CiberPatrulla

Técnicas OSINT para investigación en Internet

Manual para investigadores

Julián GL

Índice

Introducción

Qué es OSINT

En este libro te voy a hablar de las técnicas, pasos y herramientas que puedes usar para llevar a cabo una investigación en Internet. Todo ello desde una perspectiva policial, aunque intentaré abarcar otras áreas, ya que entiendo que no todos los profesionales tienen acceso a determinadas bases de datos, a las que sí tiene acceso un policía, por lo que te daré diversas alternativas.

Para ello vamos a utilizar como metodología las técnicas OSINT (Open Source Intelligence).

La inteligencia en fuentes abiertas u OSINT es parte del proceso de reconocimiento que consiste en utilizar cualquier fuente de información pública que pueda proporcionar información sobre una empresa, organización o individuo.

Como investigador puedes utilizar esta información para responder preguntas.

Utilizando técnicas OSINT se puede obtener información de personas y empresas.

Hoy en día, con la expansión de Internet y las redes sociales existe una gran cantidad de información pública, compartida por los propios usuarios.

A través de la obtención de esta información, y realizando inteligencia con la misma, podemos identificar personas y organizaciones, así como anticiparnos a determinadas situaciones.

Aunque en este libro me voy a centrar en Internet, existen multitud de

fuentes abiertas a partir de las cuales se puede obtener información relevante, entre las que destacan:

- Medios de comunicación: revistas, periódicos, radio, etc.
- Información pública de fuentes gubernamentales.
- Conferencias, simposios, «papers», bibliotecas online.
- Foros, redes sociales, blogs, wikis, etc.
- Archivos y bibliotecas
- Boletines oficiales
- Buzones
- Páginas blancas y amarillas
- Cementerios

Historia de OSINT

Parece ser que OSINT nació en el año 1941 en Estados Unidos, con la organización FBIS[1] (Foreign Broadcast Information Service). La organización FBIS tenía como objetivo recopilar o generar inteligencia a partir del rastreo, traducción y análisis de transmisiones extranjeras con fines propagandísticos de guerra, incluso se cree que llegaron a anticipar la intención de Japón de entrar en guerra.

En el año 2013 la agencia estadounidense NSA publicó un manual[2] con el que enseñaba a sus agentes a utilizar Google para buscar información relevante

1. FBIS (Foreign Broadcast Information Service) https://en.wikipedia.org/wiki/Foreign_Broadcast_Information_Service
2. NSA publica manual para buscar en Google https://hipertextual.com/2015/07/manual-de-la-nsa-busquedas

desde el punto de vista de la inteligencia.

Actualmente OSINT es una disciplina utilizada, no solo en el ámbito militar, sino que también tiene sus aplicaciones en el mundo policial, civil y empresarial.

Si tienes tiempo, te recomiendo que veas la película "Los tres días del cóndor"[3], donde Robert Redford hace de un analista de fuentes abiertas, pero en este caso, sus fuentes son los libros.

Qué se puede hacer con OSINT

Se puede decir que obtener información personal de personas, empresas y organizaciones en internet es relativamente sencillo. Existe poca conciencia de la gran exposición que hacemos de nuestros datos personales en internet. Compartimos desde lo que comemos, hasta dónde vamos de vacaciones, incluso las fotos de nuestros hijos.

En una ocasión leí algo que me dejó perplejo. Y es que solo se necesitan 3 datos para identificar a una persona completamente: su sexo, su fecha de nacimiento y el código postal de donde reside. Y la verdad es que tiene sentido.

Con un poco de paciencia se puede hacer un perfil de una persona lo suficientemente detallado como para saber de esta, incluso más que ella de sí misma.

A ello hay que sumar el analfabetismo tecnológico. Motivo por el que, ante la falta de conocimiento, dejamos expuestos multitud de datos personales[4].

A nivel policial nos sirve para identificar a autores de actos delictivos, para prevenir estos, para llevar a cabo seguimientos en tiempo real de sucesos a través del monitoreo de las redes sociales, así como para llevar a cabo

3. Película "Los tres días del cóndor" https://www.filmaffinity.com/es/film759291.html
4. La magia gracias a Facebook https://www.youtube.com/watch?v=N_Jj4y1ZTNg

complejos análisis de redes sociales con el objeto de encontrar conexiones dentro de grupos de personas.

Estos son algunos ejemplos de lo que podemos hacer con OSINT:

- Anticiparnos a acontecimientos, atentados terroristas, etc.
- Analizar robos y fugas de información de empresas, gobiernos, etc.
- Investigar a personas, organizaciones, objetivos, eventos, etc.
- Monitorizar lo que se habla en redes sociales, foros, IRCs, chats y blogs.
- Analizar relaciones entre personas, empresas, asociaciones, partidos, etc.
- Detectar fallos de configuración que impliquen la exposición de información.
- Monitorizar e investigar páginas fraudulentas y phishing.
- Monitorizar tendencias sobre lo que se habla en Internet de una organización, producto, persona, etc.
- Conocer la reputación online de un usuario o empresa.
- Realizar estudios sociológicos, psicológicos, lingüísticos, etc.
- Auditoría de empresas y diferentes organismos con el fin de evaluar el nivel de privacidad y seguridad.
- Evaluar tendencias de mercados.
- Identificación y prevención de posibles amenazas en el ámbito militar o de la seguridad nacional.

Como punto negativo hay que tener en cuenta que los ciberdelicuentes también usan estas técnicas para cometer los delitos. Por tanto es necesario conocerlas, no solo para llevar a cabo investigaciones, sino para evitar ser víctimas de delitos.

A quién va dirigido

OSINT es de interés para diversos profesionales y en diferentes contextos:

- Recursos humanos
- Investigadores privados
- Cuerpos y fuerzas de seguridad
- Ámbito militar
- Ingenieros sociales
- Periodistas
- Analistas de seguridad
- Abogados

Y poco a poco, según se vaya conociendo su potencial, se convertirá en una herramienta utilizada en cualquier ámbito.

Ciclo OSINT

Cuando hablamos de OSINT no hablamos de obtener información sin más. Estamos hablando de un método, y me atrevería a decir que, hasta un método científico, el cual consta de varios procesos, y que de no cumplirlos perderíamos la rigurosidad que merece toda investigación.

El proceso de inteligencia en fuentes abiertas (OSINT) consta de las siguientes fases:

Requisitos: podríamos decir que es la fase en la que se definen las preguntas a las que tenemos que responder. Las veremos en la siguiente sección sobre los *Preparativos*.

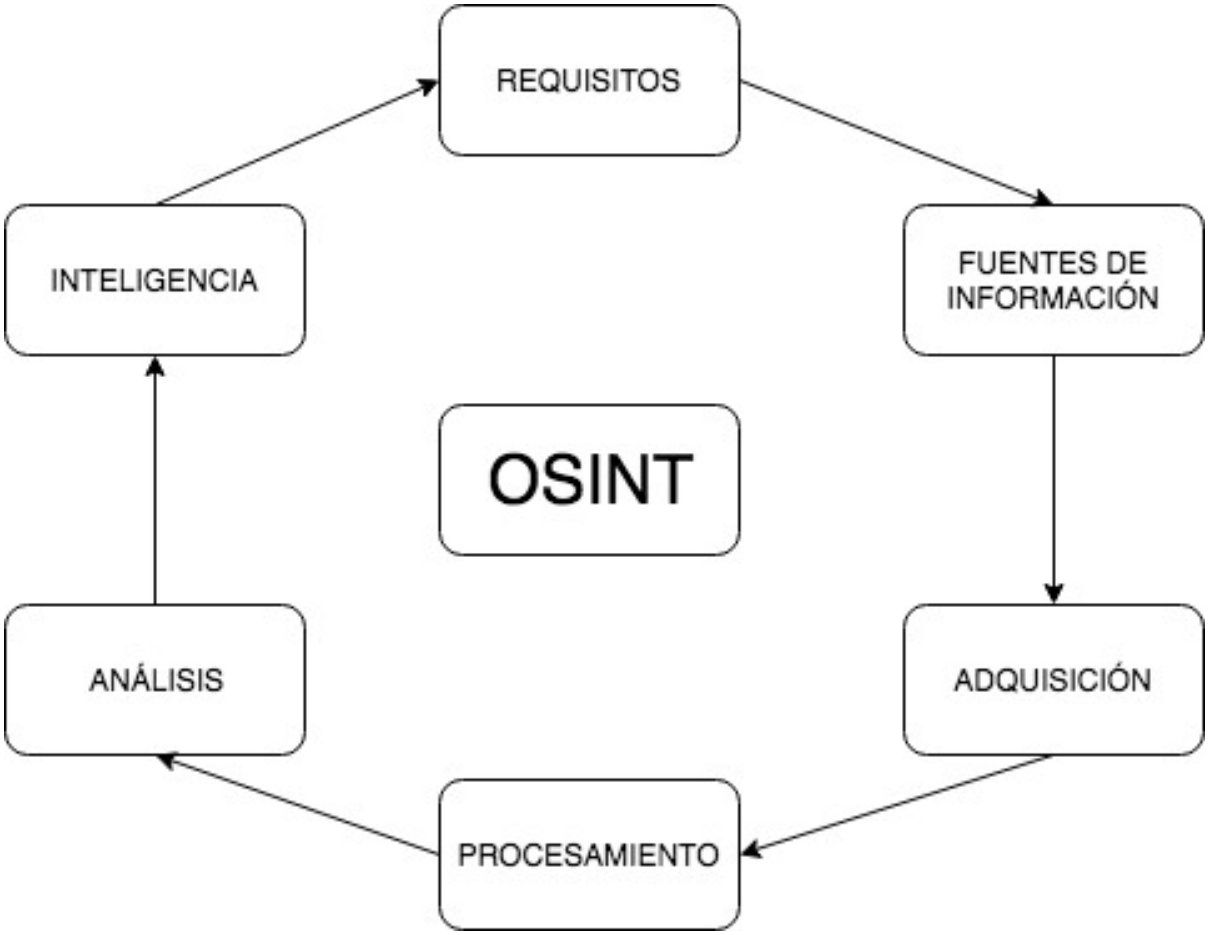
Fuentes de información: en esta fase se definen las fuentes de donde se obtendrá la información y las herramientas a utilizar.

Adquisición: etapa en la que se obtiene la información. Normalmente es la de mayor duración.

Procesamiento: consiste en dar forma a toda la información recopilada de manera que, posteriormente. pueda ser analizada.

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

Presentación de inteligencia: consiste en presentar la información obtenida de manera comprensible y útil para la toma de decisiones posteriores.



Preparativos

Justo cuando empecé a escribir este libro encontré un artículo[5] que hablaba de

5. Mapa mental con procesos OSINT https://webbreacher.com/2018/07/12/osint-map/

los aspectos a tener en cuenta antes de comenzar con cualquier investigación. Aunque está más enfocado al ámbito civil, creo que puede servir, con matices, a cualquier ámbito.

Estas serían las preguntas, que, antes de comenzar, deberíamos tener respondidas:

Objetivos a conseguir

- ¿Qué información quiere el peticionario?
- ¿Lo quiere todo o algo en concreto?
- ¿Cómo quiere que se le muestre el informe?
- ¿Qué consideraría como una investigación exitosa?
    - ¿Qué resultado está buscando?
- ¿Cuál es el motivo del peticionario?
    - ¿Entra dentro de la legalidad?

Analizando la investigación

- Nivel de interacción con el objetivo deseado
- Nivel de camuflaje para la investigación
- Cantidad de tiempo para llevar a cabo la investigación
- Resultado requerido al final de la investigación
    - Nivel de detalle
    - Tipo de informe
    - ¿Resumen?
- Almacenamiento de datos

    - ¿Requiere encriptación para almacenarlo?

