



Los Lunes del Instituto de Auditores Internos

www.auditoresinternos.tv

#LosLunesIAI - @Auditorinterno

Índice

Quien soy yo

Qué es OSINT

Técnicas de búsqueda

Ejemplos de uso

Quien soy yo

Javier Rodríguez

BIO

- Experto en Ciberinteligencia, proveniente de la Guardia Civil, actualmente sector privado.
- Destinos
 - PJ
 - SIGC

Certificaciones

- Analista Programador – (Universidad Cantabria)
- OSCP – (Israel – 2015)
- Windows Exploiting (Corelan – 2015)
- Undercover Online Operations (FBI – 2016)
- WEBINT (Israel- 2016)
- Técnicas Estructuradas de Análisis (España - 2019)

• Formaciones impartidas

- INCIBE SummerCamp (2017 a 2019)
- Servicios y FCS
- Unidades de análisis e inteligencia
- Formaciones ad hoc en masters y trainings.

Y cuanto más leo, cuanto más profundizo, más sé que no sé nada

Que es OSINT

Primera aproximación

- Se entiende por **OSINT** como la obtención de información y posterior transformación en inteligencia a través de fuentes abiertas.
 - A veces se denomina WEBINT – *Web Intelligence*, o inteligencia proveniente del ámbito Web.
 - Se entiende por **ciber inteligencia** como la adquisición y el análisis de información para identificar, rastrear y predecir las capacidades, intenciones y actividades cibernéticas que apoye en la toma de decisiones.
 - A veces se la denomina CYBINT.
 - Hay que significar que no hay un acuerdo sobre la definición de ciber inteligencia, existiendo por tanto lo que se denomina focos o ámbitos de aplicación de CYBINT.
- Desde hace unos años existe lo que se denomina el “operador OSINT” u “analista OSINT”, que es una persona formada en las labores de obtención y, a veces, análisis de la información obtenida.
 - La ciber inteligencia tiene su ciclo y/o fases propias.
 - Sin herramientas especializadas no es posible ni realizar una buena labor de obtención.
 - Sin formación en análisis es imposible realizar una buena labor de interpretación, integración y valoración de la información (en el ámbito de la inteligencia).
 - La tendencia actual es formar unidades únicas (servicios gestionados) especializadas en el ámbito OSINT que sean transversales.

