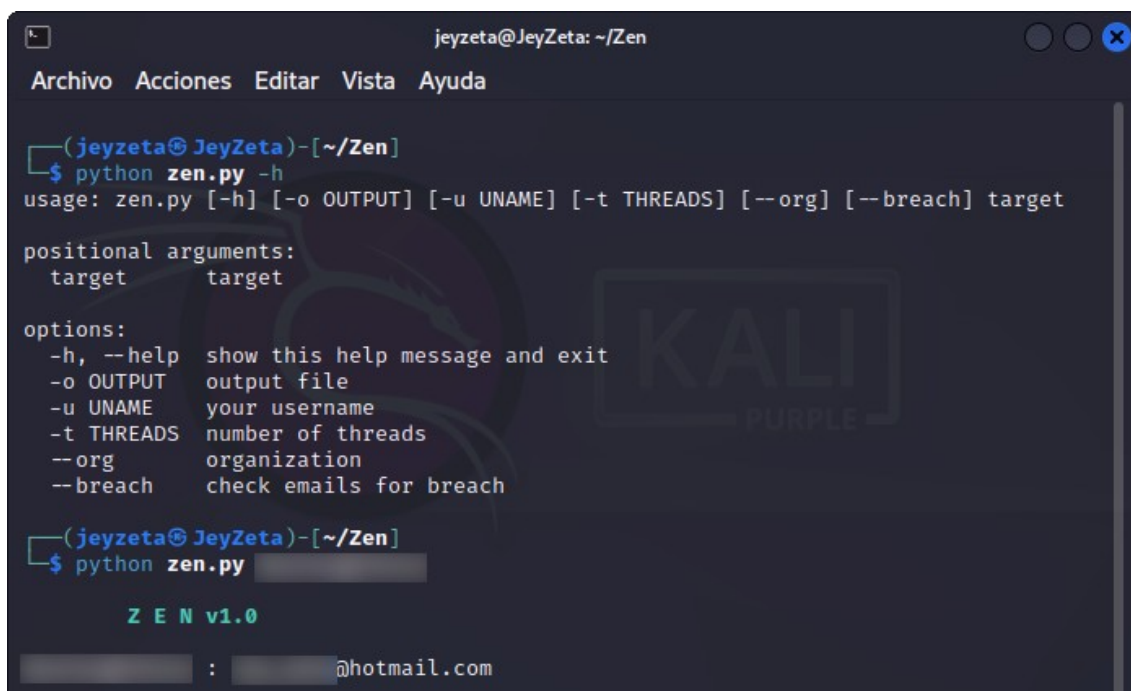
[+] login : HackUnderway
[+] id : 75584352
[+] avatar_url : https://avatars.githubusercontent.com/u/75584352?v=4
[+] name : Hack Underway
[+] blog : HackUnderway.com
[+] location : Lima - Perú
[+] bio : Empresa de tecnología de la información.::
[+] twitter_username : HackUnderway
[+] public_repos : 9
[+] public_gists : 0
[+] followers : 4
[+] following : 0
[+] created_at : 2020-12-06T19:21:07Z
[+] updated_at : 2023-03-02T05:05:49Z
[+] public_gists : https://gist.github.com/HackUnderway
[+] email : 75584352+HackUnderway@users.noreply.github.com

(jeyzeta@JeyZeta)-[~/osgint]
$
```

Zen:

<https://github.com/s0md3v/Zen>

Es una herramienta OSINT para encontrar y recopilar correos electrónicos de usuarios de Github.

A screenshot of a terminal window titled 'jeyzeta@JeyZeta: ~/Zen'. The window has a menu bar with 'Archivo', 'Acciones', 'Editar', 'Vista', and 'Ayuda'. The terminal shows the command 'python zen.py -h' being executed, which displays the usage and options for the script. The options include -h for help, -o for output file, -u for username, -t for number of threads, --org for organization, and --breach for checking emails for breach. Below the options, the version 'ZEN v1.0' is displayed. The terminal also shows a partial command 'python zen.py' followed by a redacted input field.

```
jeyzeta@JeyZeta: ~/Zen
Archivo Acciones Editar Vista Ayuda

(jeyzeta@JeyZeta)~[~/Zen]
$ python zen.py -h
usage: zen.py [-h] [-o OUTPUT] [-u UNAME] [-t THREADS] [--org] [--breach] target

positional arguments:
  target      target

options:
  -h, --help      show this help message and exit
  -o OUTPUT        output file
  -u UNAME         your username
  -t THREADS       number of threads
  --org            organization
  --breach         check emails for breach

(jeyzeta@JeyZeta)~[~/Zen]
$ python zen.py
ZEN v1.0
: @hotmail.com
```

Octosuite:

<https://github.com/bellingcat/octosuite>

Octosuite es un marco avanzado de GitHub escrito en Python que utiliza la API pública de GitHub para hacer que el proceso de investigación de cuentas y repositorios en la plataforma sea más eficiente, al mismo tiempo que crea un conjunto de consultas automatizadas y fácilmente reproducibles.

Uso básico:

En este ejemplo lo vamos a ejecutar con Docker.

Guía de instalación:

<https://github.com/bellingcat/octosuite/wiki/Geting-started,-Help-&-Usage>

```
docker run -it octosuite
```

```

root@JeyZeta: /home/jeyzeta/octosuite

Archivo Acciones Editar Vista Ayuda

(root@JeyZeta)-[/home/jeyzeta/octosuite]
# docker run -it octosuite

OCTOSUITE © 2023 Richard Mwewa
Tuesday 04 April 2023, 18:16:40PM

Linux
├─ RAM: 
├─ Node: 
├─ Release: 6.1.0-kali5-amd64
├─ Version: #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali2 (2023-02-23)
├─ Processor:
└─ Architecture: ('64bit', 'ELF')

Welcome, would you like to enable colo(u)rs for this session? [y/n]: y
[UPDATE] A new release of Octosuite is available (3.1.0). Run 'pip install --upgrade o
to get the updates.

• [x] [IMPROVED] Added a subcommand to the 'user' commands, that will be used to get
email 'user:email' (CLI only)

Full Changelog: https://github.com/bellingcat/octosuite/compare/3.0.4 ... 3.1.0

root@JeyZeta: /home/jeyzeta/octosuite

Archivo Acciones Editar Vista Ayuda

├─ Processor:
└─ Architecture: ('64bit', 'ELF')

Welcome, would you like to enable colo(u)rs for this session? [y/n]: y
[UPDATE] A new release of Octosuite is available (3.1.0). Run 'pip install --upgrade o
to get the updates.

• [x] [IMPROVED] Added a subcommand to the 'user' commands, that will be used to get
email 'user:email' (CLI only)

Full Changelog: https://github.com/bellingcat/octosuite/compare/3.0.4 ... 3.1.0

┌───┴───┐ ┌───┴───┐ ┌───┴───┐ ┌───┴───┐ ┌───┴───┐ ┌───┴───┐ ┌───┴───┐
| - | | - | | - | | - | | - | | - | | - | | - | | - |
└───┴───┘ └───┴───┘ └───┴───┘ └───┴───┘ └───┴───┘ └───┴───┘ └───┴───┘

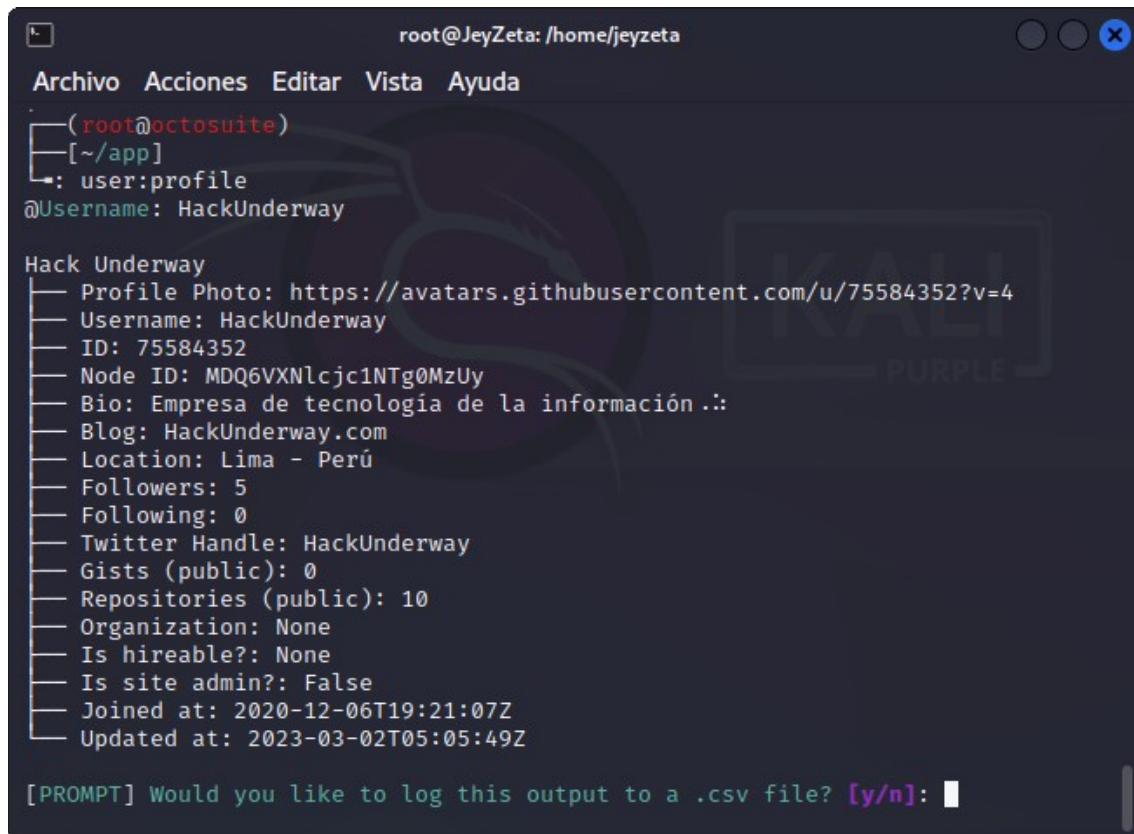
v3.1.1
- Advanced Github OSINT Framework

root
├─ use 'help' command for usage
└─ commands are case insensitive

```


Obtener información del perfil de usuario:

user:profile



```
root@JeyZeta: /home/jeyzeta
Archivo Acciones Editar Vista Ayuda
(root@octosuite)
[~/app]
➔ user:profile
@Username: HackUnderway

Hack Underway
— Profile Photo: https://avatars.githubusercontent.com/u/75584352?v=4
— Username: HackUnderway
— ID: 75584352
— Node ID: MDQ6VXNlcjc1NTg0MzUy
— Bio: Empresa de tecnología de la información.∴
— Blog: HackUnderway.com
— Location: Lima - Perú
— Followers: 5
— Following: 0
— Twitter Handle: HackUnderway
— Gists (public): 0
— Repositories (public): 10
— Organization: None
— Is hireable?: None
— Is site admin?: False
— Joined at: 2020-12-06T19:21:07Z
— Updated at: 2023-03-02T05:05:49Z

[PROMPT] Would you like to log this output to a .csv file? [y/n]:
```

Nos pregunta si queremos continuar, le damos “y” (enter).

En caso ya no quieran seguir buscando le ponen “n” (enter).

Obtener repos de usuario:

user:repos

- En este ejemplo vamos a poner 3, ya que solo veremos 3 repositorio, ustedes pueden poner la cantidad de repositorios que quieran obtener información, muy aparte va a buscar los 3 primeros de forma ordenada, guiándose de forma ascendente del abecedario. Quiero decir es que si el repositorio comienza con

la letra “C” lo va a tomar en cuenta primero antes que a los repositorios que tengan como nombre la inicial “O”. Depende con qué letra empieza el nombre del repositorio.

