periodistas ambientales

Herramientas para el Periodismo Open Source

Aprende a armar y gestionar tu propio tool kit para la investigación ambiental

Por Diego Bruno y Miguel Sumer Elías*

En esta guía encontrarás:

1- Crear un entorno de trabajo adecuado.
2- Herramientas y recursos.
3- Privacidad y anonimato.
4- Cómo trabajar con fuentes a través del cifrado y anonimato.
5- Google hacking y otros buscadores especializados.
6- Utilización de palabras clave para la investigación ambiental.

1. CREAR UN ENTORNO DE TRABAJO ADECUADO

Si bien para aplicar técnicas de OSINT se supone que sólo necesitamos una PC o notebook conectada a Internet, en realidad, una persona que se dedica a la investigación utiliza bastante más que eso ya que, para ser eficientes, se debe contar con el entorno y con las herramientas adecuadas para los diferentes escenarios y contextos.
En este contexto, investigar en un entorno de seguridad, privacidad y anonimato es fundamental ya que un investigador de OSINT debe pasar lo más desapercibido posible.

Para plantear un entorno de trabajo óptimo deberíamos tomar en cuenta lo siguiente:

a. El equipo PC o notebook. Lo primero que necesitamos es una PC o notebook moderna que cumpla con estándares de tecnología actuales, cómo, por ejemplo:

- Que tenga bastante memoria RAM (mínimo 8 GB a 16 GB de RAM) ya que, en muchos casos, se necesitará emular una máquina virtual o usar diferentes aplicaciones, las cuales en muchos casos consumen mucha memoria.

- Que el procesador tenga varios núcleos de procesamiento ya que esto otorga más poder de cómputo al equipo para poder correr varias tareas en paralelo.
- Que el equipo tenga al menos un disco SSD o unidad de disco de estado sólido ya que brinda una mayor velocidad para acceder a las aplicaciones y programas y un mejor comportamiento cuando varios de ellos están trabajando al mismo tiempo.
- Que el sistema operativo que se utilice (MacOS, Windows o Linux) no esté obsoleto, es decir, que se encuentre instalada la última versión actualizada del software para tener 100% de compatibilidad con las herramientas que luego utilizaremos sobre él.

b. Navegador web. Los periodistas de investigación que trabajen con la metodología de OSINT, muchas veces deberán utilizar más de un navegador web, ya que, si bien todos cumplen una misma función, algunos de ellos tienen fortalezas y debilidades que, de acuerdo con cada escenario, serán útiles de usar.

Google Chrome. Google Chrome es uno de los buscadores más aceptados y usados pues cuenta con una enorme cantidad de extensiones muy útiles para nuestro trabajo.

Sitio Web: www.google.com/chrome

TOR Browser. El navegador de TOR ayuda no sólo a navegar por la red en forma anónima (pues oculta la dirección IP real) sino que también es útil para navegar lo que se conoce como la Deep Web o Internet Profunda.

Sitio Web: https://www.torproject.org/download/

Firefox. Similar a Chrome funcionalmente hablando, pero con un nivel de configuración de la privacidad mayor, lo cual lo convierte en un excelente navegador para la web superficial (es decir la web que conocemos y que no es Deep Web).
Sitio Web: https://www.mozilla.org/en-US/firefox/new/

Brave. Está basado en el motor de Chrome, pero con muchas mejoras relacionadas a la seguridad y a la privacidad ya que fue concebido para eso. Algo súper útil de Brave es que ya trae el cliente de TOR Browser embebido, con lo cual en caso de querer navegar por la Deep Web o navegar en forma anónima sólo debemos ir al extremo derecho del navegador y del menú seleccionar “New private Windows with TOR” y ya automáticamente nos abre una nueva ventana con el servicio de TOR activado.
Sitio Web: https://brave.com/

Recursos Relacionados:

- https://support.mozilla.org/en-US/products/firefox/privacy-and-security
- https://proprivacy.com/privacy-service/guides/firefox-privacy-security-guide
- https://support.google.com/chrome/answer/114836?co=GENIE.Platform%3DDesktop&hl=en
- https://www.theverge.com/2020/2/11/21126427/google-chrome-privacy-tools-private-network-browser-settings

- https://www.theverge.com/2020/2/21/21138403/tor-privacy-tools-private-network-browser-settings-security
- https://support.brave.com/hc/en-us/articles/360017989132-How-do-I-change-my-Privacy-Settings-

2. HERRAMIENTAS Y RECURSOS

Existen literalmente miles de herramientas en el universo de OSINT. A veces podemos encontrar decenas de herramientas que cumplen la misma función. Pero lo que es seguro es que no existe una que sirva para absolutamente todo, con lo cual hay que ir probando y armando nuestro propio *tool kit* personalizado de herramientas organizadas por funcionalidad con el que nos sintamos cómodos para trabajar.

Sin embargo, la cuestión más importante con el uso de las herramientas es entender el contexto y el escenario en el que nos estamos moviendo para no desperdiciar tiempo, energía y recursos utilizando herramientas que no tendrán demasiado sentido.

A continuación, brindamos un listado de sitios web con repositorios públicos de herramientas de OSINT:

- Ciberpatrulla.com
- Netbootcamp.org
- OSINTframework.com
- OSINTessentials.com
- I-intelligence.eu
- Rr-reuser.biz
- Researchclinic.net

Asimismo, existe otro recurso recomendado y valioso llamado OSINTframework ya que nos va a enseñar a comprender mejor la metodología de OSINT pues muestra a modo de mapa de mente los diferentes recursos con los que moverse de acuerdo a lo que se quiera realizar.
Sitio web: https://ciberpatrulla.com/osint-framework/

Sistemas Operativos para uso seguro de OSINT

A través de lo que se conoce como máquinas virtuales o en inglés “virtual machines” se puede emular la instalación y uso de un sistema operativo completo dentro de nuestro equipo a través de programas especiales que nos hacen de intermediario entre el hardware de nuestra máquina (memoria, RAM, disco, procesador, etc.) y el sistema operativo invitado (o guest, como se lo denomina comúnmente).

Esto es una gran ventaja ya que nos permite instalar como parte de nuestro *tool kit* un sistema operativo totalmente diferente al nuestro, lo cual tiene enormes beneficios porque podemos utilizar sistemas creados únicamente para el uso de investigaciones y otros para los cuales quizás una determinada herramienta funciona y que en el nuestro no.

Los dos sistemas operativos más utilizados para el mundo de OSINT y el anonimato en Internet son:

- TAILS – Sistema Operativo
- Whonix – Sistema Operativo

Los programas que nos permiten instalar estos sistemas operativos dentro de nuestros propios sistemas de PC o notebooks se denominan Hipervisores. Los más conocidos y utilizados son VirtualBox (de uso gratuito) y VMware Workstation (licencia comercial paga).

a. VirtualBox. Es de uso gratuito u open source y muy sencillo de utilizar. El mismo fue adquirido por Oracle. Les dejamos algunos links de soporte de referencia, uno oficial y los otros dos de YouTube:

- https://www.virtualbox.org/wiki/End-user_documentation
- https://www.youtube.com/watch?v=WD1vMhJGPn8
- https://www.youtube.com/watch?v=qFghwcKkM8Q
- VMWARE Workstation

Página web: VirtualBox

b. VMware Workstation. Es un pionero en el campo de la virtualización (es anterior a VirtualBox) y un producto extremadamente maduro. Tiene una versión reducida gratuita que se llama VMware Player. La versión paga tiene soporte para ser instalada en Windows y Linux, pero no en Mac. En caso de usar Mac OSX existe una versión específica llamada VMware Fusion. Les dejamos los links de soporte correspondientes:

- VMware workstation Pro User Guide
- https://www.youtube.com/watch?v=OMIpKxZbfws
- https://www.youtube.com/watch?v=-4c3MO3Hm_c

3. PRIVACIDAD Y ANONIMATO

Este punto es clave. En todo trabajo de OSINT e investigación vamos a tener que tomar medidas de seguridad elementales y básicas para evitar poner en riesgo la privacidad del investigador. Un periodista de investigación que utiliza OSINT debe saber cómo obtener información, pero también como proteger la suya.