Peculiaridades

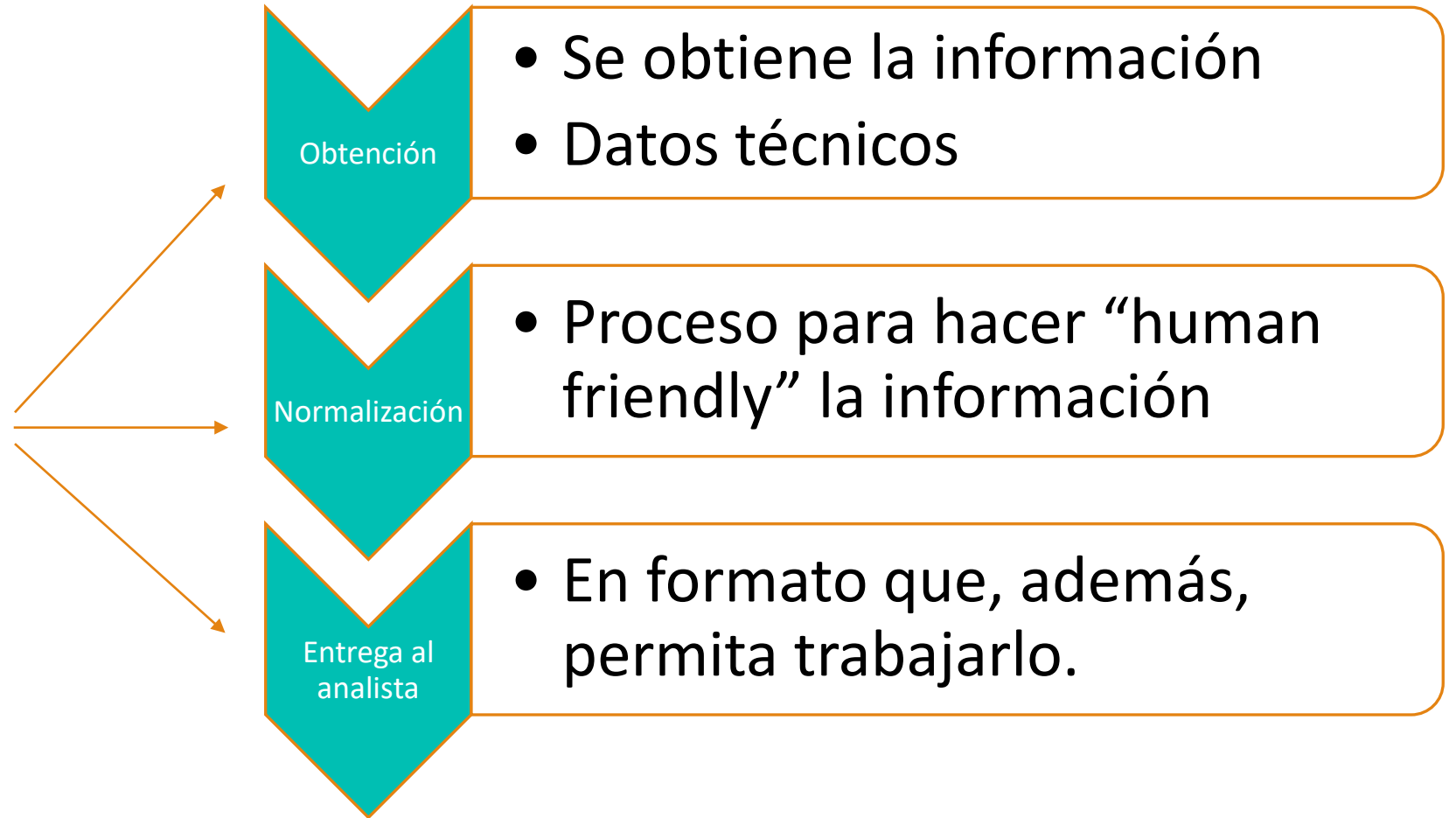
- Es recurrente observar como se lanza la gente a buscar sin ningún tipo de plan inicial, sin saber qué buscar.
 - Por parte del jefe de equipo o responsable de la investigación, no dar instrucciones precisas sobre lo que se necesita.
 - Por parte del operador OSINT, no contar con los conocimientos suficientes, no estar familiarizado con conceptos modernos de búsquedas en fuentes abiertas.
 - No contar con una metodología de análisis, más allá de la experiencia propia y el sesgo que cada uno tenga.
 - El problema de la infoxicación, demasiada información repetida que carece de valor.
- Desde el año 2018 en adelante las medidas de privacidad y seguridad están impidiendo el acceso a información de calidad de forma directa.
 - El teléfono móvil y tarjeta SIM/Wifi es imprescindible para realizar labores de obtención.
 - Se observa que muchos productos denominados de ciber inteligencia/OSINT son fundamentalmente descriptivos, pero no aportan datos para las investigaciones.
 - Sigue existiendo la creencia de que es gratis, hace tiempo que dejó de serlo.
 - Ausencia de personal técnico

Problemas asociados a la información

- En la fase de recolección de información, ésta se obtiene en una variedad de formatos
 - JSON
 - XML
 - Binario
 - Strings de datos
 - *.sql
 - URLs
 - Imágenes
 - Texto
 - Voz
 - Multimedia
 - Coordenadas GPS
 - Timelines
 - Etc
- Si no sabemos transformar esa información en algo legible y entendible, no se podrá trabajar.
- Por ello es necesario contar con personal que tenga ciertas **habilidades técnicas**.
- En redes sociales esto es más que obvio.
- Además, muchas veces se necesita crear programas ad hoc que resuelvan una incidencia.
- **Ejemplo:**
 - Lista de amigos de una persona
 - Lista de miembros de un grupo

Ejemplo obtención información sustraída

Bases de datos que un actor del ámbito cibercrimen ha sustraído de una compañía.



La ciber inteligencia en tiempos modernos

- **Las unidades se articulan de la siguiente manera**
 - Analistas
 - Operadores OSINT
 - Operadores Obtención Técnica
- **Se cree en el ciclo de inteligencia**
 - Existe una modificación del ciclo clásico, donde se introducen las peculiaridades propias del ámbito ciber.
- **Respecto a las fuentes**
 - Se discrimina el tipo de fuente según el foco del trabajo.
 - Previamente se clasifican.