```
root@JeyZeta: /home/jeyzeta
Archivo Acciones Editar Vista Ayuda
(root@octosuite)
[~/app]
➔ user:repos
@Username: HackUnderway
Limit 'repositories' output to how many? (1-100): 3

HackUnderway/CheckCloudFlare
— ID: 602378792
— About: Verificar si un sitio web tiene CLOUDFLARE
— Forks: 0
— Stars: 0
— Watchers: 0
— License: {'key': 'mit', 'name': 'MIT License', 'spdx_id': 'MIT', 'url':
'https://api.github.com/licenses/mit', 'node_id': 'MDc6TGljZW5zZTEz'}
— Branch: main
— Visibility: public
— Language(s): Python
— Open issues: 0
— Topics: []
— Homepage: None
— Clone URL: https://github.com/HackUnderway/CheckCloudFlare.git
— SSH URL: git@github.com:HackUnderway/CheckCloudFlare.git
— Is fork?: False
— Is forkable?: True
— Is private?: False
— Is archived?: False
— Has downloads?: True
— Has issues?: True
— Has pages?: False
— Has projects?: True
— Has wiki?: True
— Pushed at: 2023-02-16T04:39:36Z
— Created at: 2023-02-16T04:33:16Z
```

Pueden poner del 1-100, en este ejemplo solo se verán 3 repositorios.

Nos muestra los datos de creación, si tiene Forks, Stars, tipo de licencia, watchers, actualización, etc.

```
root@JeyZeta: /home/jeyzeta

Archivo Acciones Editar Vista Ayuda

[PROMPT] Would you like to log this output to a .csv file? [y/n]: y
[POSITIVE] Output logged: output/CheckCloudFlare_HackUnderway.csv

HackUnderway/CrypTool
├── ID: 559656586
├── About: HERRAMIENTA PARA CIFRAR TEXTO, EN CIFRADO CESAR Y VIGENERE, HECHO EN PYTHON
├── Forks: 0
├── Stars: 2
├── Watchers: 2
├── License: {'key': 'mit', 'name': 'MIT License', 'spdx_id': 'MIT', 'url': 'https://api.github.com/licenses/mit', 'node_id': 'MDC6TGljZW5zZTEz'}
├── Branch: main
├── Visibility: public
├── Language(s): Python
├── Open issues: 0
├── Topics: []
├── Homepage:
├── Clone URL: https://github.com/HackUnderway/CrypTool.git
├── SSH URL: git@github.com:HackUnderway/CrypTool.git
├── Is fork?: False
├── Is forkable?: True
├── Is private?: False
├── Is archived?: False
├── Has downloads?: True
├── Has issues?: True
├── Has pages?: False
├── Has projects?: True
├── Has wiki?: True
├── Pushed at: 2022-11-02T03:10:22Z
├── Created at: 2022-10-30T19:28:32Z
└── Updated at: 2023-01-19T06:03:06Z

root@JeyZeta: /home/jeyzeta

Archivo Acciones Editar Vista Ayuda

[PROMPT] Would you like to log this output to a .csv file? [y/n]: y
[POSITIVE] Output logged: output/CrypTool_HackUnderway.csv

HackUnderway/HackUnderway
├── ID: 535037747
├── About: Config files for my GitHub profile.
├── Forks: 0
├── Stars: 0
├── Watchers: 0
├── License: None
├── Branch: main
├── Visibility: public
├── Language(s): None
├── Open issues: 0
├── Topics: ['config', 'github-config']
├── Homepage: https://github.com/HackUnderway
├── Clone URL: https://github.com/HackUnderway/HackUnderway.git
├── SSH URL: git@github.com:HackUnderway/HackUnderway.git
├── Is fork?: False
├── Is forkable?: True
├── Is private?: False
├── Is archived?: False
├── Has downloads?: True
├── Has issues?: False
├── Has pages?: False
├── Has projects?: True
├── Has wiki?: False
├── Pushed at: 2022-12-03T03:05:51Z
├── Created at: 2022-09-10T15:25:35Z
└── Updated at: 2022-09-10T15:25:35Z


[PROMPT] Would you like to log this output to a .csv file? [y/n]: y
[POSITIVE] Output logged: output/HackUnderway_HackUnderway.csv
```

Obtener información del perfil de organización:

org:profile


```
root@JeyZeta: /home/jeyzeta
Archivo Acciones Editar Vista Ayuda
(root@octosuite)
[~/app]
➔ org:profile
@Organization: HackingLive

{response.json()['name']}
— Profile Photo: https://avatars.githubusercontent.com/u/16280786?v=4
— Username: HackingLive
— ID: 16280786
— Node ID: MDEyOk9yZ2FuaXphdGlvb2E2MjgwNzg2
— Email: hackinglivebooking@gmail.com
— About:
— Blog: https://hackingenvivo.blogspot.com/
— Location: None
— Followers: 0
— Following: 0
— Twitter handle: None
— Gists: 0
— Repositories: 0
— Account type: Organization
— Is verified?: False
— Has organization projects?: True
— Has repository projects?: True
— Created at: 2015-12-13T21:55:52Z
— Updated at: 2017-11-08T08:57:36Z
```



**HackingEnVivo** [Follow](#)

Empresa que brinda servicios de Seguridad Informática, con diferentes servicios: Auditorías web con reporte incluido, ventas de manuales hacking, conferencias.

86 followers · 0 following


 Hacking Live
Perú · Venezuela
hackinglivebooking@gmail.com
<https://twitter.com/HackingEnVivo>

Achievements



[Beta](#) [Send feedback](#)

Organizations



[Block or Report](#)

Overview [Repositories](#) 12 [Projects](#) [Packages](#) [Stars](#) 4





[Python](#) ☆ 4 🍴 5

[Python](#) ☆ 4 🍴 2

0 contributions in the last year

	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May
Mon													
Wed													
Fri													

[Learn how we count contributions](#)

Less     More

Contribution activity

May 2023

HackingEnVivo has no activity yet for this period.

[Show more activity](#)

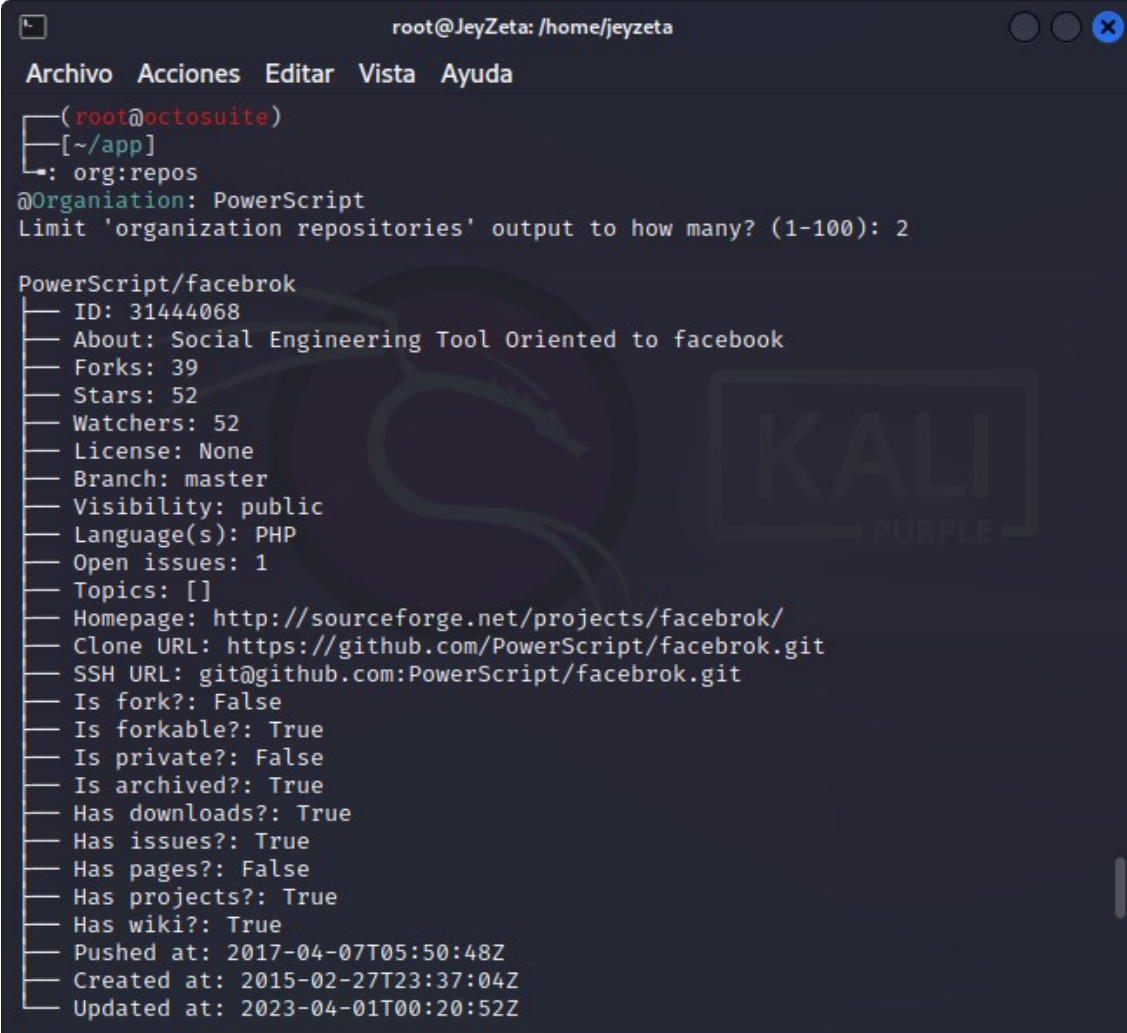
Seeing something unexpected? Take a look at the [GitHub profile guide](#).

[2023](#)
2022
2021
2020
2019
2018

El perfil de Organización, en este caso lo saqué de mi repositorio antiguo, tenía creado un perfil de Organización, que lo pueden ver en la imagen de arriba, en la parte inferior izquierda dice “Organizations”. Hay cuentas que no se crean un perfil de organización, pero hay otras que si.

Obtener los repositorios de organizaciones:

org:repos