- ¿Conservación de los datos requeridos al finalizar?
    - Si es así, ¿cuál es la duración?
    - Si es así, ¿qué formato?
- Cuestiones éticas
    - ¿Se pueden usar avatares? (Más adelante veremos qué es un avatar)
    - ¿Podemos contactar con el objetivo?
    - ¿Puedes contactar con los amigos y / o familiares del objetivo?
    - ¿Existe alguna restricción en las condiciones del cliente para llevar a cabo la investigación?
- Asuntos legales
    - ¿Ha consultado el cliente a un abogado sobre esta solicitud de OSINT?
        - ¿Cuál fue el resultado?
    - ¿Has consultado con un abogado sobre esta solicitud de OSINT?

Como ves son preguntas que nos ayudan a tener una idea más clara del trabajo que tendremos que llevar a cabo, el alcance del mismo, así como hasta dónde podemos llegar.

Si estás empezando en OSINT, créate un checklist de cosas por hacer y sobre qué buscar en cada caso y qué acciones tomar. Planifica cada paso para asegurarte de recordar recolectar todos los datos relevantes. Asegúrate de responder las preguntas clásicas de "qué, cuándo, dónde, quién, por qué y cómo".

Problemas

Existen algunos problemas que tendrás que tener en cuenta a la hora de realizar OSINT.

Demasiada información: debido a la gran cantidad de información que podemos llegar a obtener, debemos ser selectivos con las fuentes, y evitar el exceso de información. Como analista OSINT debes saber cuando parar.

Fiabilidad de las fuentes: equivocarnos con la elección de la fuente puede provocar que todos los datos obtenidos sean erróneos (fruto del árbol envenenado)[6]. Debemos asegurarnos mediante técnicas de verificación que la fuente es la correcta.

Herramientas OSINT

Hay multitud de herramientas y servicios útiles a la hora de realizar OSINT.

Llevo más de un año recopilando todas las herramientas OSINT[7] que encuentro para crear un gran repositorio organizado por categorías. Hoy en día dispones de herramientas para prácticamente cualquier cosa que necesites averiguar.

Las herramientas aparecen y desaparecen. Es posible que cuando publique este libro, algunas de las que hablo ya no se encuentren funcionando o hayan cambiado, pero lo que nos interesa es la metodología, esta siempre será la misma, independientemente de las herramientas que existan en cada momento.

De forma general podríamos organizarlos en:

6. La teoría de "los frutos del árbol envenenado". http://noticias.juridicas.com/conocimiento/articulos-doctrinales/8944-la-doctrina-del-fruto-del-arbol-envenenado/
7. Repositorio de herramientas OSINT de ciberpatrulla.com https://ciberpatrulla.com/links/

- Buscadores habituales
- Buscadores especializados
- Herramientas de recolección de metadato
- Servicios para obtener información a partir de un dominio
- Herramientas de extracción de información de redes sociales

En las siguientes secciones y capítulos las veremos con más detalle.

Consejos previos

Antes de adentrarnos de lleno en el mundo OSINT me gustaría darte algunos consejos:

Yo no he inventado nada. Solo intento recopilar toda la información que existe en internet sobre OSINT, procesarla, analizarla, y haciendo inteligencia, generar un producto útil, en este caso, un libro.

Si estás empezando en el mundo OSINT **necesitarás pasar muchas horas experimentando** para tener una idea general de todas las posibilidades que ofrece. Este libro y ciberpatrulla.com te van a facilitar muchísimo todo ese proceso.

OSINT es un **análisis forense de Internet** y como tal, se requiere de una experiencia considerable para comprender aspectos como el código HTML, los algoritmos, la tecnología de búsqueda y de servidor. Antes de aventurarte a realizar OSINT en Internet te animo a que te formes adecuadamente. Piensa que tus conclusiones serán tenidas en cuenta a procesos muy delicados, y una vaga comprensión de Internet puede perjudicar a terceros o llevar al traste tu investigación. Sé honesto contigo y con los demás, métete solo hasta donde tus conocimientos te permitan.

Te aviso, **OSINT crea adicción**. Al igual que en una investigación hay que saber parar de recopilar información, en la recopilación de herramientas OSINT también, porque, por experiencia propia, cada día encontrarás una herramienta nueva y un servicio nuevo, y puedes convertir tu barra de favoritos o tu gestor de marcadores en un océano de herramientas, creándote más inconvenientes que beneficios.

Lo siento. **No existe una herramienta que automatice todo el proceso**, o al menos yo no la he encontrado. En muchos casos necesitarás utilizar varias herramientas que se complementen entre ellas.

Lo importante es el método. Es importante que te quedes con la idea general de la herramienta y no generes mucho vínculo con ella. Hoy está y mañana no. Aparecen y desaparecen como flores de temporada. Llegado ese día triste, solo tendrás que buscar una alternativa. Si tu herramienta favorita desaparece, prueba a buscar alguna alternativa. Puedes usar este comando en Google (related:www.google.com), el cual te mostrará alternativas a la herramienta online que le pongas, o puedes usar esta web https://alternativeto.net/ si lo que estás buscando es una alternativa a software que ha desaparecido.

Existen herramientas muy potentes, las cuales pueden tener una curva de aprendizaje media o alta. Antes de profundizar en estas, es conveniente valorar si podemos **hacer lo mismo**, en menos tiempo, **de forma manual**.

Te animo a profundizar en este mundo. **Haces mucha falta**. No es el futuro, es el presente. Se necesitan profesionales que sepan dar respuesta a las diferentes problemáticas del mundo digital. De nada sirve que una persona denuncie un hecho, si lo único que se lleva a casa es una copia de la denuncia, sin una respuesta adecuada a su problema.

Sobre el libro

Este libro está organizado por entradas de datos, es decir, cada capítulo está

basado en los pasos a seguir cuando disponemos de un dato determinado, por ejemplo, un email o un número de teléfono. Puedes leer el libro entero o puedes consultar cada capítulo en base al dato que dispongas. Si necesitas obtener información de un perfil social, solo tienes que dirigirte al capítulo que corresponda con esa red social, o si necesitas obtener información a partir de un número de teléfono, puedes dirigirte a dicho capítulo. La idea es que sea un documento práctico de consulta que te ayude como una herramienta más en tu trabajo.

Internet

Existen otros mundos

Como muchos de los grandes avances de nuestra sociedad, Internet[8] también tiene descendencia militar. Su primera versión fue creada en 1969 con el nombre de ARPANET. En aquel año se estableció la primera conexión de computadoras entre tres universidades en California (Estados Unidos).

No te voy a dar cifras ni estadísticas del uso de Internet, creo que no son necesarias para saber que hoy en día es utilizado por la gran mayoría de la población.

Internet nos ha facilitado a todos multitud de gestiones, tanto comerciales como personales. Al igual que nos facilita a nosotros, también lo hace a los delincuentes, los cuales se han mudado al mundo digital. Está claro el motivo, se pueden ocultar más fácilmente, no necesitan grandes infraestructuras, y pueden llegar a más víctimas, incluso a nivel internacional. Un delincuente puede estar extorsionando a una persona que se encuentra a miles de kilómetros de distancia y hacerle creer que son vecinos, y solo con disponer de un ordenador y conexión a internet.

En las siguientes secciones quiero contarte algo, y es que, Internet no es todo lo que vemos, hay otros mundos, y un analista OSINT tiene que conocerlos y saber moverse por ellos para sacar el máximo provecho a la información disponible en Internet.

8. Internet en la Wikipedia https://es.wikipedia.org/wiki/Internet

Surface Web

La Surface Web o Web Superficial es la internet fácilmente accesible. La que usamos habitualmente para leer las noticias, reservar un viaje, o hacer gestiones bancarias.

Normalmente se accede a través de Google, Bing o Yahoo. Los buscadores genéricos son los que se han convertido en las puertas de entrada a Internet. Parece que todo lo que no se encuentra a través de ellos, no existe, pero veremos más adelante que no es así.

La Web Superficial está compuesta por menos del 10% del total de internet. Increíble, ¿verdad? Luego veremos el porqué de este dato.

La Web superficial contiene al menos 4.5 mil millones de páginas[9].

Cuando utilizamos la Web Superficial somos rastreables a través de nuestra IP y ¡mucho más!

Si tienes interés en saber todo el rastro que dejamos cuando navegamos por Internet puedes echar un ojo a esta web (https://browserleaks.com).

Los datos en sí mismos podrían no decirte nada, pero, ¿y si te digo que con esos datos se puede llegar a crear una identidad digital de un usuario?, ¿que se puede crear una huella digital ¡ÚNICA! de un usuario de Internet?

Así es. Recopilando toda esa información de nosotros, pueden llegar a crear un perfil lo suficientemente detallado como para crear una identidad única digital y poder rastrear todos nuestros movimientos por Internet.

¿Quieres hacer la prueba? Entra en esta web (https://amiunique.org/) y haz clic en "View my browser fingerprint", analizará tu navegador y te dirá si eres identificable de forma única. Más adelante te contaré cómo evitar ser rastreado.

9. The size of the World Wide Web http://www.worldwidewebsize.com/

Desde el punto de vista de una investigación, y siempre con el correspondiente respaldo legal, estas técnicas se pueden utilizar para generar una huella digital del investigado, y en el caso de realizar un peritaje informático de un ordenador, poder relacionar dicho ordenador o cuenta de usuario con la persona investigada.

Google

Creo que Google merece una sección para él solo. Sin duda es el rey dentro de los buscadores de Internet.

En este libro hablaré en más ocasiones, y de forma más extensa, de este buscador. Veremos las opciones avanzadas de las que disponemos para obtener información de Internet utilizando Google. Antes me gustaría comentar algunos aspectos generales para tener una idea más clara de qué es Google, cómo funciona, y qué contenido podemos encontrar en él.

¿Qué es Google?

Google es un índice.

Google no almacena el contenido, aunque sí almacena una copia temporal de las webs en su caché, la cual podemos consultar en caso de que la web haya sido eliminada (lo veremos más adelante).

Cuando decimos que es un índice nos estamos refiriendo a que Google no aloja, ni guarda el contenido de las webs, solamente guarda información de estas para poder mostrarnos la dirección URL[10], el título de la web y una breve descripción de la misma. Igualmente guarda una copia temporal de la web, en su caché.

10. Definición de URL en la Wikipedia https://es.wikipedia.org/wiki/Localizador_de_recursos_uniforme

¿Cómo añade Google las webs a su índice?

Mediante su araña (crawler).

El robot de Google[11] es el robot de rastreo web de Google (en ocasiones, también denominado "araña"). El rastreo es el proceso mediante el cual el robot de Google descubre páginas nuevas y actualizadas y las añade al índice de Google.

¿Todas las webs están en Google?

No.

Google no tiene capacidad de indexar todo el contenido que existe en Internet. En ocasiones no podrá porque le es imposible, como por ejemplo con servicios privados donde solo se puede acceder mediante usuario y contraseña, y otras veces no lo podrá porque el propietario de la web ha configurado la misma de forma que Google interprete que no debe indexarla en su índice. Para ello se utiliza el archivo *robots.txt*, y las meta etiquetas *no index* y *no follow*. Más adelante entraremos en detalle con este tema.

¿Google muestra los perfiles de las RRSS?

Sí.

Google es capaz de indexar perfiles sociales, de forma que, si queremos buscar a alguien en una red social, podemos utilizar este buscador para hacerlo. Igualmente lo veremos en profundidad más adelante.

¿Qué contenido indexa Google?

Google no solo es capaz de indexar páginas web. Es capaz de indexar muchos

11. El robot de Google https://support.google.com/webmasters/answer/182072?hl=es

tipos de archivos [12](.pdf, .doc, .py, etc.). Esto nos puede dar una idea del potencial que tiene Google y sus búsquedas avanzadas, las cuales veremos más adelante en profundidad.

Sitios Web

No quiero entrar en materia de investigación sin antes comentar algunos aspectos muy genéricos sobre algo tan esencial como es saber qué es un sitio web.

Todos usamos sitios webs a diario, pero es posible que no tengamos claro su funcionamiento.

Una página web no es otra cosa que un documento, normalmente con extensión .html, que se encuentra alojado en un servidor, al que se puede acceder mediante un navegador web y una conexión a Internet.