- **Respecto al análisis**
 - Se trabaja en base a la creación de escenarios.
 - Se identifican las relaciones entre actores
 - Se crean los indicadores
- **El plan de obtención**
 - Se crea un plan de obtención en base a lo que esos indicadores.
 - ¿Con qué fuente es observable ese fenómeno?
 - Ese plan de obtención es la base y sobre lo que se configura el know how de la unidad.
- **La obtención**
 - La ingesta de grandes cantidades de datos
 - Uso de herramientas

Los enfoques

Enfoque	Descripción	Ejemplos
• Ciber inteligencia en apoyo a la ciberseguridad	• Se trata de las actividades realizadas para apoyar la ciberseguridad de los sistemas informáticos • Comúnmente se denomina “Threat Intelligence”	• Indicadores de Compromiso con los que se alimenta un sistema de seguridad. • Firmas de antivirus • Foros de actores/malware
• Ciber inteligencia en apoyo investigación	• Se trata de las actividades realizadas en apoyo a la investigación clásica	• Investigaciones de cualquier tipo, desde el ámbito policial a las internas en una compañía (insider threats)
• Ciber inteligencia en apoyo a la inteligencia	• Se trata de todas las actividades que se van a realizar en apoyo de una operación de ciber inteligencia	• Inteligencia económica o competitiva.

- Por tanto las actividades que se realicen en el marco de la ciber inteligencia, y su definición, van a depender del ámbito o foco de actuación.
- La planificación, medios, preparación del personal y duración de las actividades dependerá de las capacidades de obtención y análisis que tengamos según el foco requerido.

Recordando ...



Apoyo a la investigación



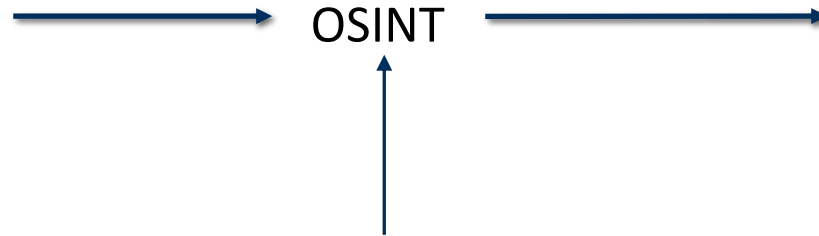
- El objetivo suele ser la detección e identificación de personas vinculadas con hechos de interés.
- En general el foco está en información relativa a fuentes como:
 - Buscadores genéricos.
 - Buscadores temáticos y/o especializados
 - Redes Sociales
 - GEOINT
 - Todo tipo de documentación de interés clásica
 - **IoT**
 - **Wearables**
 - **Aplicaciones de Mensajería**
 - **Apps móviles**

¿Qué se viene observando?