Junto con la configuración de los navegadores web, en todo *tool kit* deben existir varias direcciones de correo y perfiles de redes sociales con identidades inventadas (se las llama avatares o cuentas muleto), e inclusive chips de números telefónicos diferentes al de nuestra línea celular personal.

Nunca deben usarse datos reales o direcciones de correo personales, números de celular, etc. Inclusive si estamos creando otra cuenta de correo, no se debe asociarla a un mismo mail o número de celular. De esta forma evitamos dejar una gran huella digital con nuestras actuaciones que, a través de estas, se ven expuestos nuestros datos personales.

A continuación, les dejamos una lista de los recursos indispensables para que sean parte del toolkit para una investigación bajo la metodología de OSINT:

a. TOR Browser. Cómo mencionamos, TOR Browser es el complemento por excelencia para navegar anónimamente. Puede ser también utilizado a través del navegador Brave

b. Sistemas de VPN (Virtual Private Connection). Los sistemas de VPN son muy útiles dentro del contexto de la seguridad ya que nos ayudan también a cifrar el tráfico de nuestras conexiones punta a punta, además de enmascarar nuestra dirección IP.
Les dejamos a continuación dos links relacionados a un producto que en lo personal nos gusta y otro que es un compilado de 10 servicios de VPN con muy buena puntuación actualizado al 2020:

- Tennelbear
- https://es.vpnmentor.com/best-vpn-for-argentina/?keyword=+servicio%20vpn&geo=9070458&device=&ad=282973876965&gclid=CjwKCAjwx9_4BRAHEiwApAt0zkxjiIO4vFDMiEFqNJ9Wj0Wm9ayf82M0YcFR6g4VhPQR_SF_3sNDCBoCszAQAvD_BwE
- https://www.youtube.com/watch?v=65GUMaNrsYY
- https://www.youtube.com/watch?v=Dze0iXruyPk

c. Generador de identidades. Cómo dijimos al principio, necesitamos crear avatares falsos y tenerlos a mano cómo parte de nuestro *tool kit* de herramientas.
Para esto deberemos tomarnos el tiempo de crear identidades falsas y de alguna manera darle vida. Parte de ese trabajo consistirá en crear un correo electrónico, luego asociar dicho correo a una determinada red social como ser Twitter, Facebook, LinkedIn, etc.
Existen algunas herramientas que nos facilitan la creación de dichas identidades haciendo el proceso más automático. Una de ellas es Fake Name Generator, la cual les dejamos el link para que la puedan investigar y usar. Es muy sencilla e intuitiva.

fakenamegenerator.com

d. Sistemas de correo temporales. En muchos casos un correo electrónico, por más que lo hayamos registrado con datos falsos, puede ser no suficiente, con lo cual, en estos casos, utilizar servicios en dónde podemos crear una casilla de correo totalmente temporal se convierte en algo extremadamente útil.

A continuación, les dejamos una lista curada de los que consideramos los mejores servicios online para la creación de casillas de correo electrónicos temporales:

- Emailtemporalgratis
- Mailinator – Emails temporales
- Guerrilla mail

4- CÓMO TRABAJAR CON FUENTES A TRAVÉS DEL CIFRADO Y ANONIMATO

A lo largo de la presente guía hemos ido brindando consejos y casos de uso. Éstos deben pensarse utilizando la analogía de la cebolla, en decir, que son conceptos que se suman unos a otros, cómo las capas de una cebolla.