Estos servidores suelen estar gestionados por empresas prestadoras de servicios de alojamiento web (en inglés: hosting).

Con conocimientos suficientes, también se podría alojar un sitio web en un servidor local, es decir, configurando tu ordenador personal adecuadamente, podrías alojar un sitio web tú mismo y este podría ser accesible al resto del mundo a través de Internet.

Diferencia entre "página web" y "sitio web"

12. Tipos de archivos que indexa Google https://support.google.com/webmasters/answer/35287?hl=es

Si quieres ser riguroso a la hora de hacer un informe es importante que tengas en cuenta que no es lo mismo una *página web* que un *sitio web*. El primero hace referencia a un documento único, con una URL específica y el segundo se utiliza para referirnos al conjunto de esas páginas web que componen todo el sitio completo.

Código Fuente de una web

El código fuente de una página web, que está escrito en lenguaje de marcado HTML o en JavaScript, u otros lenguajes de programación web, es la parte no visible de una página web. En realidad, es el código que interpretan los navegadores como Google Chrome para luego mostrarnos una página web tal cual la vemos.

En momentos determinados de una investigación necesitaremos acceder al código fuente de una página web porque este nos ofrecerá información que de forma visible no obtendremos. Veremos algunos ejemplos de uso más adelante.

Para acceder al código fuente de una página web solo tenemos que colocar el cursor en cualquier parte de la misma, y con el botón derecho del ratón seleccionar "*Ver código fuente*".

Hipervínculo

Nos pasamos el día utilizándolos, de hecho, Internet no existiría sin ellos. Los hipervínculos[13], hiperenlaces, links o enlaces pueden ser de varios tipos:

Hipervínculo de texto: es un enlace que se encuentra asociado a un texto, de forma que al hacer clic sobre ese texto se carga la página que indique el hipervínculo.

Hipervínculo de imagen: este es un enlace que se encuentra asociado a una imagen, de forma que si se hace clic sobre esa imagen se carga la página que

13. Enlaces o Hipervículos https://lenguajehtml.com/p/html/semantica/enlaces-o-hipervinculos

indique el hipervínculo.

Hipervínculo local o interno: es un vínculo a una página que se encuentra en el mismo sitio web (sitio local).

Hipervínculo externo: es un vínculo a otro sitio web en Internet (sitio externo). Es un vínculo a cualquier otro lugar fuera del sitio actual.

Hipervínculo a una dirección de correo electrónico: es un vínculo que contiene una dirección de correo. Al pulsar en él, automáticamente se abre el programa de correo que tenga el usuario instalado para poder escribir a esa dirección de correo.

URL

Saber el funcionamiento de una web es muy importante, pero si algo cobra gran importancia en una investigación es la URL[14]. Este será el identificador único de cualquier evidencia que encontremos en internet.

En el caso de las redes sociales cobra especial relevancia debido a que la URL que vamos a necesitar, en ocasiones, no es la URL visible, pero no me quiero adelantar, lo veremos más adelante.

Ahora te voy a contar algunos detalles sobre las URLs que debes tener en cuenta.

Las URLs son de diversos tipos. Las más habituales son las URLs que utilizamos para identificar la ruta o dirección de una página web.

Este sería un ejemplo de una URL (he dejado espacios para diferenciar las partes de la misma):

https:// *sub.* ***dominio*** *.com* ***/ruta/*** *pagina.html* ***#ancla***

No te preocupes, te lo explico en las siguientes líneas:

https://: se trata del protocolo que utiliza la URL. Existen otros, pero este es el habitual para páginas web.

14. Partes de una URL https://lenguajehtml.com/p/html/semantica/enlaces-o-hipervinculos#partes-de-una-url

sub. dominio la siguiente parte de la URL es el dominio del sitio web que queremos enlazar. El dominio generalmente se compone de un subdominio (las famosas 3 www) y el nombre de dominio y el dominio de nivel superior o TLD[15] (**www**.ciber…).

Por ejemplo, las famosas *www* no son más que un subdominio utilizado tradicionalmente para páginas webs. Yo en mi web no lo uso.

Por otra parte, hay muchísimos TLD para sitios web (.com, .net, .org, .es…).

Rutas: la ruta de una página web sería lo equivalente a las carpetas o directorios donde almacenamos nuestros archivos en nuestro ordenador. En realidad, un servidor web es un ordenador, y el funcionamiento es idéntico. Una página web se organiza en carpetas y directorios, y dentro de estos se encuentran las páginas web y todo el contenido multimedia que utilice. En la parte de obtención de evidencias te hablaré de programas de descarga de sitios web completos, donde podrás ver cómo se distribuye un sitio web en carpetas.

Página web: cuando nos encontramos en una página web, la última parte de la URL suele ser un documento HTML como el del ejemplo: pagina.html.

Si lo que estamos enlazando es un archivo PDF, el final de la URL será .pdf.

Cuando veamos la parte de las redes sociales veremos que esto cambia, y que, en Facebook, por ejemplo, no se utilizan este tipo de extensiones.

Query strings: otro tipo de URL que nos vamos a encontrar habitualmente, en especial en las búsquedas en Google y otros buscadores, son las cadenas de consulta del usuario. Se trata de variables que contienen información y esta se envía en la URL. Si te fijas en una URL de un resultado de búsqueda de Google verás que esta contiene las palabras o frase que hayas utilizado en la búsqueda.

Ancla: esta parte de la URL se utiliza para dirigir al usuario a un lugar concreto dentro de una página. Para ello se utiliza un fragmento de texto precedido por el carácter #. Puedes ver un ejemplo si haces clic en el link de la 2ª nota al pie de esta sección.

15. TLD (Wikipedia) https://es.wikipedia.org/wiki/Dominio_de_nivel_superior

Servidor: un servidor web es un ordenador preparado y acondicionado para estar permanentemente conectado a una red de alta velocidad. Esta red de alta velocidad forma parte de Internet.

Se utiliza, principalmente, para alojar páginas web, aunque con la aparición de nuevos servicios en la nube, hoy en día, es utilizado para infinidad de servicios. Puede ser un servidor web compartido (aloja varios sitios web) o un servidor web dedicado (aloja un solo sitio web).

FTP

El FTP (del inglés «File Transfer Protocol») es un protocolo que permite subir los archivos de un sitio web a un alojamiento o descargarlos desde el mismo. Es uno de los métodos utilizados para subir un sitio web a un servidor. También es utilizado para servir archivos sin más. Tampoco quiero profundizar mucho en este tema. Si en alguna ocasión lo necesitas, puedes encontrar mucha información en Internet.

Hosting

El alojamiento web[16] (en inglés: web hosting) es el servicio que provee a los usuarios de Internet un sistema para poder almacenar los sitios web. El alojamiento web suele estar gestionado por empresas.

Al igual que las URLs, las empresas de hosting tienen gran relevancia para nosotros como investigadores. Identificar qué empresa de hosting aloja un sitio web nos servirá para realizar las gestiones oportunas para identificar al administrador de dicho sitio. También lo veremos más adelante.

Dominio: un nombre de dominio de internet[17] es un nombre único que identifica un sitio web (ejem: ciberpatrulla.com).

En realidad, cada sitio web está asociado a una IP, pero se usan los nombres de dominio porque son más fáciles de recordar, aunque se puede acceder a un sitio web a través de la IP que tenga asignada. También lo veremos con más detalle más adelante.

16. Alojamiento Web (Wikipedia) https://es.wikipedia.org/wiki/Alojamiento_web
17. Nombre de dominio de internet (Wikipedia) https://es.wikipedia.org/wiki/Dominio_de_Internet

Deep Web

La Internet profunda[18] (del inglés, deep web) está compuesta por el contenido de internet que no está indexado por los motores de búsqueda convencionales.

Es el internet no accesible a través de motores de búsqueda estándar.

Engloba toda esa información a la que, estando online, no se puede acceder de forma pública.

Algunos de los servicios que componen esta parte de Internet sería todos los servicios en la nube que son privados y para los que necesitamos usuario y contraseña para entrar, como, por ejemplo, servicios para alojar archivos, alojamiento de fotos, copias de seguridad en la nube, correos electrónicos, servidores FTP privados, archivos compartidos mediante redes P2P, etc.

También la componen las webs que bloquean a los buscadores con "Disallow" en el archivo robots.txt[19]. Ya te he hablado de este archivo más atrás.

Todos estos servicios están en Internet pero ocultos e inaccesibles, salvo para sus titulares. Se habla de que es el 90% de todo Internet y de que es unas 500 veces más grande que la web superficial. Casi nada.

Dark Web

Dentro de Internet encontramos también la Dark Web o la Internet Oscura. Está compuesta por varias redes o Darknets[20], la más popular es la Red Tor, la cual veremos con más detalle en la siguiente sección, pero también tienes otras redes, como Freenet, I2P o ZeroNet.

Cada una de estas redes es una Darknet, pero cuando nos referimos a todas

18. Internet profunda - https://es.wikipedia.org/wiki/Internet_profunda
19. Archivo robots.txt de la web del Ayuntamiento de Madrid http://www.madrid.es/robots.txt
20. ¿Qué son las Darknets? - https://medium.com/@blogdramatik/que-son-las-darknets-ce46edd1bc44

ellas en general utilizamos el término Dark Web.

¿Cuál es el objetivo de esta parte de Internet? Básicamente, quien utiliza estas redes busca el anonimato. Los motivos para querer ser anónimo en Internet son variopintos, no tiene por qué ser para delinquir[21], aunque también se utiliza para ello. De hecho, es muy probable, aunque no dispongo de datos, que el número de delitos sean infinitamente mayor en la web superficial.

Estas redes son usadas por periodistas, activistas y ciudadanos de países con censura, incluso por militares que quieren comunicarse de forma anónima, y cómo no, también por delincuentes. Como dato, se dice que el 45% de los sitios *.onion* están creados para cometer actos ilícitos[22], lo que viene a decir que el 55% de los sitios de la red Tor son legales, como por ejemplo la web del propio periódico The New York Times[23], el cual tiene versión en la red Tor.

Te dejo este programa/documental sobre la Dark Web (https://www.youtube.com/watch?v=22eOcoHRWVI).

Red Tor

Ya hemos visto que Tor es una red dentro de la Dark Web, y que no es la única, pero sí las más utilizada y popular.

La Red Tor no se creó para delinquir[24]. El proyecto Tor (acrónimo de The Onion Router) en realidad fue un proyecto militar que fue creado por Roger Dingledine, Nick Mathewson y Paul Syverson y puesto en marcha por el Laboratorio de Investigación Naval de los Estados Unidos en el año 2003.

21. Deep Web es un documental de 2015 dirigido por Alex Winter, que cubre eventos acontecidos sobre Silk Road, Bitcoin y política de la Internet profunda - http://www.deepwebthemovie.com/#land
22. 15 cosas que debes saber sobre Tor https://www.dailydot.com/layer8/tor-browser-project/
23. El New York Times abre su sitio a la 'dark web' http://www.milenio.com/estilo/new-york-times-abre-sitio-dark-web
24. Artículo de ElPais.com sobre TOR https://elfuturoesapasionante.elpais.com/el-creador-de-tor-te-explica-como-navegar-con-seguridad/

Se dice que está compuesto por el 1% de Internet con unas 60.000 páginas .onion (extensión que utilizan los dominios de la red Tor).

Tor Project (https://www.torproject.org/) es una organización sin fines de lucro que respalda la red y desarrolla el software. Hoy en día, la Oficina de Derechos Humanos del Departamento de Estado de los EEUU figura como actual donante destacado del proyecto Tor[25] (como parte de su apoyo a disidentes democráticos de todo el mundo).

La conexión en la red Tor no funciona igual que en la web superficial. En la red Tor nuestras conexiones pasan a través de varios servidores de personas voluntarias y con una configuración y características especiales. Estos servidores van filtrando nuestra conexión de forma que el destinatario final no sepa cuál es el origen de la misma. La dirección IP que el destinatario verá de nosotros no será la nuestra, sino la del último servidor por el que pasa nuestra conexión. Puedes ver mejor el funcionamiento en este vídeo (https://www.youtube.com/watch?v=Sz_J6vJ4MYw).