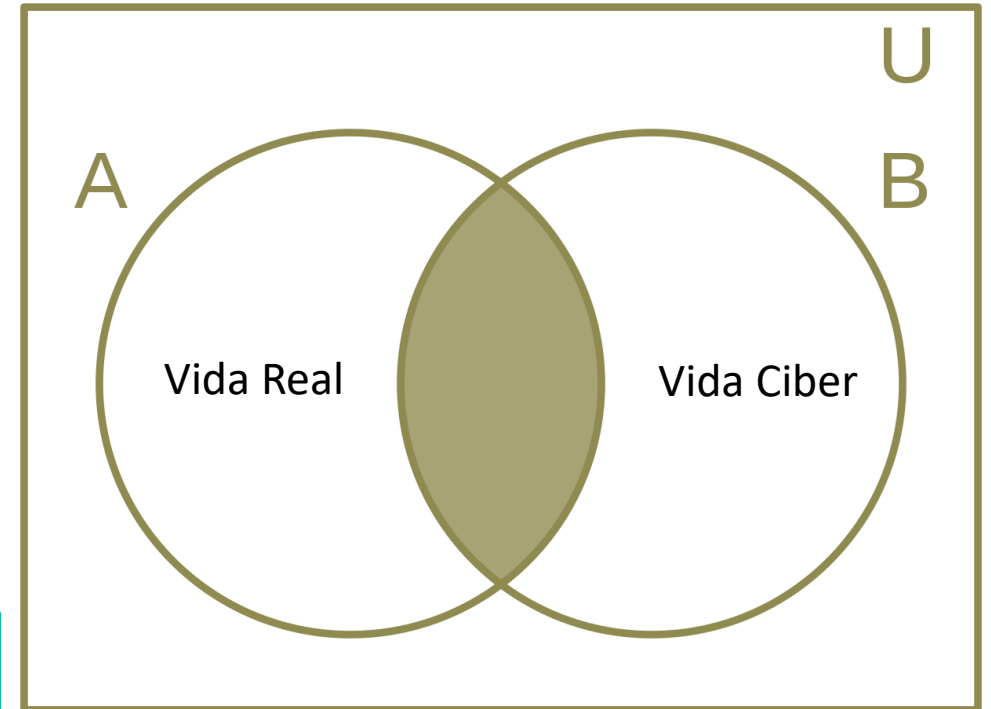
Quien

Investigador

Se necesita una mínima formación y experiencia



Hay una excesiva dependencia de esta fuente de obtención clásica.



Problemática

- En general, se enfoca la búsqueda de información a través de las fuentes clásicas, una aproximación puede ser la siguiente.

Búsqueda

- Nos lanzamos a buscar el nombre
- Averiguamos datos de su entorno

Logística

- Se carece muchas veces del material necesario.
- Se carece del conocimiento necesario.

Problemas

- No se explota ni comprende la experiencia de usuario
- Siempre de manera REACTIVA

- Nos olvidamos de cuatro fuentes**
 - IoT
 - Wearables
 - Aplicaciones de Mensajería
 - Apps móviles
- Y de la experiencia de USUARIO**