En este contexto, debemos considerar tres servicios esenciales y excelentes para realizar nuestras comunicaciones con diferentes fuentes físicas en forma 100% segura: la primera se llama Protonmail, la segunda Wire y la tercera Signal.

a. Protonmail es un servicio de correo electrónico cifrado creado en 2013 por los científicos e ingenieros del CERN Jason Stockman, Andy Yen, y Wei Sun a raíz de las revelaciones del ex trabajador de la CIA, Edward Snowden, sobre las prácticas de vigilancia masiva de las agencias de seguridad estadounidenses. Además. ProtonMail está desarrollado en Suiza y todos sus servidores y sus datos almacenados se encuentran en ese país, lo que significa que toda la información está protegida por las estrictas leyes de privacidad suizas.

El proyecto es open source y la registración es gratuita. El uso es muy sencillo y se lo puede usar tanto por un web browser cómo también instalando la aplicación en el celular.

b. Wire, por su parte, es una aplicación de plataforma de colaboración pensada en la seguridad, la privacidad y el anonimato. Si bien la aplicación es paga, tiene una versión free limitada que se puede instalar si se la baja al celular desde la tienda en forma directa.

Wire es una de las plataformas más galardonadas del mundo en materia de cifrado junto a su anonimato. Nos permite por ejemplo generar videollamadas o chats 100% indescifrables con otras personas (que deben tener la aplicación instalada) de la misma manera que lo podemos hacer con WhatsApp o Telegram. Está muy bien desarrollada, con una interfaz muy bien pulida y se puede bajar a nuestro dispositivo móvil. Trabaja tanto en IOS (Apple) como en Android.

c. Signal es una aplicación de mensajería instantánea y llamadas, libre, gratuita y de código abierto, con énfasis en la privacidad y la seguridad. Puede ser utilizada para enviar y recibir mensajes 100% cifrados. Al igual que las dos soluciones anteriores mencionadas se puede bajar el cliente móvil ya que trabaja tanto para IOS cómo para Android.

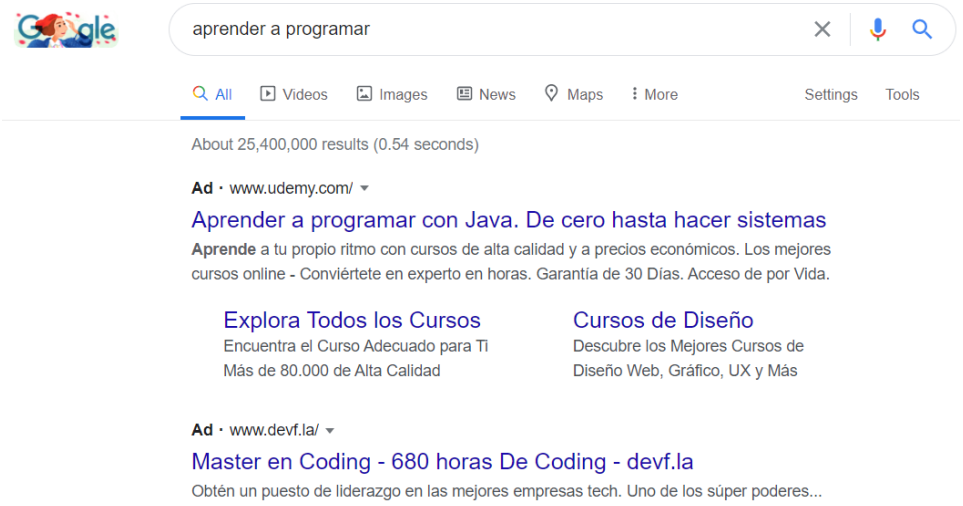
Les dejamos a continuación los links correspondientes a las tres soluciones:

- Protonmail
- Wire
- Signal

5- GOOGLE HACKING Y OTROS BUSCADORES ESPECIALIZADOS

Cuando la mayoría de las personas necesita encontrar o saber algo, normalmente se dirigen a un buscador y el más conocido y utilizado de todos es Google.