```
root@JeyZeta: /home/jeyzeta
Archivo Acciones Editar Vista Ayuda
(root@octosuite)
[~/app]
: org:repos
@Organization: PowerScript
Limit 'organization repositories' output to how many? (1-100): 2

PowerScript/facebrok
— ID: 31444068
— About: Social Engineering Tool Oriented to facebook
— Forks: 39
— Stars: 52
— Watchers: 52
— License: None
— Branch: master
— Visibility: public
— Language(s): PHP
— Open issues: 1
— Topics: []
— Homepage: http://sourceforge.net/projects/facebrok/
— Clone URL: https://github.com/PowerScript/facebrok.git
— SSH URL: git@github.com:PowerScript/facebrok.git
— Is fork?: False
— Is forkable?: True
— Is private?: False
— Is archived?: True
— Has downloads?: True
— Has issues?: True
— Has pages?: False
— Has projects?: True
— Has wiki?: True
— Pushed at: 2017-04-07T05:50:48Z
— Created at: 2015-02-27T23:37:04Z
— Updated at: 2023-04-01T00:20:52Z
```




```
root@JeyZeta: /home/jeyzeta

Archivo Acciones Editar Vista Ayuda

[PROMPT] Would you like to log this output to a .csv file?: y

PowerScript/KatanaFramework
├── ID: 31444615
├── About: The New Hacking Framework
├── Forks: 237
├── Stars: 644
├── Watchers: 644
├── License: None
├── Branch: master
├── Visibility: public
├── Language(s): Python
├── Open issues: 22
├── Topics: []
├── Homepage: http://powerscript.github.io/KatanaFramework/
├── Clone URL: https://github.com/PowerScript/KatanaFramework.git
├── SSH URL: git@github.com:PowerScript/KatanaFramework.git
├── Is fork?: False
├── Is forkable?: True
├── Is private?: False
├── Is archived?: False
├── Has downloads?: True
├── Has issues?: True
├── Has pages?: True
├── Has projects?: True
├── Has wiki?: True
├── Pushed at: 2021-04-05T02:05:59Z
├── Created at: 2015-02-27T23:58:34Z
├── Updated at: 2023-05-23T07:40:35Z
└── [PROMPT] Would you like to log this output to a .csv file?: y
```

En este ejemplo vemos la siguiente organización “**PowerScript**”




PowerScript
Hacking projects
14 followers • Cyber Space


[Follow](#)

[Overview](#) [Repositories](#) [5](#) [Projects](#) [Packages](#) [People](#)

Pinned




KatanaFramework (Public)
The New Hacking Framework
Python 644 237



h2Polar (Public)
Lightweight http/s proxy written in C with ssl intercepting 'n traffic features.
C 2

Repositories

Type Language Sort



h2Polar (Public)
Lightweight http/s proxy written in C with ssl intercepting 'n traffic features.
C 2 0 0 Updated on Feb 1, 2022

People

This organization has no public members. You must be a member to see who's a part of this organization.

Top languages

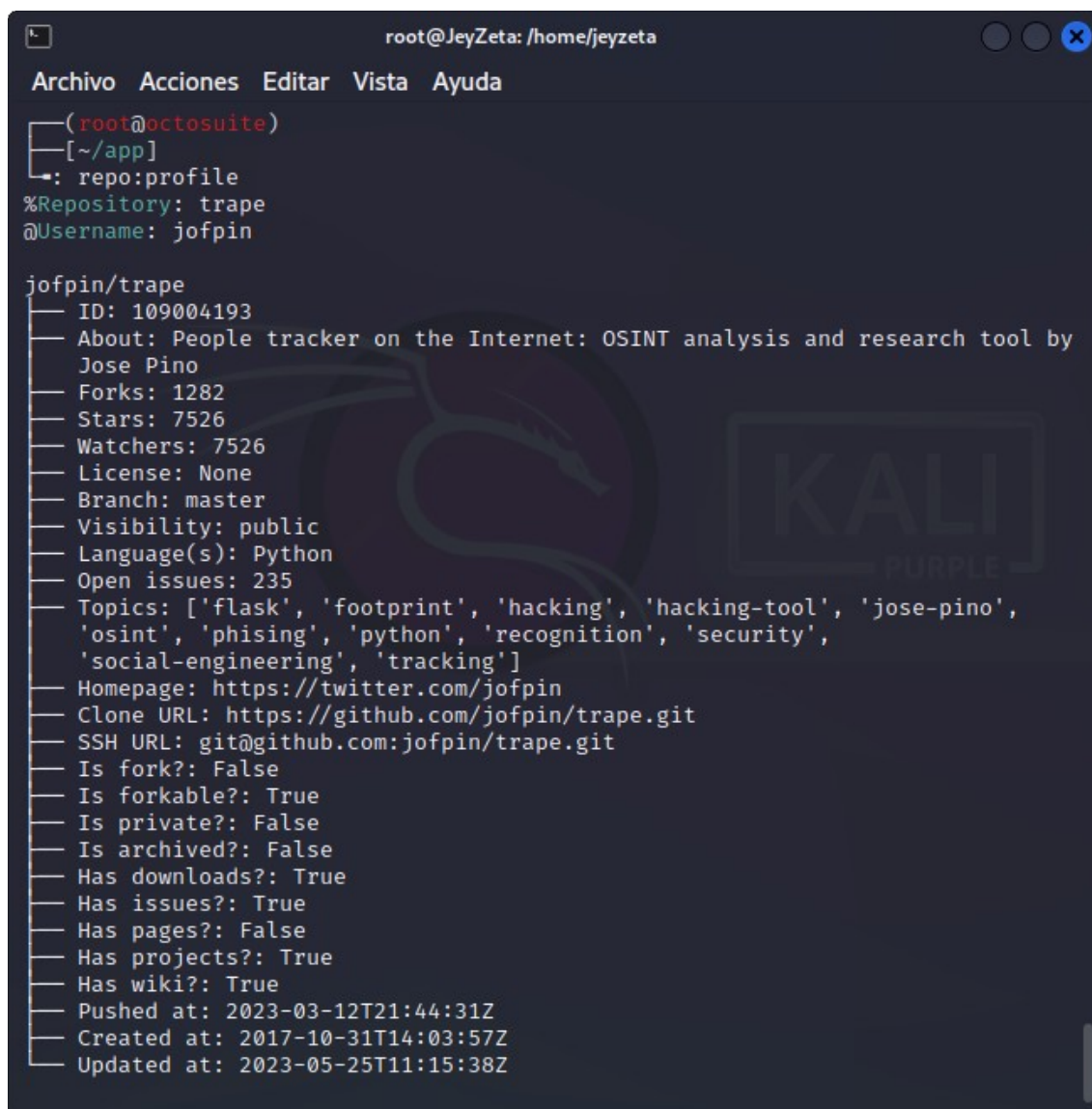
PHP Python C HTML

[Report abuse](#)

265

Obtener información sobre el perfil de Repo:

repo:profile



```
root@JeyZeta: /home/jeyzeta
Archivo Acciones Editar Vista Ayuda
(root@octosuite)
[~/app]
→ repo:profile
%Repository: trape
@Username: jofpin

jofpin/trape
— ID: 109004193
— About: People tracker on the Internet: OSINT analysis and research tool by Jose Pino
— Forks: 1282
— Stars: 7526
— Watchers: 7526
— License: None
— Branch: master
— Visibility: public
— Language(s): Python
— Open issues: 235
— Topics: ['flask', 'footprint', 'hacking', 'hacking-tool', 'jose-pino', 'osint', 'phising', 'python', 'recognition', 'security', 'social-engineering', 'tracking']
— Homepage: https://twitter.com/jofpin
— Clone URL: https://github.com/jofpin/trape.git
— SSH URL: git@github.com:jofpin/trape.git
— Is fork?: False
— Is forkable?: True
— Is private?: False
— Is archived?: False
— Has downloads?: True
— Has issues?: True
— Has pages?: False
— Has projects?: True
— Has wiki?: True
— Pushed at: 2023-03-12T21:44:31Z
— Created at: 2017-10-31T14:03:57Z
— Updated at: 2023-05-25T11:15:38Z
```

Obtener forks de repo:

repo:forks

Nos muestra diferentes resultados, entre ellas los usuarios que le hicieron Fork al repositorio. En este ejemplo sólo puse 1 para no hacerla muy larga.