Para navegar de forma anónima por la red Tor necesitamos un navegador especial que podemos descargar en (https://www.torproject.org). Antes de comenzar a navegar por la red Tor te recomiendo que leas las recomendaciones de configuración del navegador que podrás encontrar en su propia página (https://www.torproject.org/download/download.html.es).
Podemos navegar por la red Tor con cualquier navegador sin necesidad del navegador Tor, pero entonces nuestra conexión no será anónima. Si queremos entrar en la red Tor con otros navegadores podemos hacerlo añadiendo al final de la extensión *.onion* la extensión *.to (ejem: .onion.to)*.

Una vez descargado el navegador Tor, para empezar a navegar por esta red podemos usar el portal *THE HIDDEN WIKI* desde esta URL (http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page). Este portal ofrece una serie de enlaces a webs .onion ordenadas por categorías.

También podemos usar el navegador Tor para navegar por la web superficial y

25. El gobierno de los EE. UU. Aumenta los fondos para Tor https://www.theguardian.com/technology/2014/jul/29/us-government-funding-tor-18m-onion-router

navegar por la misma de forma anónima.

Podemos instalar el navegador Tor en un USB y usarlo en el ordenador que queramos.

Te dejo un vídeo de un taller sobre Tor bastante interesante (https://www.youtube.com/watch?v=PYu9Zkwmhw0).

Bitcoin

Creo que es necesario tratar el tema de las monedas virtuales. Seguro que has oído hablar del Bitcoin.

Bitcoin es una moneda virtual, la cual, combinando redes de ordenadores, criptografía y software es posible usarla sin necesidad de una entidad central que la emita y controle.

El uso de las monedas virtuales se ha disparado, y para nosotros como investigadores será importante estar al día en su funcionamiento.

¿Cómo se obtienen Bitcoin?

Con Bitcoin no existe un emisor, los ordenadores distribuidos que velan porque las transacciones sean correctas obtienen, de vez en cuando, monedas como premio. Esto se denomina minería, y es la forma en la que se crea el dinero con los Bitcoin.

Es la moneda usada en la Red Tor. Tiene sentido, teniendo en cuenta que, al igual que Tor, el objetivo de esta moneda es usarla sin que haya nadie que controle nuestros movimientos ni haga de mediador en las transacciones, impidiendo que se pueda identificar al titular de una cuenta de Bitcoin.

No quiero entrar en más detalles sobre las criptomonedas, puedes encontrar mucha información en Internet, pero sí quiero dejarte unas recomendaciones que, si no estás muy al día en criptomonedas, pueden ayudarte a entender

mejor su funcionamiento:

La primera recomendación es el canal de YouTube Crypto Español (https://www.youtube.com/channel/UC_TmOIPWu-hCVuE2fA3M8Tg) que, a día de la fecha, cuenta con 4 vídeos muy didácticos del funcionamiento de las criptomonedas.

La segunda es una ponencia sobre el rastreo de ransomware a través de la red de Bitcoin (https://www.youtube.com/watch?v=Po6lxnt-xBI) donde hablan, también de forma muy didáctica, sobre el funcionamiento de las criptomonedas.

La tercera y última recomendación es este artículo (https://academy.bit2me.com/bitcoin-no-es-anonimo/) que habla del anonimato del Bitcoin.

Aspectos legales

Introducción

A la hora de llevar a cabo una investigación en Internet tenemos que tener en cuenta aspectos legales que, de pasar por alto, nos pueden acarrear problemas serios.

Es importante que ante cualquier duda sobre la legalidad de tus actuaciones consultes con un abogado o asesoría jurídica.

Toda la información que te voy a dar a continuación está basada en un estudio propio realizado con información obtenida de Internet. No soy experto en Derecho. Esta es mi interpretación, y es posible que haya detalles que se me hayan escapado. Aun así, toda esta información legal que te voy a dar te dará una visión global de qué aspectos legales tienes que tener en cuenta en tu investigación.

En las siguientes secciones vamos a ver qué legislación es de aplicación en esta materia. También daremos un breve repaso a los derechos fundamentales a los que deberemos prestar especial atención. Igualmente trataré la parte de protección de datos, conservación de datos en relación a los prestadores de servicios de Internet, la figura del agente encubierto informático, hablaré sobre el delito provocado, así como aspectos legales a tener en cuenta sobre la obtención y presentación de las evidencias, la importantísima cadena de custodia, y qué medidas accesorias se pueden solicitar en el transcurso de una Instrucción.

Legislación aplicable

Solo a modo de referencia y sin entrar en detalles, quiero dejarte el marco jurídico que tendrás que tener a mano a modo de consulta.

El marco jurídico vigente para la investigación de delitos cometidos por medio de los servicios de la sociedad de la información (Internet, redes sociales, correos electrónicos, etc.), viene dado por los siguientes textos legales:

- Ley 34/2002, de 11 de julio de Servicios de la Sociedad de la Información y Comercio Electrónico (redacción según Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, modificada posteriormente por la Ley 2/2011, de 4 de marzo, de Economía Sostenible)[26].

- Ley 25/2007, de 18 de octubre de conservación de datos de comunicaciones electrónicas y redes públicas de comunicación[27].

- Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal[28].

- Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica[29].

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal[30].

- La Constitución española de 1978. Título I. De los derechos y deberes fundamentales[31].

Derechos fundamentales

26. https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758
27. https://www.boe.es/buscar/doc.php?id=BOE-A-2007-18243
28. https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036
29. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725
30. https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444
31. http://www.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=10&fin=55&tipo=2

Autorización judicial

La investigación de un delito en Internet en su conjunto o a través de medios informáticos, no siempre requerirá la previa habilitación judicial, ya que muchos de los datos que se pueden aportar a un proceso judicial se pueden conseguir sin que suponga una vulneración a los derechos fundamentales de la persona[32].

Se puede dar el caso de que dichos datos sean aportados por la propia víctima al ser esta partícipe de dicha comunicación.

Es decir, cualquier persona que participe en una comunicación, ya sea telefónica, vía email, aplicaciones de mensajería o cualquier otra, puede presentar como prueba el contenido de la misma:

"STC 114/1984, de 29 de noviembre de 1984[33]: «debe afirmarse que no constituye contravención alguna del secreto de las comunicaciones la conducta del interlocutor en la conversación que graba ésta (que graba también, por lo tanto, sus propias manifestaciones personales...».

En el mismo sentido, la STS 710/2000, de 6 de julio[34], dispone que:

«En consecuencia, no cabe apreciar, en principio, que la grabación de una conversación por un interlocutor privado implique la violación de un derecho constitucional, que determine la prohibición de valoración de la prueba así obtenida»"

También puede darse el caso que dichos datos se encuentren de forma pública en alguna red social, aplicación informática o página web, en cuyo caso no será necesaria la autorización para utilizarlos como prueba.

De los Derechos fundamentales

La Ley de Enjuiciamiento Criminal en su artículo 282 bis. 3 establece:

---

32. Cuestiones procesales relativas a la investigación de los delitos en la red https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Sr.%20VALVERDE.pdf?idFile=98ee6878-f370-403a-911b-7d71200a932a

33. Sentencia 114/1984, de 29 de noviembre - (BOE núm. 305, de 21 de diciembre de 1984) - ECLI:ES:TC:1984:114 http://hj.tribunalconstitucional.es/es/Resolucion/Show/367

34. Sentencia nº 710/2000 de TS, Sala 2ª, de lo Penal, 6 de Julio de 2000 https://supremo.vlex.es/vid/-15200921

«Cuando las actuaciones de investigación puedan afectar a derechos fundamentales el agente encubierto deberá solicitar del órgano judicial competente las autorizaciones que al respecto establezca la Constitución y la Ley, así como cumplir las demás previsiones legales aplicables».

La autorización judicial, previa, será exigible en todos aquellos casos en los que la Constitución lo haya previsto de forma expresa, es decir, cuando se trate de restringir los derechos previstos en los artículos 18.2 (inviolabilidad del domicilio), 18.3 (secreto de las comunicaciones), 20.5 (secuestro de las publicaciones) y 22.4 (derecho de asociación).

Por ello es necesario revisar qué tipo de derechos pueden ser vulnerados en una investigación realizada a través de medios informáticos, y para lo cual necesitaremos la preceptiva autorización judicial.

El Secreto De Las Comunicaciones (Art. 18.3 de la Constitución Española)

Cuando hablamos del secreto de las comunicaciones, lo que se protege es el medio utilizado y no el contenido transmitido.

Se protege la interceptación de comunicaciones vía teléfono, SMS, email, Skype, WhatsApp u otros similares. No siendo necesario que sea la comunicación bidireccional, como en el caso del teléfono, pudiendo ser unidireccional como es el caso de un email, o un SMS. Siendo necesario que los destinatarios estén predefinidos, porque en el caso de no estar predefinidos no hablamos de una comunicación, sino de una difusión, como por ejemplo, las que realizan los programas de radio tradicionales.

La comunicación, aunque no sea bidireccional, como ocurre con los correos electrónicos, debe ser cerrada, entendiendo ese carácter cerrado en el sentido de que el número de destinatarios o interlocutores está, inicialmente, determinado y que sean identificables, aunque estos puedan ampliarse o ir variando en el curso de la comunicación, pero esos interlocutores, aunque sean variables, deben estar determinados. Un ejemplo sería un grupo de WhatsApp, donde, aunque el número de interlocutores sea elevado, al estar definidos y cerrado, y aunque se vayan sumando nuevos miembros, estaría protegido por el secreto de las comunicaciones.

Público o Privado

Definir qué es público o privado en Internet no es sencillo. Esto es debido a la gran cantidad de variantes que existen en el mundo digital.

Quizás con el tiempo y cuando haya jurisprudencia, se vayan aclarando algunas dudas al respecto.

Como hemos visto antes, para definir qué es una "comunicación" tenemos que tener en cuenta que los interlocutores estén predefinidos.

En este sentido, podríamos decir que Netflix realiza comunicaciones protegidas por el Secreto las Comunicaciones, ya que sus abonados están predefinidos. Recuerda que lo que se protege no es el contenido, sino el medio. Da igual que sean películas, o que sea una conversación.

Quizás esta sea la clave para determinar la diferencia entre una "comunicación" y una simple exposición de datos personales, como por ejemplo lo que hacemos cuando publicamos contenido en nuestros perfiles sociales.

El hecho de que hayamos definido en nuestro perfil social ciertas restricciones para que el contenido que publicamos solo sea visto por nuestros "amigos", no quiere decir que sea una "comunicación" protegida, ya que tendremos que tener en cuenta el funcionamiento de dicha red social y los Términos y Condiciones de la misma, la cual puede permitir que nuestros "amigos" o los miembros de un grupo cerrado, puedan hacer público nuestro contenido compartido con ellos, y que a través de las publicaciones de estos "amigos", terceras personas puedan tener acceso de forma pública a dicha información.

Protección de datos

Cesión de datos a la Policía Judicial

¿Qué información nos deben facilitar las operadoras o prestadores de servicio sin necesidad de autorización judicial, o qué información podremos solicitar a dichas empresas directamente como Policía Judicial?

En ocasiones, dentro de una investigación policial, necesitaremos obtener los datos asociados a un número de teléfono, una IP o un dominio, como, por ejemplo, datos de identificación sobre las personas que han contratado un servicio, datos de la persona, física o jurídica, que ha contratado un número de teléfono o un número de tarificación adicional o los datos de facturación relativos a dichos contratos desde el inicio de la actividad contractual.

Debemos separar los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso, de los datos del titular o abonado de una línea telefónica, ya que no es lo mismo, y no están bajo el paraguas de la misma protección.

Dichos datos personales podremos solicitarlos sin autorización judicial dentro de nuestra investigación y debiendo justificarlo en la solicitud.