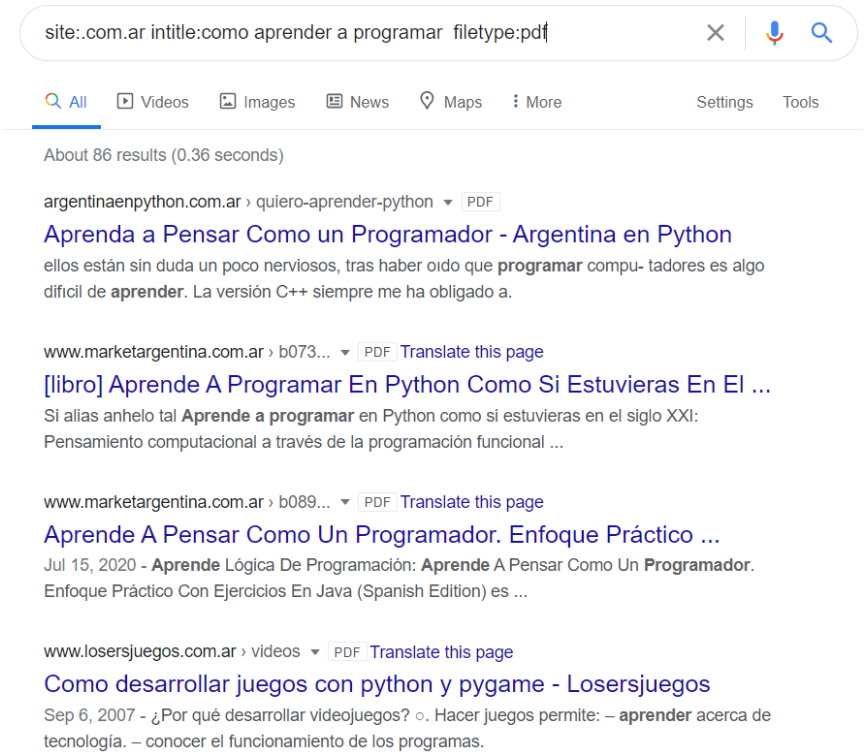
El problema es que la gran mayoría de las personas no sabe utilizar correctamente los buscadores y, en la mayoría de los casos, cuando se quiere buscar algo se realiza la búsqueda pura y exclusivamente a través de una frase o palabra en particular. Supongamos que una persona quiere buscar una determinada información como, por ejemplo, “aprender a programar”. Entonces normalmente lo que se suele hacer es ingresar en la barra del buscador la frase “aprender a programar” o “tutoriales para aprender a programar” lo cual está bien en una primera instancia, pero los resultados obtenidos serán cientos o miles y de una versatilidad tal que probablemente pasemos horas analizando cuáles son los verdaderamente útiles.



Google tiene, como todo motor de búsqueda, un algoritmo de trabajo y “operadores” que se pueden utilizar llamados “Google Dorks”. Estos operadores se pueden usar en conjunto o inclusive en la barra de búsqueda del motor. Entonces, podríamos reemplazar la forma de búsqueda original de “aprender a programar” por algo mucho más granular como por ejemplo “como aprender a programar en Python” y que además los resultados sean solo para sitios argentinos, es decir, .com.ar, y que, además, los resultados sean en formato PDF.

Para ello entonces tipearíamos algo como, por ejemplo:

site:.com.ar intitle:como aprender a programar filetype:pdf



Cómo podemos ver en la siguiente imagen, los resultados son mucho más precisos que en la primera búsqueda. Al poner site: y luego a continuación el .com.ar estamos limitando nuestra búsqueda a sitios argentinos específicamente. El operador "intittle:" es para especificar el título de lo que queremos buscar, y por último el operador "filetype:" es con el cual le especificamos el formato del archivo, en este caso fue el formato PDF, y por ende todos los resultados que trajo son "PDF".