```
root@JeyZeta: /home/jeyzeta
Archivo Acciones Editar Vista Ayuda

(root@octosuite)
[~/app]
→ repo: forks
%Repository: trape
@Username: jofpin
Limit 'forks' output to how many? (1-100): 1
9tanu0naphtro/trape
— ID: 642533422
— About: People tracker on the Internet: OSINT analysis and research tool by
  Jose Pino
— Forks: 0
— Stars: 0
— Watchers: 0
— License: None
— Branch: master
— Visibility: public
— Language(s): Python
— Open issues: 0
— Topics: []
— Homepage: https://twitter.com/jofpin
— Clone URL: https://github.com/9tanu0naphtro/trape.git
— SSH URL: git@github.com:9tanu0naphtro/trape.git
— Is fork?: True
— Is forkable?: True
— Is private?: False
— Is archived?: False
— Has downloads?: True
— Has issues?: False
— Has pages?: False
— Has projects?: True
— Has wiki?: True
— Pushed at: 2023-05-18T19:48:07Z
— Created at: 2023-05-18T19:37:54Z
— Updated at: 2023-05-18T19:44:08Z
```

<https://hackunderway.com/octosuite-la-herramienta-de-osint-a-github/>

OSINT a Instagram:

Instaloader:

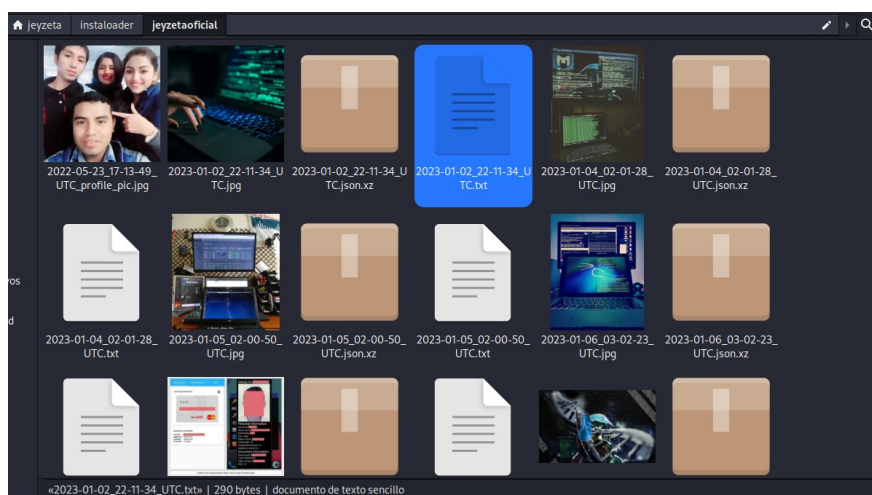
Descarga imágenes (o vídeos) junto con su descripción, fotos y otros metadatos desde Instagram.

<https://github.com/instaloder/instaloder>

En este caso he puesto mi username de instagram.

```
jeyzeta@JeyZeta: ~/instaloder
Archivo Acciones Editar Vista Ayuda
(jeyzeta@JeyZeta)~(~/instaloder)
$ python instaloder.py jeyzetaoficial
Stored ID 53594800333 for profile jeyzetaoficial.
Hint: Use --login to download higher-quality versions of pictures.
[1/1] Downloading profile jeyzetaoficial
jeyzetaoficial/2022-05-23_17-13-49.UTC_profile_pic.jpg
Retrieving posts from profile jeyzetaoficial.
[ 1/71] jeyzetaoficial/2023-01-13_13-00-08.UTC.jpg [Viernes de Tools (Herramienta...)] json
[ 2/71] jeyzetaoficial/2023-03-21_12-00-13.UTC.jpg [eJPT https://drive.google.co...] json
[ 3/71] jeyzetaoficial/2023-03-19_12-00-08.UTC.jpg [CRT0 - Notes to Exam Preparat...] json
[ 4/71] jeyzetaoficial/2023-03-18_12-00-07.UTC.jpg [eCPPT (eLearnSecurity Certifi...) json
[ 5/71] jeyzetaoficial/2023-03-17_12-00-11.UTC.jpg [Viernes de Tools (Herramienta...)] json
[ 6/71] jeyzetaoficial/2023-03-16_12-00-08.UTC.jpg [Offensive Security Defense An...] json
[ 7/71] jeyzetaoficial/2023-03-13_12-00-04.UTC.jpg [Linux Essentials https://dri...] json
[ 8/71] jeyzetaoficial/2023-03-12_13-00-05.UTC.jpg [LPIC-1 https://drive.google....] json
[ 9/71] jeyzetaoficial/2023-03-10_12-00-08.UTC.jpg [Viernes de Tools (Herramienta...)] json
[10/71] jeyzetaoficial/2023-03-09_01-00-07.UTC.jpg [AWAE (WEB-300) aHR0cHM6Ly9kc...] json
[11/71] jeyzetaoficial/2023-03-08_00-00-05.UTC_1.jpg jeyzetaoficial/2023-03-08_00-00-05_UT
C_2.jpg [OSDA-Soc200 aHR0cHM6Ly9kcml2...] json
[12/71] jeyzetaoficial/2023-03-06_17-00-14.UTC.jpg [Comandos relevantes para Shod...] json
[13/71] jeyzetaoficial/2023-03-06_00-00-08.UTC.jpg [Ya lo pueden ver mi tutorial,...] json
[14/71] jeyzetaoficial/2023-03-04_13-00-18.UTC.jpg [Buen sábado para todos people...] json
[15/71] jeyzetaoficial/2023-03-03_12-00-05.UTC.jpg [Viernes de Tools (Herramienta...)] json
[16/71] jeyzetaoficial/2023-03-02_12-00-10.UTC.jpg [Buen día fieles seguidores! ...] json
[17/71] jeyzetaoficial/2023-03-01_12-00-16.UTC.jpg [Para entender mejor qué es Ne...] json
[18/71] jeyzetaoficial/2023-02-28_13-00-09.UTC.jpg [Buen día fieles seguidores! 😊...] json
[19/71] jeyzetaoficial/2023-02-24_17-10-54.UTC.jpg [Esteganografía con Stegosuite...] json
[20/71] jeyzetaoficial/2023-02-23_16-02-07.UTC.jpg [Ya puede ver el tutorial que ...] json
[21/71] jeyzetaoficial/2023-02-23_12-00-10.UTC.jpg [Buen día futuros expertos en ...] json
[22/71] jeyzetaoficial/2023-02-22_12-00-05.UTC.jpg [Estimados reclutadores, Si ...] json
[23/71] jeyzetaoficial/2023-02-21_17-10-24.UTC.jpg [Buenas fieles seguidores! - ...] json
[24/71] jeyzetaoficial/2023-02-20_20-59-15.UTC.jpg [Burp Suite https://portswigg...] json
[25/71] jeyzetaoficial/2023-02-19_13-00-05.UTC.jpg [Ya está por salir mi manual d...] json
[26/71] jeyzetaoficial/2023-02-18_13-00-04.UTC.jpg [¿Que curso quisieran que haga...] json
[27/71] jeyzetaoficial/2023-02-17_17-30-05.UTC.jpg [Viernes de Tools (Herramienta...)] json
```

Al terminar nos muestra lo que descargó en la terminal y en la carpeta donde se encuentra la herramienta, se crea un reporte dentro de una carpeta, que va a depender del usuario que ustedes pongan, nos muestra imágenes y txt de la descripción de cada post.

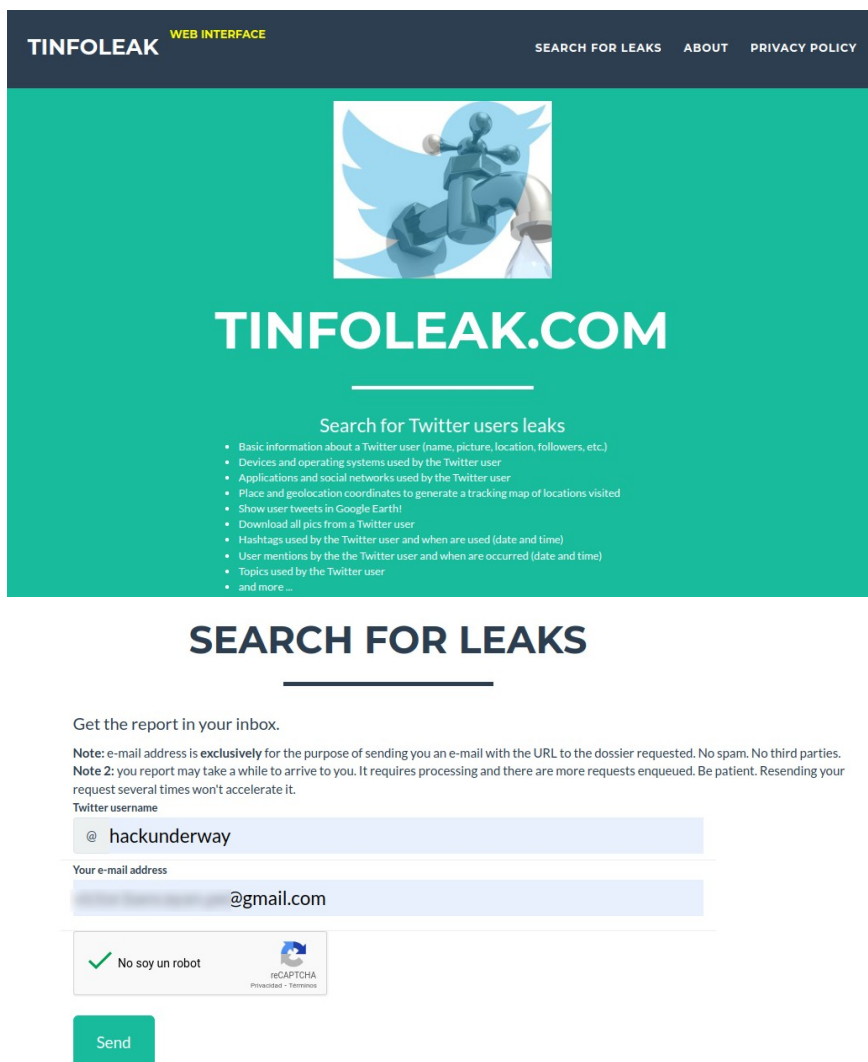


OSINT a Twitter:

Tinfoleak:

Es una herramienta online muy usada al momento de hacer OSINT, ya que busca Información básica sobre un usuario de Twitter (nombre, foto, ubicación, seguidores, dispositivos y sistemas operativos utilizados, aplicaciones y redes sociales utilizadas, coordenadas de lugar y geolocalización para generar un mapa de seguimiento de los lugares visitados, hashtags utilizados y cuándo se utilizan (fecha y hora), menciones y cuándo se produjeron (fecha y hora), temas utilizados por el usuario de Twitter y más) ...

<https://tinfoleak.com/>



TINFOLEAK WEB INTERFACE SEARCH FOR LEAKS ABOUT PRIVACY POLICY

TINFOLEAK.COM

Search for Twitter users leaks

- Basic information about a Twitter user (name, picture, location, followers, etc.)
- Devices and operating systems used by the Twitter user
- Applications and social networks used by the Twitter user
- Place and geolocation coordinates to generate a tracking map of locations visited
- Show user tweets in Google Earth!
- Download all pics from a Twitter user
- Hashtags used by the Twitter user and when are used (date and time)
- User mentions by the Twitter user and when are occurred (date and time)
- Topics used by the Twitter user
- and more ...

SEARCH FOR LEAKS

Get the report in your inbox.

Note: e-mail address is exclusively for the purpose of sending you an e-mail with the URL to the dossier requested. No spam. No third parties.
Note 2: your report may take a while to arrive to you. It requires processing and there are more requests enqueued. Be patient. Resending your request several times won't accelerate it.

Twitter username

@ hackunderway

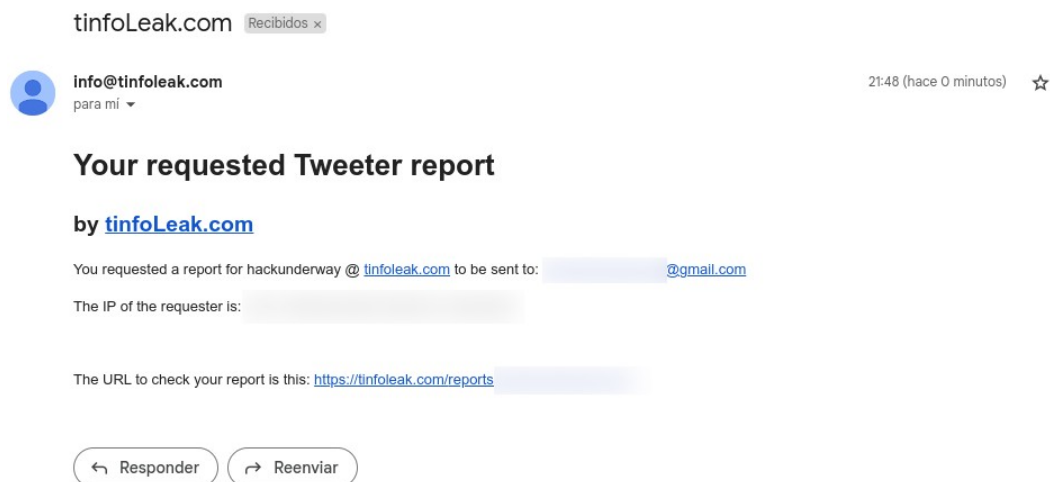
Your e-mail address

@gmail.com

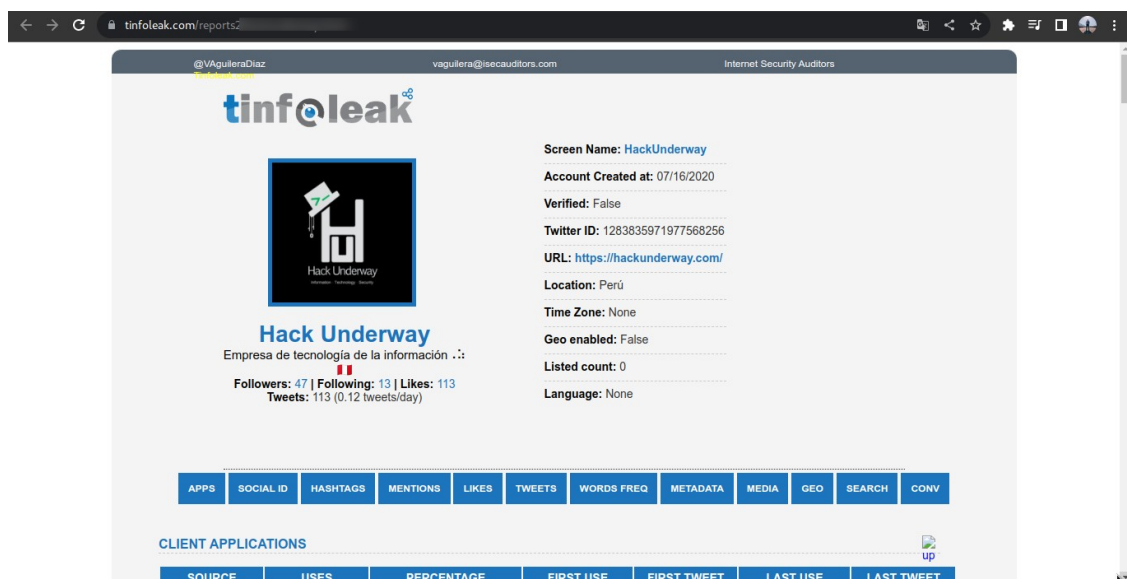
✓ No soy un robot reCAPTCHA

Send

Debemos poner el usuario de twitter del cuál queremos obtener información, de hashtag, menciones, fotos, dispositivos del cual hemos tuiteado, gps, etc.



Nos llega al correo que hemos puesto, e ingresamos a la url que nos muestra.



Nos muestra una cantidad de información relevante para OSINT, depende si el usuario es muy activo en twitter, va a mostrar la información.

Podemos ver más ejemplos, pero ya dejé muchos enlaces en la sección de arriba, es cuestión que vayan probando cuál les parece más útil dependiendo el caso e información que quieran obtener.

OSINT a WahtsApp:

WhatsApp-OSINT: Registra los eventos online/offline de cualquier contacto de whatsapp. Al momento de añadir el nombre de tu contacto de WhatsApp, podrás ver desde la terminal si está en línea, cuáles fueron sus momentos que estuvo online.

<https://github.com/jasperan/whatsapp-osint>

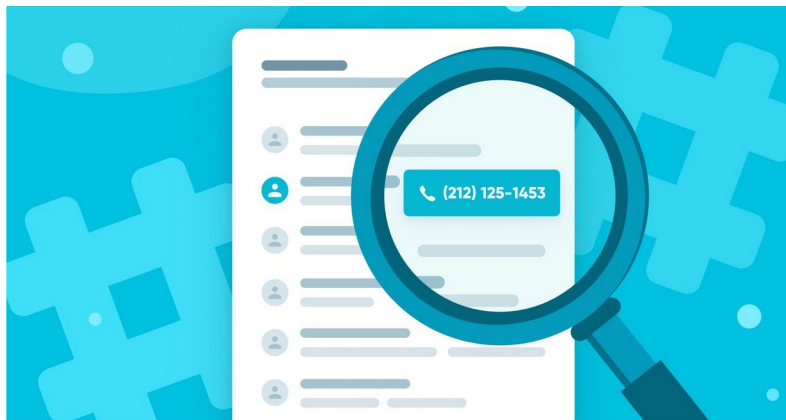
```
(jeyzeta@JeyZeta)-[~/whatsapp-osint]
$ python whatsappbeacon.py --username " " --language "es"
In order to make this program to work, you will need to log-in once in WhatsApp. After that
, your session will be saved until you revoke it.
Press any key when you are at the chat menu...
There has been created in the folder ./logs a text file to log every connection and disconn
ection of the user 
Trying to find: //span[contains(text(), ' ')]
Found and clicked!
Trying to find: //span[@title='en línea'] in user 
[2023-03-28 16:54:51][ONLINE] 
[2023-03-28 16:55:30][DISCONNECTED]  was online for 27 seconds. Session total: 27 secon
ds
[2023-03-28 16:56:36][ONLINE] 
[2023-03-28 16:56:48][DISCONNECTED]  was online for 0 seconds. Session total: 27 second
s
[2023-03-28 16:57:28][ONLINE] 
[2023-03-28 16:57:44][DISCONNECTED]  was online for 4 seconds. Session total: 31 second
s
[2023-03-28 16:57:47][ONLINE] 
[2023-03-28 16:58:10][DISCONNECTED]  was online for 10 seconds. Session total: 42 secon
ds
█
```

NÚMEROS

Veremos la información de números de teléfonos.

Usando plataformas online y scripts, para automatizar los procesos.

Recopilando información de que cuentas tiene vinculado con el número en diferentes plataformas, a qué operador pertenece el número, que país es, en qué dispositivo está siendo usado el número como Android, Iphone, etc.



DePerú:

<https://www.deperu.com/celulares/index.php>

¿Quién te llama al celular?

En base a tu colaboración podemos determinar la probabilidad de que el número que te marca procede de un remitente no deseado.

válido solo para Perú

Para encontrar la información de probabilidades debe ingresar en número celular sin espacios, rayas o paréntesis, todo junto y sin código de país. Por ejemplo ingrese solamente **999999999**



El número [redacted] pertenece al operador Bitel

Un porcentaje pequeño de números han migrado entre operadores por lo que puede ser posible que en muy pocos casos los datos mostrados sean erróneos.

Nos muestra a que operadora pertenece el número que ingresamos, esto funciona para Perú.

Ahora veremos una herramienta de GitHub, para obtener el mismo resultado, pero esta si es a nivel global.

Phonenumbers:

<https://github.com/HackUnderway/Ph0n3Numb3rs>