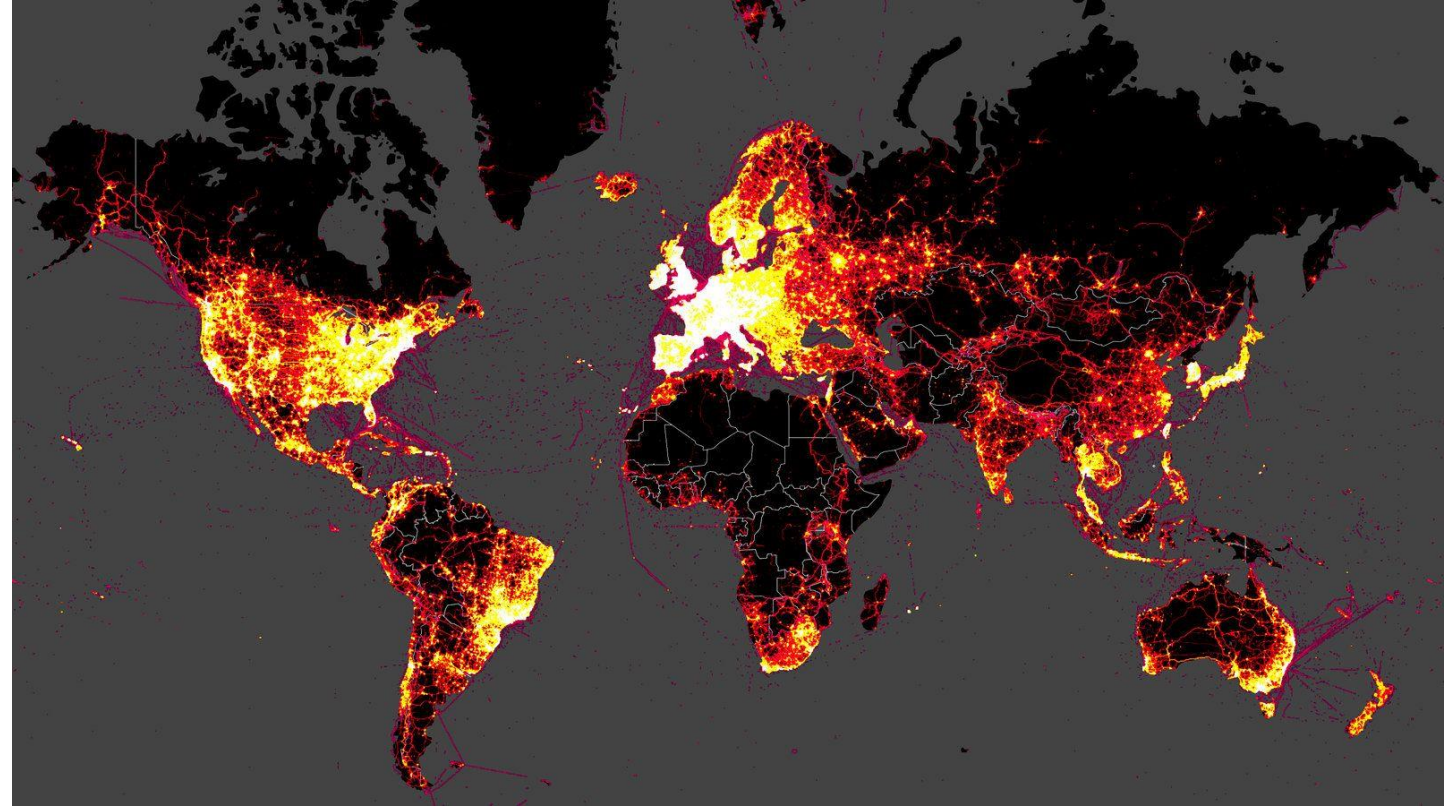


El caso Strava



<https://www.bbc.com/mundo/noticias-42859883>

Strava: cómo una aplicación de deportes dejó al descubierto secretos de bases militares de Estados Unidos

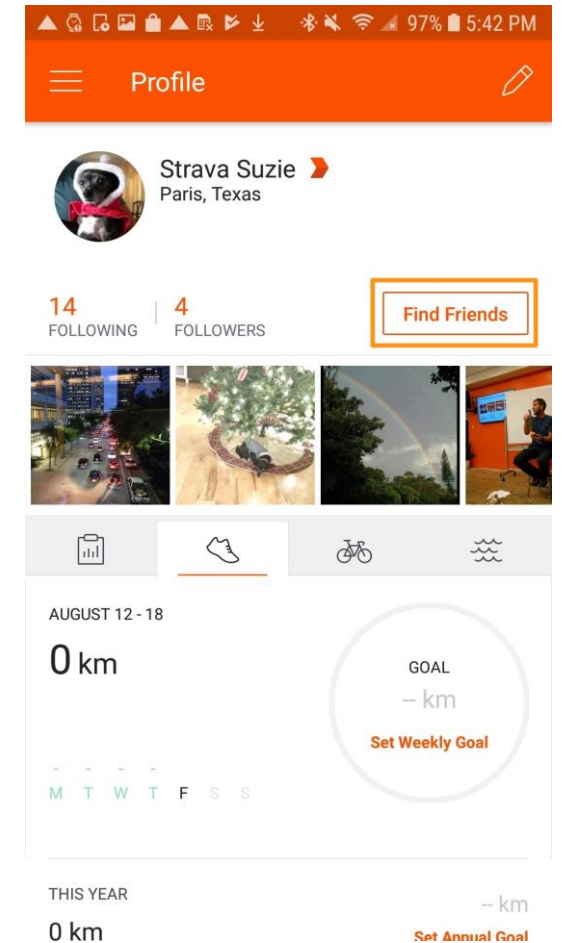
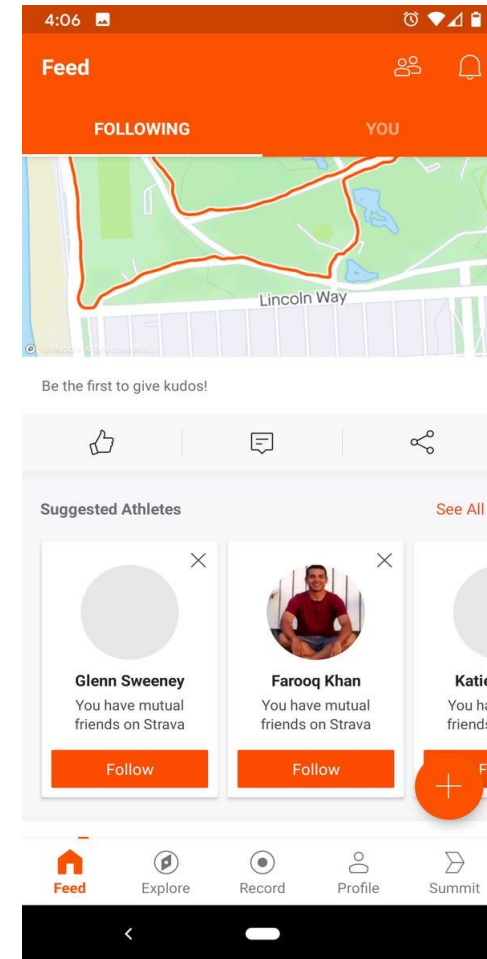


El caso Strava: Experiencia de Usuario



<https://support.strava.com/hc/en-us/articles/360049642391>

Esta es la "ventaja"



¿Qué podemos hacer con esto?