Así se ha pronunciado la Agencia de Protección de Datos en cuanto a la cesión de datos de abonados a las FFCCSS[35].

Igualmente, el artículo 588 ter.m[36] de la LECrim, de forma expresa dispensa esta exigencia judicial entendiendo que dicha titularidad es un dato contractual que debe quedar excluido de cualquier protección dispensada al secreto de las comunicaciones, por lo que tanto el Ministerio Fiscal como la Policía Judicial podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información cuando *"necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio decomunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación"*.

En este sentido se podrá requerir el titular de un número de teléfono o de cualquier medio de comunicación, sin autorización judicial directamente al prestador de servicios. De igual forma, se podrá solicitar de forma inversa, es decir, qué número de teléfono tiene asignado dicho titular.

---

35. Agencia de Protección de Datos - Cesión de datos de abonados a las FFCCSS https://ciberpatrulla.com/wp-content/uploads/2018/07/2005-0297_Cesi-oo-n-de-datos-de-abonados-a-la-Polic-ii-a-Judicial.pdf
36. Cuestiones procesales relativas a la investigación de los delitos en red -
Roberto Valverde Megías - Delegado de Criminalidad Informática
de la Fiscalía Provincial de Barcelona - https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Sr.%20VALVERDE.pdf?idFile=98ee6878-f370-403a-911b-7d71200a932a

En todo momento la LECrim habla de datos técnicos relativos a las llamadas o mensajes para requerir autorización judicial, no a la titularidad, es decir, habla de horas, posiciones y otros datos que puedan llevar a la identificación de que el titular u otra persona es el autor.

Identificación mediante número IP (Artículo 588 ter k de la LECrim)

Este artículo dispone:

"Cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada para la comisión de algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el artículo 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso."

Del artículo anterior se entiende que dentro del ejercicio de prevención y descubrimiento de delitos en internet podemos obtener la IP sin autorización judicial, utilizando mecanismos a nuestro alcance[37].

Aunque como dice la Circular 1/2013, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas[38], una vez obtenida la dirección IP mediante el rastreo, la solicitud de los datos asociados a dicha IP dirigida a las operadoras deberá ser mediante autorización judicial:

"El principio básico es el de que no se precisa autorización judicial para conseguir lo que es público. El Tribunal Supremo considera que estos datos no se encuentran protegidos ni por el art. 18.1 CE, ni por el art. 18.3 CE (SSTS nº 292/2008, de 28 de mayo; y 776/2008, de 18 de noviembre). Tras la averiguación del IP, las subsiguientes

37. Los códigos IMSI e IMEI y la dirección IP: ¿se pueden obtener y aportar en un proceso judicial? - https://nivolap.es/los-codigos-imsi-e-imei-y-la-direccion-ip-se-pueden-obtener-y-aportar-en-un-proceso-judicial/

38. Circular 1/2013, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas. - https://www.fiscal.es/memorias/memoria2014/FISCALIA_SITE/recursos/cir_inst_cons/circular_1_2013.pdf

actuaciones de identificación y localización de quién sea la persona que tiene asignado ese IP se deben llevar a cabo bajo control judicial. Debe, no obstante, tenerse presente una matización: la jurisprudencia distingue por un lado los casos de rastreo policial del espacio público y por otro lado los supuestos en los que para acceder a una información sobre IP es necesario oficiar a una operadora. En este último supuesto, sí debe considerarse necesario obtener autorización judicial conforme a las previsiones de la Ley 25/2007 (SSTS nº 292/2008, de 28 de mayo, 236/2008,de 9 de mayo, nº 680/2010, de 14 de julio). Aquí de nuevo la exigencia deriva del mandato legal contenido en la Ley 25/2007, pese a que el dato no pueda cobijarse bajo el manto protector del secreto de las comunicaciones. Los rastreos policiales para localizar direcciones IP pueden por tanto realizarse sin necesidad de autorización judicial, ya que no se trata de datos confidenciales preservados del conocimiento público.".

Igualmente, el 588 ter L, habla de que podremos identificar el nº IMEI o IMSI con dispositivos a nuestro alcance sin autorización judicial.

Conservación de datos

Con la entrada en vigor de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones[39], se impone a los prestadores de servicios de comunicaciones electrónicas y de redes públicas de comunicación (prestadores de servicios de telefonía fija, móvil o por Internet) la obligación de conservar una serie de datos de tráfico, localización y otros datos de sus usuarios que se generan como consecuencia del uso de los servicios.

Los datos que deben ser conservados son los datos de tráfico, localización y otros datos[40] necesarios para identificar al abonado o usuario registrado, pero en ningún caso incluyen datos relativos al contenido de las comunicaciones.

La finalidad de la conservación es que las autoridades policiales, inmersas en una investigación de un delito, puedan acceder a dichos datos, previa

39. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones - https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243

40. ¿Cómo influirá el nuevo tratamiento de datos en la investigación de delitos? El caso de la peregrina de Astorga - https://sbarrera.es/el-caso-de-la-peregrina-de-astorga-como-influira-el-nuevo-tratamiento-de-datos-en-la-investigacion-de-delitos/

solicitud a los operadores y con autorización judicial.

Si ya se está instruyendo el caso, se solicitarán al Juez Instructor y si solo se está investigando, se pedirá al Juzgado de Guardia.

Datos que deben guardar los prestadores de servicios

la Ley 25/2007 dispone un listado detallado de cuáles deben ser los datos que deben conservar. Este listado[41] comprende los datos necesarios para: (i) rastrear e identificar el origen y el destino de la comunicación; (ii) determinar su fecha, hora y duración; (iii) identificar el tipo de comunicación y el equipo de comunicación utilizado; e (iv) identificar la localización en los casos de equipos de comunicación móvil.

Igualmente esta ley habla de la identificación de los usuarios de teléfonos móviles que funcionan bajo la modalidad de prepago.

No es ninguna novedad si digo que este tipo de servicios, que facilitan el anonimato del usuario, son los que de manera más frecuente se utilizan en la comisión de actos delictivos.

La Ley obliga a los operadores de servicios de telefonía móvil que comercialicen servicios de tarjetas de prepago a llevar, desde la entrada en vigor de la Ley, un libro-registro en el que conste la identidad de los usuarios que adquieran una tarjeta de este tipo, quedando tales datos sometidos a la Ley de Conservación de Datos.

Agente encubierto informático

La Ley de Enjuiciamiento Criminal en un nuevo artículo 282 bis, proporciona habilitación legal a la figura del «agente encubierto» en el marco de las

41. Ley 25/2007, de 18 de octubre - Artículo 3. Datos objeto de conservación - https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243&p=20140510&tn=1#a3

investigaciones relacionadas con la denominada «delincuencia organizada».

El artículo 282 bis de la LECrim dispone que cuando las actuaciones policiales afecten a los derechos fundamentales de los investigados, el agente infiltrado deberá solicitar la autorización del órgano judicial.

"Art. 282 bis 6 de la LECrim: El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a."

Para actuar como agente encubierto informático necesitamos autorización judicial si los canales son cerrados.

Se puede dar el caso de que lleguemos a realizar una comunicación vía Skype y que grabemos dicha conversación, si esta conversación se realiza desde el domicilio del sospechoso, al estar grabando la morada del mismo, necesitaremos autorización expresa para ello, no será suficiente con la figura del agente encubierto:

Solicitud de la figura de Agente Encubierto Informático

Una vez tengamos conocimiento de la existencia de indicios de la comisión de una actividad ilícita, y creamos que para conseguir la identificación del autor o para conseguir pruebas para demostrar el hecho ilícito, sea necesaria la técnica del Agente Encubierto, corresponde a los responsables de la investigación solicitar la misma.

Para ello, se elaborarán los informes oportunos, aportando todo indicio que nos haga pensar que dicha persona es el autor del ilícito, dando traslado al Juez de Instrucción, para que valore la adopción de la medida.

La iniciativa de esta medida corresponde a la policía judicial, ya que somos

los que tenemos la información y los conocimientos para llevarla a cabo. Somos nosotros los que valoraremos la idoneidad de esta medida. El Juez podrá solicitar un estudio de viabilidad de la infiltración, pero no ordenar la misma.

De lo anterior se desprende que para realizar tareas de investigación en grupos o perfiles privados como policía judicial y sin revelar nuestra condición de agentes de la autoridad, accediendo mediante engaño, necesitamos autorización judicial.

Jurisprudencia

La sentencia 39/2016 del Juzgado de lo Penal de Gijón[42] sobre el caso Anonymous sentó los criterios para la utilización del agente encubierto tecnológico, analizando que unos de los agentes de policía se habían ganado la confianza de los acusados en las conversaciones de la red social y esta medida no estaba amparada por autorización judicial, pudiendo haber incurrido, incluso, en un delito provocado.

En esa misma sentencia se menciona la sentencia de fecha 14/07/2010 del Tribunal Supremo, en relación a la posible vulneración del secreto de comunicaciones a través de internet, en la que se declara que:

"el acceso a la información puede efectuarla cualquier usuario, no precisando autorización judicial para lo que es público cuando el propio usuario de la red ha introducido dicha información"

Concluyendo, dicha sentencia, que, la actuación del agente que actuó de forma encubierta haciéndose pasar por un usuario más de la red contactando con el acusado, fue una actuación de investigación lícita. La actividad de un agente que va encaminada a efectuar averiguaciones y a abortar una actividad delictiva, habiendo intervenido solo en zonas públicas en las redes sociales, chats públicos en los que todos participan con identidades supuestas, no necesita autorización judicial.

Como queda claro en la sentencia del TS, para investigaciones en fuentes

42. Sentencia 39/2016 del Juzgado de lo Penal de Gijón http://www.poderjudicial.es/stfls/TRIBUNALES%20SUPERIORES%20DE%20JUSTICIA/TSJ%20Asturias/DOCUMENTOS%20DE%20INTER%C3%89S/Jdo.%20Penal%20Gij%C3%B3n%206%20julio%202016.pdf

abiertas, como puede ser un perfil en una red social donde el contenido es público, no es necesaria la autorización judicial para actuar como agente encubierto, si bien, señala en esa misma sentencia que, sí será necesaria en la ejecución de comunicaciones privadas.

Si conseguimos entrar en una red social o chat, donde la comunicación es cerrada a un número determinado de usuarios, y para acceder a este grupo, perfil o chat es necesaria la previa aceptación de un administrador o titular de dicha cuenta, y una vez dentro, hacemos capturas de los comentarios que pudieran ser ilícitos para aportarlas como prueba sin orden judicial, esa aportación se va a considerar ilícita y, por tanto, debería invalidar el proceso penal.

Un perfil, chat o grupo cerrado dispone de una mayor protección de la intimidad. Todo su contenido se considera un dato privado y las pruebas obtenidas sin autorización judicial o sin la figura del agente encubierto son nulas.

Las actividades públicas realizadas en internet, susceptibles de ser conocidas por todo el mundo, incluida la propia policía no se hallan protegidas por el art.18.1 ni por el 18.3 de la Constitución[43] (Así, STS 249/08, 630/08, 776/08, 940/08, 960/08, 40/09, 688/09 o 921/09).

¿Qué debemos considerar como canal cerrado de comunicación?

Como hemos visto en la sección de Derechos Fundamentales, un canal cerrado se refiere a que va dirigido a un número determinado de personas las cuales están previamente predefinidas.

De las autorizaciones

Las autorizaciones para ejercer como agente encubierto informático las da el Juez Instructor, nunca el Fiscal. (Art. 282 bis . Apartado 6)

"*Art. 282 bis . Apartado 6. El juez de instrucción podrá autorizar a funcionarios de la*

43. Cuestiones procesales relativas a la investigación de los delitos en red - Roberto Valverde Megías - Delegado de Criminalidad Informática de la Fiscalía Provincial de Barcelona - https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Sr.%20VALVERDE.pdf?idFile=98ee6878-f370-403a-911b-7d71200a932a

Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a."