```
(jeyzeta@JeyZeta)-[~/Ph0n3Numb3rs]
$ python Ph0n3Numb3rs.py
Ingresar número: +51 [redacted]
| País | Proveedora |
|-----|-----|
| Peru | Claro      |
```

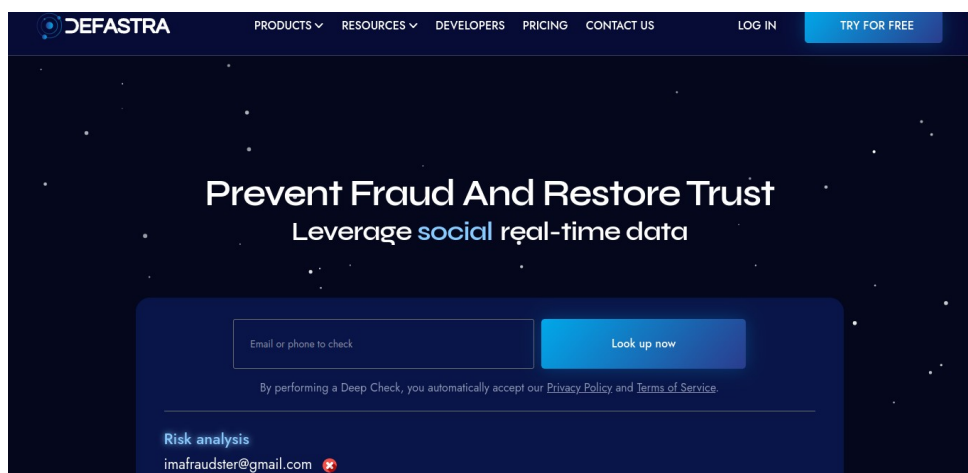
Realizé un post con más detalles.

<https://hackunderway.com/ph0n3numb3rs/>

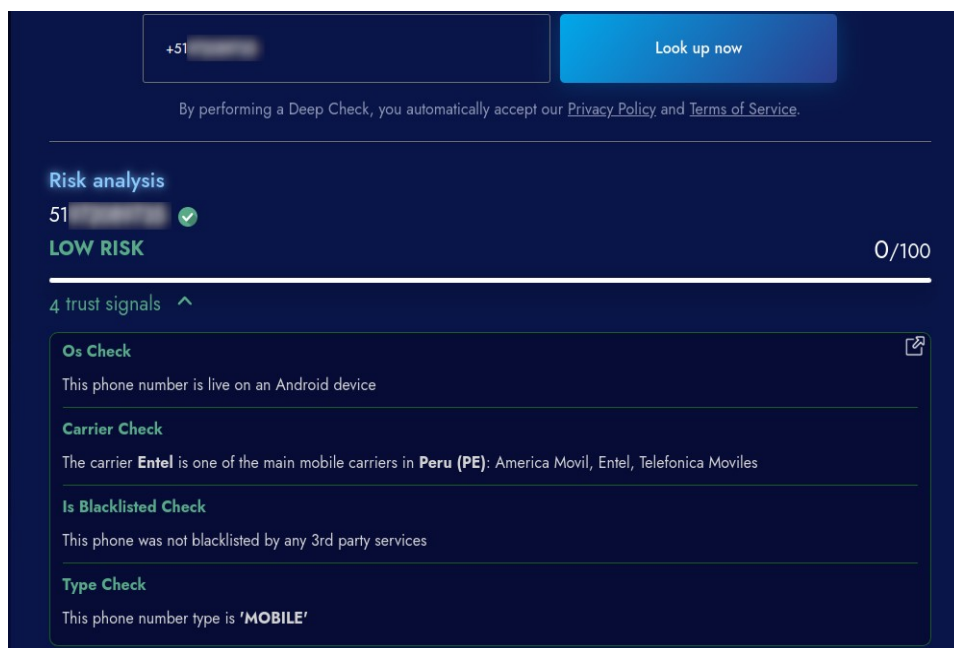
Ahora veremos otra herramienta online muy efectiva para encontrar información con más detalles, como por ejemplo, que sistema operativo usa en su smartphone (Android, Iphone, Windows, etc), también a que plataformas está vinculado el número, operadora y otros detalles relevantes que nos sirven en el proceso de OSINT.

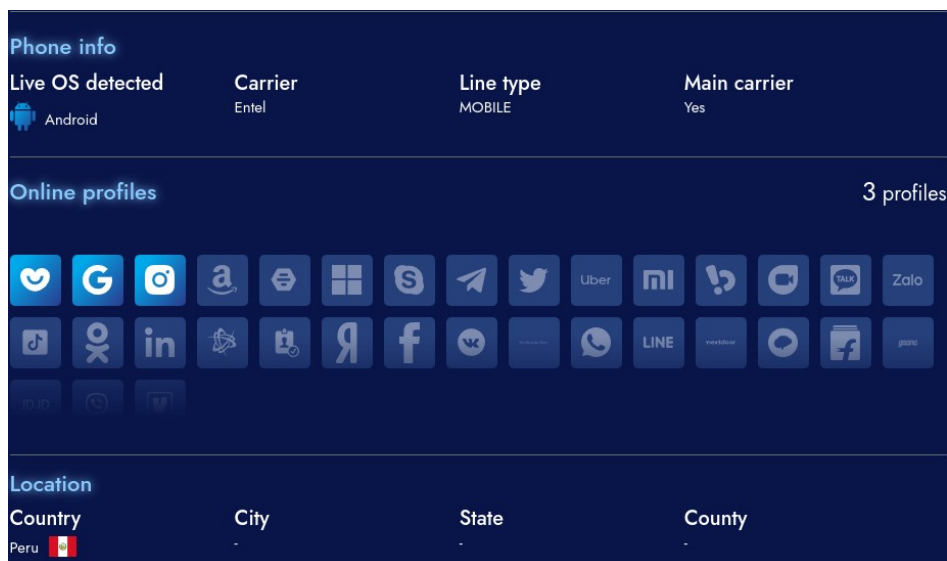
Defastra: Una herramienta muy recomendada para obtener información.

<https://defastra.com/>



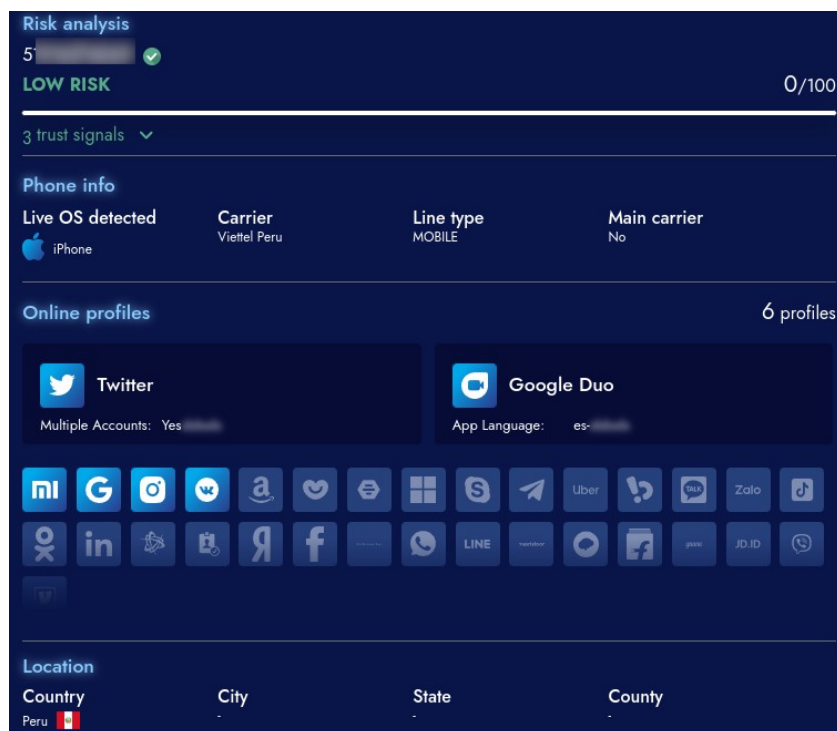
Al agregar un número nos muestra la siguiente información.





Como ven en la imagen anterior, nos muestra que está siendo usado desde un Android, el operador es de Entel, está vinculado a 3 plataformas y es de Perú.

Veremos otro ejemplo con otro número.



Vemos un resultado diferente, pueden probar con varios números, para recolectar información.

Cabe recalcar que antes del número se pone el código postal (zip code), en nuestro caso es +51 (es el código que va antes del número de teléfono).

Código Postal:

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

Base de datos de códigos postales y regiones administrativas para 241 países

Buscar

Códigos postales y regiones administrativas por países

El código postal es un esquema que se asigna a distintas zonas o lugares de un país, un código que sirve para facilitar y mecanizar el encaminamiento de una pieza de correo. Generalmente, es una serie de dígitos, aunque en algunos países incluyen letras. También se utiliza en los navegadores GPS para ubicar lugares.

Los códigos postales tienen distintos formatos y normas de uso dependiendo del país. En la mayor parte de Europa, el código postal va antes del nombre del lugar o ciudad y a veces precedido por el código del país, mientras que en los países anglófonos suele ir detrás del nombre del lugar.

Códigos postales por país y tipo de dígitos.

Cifras numéricas::

Dedos alfanuméricos::

Códigos postales no utilizados:

Asia

Europa del Oeste

América del Norte

Oceanía

Oriente Medio

África

América Central y del Sur











Europa del Este

Por defecto viene seleccionado Europa del Oeste, pero ustedes pueden seleccionar el continente en el que quieran saber sus códigos de país.

ISO	País	Capital	Formato	Nombre	Código de país	Latitud/Longitud
ARG / AR	Argentina	Buenos Aires	A0000 AAA	CPA	54	38°25'16"S/63°35'14"W
BRB / BB	Barbados	Bridgetown	00000	Postal code	1-246	13°11'0"N/59°32'4"W
BLZ / BZ	Belice	Belmopan	-	-	501	17°11'34"N/88°30'3"W
BOL / BO	Bolivia	Sucre	-	-	591	16°17'18"S/63°32'58"W
BRA / BR	Brasil	Brasilia	00000-000	CEP	55	14°14'34"S/53°11'21"W
CHL / CL	Chile	Santiago	000 0000	Código postal	56	36°42'59"S/73°36'6"W
COL / CO	Colombia	Bogota	000000	Código postal	57	4°34'38"N/74°17'56"W
CRI / CR	Costa Rica	San Jose	00000	Código postal	506	9°37'29"N/84°15'11"W
CUW / CW	Curazao	Willemstad	-	-	599	12°12'33"N/68°56'43"W
ECU / EC	Ecuador	Quito	000000	Código postal	593	1°46'47"S/78°7'53"W
SLV / SV	El Salvador	San Salvador	00000	Código postal	503	13°47'48"N/88°54'37"W
FLK / FK	Islas Malvinas	Stanley	FIQQ 1ZZ	Postcode	500	51°48'2"S/59°31'43"W
GTM / GT	Guatemala	Guatemala City	00000	Código postal	502	15°46'34"N/90°13'47"W

276

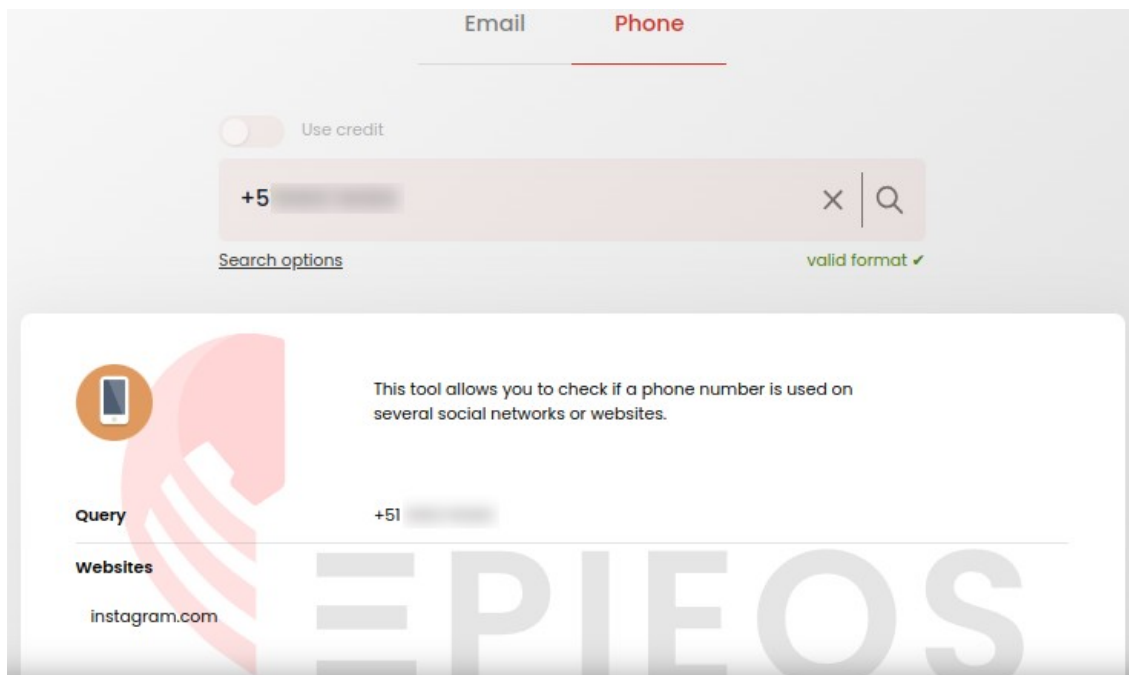
INVESTIGADOR_Z

GUY / GY	 Guyana	Georgetown	-	-	592	4°51'58"N/58°55'57"W
HND / HN	 Honduras	Tegucigalpa	-	-	504	14°44'46"N/86°15'11"W
NIC / NI	 Nicaragua	Managua	00000	Código postal	505	12°52'0"N/85°12'51"W
PAN / PA	 Panamá	Panama City	-	-	507	8°25'3"N/80°6'45"W
PRY / PY	 Paraguay	Asuncion	000000	Código postal	595	23°27'4"S/58°27'11"W
PER / PE	 Perú	Lima	00000	Código postal	51	9°10'52"S/75°0'8"W
SUR / SR	 Surinam	Paramaribo	-	-	597	3°55'4"N/56°1'55"W
TTO / TT	 Trinidad y Tobago	Port of Spain	000000	-	1-868	10°41'13"N/61°13'15"W
URY / UY	 Uruguay	Montevideo	00000	Código postal	598	32°31'53"S/55°45'29"W
VEN / VE	 Venezuela	Caracas	0000	Código postal	58	6°24'50"N/66°34'44"W

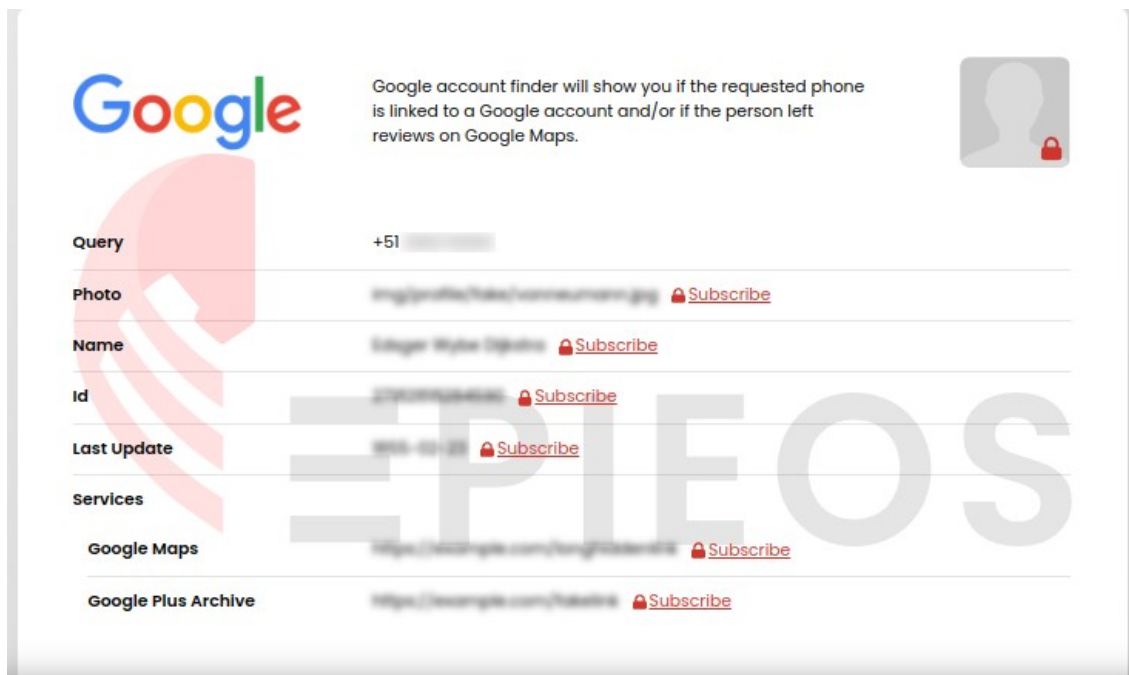
Anteriormente vimos Epieos, pero para email, ahora lo veremos para números.

Epieos:

<https://epieos.com/>



Nos da como resultado una cuenta de instagram asociada al número.



Ahora vemos que esta asociada a una cuenta de google, sólo que para acceder a la información completa debemos tener una suscripción premium.

DeadTrapv2: (<https://github.com/legly/DeadTrapv2>)

Una herramienta OSINT para rastrear las huellas de un número de teléfono.