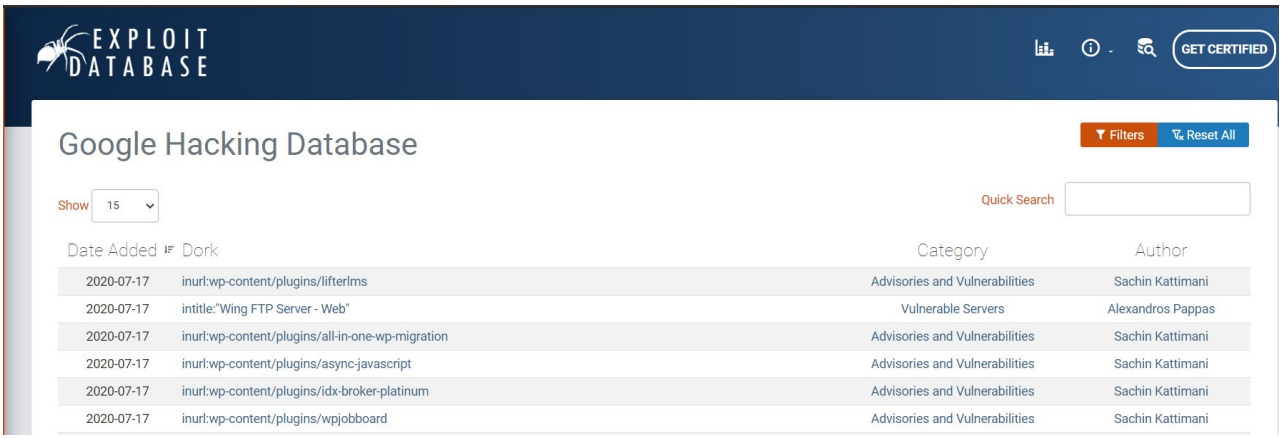
En el año 2004 un investigador de seguridad informática norteamericano llamado "Johnny Long" escribió un libro llamado "Google Hacking for penetration testers" a través de la editorial Syngress el cual tuvo 3 ediciones, la última a fines del 2018. En dicho material el autor enseña a los investigadores de seguridad informática a recopilar información de empresas o personas o, incluso, de documentos con información sensible públicamente expuesta a través del uso pura y exclusivamente de los operadores de Google.

El libro es una obra de referencia para todos los profesionales de seguridad de la información.

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

Otro Proyecto online open source super interesante en el que Johnny Long también participa es el de Google Hacking Database el cual se encuentra dentro del sitio de "Exploit Database" se accede al mismo a través del siguiente link: https://www.exploit-db.com/google-hacking-database