- Se entiende por inteligencia como la disciplina que proporciona información útil al objeto de ayudar a tomar decisiones o modificar una tomada con anterioridad.
- La ciber inteligencia en este caso es usada para
 - Informes de riesgo país.
 - Informes de actores hostiles.
 - Competidores
 - Mercados / Desarrollo de negocio
 - Due Diligence
 - KYC/KYE
 - Monitorización



- En este caso tiene una fuerte carga de trabajo por parte del analista, sobre quien recae la responsabilidad de crear y defender el producto.
- Las fuentes de obtención prácticamente son las mismas.

Técnicas de Búsqueda

Las herramientas

Tipología	Descripción
Navegadores y complementos	Consiste en el software usado para “navegar” por internet de manera directa, así como los complementos y ampliaciones de los mismos.
Herramientas “online”	Consiste en aplicaciones y herramientas de obtención de información, que se accede a las mismas vía “online”
Herramientas instalación local	Consiste en aplicaciones y herramientas que deben ser instaladas directamente en el equipo informático.
Sistemas Operativos específicos*	Consiste en software, en modo sistema operativo, especializado en actividades OSINT y que contiene herramientas pre-instaladas.

Se pueden agrupar de diversos modos, pero en síntesis siguen la tabla mostrada.

WHOIS



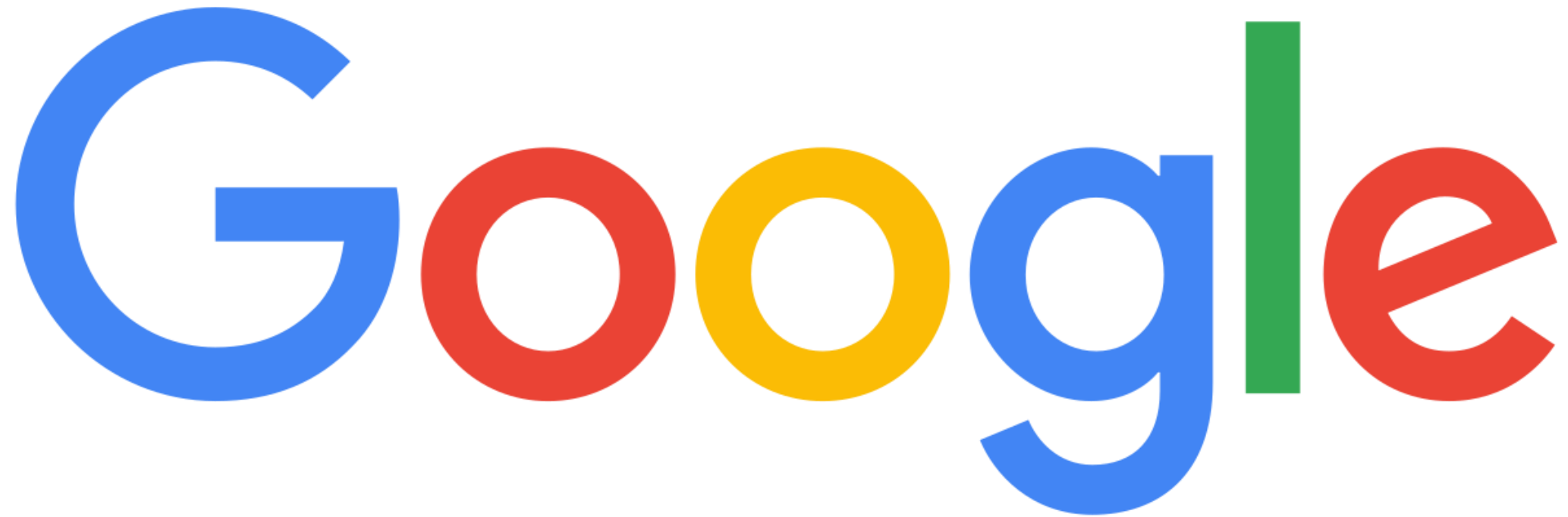
- Base de datos que contiene los titulares de los dominios que han sido adquiridos.