```

jeyzeta@JeyZeta: ~/DeadTrapv2
Archivo Acciones Editar Vista Ayuda
(jeyzeta@JeyZeta)-[~/DeadTrapv2]
$ python main.py -n 1

||D||e||a||d||T||r||a||p|| | |
||_||_||_||_||_||_||_||_||_||
|/_|/_|/_|/_|/_|/_|/_|/_|/_|

[*] Running local scan ...

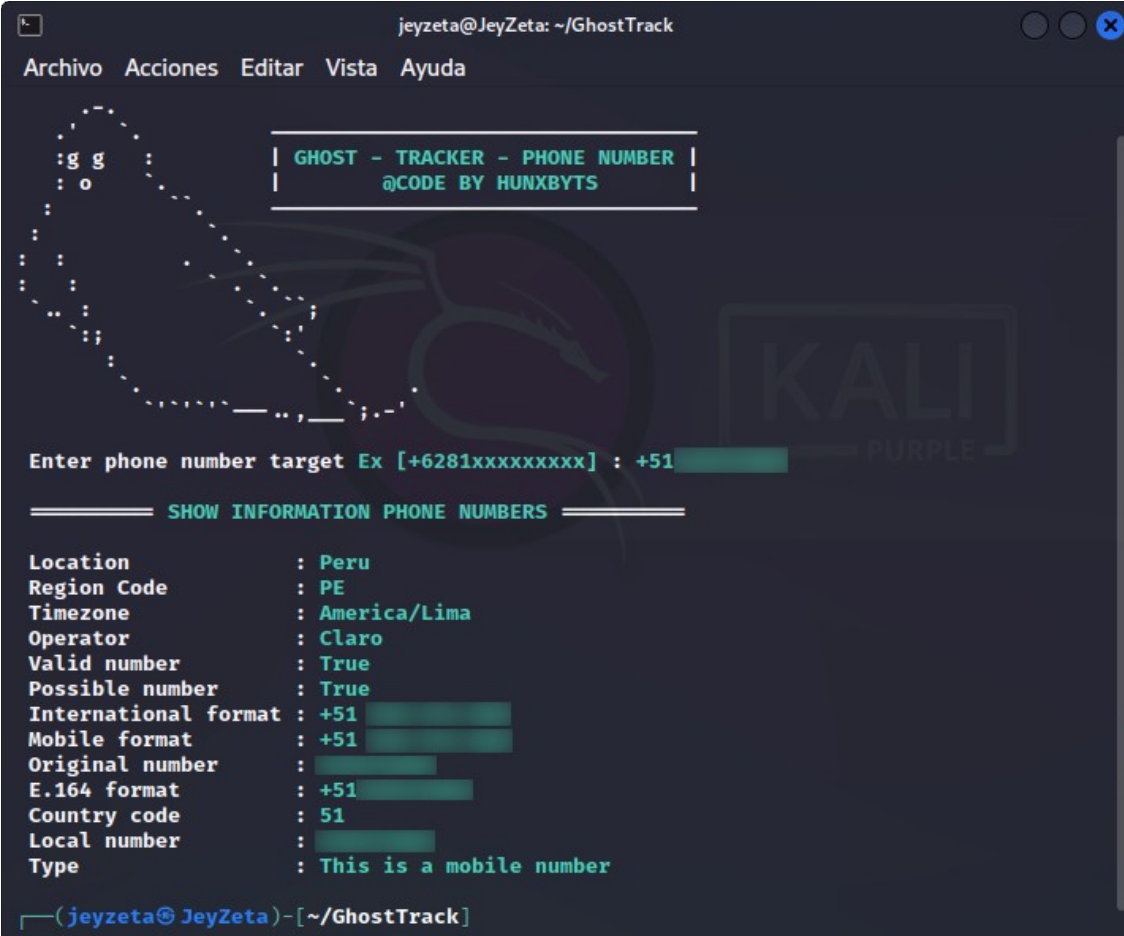
[*] Running Numverify scan ...

Country Prefix: +1
Number: 41
Country: United States of America
Country Code: US
Location: Novato
Carrier: AT&T Mobility LLC
Line type: mobile
usage: main.py [-h] [-n number] [-i input_file] [-v] [-s scanner] [-o] [-rep] [-q]

DEADTRAP v1.0.2
  
```

GhostTrack: (<https://github.com/HunxByts/GhostTrack>)

Herramienta útil para rastrear la ubicación de una dirección IP o número de teléfono, por lo que esta herramienta se usa para OSINT a IP y números, cabe resaltar que se debe corroborar la información brindada con diferentes medios e ir seleccionando la información comprobada y verídica, para nuestras investigaciones OSINT. Ya que esta y otras herramientas arrojan resultados diferentes.