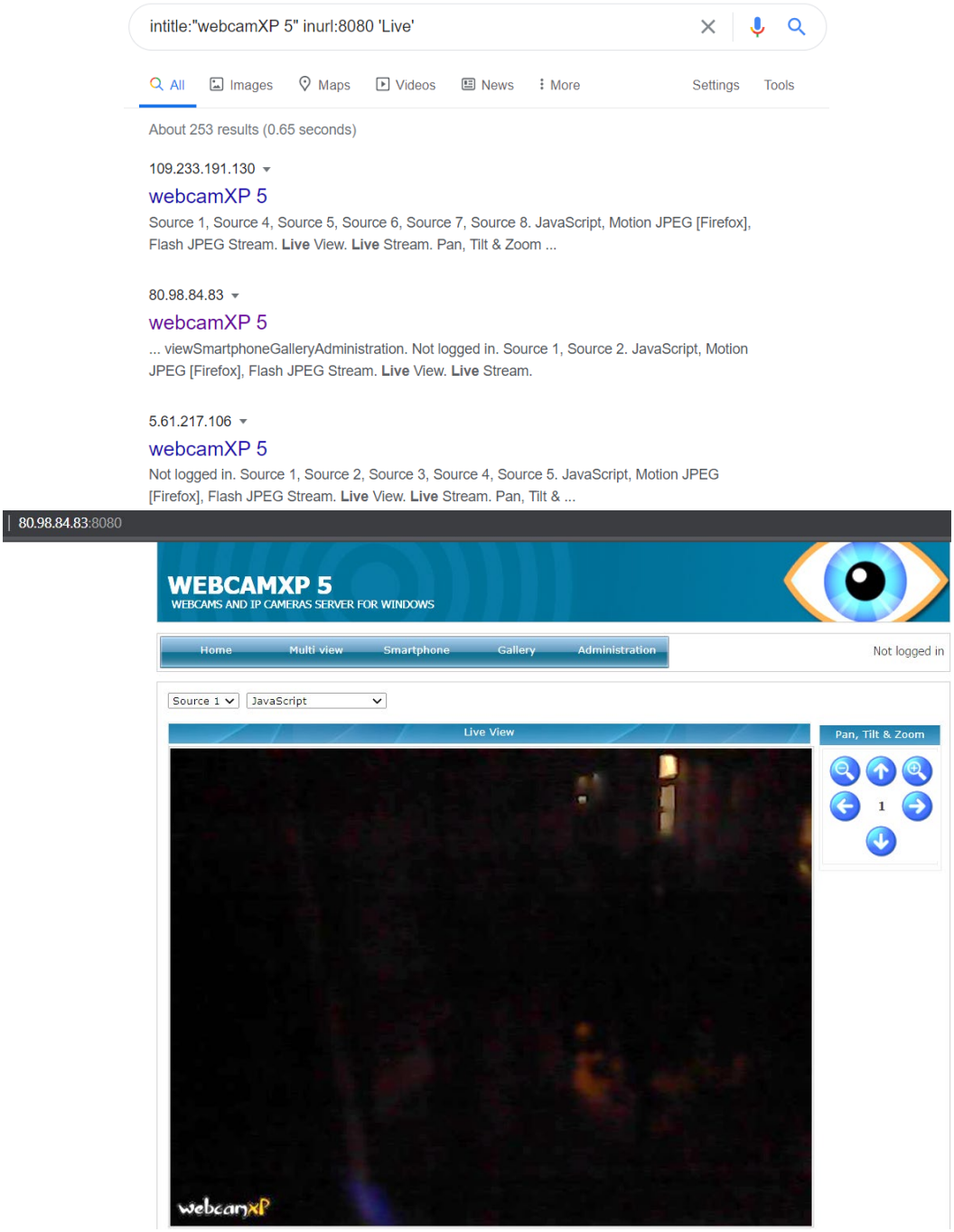
Al ingresar veremos la siguiente interfaz web:



Aquí veremos un montón de operadores ya que este proyecto se actualiza prácticamente a diario por toda una comunidad muy grande de seguridad informática en forma constante, en dónde veremos siempre al ingresar en la columna de la izquierda que están ordenados por fecha (año, mes y día).

Pero, por ejemplo, arriba a la derecha en la opción de "Quick Search" podemos poner un filtro como, por ejemplo, la palabra "webcam". Al hacerlo vemos que la vista cambia y nos muestra diferentes búsquedas que se pueden hacer para encontrar, por ejemplo, webcams conectadas a Internet que puedan estar expuestas de manera pública:

Por ejemplo, seleccionamos uno de estos resultados y lo ponemos en la barra de Google y le damos buscar y veremos que nos trae varios resultados relacionados a diferentes direcciones IP del mundo en dónde podríamos ingresar y ver lo que está enfocando la cámara, cómo se ve a continuación en las siguientes dos imágenes.



Entender cómo funciona el Google en profundidad es esencial para todo periodista de investigación. La realidad es que se podría escribir una verdadera enciclopedia con todo lo relacionado a Google Hacking y búsqueda avanzada pero lo ideal es familiarizarse con los operadores de Google, entender bien cómo y en qué contexto utilizarlos correctamente e ir dominándolos cada vez más.