"*Artículo 588 ter a Presupuestos. La autorización para la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.*"

Identidad de Agente Encubierto Informático

La identidad ficticia para poder profundizar dentro de los espacios cerrados de interés en la investigación, será otorgada siempre por el Ministerio del Interior.

El procedimiento en este caso sería muy sencillo a la hora de obtener esta Identificación ficticia, puesto que valdría una autorización con una serie de datos personales básicos, pero sin llegar a las características que se le dan al agente encubierto físico tradicional.

La tarea del otorgamiento de identidad ficticia quedaría reducida a trámites muy sencillos, nada equiparable con el Agente encubierto que trabaja en el plano físico.

Todas las informaciones personales que tenga que rellenar en los campos necesarios para autenticar dicho perfil serán los proporcionados por el Ministerio del Interior para que así se pueda llevar un control externo de la figura del Agente Encubierto en la Red.

Delito provocado

Otra duda que se genera en la actuación como agente encubierto en fuentes abiertas o cerradas, es la de la comisión del Delito Provocado.

En este sentido existe diversa jurisprudencia, como por ejemplo, la STS

1688/2017[44].

Para cometer el delito provocado es necesaria la incitación engañosa por parte del agente a una persona que no está decidida a delinquir.

Si nos encontramos en un supuesto en el que la comisión de un ilícito ha sido realizada o hay indicios suficientes de que hay intención de realizarla, el delito provocado no se daría.

Medidas accesorias

En el transcurso de una investigación podemos solicitar una serie de medidas accesorias, sin que haya habido sentencia alguna sobre el caso. Estas medidas las podemos solicitar sobre la conservación de los datos de los prestadores, sobre los contenidos publicados en Internet, y sobre las personas implicadas en dicho caso.

Roberto Valverde Megías - Delegado de Criminalidad Informática, en su ponencia[45] sobre "Cuestiones procesales relativas a la investigación de los delitos en red", explica cuáles son estas medidas y que, muy resumidamente, te detallo:

Sobre los datos

Como hemos visto en la sección de Conservación de datos, la Ley 25/2007 obliga a los proveedores de acceso a Internet y los operadores de telefonía fija, móvil o por Internet, a guardar los datos relativos a comunicaciones, no así el contenido de las mismas. Pasado el plazo (1 año), estos datos pueden ser borrados.

---

44. Sentencia del Tribunal Supremo de Madrid 1688/2017 de 03/05/2017 - http://www.poderjudicial.es/search_old/documento/TS/8015818/Presuncion%20de%20inocencia/20170512

45. Cuestiones procesales relativas a la investigación de los delitos en red - Roberto Valverde Megías - Delegado de Criminalidad Informática de la Fiscalía Provincial de Barcelona - https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Sr.%20VALVERDE.pdf?idFile=98ee6878-f370-403a-911b-7d71200a932a

Podemos requerir la conservación y protección de estos u otros datos informáticos por un plazo máximo de 90 días (prorrogables sólo una vez) hasta que se obtenga la autorización judicial para la cesión

Sobre los contenidos

Cuando el hecho delictivo, por sus características, lo requiera y con el objeto de proteger a la víctima, se podrá, mediante mandamiento judicial, solicitar la eliminación o el bloqueo del contenido a los prestadores que alojen los mismos.

Sobre las personas

Junto a las medidas cautelares personales tradicionales (prisión provisional, órdenes de alejamiento y comunicación, etc.) se puede plantear la opción de la medida cautelar de prohibición de acceder a Internet, de acceder a sistemas o equipos informáticos o alguna otra forma de impedir al investigado el uso de Internet.

Evidencias digitales

En esta sección vamos a ver cómo aportar una prueba con todas las garantías necesarias para que sea aceptada y no tengamos problemas con impugnaciones.

Requisitos:

Licitud

Como hemos visto en la sección de derechos fundamentales, las pruebas que presentemos deben haber sido obtenidas de forma que no vulneren ningún derecho fundamental. De lo contrario estaríamos antes una prueba nula.

Autenticidad

Es imprescindible garantizar la autenticidad del documento. Para ello deberemos aportar cuanta información sea necesaria para robustecer y blindar la prueba. Cualquier duda que se genere sobre su autenticidad puede convertirla en nula.

Integridad

Garantizar que la prueba no ha sido manipulada, modificada o alterada desde el momento de la obtención hasta el momento de su aportación en juicio.

Hay que respetar la llamada "cadena de custodia", que veremos en la siguiente sección.

Prueba preconstituida

Las pruebas preconstituidas son todas aquellas pruebas cuya realización deba practicarse en la fase de investigación sin demora y antes de que se celebre el juicio oral.

Debido a lo fácil que es manipular una evidencia digital, unido a la volatilidad de la misma, con el riesgo de que dicho contenido pueda perderse, es necesaria la preconstitución de la prueba o anticipación de la misma.

Lo más conveniente, es que un fedatario público levante acta del contenido de la misma (Notario o Letrado de la Administración de justicia). Otra opción son las empresas que emiten certificados digitales, y que como terceros de confianza[46] y basándose en la normativa de firma electrónica pueden acreditar tales contenidos, que podrán ser aportados en juicio (tengamos en cuenta por ejemplo entidades como Egarante[47], términis[48] o doy fe[49]).

46. eGarante, así actúa un testigo online frente al acoso y ataques en la Red - https://www.xataka.com/legislacion-y-derechos/egarante-asi-actua-testigo-online-frente-al-acoso-ataques-red
47. https://www.egarante.com
48. https://www.terminis.com
49. https://doyfe.es

La cuestión que se plantea en el párrafo anterior se refiere básicamente a medios de prueba aportados por las partes, no a evidencias obtenidas como consecuencia de una intervención policial en los procesos de rastreo de Internet.

Estamos en todo caso ante evidencias[50] fácilmente manipulables que exigen que adoptemos todas las medidas necesarias para no generar ningún tipo de duda en cuanto a la veracidad de la misma.

La Sala Segunda del Tribunal Supremo, en la reciente sentencia 300/2015 de 19 de mayo, a propósito de unos "pantallazos" incorporados a la causa para acreditar una supuesta conversación mantenida entre dos personas a través de Tuenti. Según el alto Tribunal la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido. Similar reflexión se ha reiterado en la más reciente sentencia del Alto Tribunal 754/2015 de 27 de noviembre.

Dicho pronunciamiento se refiere a las pruebas presentadas como documentos impresos, pero el razonamiento que se efectúa en la sentencia es

50. Dictamen nº 1/2016 Sobre la valoración de las evidencias en soporte papel o en soporte electrónico aportadas al proceso penal como medio de prueba de comunicaciones electrónicas - https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Dictamen%20n%C2%BA%201-2016%20sobre%20el%20valor%20probatorio%20de%20las%20capturas%20de%20pantallas.%20Unidad%20Criminalidad%20Inform%C3%A1tica.pdf?idFile=5838c1ef-1b11-49bf-92f4-066d003af630

aplicable a todo tipo de evidencias digitales, pues la manipulación puede darse en ambos casos.

Un ejemplo podría ser, en el caso de querer obtener evidencias de una página web, es presentar la URL al archivo original, una copia de la página web en formato html, una captura en formato imagen o pdf de la página web, y un documento impreso para facilitar la visualización por parte del destinatario de la evidencia.

Impugnación de la prueba

Si cumplimos todos los requisitos será muy difícil la impugnación de la prueba.

Pero, ¿qué pasa si la impugnan?

Si aún habiendo tomado todas las medidas a nuestro alcance para obtener y preservar las pruebas de la forma más idónea, estas son impugnadas, hay que tener en cuenta los siguientes aspectos:

-La impugnación de la prueba por la parte contraria no implica que el juez vaya a admitir dicha impugnación. El juez puede no admitir dicha impugnación.

-En el caso de que prospere la impugnación, será la parte que impugna quien deberá aportar los medios probatorios para acreditar la integridad y / o autenticidad de las misma. Esto se traduce finalmente en la necesidad de una pericial informática que acredite tales extremos.

Aceptación de la prueba

El TSJ de Galicia, hizo un detallado análisis de la cuestión en su sentencia de 28 de enero de 2016[51], al señalar cuatro supuestos que pueden darse para que

51. Cómo asegurar la validez de los Whatsapp en un juicio - https://cincodias.elpais.com/cincodias/2018/03/19/legal/1521447030_123722.html

una prueba sea aceptada:

1.Cuando la parte interlocutora de la conversación no la impugna.

2..Cuando la reconoce expresamente.

3.Cuando se compruebe su realidad mediante el cotejo con el otro terminal implicado (a través de la exhibición).

4.Cuando una pericial acredita la autenticidad y el envío de la conversación "para un supuesto diferente de los anteriores".

Aunque esta sentencia trata unas conversaciones de WhatsApp, estos cuatro aspectos son extrapolables a otros tipos de casos con evidencias digitales como prueba.

Cadena de custodia

La cadena de custodia[52] es el procedimiento por el cual se garantiza la identidad, integridad y autenticidad de la evidencia digital sobre el hecho que se pretende probar, desde el momento en que se encuentra o se obtiene hasta que se aporta al proceso como prueba.

Para garantizar que la cadena de custodia no se ha roto o alterado[53], en el caso de que las evidencias sean aportadas por las partes, es recomendable que se garantice la misma mediante la intervención de un fedatario público (Notario, Letrado de la Administración de Justicia o tercero de confianza, como hemos visto en la sección de evidencias digitales) durante todo el proceso de obtención hasta su aportación.

Dentro de las labores de prevención e investigación policial y para garantizar la cadena de custodia, es recomendable utilizar sistemas automáticos de

52. La cadena de custodia: Fuente de prueba de dispositivos informáticos y electrónicos - https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/PONENCIA_BENITEZ_IGLESIAS%20(2).pdf?idFile=f78ecda3-8fba-4b8b-bd1e-d97b25f424e3

53. Absolución por falta de garantías en la Cadena de Custodia - https://peritoit.com/2016/07/13/absolucion-por-falta-de-garantias-en-la-cadena-de-custodia/

obtención de evidencias, como por ejemplo (http://osirtbrowser.com/). Estos sistemas realizan las obtenciones de las evidencias digitales y, de forma automática, generan el valor HASH[54] de las mismas, quedando registrado dichos valores en el informe generado por dicho software.

El valor HASH de una evidencia digital es un algoritmo de formulación matemática, el cual, a partir de un elemento digital de entrada, son capaces de proporcionar una salida de caracteres alfanuméricos de longitud fija, constante, estable y única para cada entrada. Sería como la huella digital de dicho archivo. Si el documento o archivo de origen sufre la más mínima modificación, este valor alfanumérico cambiaría, y podríamos saber que dicha evidencia ha sido alterada.

Por supuesto el valor HASH, en sí mismo, no es una garantía total de la veracidad de la prueba digital, solo de la integridad de la evidencia obtenida y de que, desde su obtención hasta la presentación en el juzgado, no ha sufrido alteraciones, siendo este el objetivo principal del cumplimiento de la cadena de custodia.

Para garantizar la cadena de custodia se debe detallar todo el proceso, desde el descubrimiento de la evidencia, su obtención y custodia, hasta la puesta a disposición de la autoridad judicial.

Lo ideal es preservar la evidencia digital original, pero como hemos visto en secciones anteriores, en ocasiones, como es en el caso de las redes sociales o páginas web, el contenido original no depende de nosotros, ni tenemos capacidad de preservarlo, pudiendo ser modificado o eliminado por sus titulares, siendo las capturas que hagamos de dicho contenido el único elemento de prueba del que dispongamos.

La prueba se debe presentar en formato digital o informático. Se podrá incluir en papel para facilitar la labor de los juristas (abogados, fiscal y juez), pero la prueba, debe incluirse siempre en soporte informático, preferiblemente óptico (CD-ROM o un DVD) o magnético (Disco duro o USB) en el caso de que por el tamaño no entre en uno óptico.