```
jeyzeta@JeyZeta: ~/GhostTrack
Archivo  Acciones  Editar  Vista  Ayuda

: g g :
: o   :

| GHOST - TRACKER - PHONE NUMBER |
| @CODE BY HUNXBYTS             |

Enter phone number target Ex [+6281xxxxxxxxx] : +51

===== SHOW INFORMATION PHONE NUMBERS =====

Location       : Peru
Region Code    : PE
Timezone       : America/Lima
Operator       : Claro
Valid number    : True
Possible number : True
International format : +51
Mobile format  : +51
Original number : 
E.164 format   : +51
Country code   : 51
Local number   : 
Type           : This is a mobile number

(jeyzeta@JeyZeta)-[~/GhostTrack]
```

Ghoulbond: (<https://github.com/hitesh22rana/ghoulbond>)

Utilidad de sistema de código abierto, escáner y herramienta OSINT.

Otros enlaces:

<https://thatsthem.com/>

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

RECURSOS Y CERTIFICACIONES

Offensive OSINT:

<https://www.offensiveosint.io/offensive-osint-s01e03-intelligence-gathering-on-critical-infrastructure-in-southeast-asia/>

<https://www.offensiveosint.io/offensive-osint-s01e02-deobfuscation-source-code-analysis-uncovering-cp-distribution-network/>

<https://www.offensiveosint.io/offensive-osint-s01e01-osint-rdp/>

SANS:

<https://www.sans.org/cyber-security-courses/advanced-open-source-intelligence-gathering-analysis/>

<https://www.sans.org/blog/what-is-open-source-intelligence/>

Referencias:

Todas las referencias las he puesto en cada explicación, en caso se aya omitido alguno las disculpas del caso. Antes de ahcer este manual estube preparandome por mucho tiempo tanto en cursos online y libros en español, inglés, portugues y ruso.

Otros enlaces:

<https://ciberpatrulla.com/libro-osint-ciberpatrulla/>

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

<https://github.com/Drew-Alleman/DataSurgeon>

<https://booleanstrings.com/tools/>

<https://github.com/cipher387/Advanced-search-operators-list>

<https://github.com/WebBreachr/obsidian-osint-templates/>


https://github.com/ManuelBot59/OSINT_TIPS

<https://github.com/ManuelBot59/RecursosOsint>

https://medium.com/@cyb_detective/4-easy-tricks-for-using-gravatar-in-osint-99c0910d933

<http://hunter.how>

https://github.com/cipher387/osint_stuff_tool_collection/

**Anton**
@therceman

[Twitter](#) [LinkedIn](#) [Instagram](#) [Facebook](#) [YouTube](#) [TikTok](#)
www.therceman.dev

GitHub Dorks for Finding Files

filename:manifest.xml	filename:config.php	filename:ovpn
filename:travis.yml	filename:config.inc.php	filename:cscfg
filename:vim_settings.xml	filename:prod.secret.exs	filename:rdp
filename:database	filename:configuration.php	filename:mdf
filename:prod.exs	filename:sh_history	filename:sdf
filename:prod.secret.exs	filename:shadow	filename:sqlite
filename:npmrc_auth	filename:proftpdpasswd	filename:psafe3
filename:dockercfg	filename:pgpass	filename:secret_token.rb
filename:WebServers.xml	filename:idea14.key	filename:carrierwave.rb
filename:bash_history	filename:hub	filename:database.yml
filename:sftp-config.json	filename:bash_profile	filename:keychain
filename:sftp.json	filename:env	filename:kwallet
filename:secrets.yml	filename:wp-config.php	filename:exports
filename:esmtprc	filename:credentials	filename:config.yaml
filename:passwd	filename:id_rsa	filename:settings.py
filename:LocalSettings.php	filename:id_dsa	filename:credentials.xml

GitHub Dorks for Finding API Keys, Tokens and Passwords

api_key	OTP	password
authorization_bearer:	HOME BREW_GITHUB_API_TOKEN	user_password
oauth	SF_USERNAME	user_pass
auth	HEROKU_API_KEY	passcode
authentication	JEKYLL_GITHUB_TOKEN	client_secret
client_secret	shodan_api_key	secret
api_token:	api.forecast.io	password hash
client_id		user auth

GitHub Dorks Automation Tools

TruggleHog	- https://github.com/dxa4481/truffleHog
Github-Dorks	- https://github.com/techgaun/github-dorks
GitGot	- https://github.com/BishopFox/GitGot
GitMonitor	- https://github.com/Talkaboutcybersecurity/GitMonitor
GitRob	- https://github.com/michenriksen/gitrob
GitHound	- https://github.com/tillson/git-hound
GittyLeaks	- https://github.com/kootenpv/gittyleaks
GitSecrets	- https://github.com/aws-labs/git-secrets
Watchtower	- https://radar.nightfall.ai

CURSO Y RECOMENDACIONES FINALES

Hack Underway: Empresa de ciberseguridad.

<https://hackunderway.com/>

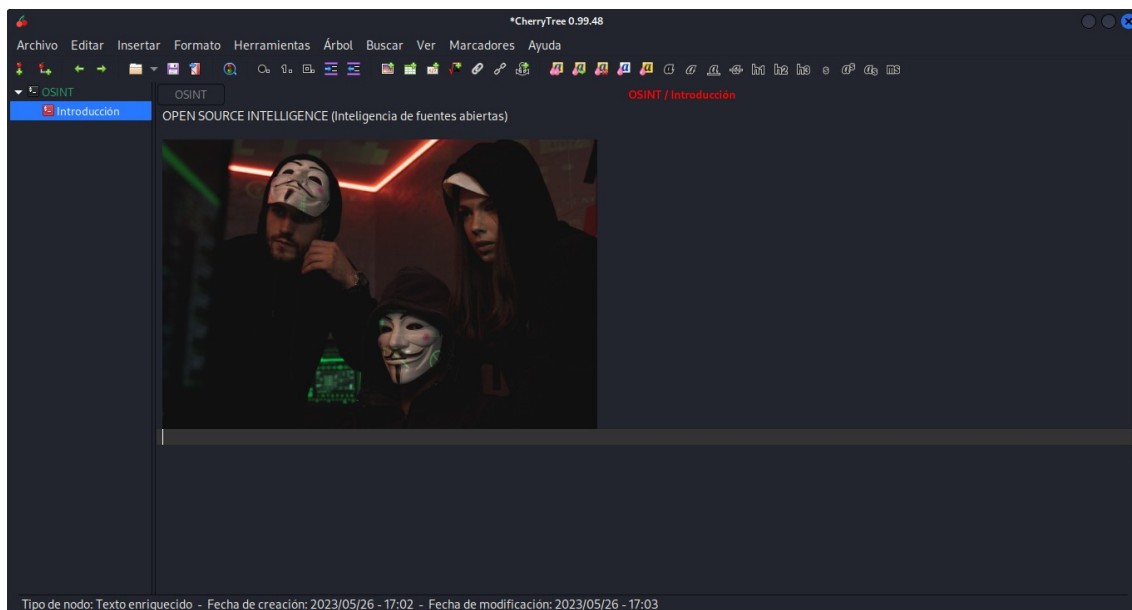
Próximamente estaré realizando cursos y libros en mi pagina y demás plataformas.

Recomendaciones finales:

Espero puedan haber aprendido mucho al terminar de leer este libro de OSINT y que lo practiquen en sus trabajos de investigación de la mejor manera, no me responsabilizo si usan la información transmitida de manera ilegal, por favor hagan cosas buenas con el conocimiento que puedan adquirir, siempre usen sus conocimientos para ayudar a los demás, para resolver un caso necesario para el beneficio de las personas y de ustedes.

Para tomar sus notas:

CherryTree: (<https://github.com/giuspen/cherrytree>)



CherryTree es una aplicación jerárquica para tomar notas, con texto enriquecido, resaltado de sintaxis, manejo de imágenes, hipervínculos, importación/exportación con soporte para múltiples formatos, soporte para múltiples idiomas y es multiplataforma.

Por defecto, ya viene instalado en Kali Linux, pero también lo pueden instalar manualmente.

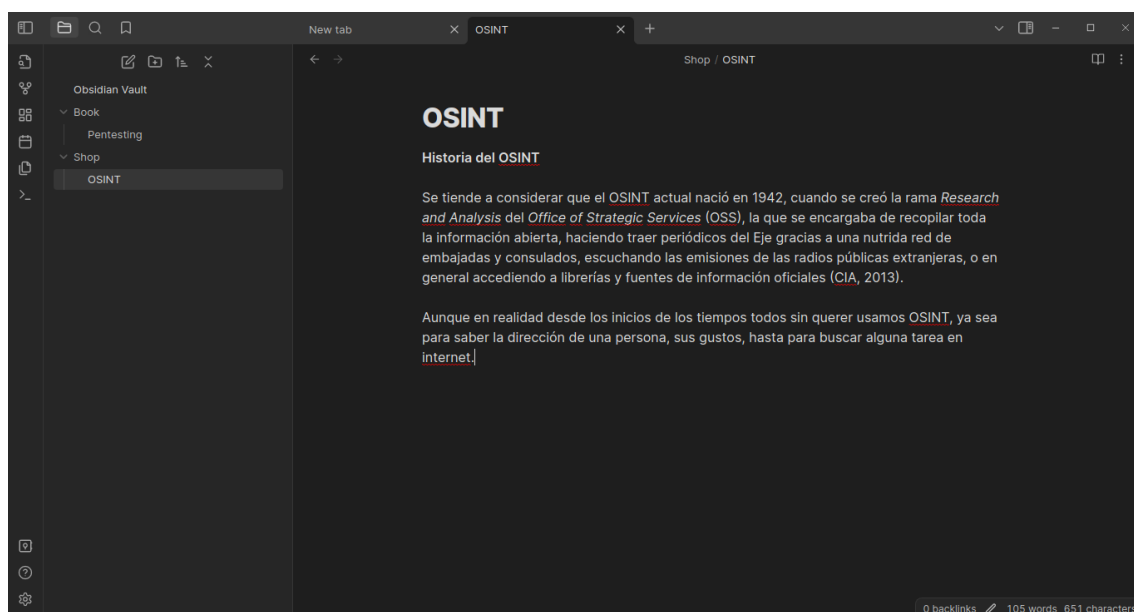
<https://www.kali.org/tools/cherrytree/>

Les dejo un video del uso de CherryTree.

https://www.youtube.com/watch?v=sjghV5_Z1z0

Obsidian: (<https://obsidian.md/download>)

Obsidian es una base de conocimiento personal y una aplicación de software para tomar notas que funciona con archivos Markdown. Permite a los usuarios hacer enlaces internos para notas y luego visualizar las conexiones como un gráfico.



Para instalar el programa, si están en Kali Linux, descargan el archivo .deb y ejecutan el siguiente comando. Dentro de la carpeta donde lo descargaron.

sudo dpkg -i obsidian_1.3.4_amd64.deb

Les pedirá su clave de super usuario (root) le dan “Enter”, y automáticamente se les instalará.

Les dejo un video del su uso de Obsidian.

https://www.youtube.com/watch?v=64pl_dKYZOg

The end:

Si tienen la oportunidad de trabajar para el gobierno o empresas o incluso emprender por su cuenta, siempre hagan las cosas bien y respetando a los demás.

Por más duro que te aya golpeado la vida, intenta una y otra vez hasta que lo logres, no te pongas límites y sobretodo confía en tí mismo.

Abrazo para todos mis seguidores de latinoamérica, europa y todos los países donde me siguen!...

Este debe ser tu lema, todos los días... (“**Me gusta lo difícil**”)

#HappyOSINT

Atte: **Jey Zeta**