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

<https://domainbigdata.com/>

<http://nic.es>

Google



Logical Operators

OPERATOR	EXAMPLE	WHAT IT DOES
OR	Ball OR stick OR step	Shows you results that contain any of the words you entered.
AND	Xataka and Basics	Search for pages that include both of the specified terms.
" "	"Xataka Basics" or "Women's Football League".	It shows you results where the exact term or terms you have added between the " .
-	Xataka -Basics	Shows you results where the word you put after the - is excluded.
*	"Women's * League"	A wildcard that can match any word in the search.
#..#	Mobile 200..500 euros	It shows you results where you add a range of numbers that you specify.
()	("social networks" OR "social platforms") -Twitter	It allows you to combine operators. In the example you will search for social networks or social platforms, but excluding Twitter from the results.

Logical Operators

OPERATOR	EXAMPLE	WHAT IT DOES
AROUND	Tricks around(3) Instagram	Results where the two specified words appear, but with the determined number of terms between them.
EN	300 dollars in euros	Used to convert units of the same type of measurement.
MAP	map:Castellon	The search returns results with maps of the place where you tell it to.
DEFINE	define:cheat	Look up the definition of a word you don't know
SITE	Smartphone site:www.xataka.com	It searches for results within a website that you have specified.
INFO	info:www.xataka.com	Shows you results where information about a web page is offered.
RELATED	related:www.xataka.com	It shows you in the results other pages similar to the one you have written.
LINK	Phones link:www.xataka.com	It shows you in the results pages that have links to the website you have specified.

Logical Operators

OPERATOR	EXAMPLE	WHAT IT DOES
CACHÉ	cache:www.xataka.com	It shows you the copy of the page that is in Google's cache.
FILETYPE	filetype:pdf budgets 2019	Searches for results that contain files in the format you specified
ALLINTEXT OR INTEXT	allintext: "cheap mobiles".	Find pages that include in their text some or all of the terms you have included in the command.
ALLINTITLE OR INTITLE	allintitle:price and availability	Displays pages that have some or all of the terms you have included in the command in their title
INURL OR ALLINURL	inurl: "apple iphone" allinurl: "apple sfera" allinurl: "apple sphere"	Shows you pages with some or all of the terms you have included in the command
ALLINANCHOR OR INANCHOR	allinanchor: "cheap mobiles".	Results with pages that include a link to anchored text that includes one or more of the specified terms.
STOCKS	stocks:Facebook	Search for the current status of the company you are looking for on the stock exchange.

Texto Predictivo

❖ Autocompletar.

- ❖ ~~La función autocompletar muestra las búsquedas más repetidas por la gente~~
- ❖ La función autocompletar/texto predictivo nos dice las búsquedas más probables en base a *nuestra experiencia de usuario*
 - ❖ <https://www.google.com/dashboard/>
 - ❖ <https://adssettings.google.com/authenticated?hl=es>

❖ Ejemplo

- ❖ La “curva” de la vida.
 - ❖ Tengo 12 años y ..

Texto Predictivo(2)

- ❖ ¿Cómo obtener todas las búsquedas predictivas?
- ❖ Herramienta Keyword Tool. (keywordtool.io)
- ❖ Es una buena técnica investigativa para conocer las posibles búsquedas de interés de nuestros objetivos.

Keyword Suggestions

Search for "comprar armas" found **383** unique keywords [Copy all](#)

Want to get up to 2x more keywords instead? [Subscribe to Keyword Tool Pro now!](#)

☐ Keywords ?	Search Volume ?	CPC ?	AdWords Competition ?
☐ comprar armas airsoft	10,000	0.50	0.50
☐ comprar armas de fuego	10,000	0.50	0.50
☐ comprar armas cs go	10,000	0.50	0.50
☐ comprar armas sin licencia	10,000	0.50	0.50
☐ comprar armas de foguero	10,000	0.50	0.50
☐ comprar armas ilegales	10,000	0.50	0.50
☐ comprar armas online	10,000	0.50	0.50
☐ comprar armas paintball	10,000	0.50	0.50
☐ comprar armas antiguas	10,000	0.50	0.50
☐ comprar armas de fuego sin papeles	10,000	0.50	0.50

Do You Need This Information?
Keyword Tool Pro Provides Search Volume Data For Spanish Keywords.
Try It Now!

Emails



<https://hunter.io/>

<https://haveibeenpwned.com/>

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

Bonus Track ;-)

-> ¿Y qué hago para saber su titular?

- Opciones de recuperar la contraseña
- Redes Sociales.
- Medios de pago.