54. Funciones Hash en la investigación forense - https://peritoit.com/2016/05/23/funciones-hash-en-la-investigacion-forense/

Al presentarlo en un soporte óptico estamos garantizando que los archivos digitales estarán protegidos contra escritura, añadiendo un plus de seguridad sumado al valor HASH. Por el contrario, si lo presentamos en un disco duro o USB tendremos que informar que únicamente deberá conectarse siguiendo protocolos adecuados de bloqueo de escritura.

Si optamos por guardar las evidencias en un disco SSD, el cálculo del HASH, nunca va a ser igual. Esta circunstancia es debida a que un disco SSD siempre está optimizando la información en cuanto se conecta a la corriente. ¿Solución?

Como dice Manuel Guerra en su blog[55]:

"*se puede utilizar otra técnica totalmente innovadora y de última generación, que no es otra que meter el disco duro SSD dentro de una bolsa debidamente precintada y referenciada. Es decir, lo que viene a ser una Cadena de Custodia tradicional de toda la vida, la misma que se utiliza para resguardar un cuchillo con restos de sangre de un asesinato o la vaina del cartucho de una pistola utilizada. A veces nos empeñamos en que tiene que ser todo "ciber" o "digital" con sus hashes, firmas, claves privadas… cuando existen métodos tradicionales totalmente validos, mucho más rápidos y muy efectivos para mantener y garantizar una debida cadena de custodia, que se considere valida en cualquier procedimiento judicial. Es decir, la cadena de custodia "ciber" o "digital" es un elemento adicional a la garantía de la prueba, ya que en todo caso, siempre existirá una cadena de custodia tradicional, que en procedimientos penales estará supervisada por la propia Autoridad Judicial.*"

55. Prueba Nula: El hash no coincide - https://glider.es/prueba-nula-el-hash-no-coincide/

Entorno de trabajo

Introducción

En este capítulo vamos a ver qué opciones tenemos para crear un entorno de trabajo idóneo para las tareas relacionadas con OSINT.

Veremos qué características debe incluir nuestro equipo; cómo podemos trabajar con diferentes sistemas operativos desde el mismo dispositivo; qué pautas de seguridad son convenientes seguir; qué navegadores usar; cuáles son las extensiones más recomendadas para hacer OSINT; cómo podemos gestionar las evidencias; qué sistemas de encriptación podemos usar; y qué sistemas operativos preconfigurados existen para realizar OSINT.

Elección del equipo

Cualquier ordenador moderno, nos puede servir para realizar tareas de investigación en Internet. Es importante asegurarse que el sistema operativo que estamos usando no se encuentra sin soporte y obsoleto[56].

Dependiendo de nuestras necesidades, puede que necesitemos utilizar máquinas virtuales de forma paralela a nuestro sistema operativo nativo. En este caso las características del ordenador tendrán que ser especiales. Habrá que tener en cuenta la memoria RAM, que tenga suficiente como para trabajar con dos sistemas operativos a la vez.

De igual forma, el espacio en disco habrá que tenerlo en cuenta, y calcular las necesidades de espacio de cada máquina virtual, más el espacio que ocupa el

56. Hoja de datos del ciclo de vida de Windows - https://support.microsoft.com/es-es/help/13853/windows-lifecycle-fact-sheet

sistema operativo nativo.

El procesador, será conveniente que disponga de varios núcleos, ya que vendrán muy bien a la hora de la fluidez y velocidad en el trabajo.

Nos puede surgir la duda de si adquirir un equipo de sobremesa o un portátil.

Mi consejo es que adquieras un portátil. La movilidad es un plus que cuando no la tienes la echas en falta. Además, en momentos determinados puede ser imprescindible.

Trabajar con un sistema operativo u otro (Windows, MAC o Linux) no tiene por qué ser mejor ni peor, va a depender de a cuál de ellos estés más acostumbrado y de las necesidades de cada caso, pero sí es aconsejable que te manejes en todos los entornos, especialmente Linux, tarde o temprano tendrás que trabajar con él.

Seguridad digital

Si estás al día de las novedades en ciberseguridad, sabrás lo importante que es tomar ciertas medidas para proteger nuestros equipos, nuestro contenido y a nosotros mismos de ataques e intrusiones.

Es importante que separes tu vida profesional de la personal. Si lo haces utilizando equipos diferentes, mejor. Evitarás errores y disgustos.

En este apartado vamos a ver algunas medidas que es conveniente que tengas en cuenta para evitar sustos, como robo de información o pérdida de la misma, así como comprometer tu propia seguridad y la de terceros.

Medidas generales de seguridad

- Actualizar los programas antivirus y activar los cortafuegos del ordenador.

- Tener todo el software siempre actualizado a las últimas versiones.
- Prestar especial atención a las direcciones de email que recibimos.
- Desconfiar de los archivos adjuntos, y si tenemos que descargarlos, revisarlos con el antivirus o ejecutarlo en un entorno aislado[57].
- Desconfiar de los enlaces que nos envían contactos desconocidos.
- Utilizar contraseñas seguras

Medidas básicas de seguridad en el puesto de trabajo

- Proteger el ordenador con una contraseña fuerte.
- Respaldar y organizar de manera permanente la información.
- Encriptar[58] la información confidencial.
- No usar el ordenador de trabajo para fines personales.
- Si es una computadora compartida, cree una cuenta de usuario con una contraseña fuerte.

Protocolo de protección de móviles

- Evitar almacenar información sensible en el móvil.
- Hacer copias de seguridad y configurarlo para en caso de pérdida poder eliminar todo su contenido y bloquear el acceso al mismo.
- Al igual que con el ordenador, separar la vida profesional de la personal.
- Si el dispositivo lo requiere, usar antivirus y mantener actualizado todo el software.

57. Sandboxie: El software para ejecutar programas o archivos en un entorno aislado - https://www.ardilu.com/software/sandboxie-ejecutar-programas-entorno-aislado
58. Cómo encriptar archivos desde el ordenador de casa - https://blog.prosegur.es/encriptar-archivos/

- Para navegar de forma anónima desde el móvil puedes usar Orbot[59] para Android u Onion Browser[60] para iOS.

- En el caso de necesitarlo, encriptar[61] las llamadas, SMS y chats.

• Protocolo sobre las contraseñas

- Usa una contraseña distinta para cada cuenta. Puedes utilizar un gestor como KeePassXC[62] para gestionar todas tus contraseñas de forma segura.

- Crea passphrases[63] en lugar de passwords.

- Mide[64] la fortaleza de las contraseñas para asegurarte que lo suficientemente robusta.

Protocolo de almacenamiento seguro

- Los documentos que se consideren confidenciales deben guardarse en carpetas encriptadas. Puedes utilizar VeraCrypt[65]. Es un software gratuito de cifrado de disco de código abierto para Windows, Mac OSX y Linux, basado en TrueCrypt.

- En el caso de tener que viajar con los dispositivos de trabajo, es conveniente extraer toda la información sensible y viajar solo con la información no sensible, así evitaremos poner en riesgo dicha información en caso de pérdida o robo.

- Si es necesario llevar los archivos con nosotros, podemos usar servicios en la nube Como Dropbox o Google Drive, donde podemos subir nuestros archivos, previamente encriptados[66].

---

59. Aplicación Orbot - https://guardianproject.info/apps/orbot/
60. Onion Browser - https://itunes.apple.com/es/app/onion-browser/id519296448?mt=8
61. 9 apps para cifrar llamadas, SMS y mensajes en el móvil - https://www.eldiario.es/turing/vigilancia_y_privacidad/Aplicaciones-llamadas-intercambiar-mensajes-segura_0_391612033.html
62. https://ssd.eff.org/es/module/c%C3%B3mo-usar-keepassxc
63. Así son las contraseñas que propone Stanford - https://www.genbeta.com/seguridad/asi-son-las-contrasenas-que-propone-standford
64. Medir fortaleza de tu contraseña - https://password.kaspersky.com/es/
65. https://www.veracrypt.fr/en/Home.html
66. Cómo encriptar archivos desde el ordenador de casa - https://blog.prosegur.es/encriptar-archivos/

Navegación anónima en internet

La navegación anónima será necesaria en determinadas circunstancias. Ya hemos visto en capítulos anteriores cómo navegar de forma anónima usando Tor Browser.

Hay que tener en cuenta que cuando nos conectamos a determinados servicios, nuestra IP queda registrada, y si hacemos repetidas conexiones desde la misma IP, a un servicio que no tiene mucho tráfico de visitantes, podemos levantar sospechas. El administrador de un sitio web tiene acceso a ver las estadísticas de las visitas, y verá desde dónde se conectan los visitantes y qué IP han usado.

La IP también puede ser mostrada en los encabezados de correo electrónicos. Aunque, hace algún tiempo, la dirección IP del remitente dejó de aparecer de la cabecera por motivos de protección de datos, es conveniente asegurarse camuflando nuestra IP real.

También es conveniente usar Redes Privadas Virtuales[67] (VPN) para navegar en internet. Te hablaré de ello más adelante.

Para proteger tu privacidad es conveniente que te fijes en el prefijo *https* en todos los sitios donde vayas a intercambiar información, como contraseñas o datos personales. Puedes usar la herramienta https Everywhere[68] en el navegador la cual garantiza que todas tus conexiones serán a través de protocolos seguros.

Otra medida de seguridad a tener en cuenta es la de no conectarse a servicios, en los que debemos introducir credenciales desde redes inalámbricas, abiertas y sin contraseña. Lo mejor es vincular el móvil al PC y usar la conexión de datos del mismo, o utilizar algún dispositivo de conexión de datos conectado al PC por USB.

67. Te explicamos qué es una VPN y para qué se usa - https://www.osi.es/es/actualidad/blog/2016/11/08/te-explicamos-que-es-una-vpn-y-para-que-se-usa
68. https://www.eff.org/https-everywhere

Comunicación segura por email

En el caso de tener que comunicarnos, tratando con información sensible, es conveniente disponer de protocolos para enviar esta información de forma segura.

Para los emails, existen servicios como Protonmail[69] que ofrecen el envío de correos electrónicos protegidos automáticamente con cifrado de extremo a extremo. Esto significa que incluso la propia empresa de email no puede descifrar y leer tus correos electrónicos. Lo ideal es que tanto el emisor, como el receptor usen Protonmail para tener el máximo nivel de seguridad.

Comunicación móvil segura

Muchas de las plataformas de mensajería no son seguras porque transmiten los mensajes sin encriptar.

Existen algunas herramientas para encriptar las plataformas de chat o mensajería instantánea, pero si de verdad quieres asegurar tus mensajes, lo ideal es que uses una aplicación como Signal[70]. Es posible que pensaras que te iba a hablar de Telegram, la cual también recomiendo, pero Signal va un paso más allá en seguridad[71]. Con Signal, además de poder chatear de forma segura, podrás hacer llamadas de teléfono también cifradas.

Seguridad en email y redes sociales

Estos son algunos consejos a la hora de usar las redes sociales:

- Utilizar el sistema de doble factor de autenticación.
- Fijarse siempre en el navegador, que estamos conectados a través de *https,* mientras las utilizas.
- No abrir emails de desconocidos. Pueden obtener tu IP con solo abrir el email (lo veremos más adelante).

69. https://protonmail.com/es/
70. https://signal.org/
71. Ni Telegram ni WhatsApp: esta es la app de mensajería más segura que existe - https://andro4all.com/2018/01/app-mensajeria-mas-segura-whatsapp-telegram-signal

- Evitar geolocalizar los mensajes que envíes.
- Precaución con las aplicaciones a las que damos acceso.
- Usar una contraseña única, diferente de otros servicios.
- Desconfiar y verificar las solicitudes de amistad de personas desconocidas.
- Crea grupos de amistades con diferentes niveles de acceso a tu información.
- Si aceptas una solicitud de amistad de un desconocido, añádelo a un grupo con los mínimos privilegios.
- Mantén tus contactos privados.
- Ten precaución de no compartir ningún dato personal por error.
- Las redes sociales son accesibles por los buscadores, deshabilita que puedas ser rastreado por ellos.
- Ten en cuenta que lo que compartas puede terminar siendo visto por personas que no deseas.
- Vigila las imágenes donde sales etiquetado y elimina las etiquetas.
- Activa las notificaciones por correo electrónico para recibir avisos de seguridad de tu cuenta.
- Configura las notificaciones de *Seguridad e Inicio de Sesión*.
- Limita el número de dispositivos reconocidos para evitar que otras personas puedan acceder a tu cuenta.
- Revisa las sesiones activas y desactiva las que no estés usando.