A continuación, mostramos un par de últimos ejemplos que también van a ayudar a la comprensión. Supongamos que queremos encontrar listas públicas de correos electrónicos de los CEO de las compañías. Podríamos realizar la búsqueda en Google de la siguiente manera:
+CEO "email" filetype:csv | filetype:xls | filetype:xlsx

O si quisiéramos encontrar listas de contacto de marketing pondríamos:
filetype:csv OR filetype:xls OR filetype:xlsx "Marketing" "email" "contact" OR "lead" OR "prospect" -sample 2017 "website" –template

Estos mismos ejemplos si los quisiera acotar a un país en particular, debería entonces utilizar en la cadena de operadores el dork “site:” y a continuación la extensión del dominio país (por ejemplo .com.ar).

NOTA DE SEGURIDAD: Cuando busquemos información a través de Google u otro buscador, tenemos que hacerlo de un modo en el que no queden registros almacenados asociados a nuestra identidad, por lo tanto, se sugiere utilizar un navegador como Brave con el motor de TOR habilitado.

Otros Buscadores
Pero también existen otros buscadores además de Google:

a. Bing. Se puede encontrar muchísima información. Al igual que Google, también tiene sus operadores lógicos para poder dominar y refinar nuestras búsquedas.
- Bing
- Bing soporte

b. DuckDuckGo. Su gran punto fuerte es que **se centra en ofrecer la mayor privacidad posible a sus usuarios**. Esto quiere decir que no van recopilando información cuando se hacen búsquedas como lo hace Google o Bing.

Si bien tiene su propio motor de búsqueda, adicionalmente se integra con el resto de los navegadores como Google o Bing e incluso otros, lo que significa que, cuando buscamos algo a través de DuckDuckGo, los resultados que nos traiga habrán sido obtenidos de dos maneras: a través de su propio motor y de otras 400 fuentes diferentes cómo ser Google, Bing, Yahoo, Wikipedia, etc.

Sus principales diferencias con Google son:
- **No almacena la dirección IP de sus usuarios** ni guarda ninguna información relacionada con ellos.
- No comparte los datos sobre las búsquedas de los usuarios con las páginas web.
- No almacena el historial de búsquedas. Esto significa que no existe una línea temporal con todo lo que has buscado y ni pueden utilizarla para personalizar tus resultados ni pueden dársela a las fuerzas de la ley en el caso de que las requieran para alguna investigación. Además, también ayuda a que tus hábitos de búsqueda no puedan ser utilizados por terceros.

Un punto interesante de DuckDuckGo es que tiene una forma de buscar información en determinados sitios sin tener que visitarlos primero, lo cual se realiza con una serie de operadores llamados “Bangs” que siempre arrancan con un signo de exclamación seguida de

alguna palabra en particular (por ejemplo ¡x algo). Entonces si quiero buscar la palabra pizza en Wikipedia a través de DuckDuckGo tipearía en la barra de búsqueda: **¡w pizza**

O, por ejemplo, si quisiera ver la homepage de Facebook de la serie "The Bing Bang Theory" sólo debería tipear: **Bing Bang Theory ¡facebook**

Les dejamos un par de links de soporte del sitio oficial de DuckDuckGo:

- DuckDuckGo
- DuckDuckGo Bang 1
- Duckcuck Bang Reference

6- UTILIZACION DE PALABRAS CLAVE PARA LA INVESTIGACIÓN AMBIENTAL

En relación con la utilización de las herramientas mencionadas precedentemente, el periodismo de investigación ambiental deberá comenzar a implementarlas utilizando, a su vez, las palabras clave del área, como, por ejemplo: cambio climático, calentamiento global, efecto invernadero, adaptación y mitigación al cambio climático, antropogénico, dióxido de carbono, metano, combustibles fósiles, energías alternativas, eventos extremos, olas de calor, sequías, inundaciones, IPCC (Panel Intergubernamental de Cambio Climático), Protocolo de Kyoto, Acuerdo de París, etc.