Teléfonos

- Portabilidad
 - <https://numeracionyoperadores.cnmc.es/portabilidad/movil>
- Buscadores específicos
 - <http://blancas.paginasamarillas.es/jsp/home.jsp>
 - <http://world.192.com>
 - <http://infobel.com/world/default.aspx>
 - <https://www.truecaller.com/>
 - <https://sync.me/>
 - <http://www.abctelefonos.com/>

Personas

- Buscadores especializados
 - www.pipl.com
 - Webmii.com
 - www.zoominfo.com
 - <http://itools.com/tool/wink-people-search>
 - www.spokeo.com
 - <https://thatsthem.com/>
- Búsqueda de perfiles profesionales.
 - <http://www.yasni.com>
 - LinkedIn / Xing
- Base de datos de “VIPs”
 - <https://littlesis.org/>

Empresas

- Empresas y empleados
 - <http://www.marketvisual.com/>
- Empresas en España
 - Empresa.es
 - Axesor
 - libreborme
- Empresas internacionales
 - <https://www.glassdoor.com/Reviews/index.htm>

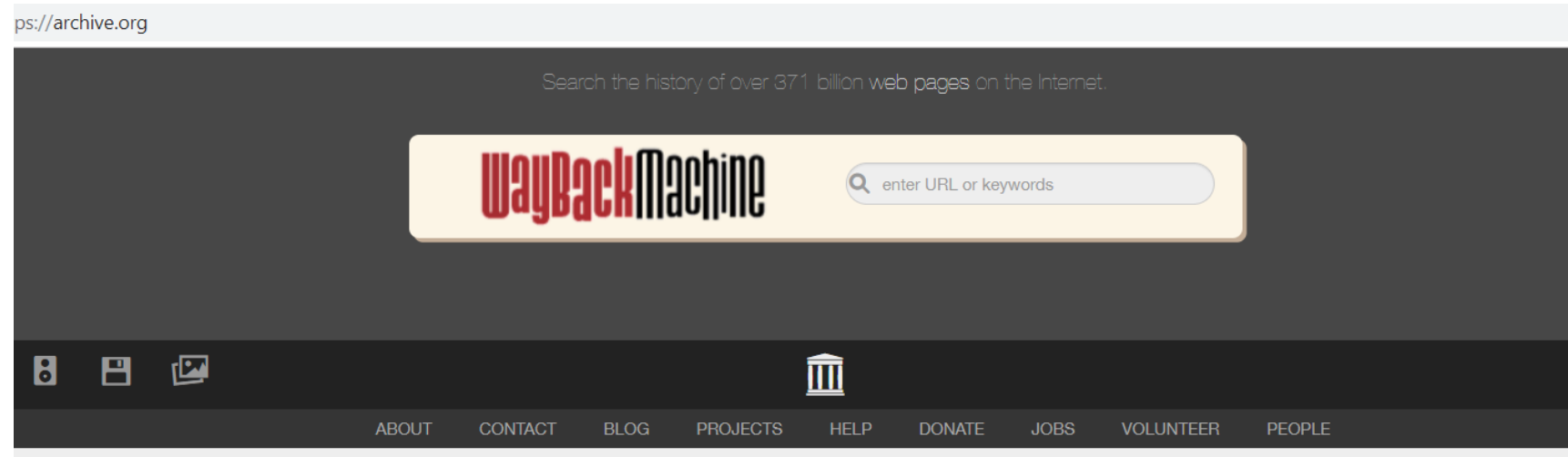
Transportes

- Ofrecen información, en general en tiempo real, sobre medios de transporte.
- Muy útiles para seguimientos.
- Tráfico aéreo.
 - <http://www.flightradar24.com>.
- Transporte marítimo
 - <http://www.marinetraffic.com/ais/es>

Archive.org

- Web que realiza “snapshots” de páginas web
 - Sites Web
 - Perfiles Redes Sociales
 - Blogs
 - Material Multimedia
- Permite acceder a los snapshots realizados mediante
 - Búsqueda de texto (indexa el Tittle de la Web)
 - Introducción de la URL
 - Posibilidad de filtrado por fecha
- Uso investigación
 - Recuperar evidencias que han sido borradas

Archive.org



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



Announcements

Lessons Learned: The DWeb Summit
UX/UI Workshop

Getting Ready for DWeb Camp: A
Conversation with Kelsey Breseman

Most 20th Century Books Unavailable
to Internet Users – We Can Fix That

[SEE MORE](#)



X.-PREGUNTAS

¡¡Gracias!!

Síguenos en
www.auditoresinternos.es



@Auditorinterno

Instituto de Auditores Internos de España