El cazador cazado

Si no queremos caer en alguna trampa, es conveniente ser un poco/muy

desconfiados.

Hay que pensar que los malos también saben OSINT, e incluso técnicas de ingeniería social. Podemos creer que hemos conseguido encontrar información relevante, y estar siendo víctimas de algunas técnicas de contraespionaje, como por ejemplo:

1.- **Dejar puertas 'abiertas'**. Un investigado puede dejar información accesible donde debería ser difícil entrar, y aparentar ser un despiste, o error, cuando el objeto es monitorizar si accedemos a esa información.

2.- **Información falsa**. Si encontramos dicha "brecha", es probable que encontremos documentación e información de interés. Hay que desconfiar de la información fácilmente accesible, sobre todo, cuando sabemos que el investigado tiene conocimientos de informática.

3.- **Entretenernos**. Creer que hemos encontrado un filón de oro puede llevarnos a un camino sin salida. En el caso de que se trate de información falsa, habremos perdido mucho tiempo con información irrelevante, y todo ese tiempo habremos podido ser monitorizados en todos nuestros movimientos.

Para protegernos, tenemos que pensar que enfrente hay alguien que tiene los mismos o más conocimientos que nosotros, no infravalorarle.

Máquinas virtuales

En informática, una máquina virtual es un software que simula un sistema operativo el cual se ejecuta como si fuese una computadora real e independiente.

¿Para qué vamos a querer usar máquinas virtuales?

Los motivos pueden ser diversos. Igual nuestro sistema operativo habitual es Windows y por situaciones diversas, podemos necesitar instalar un SO con Linux. Con una máquina virtual evitamos tener que adquirir otro PC para

ello.

Otro motivo es por seguridad, para separar nuestro sistema operativo nativo del entorno de trabajo con el que vamos a hacer las investigaciones. Separar los entornos de trabajo, no solo nos dará más seguridad, sino que además aumentaremos las posibilidades de no equivocarnos y mezclar perfiles sociales y cuentas. Un error muy habitual.

Si tienes más de una cuenta de Facebook o Twitter, ¿nunca has enviado un mensaje desde una cuenta diferente de la que querías hacerlo?

No quiero extenderme con manuales sobre cómo instalar y configurar máquinas virtuales, existe muchísima información en Internet.

Yo te recomiendo que uses VirtualBox[72]. Es totalmente gratis.

Puedes ver un tutorial muy completo de instalación y configuración aquí: (https://youtu.be/sh_4rfHD1D0).

En la siguiente sección vamos a ver qué sistemas operativos ya vienen preconfigurados y listos para usar en una máquina virtual y que nos serán de mucha utilidad para hacer OSTIN.

Sistemas Operativos

Como alternativa a tu Windows, Mac o alguna distribución[73] de Linux que uses como sistema operativo nativo, voy a hablarte de 3 alternativas para que las instales en una máquina virtual, y de las que podrás sacar partido en determinados momentos.

Buscador

Buscador es un sistema operativo que podemos utilizar con una máquina virtual. Viene con muchas herramientas de análisis y obtención instaladas.

Buscador está basado en Linux y ha sido desarrollado por David Westcott y

72. https://www.virtualbox.org/
73. Distribución Linux - https://es.wikipedia.org/wiki/Distribuci%C3%B3n_Linux

Michael Bazzell, y las distribuciones se mantienen en esta página (https://inteltechniques.com/buscador/index.html), y desde donde lo podéis descargar.

Lo positivo de usar un sistema operativo como Buscador es que te ahorras tener que instalar muchas herramientas que ya vienen por defecto instaladas.

Para mi gusto, no lo usuaría como sistema operativo principal para trabajar, pero sí en determinados momentos que tenga que usar una herramienta que ya venga instalada. Solo tendríamos que ejecutar la máquina virtual y en 1 minuto tendríamos acceso a toda la colección.

Kali Linux

Kali Linux es la herramienta perfecta para hackers. Una puntualización, hacker no es sinónimo de delincuente.

De hecho, la filosofía de Kali Linux es su utilización y desarrollo con fines educativos y éticos, para un Internet más seguro.

Aunque este sistema operativo está orientado al hacking, podemos encontrar algunas herramientas, que nos pueden servir para la investigación, como CaseFile[74], Metagoofil[75] y OSRFramework[76].

Puedes ver un listado de todas las herramientas que incluye aquí (https://tools.kali.org/tools-listing)

Igualmente podemos instalar Kali Linux en una máquina virtual.

Tails

The Amnesic Incognito Live System o Tails[77] es una distro Linux basada en

74. https://tools.kali.org/information-gathering/casefile
75. https://tools.kali.org/information-gathering/metagoofil
76. https://tools.kali.org/information-gathering/osrframework
77. ¿Qué es Tails? - https://derechodelared.com/2017/10/05/tails/

Debian. No tiene nada que ver con los dos sistemas operativos anteriores, el objetivo de Tails es la privacidad y el anonimato.

Se ejecuta en la memoria RAM, no deja ningún rastro en el ordenador en donde lo uses. Nadie sabrá que has usado Tails. También es un sistema operativo que encripta todos los datos y oculta tus conexiones a Internet y tu ubicación, así que se puede utilizar de forma totalmente anónima.

Aunque lo ideal es instalar este sistema operativo en una memoria USB y ejecutarlo en el arranque del ordenador, te dejo un tutorial donde lo instala en una máquina virtual (https://www.youtube.com/watch?v=uxiYRFLjEjI).

Navegador

Para tareas OSINT vamos a utilizar tres navegadores. De uno de ellos ya te he hablado, Tor Browser. Los otros dos son Chrome y Firefox.

Es muy posible que entre Chrome y Firefox, a nivel de privacidad, sea este último el que gane la batalla, pero en este momento yo uso más Chrome, y no por nada en particular, simplemente porque empecé con él, y ahí sigo. Por lo tanto me voy a centrar más en Chrome.

Los consejos que te voy a dar a continuación no son para que los apliques, sí o sí. Tendrás que valorar qué tipo de navegación estás realizando, y el riesgo de la misma. No es lo mismo realizar una investigación buscando en Google unos datos en concreto, que navegar por sitios web que tenemos la certeza que detrás de ellos hay personas con conocimientos avanzados de informática.

Privacidad

Configurar el navegador

Los navegadores tienen un sin fin de opciones de configuración que no

solemos prestarle mucha atención. Es conveniente que, antes de empezar a trabajar, configuremos algunos parámetros, como por ejemplo: limitar la sincronización de tus datos; activar el cifrado mediante contraseña; evitar los servicios de apoyo de Google; gestionar las Cookies de navegación; deshabilitar los complementos del navegador; y desactivar el Control de actividad de Google. Te dejo una guía de cómo hacerlo en este artículo[78] de Computerhoy.com.

Evitar rastreadores

Cuando navegamos en un sitio web, pueden utilizar técnicas para hacernos un seguimiento de nuestros movimientos por Internet, de forma que obtienen un registro de las páginas que visitamos (puedes hacer un test del nivel de privacidad de tu navegador aquí (https://panopticlick.eff.org/). Aunque en principio esto se ha normalizado en Internet, y lo normal es que el objetivo solo sea publicitario o para obtener determinados patrones de navegación (que no es poco), nosotros no queremos que nos rastreen y para ello vamos a instalar la extensión Privacy Badger[79].

WebRTC

WebRTC es una API para permitir a las aplicaciones del navegador realizar llamadas de voz, chat de vídeo y uso compartido de archivos P2P sin plugins.

Hace tiempo se descubrió una gran falla de seguridad en WebRTC, pero solo al sistema operativo Windows. La vulnerabilidad, conocida como fuga de WebRTC , afecta a los usuarios de los navegadores Chrome y Firefox, y permite a los sitios web ver la dirección IP real de los usuarios, incluso cuando están detrás de un VPN. Para evitar esto tenemos que activar en la configuración de la extensión Privacy Badger la opción "*Prevenir que WebRTC filtre números de IP locales*".

78. Cómo configurar Chrome para mejorar la privacidad y seguridad - https://computerhoy.com/paso-a-paso/software/como-configurar-chrome-mejorar-privacidad-seguridad-64617
79. https://www.eff.org/es/privacybadger

Ocultar IP

En ocasiones necesitaremos ocultar nuestra IP real. Por ejemplo, si estamos visitando un sitio web, y no queremos dejar rastro en su sistema de estadísticas de nuestra IP real, podemos usar un servicio de VPN, como por ejemplo TunnelBear VPN[80], que tiene una versión gratuita, o puedes buscar otras empresas, pero asegúrate que dispongan de IPs españolas, o del país desde donde quieras que muestre la IP ficticia.

Tenemos que tener en cuenta que si nos conectamos al servicio de VPN a través de la extensión del navegador, solo estaremos filtrando el tráfico que enviamos desde el navegador, pero si enviamos un email con una aplicación de escritorio, ese tráfico no será filtrado. Para ello deberemos instalar la versión de escritorio del la VPN.

En el siguiente capítulo te recomiendo más servicios de VPN.

Limpiar los rastros

La navegación por Internet provoca que vayamos acumulando archivos temporales, cookies y el historial de dicha navegación. Para impedir el seguimiento de nuestra actividad en línea es conveniente limpiar todos estos datos al finalizar la sesión. Hacerlo de forma manual es algo incómodo, pero te voy a dar una solución fantástica, se llama Click&Clean[81].

Esta app elimina tu historial de navegación cuando el navegador se cierra, impidiendo así el seguimiento de tu actividad en línea.

Seguridad

En internet vamos a estar introduciendo credenciales constantemente, ya sea para conectarnos a las redes sociales, email, para contratar servicios o comprar productos. A la hora de hacer todo esto, es importante que la web

80. https://chrome.google.com/webstore/detail/tunnelbear-vpn/omdakjcmkglenbhjadbccaookpfjihpa?hl=es
81. https://chrome.google.com/webstore/detail/clickclean/ghgabhipcejejjmhhchfonmamedcbeod?hl=es

donde estamos realizándolo utilice protocolos de encriptación para que nuestros datos no sean interceptados por terceros. Para asegurarnos que en todo momento estamos utilizando la versión de la web con el protocolo *https* y por tanto, la información que estamos enviando va cifrada, vamos a usar la extensión HTTPS Everywhere[82].

Evidencias

Una de las áreas más importantes cuando aplicamos OSINT es la de obtención y gestión de las evidencias. Ya te he hablado de ellas en capítulos anteriores. Ya sabemos qué requisitos debe cumplir una evidencia para que cumpla su objetivo, que no es otro que el de probar un hecho, y ya sabemos qué pasos debemos seguir para cumplir con la cadena de custodia.

Ahora te quiero hablar de qué herramientas y métodos te vendrán bien para obtener dichas evidencias, y cómo organizarlas para que tu investigación no se convierta en un caos de imágenes, URLs y archivos.

Si vas a dedicarte a tareas OSINT, debes ser metódico y ordenado.

Inmediatez

Obtén las evidencias en cuanto las encuentres. Si esperas al día siguiente, ya puede ser tarde. El investigado, en el caso de darse cuenta de que se le está investigando, puede decidir eliminar el contenido relevante.

Documentación

Anota todos tus pasos. Cuando nos ponemos a navegar perdemos un poco la conciencia de lo que estamos haciendo, y vamos saltando de un sitio a otro. Siempre nos queda revisar el historial de navegación para volver atrás, pero a

82. https://www.eff.org/https-everywhere

veces es como perderse en un bosque.

Si encuentras una dirección de interés, pero decides que la quieres revisar con posterioridad, puedes usar un servicio como Save to Pocket[83] para guardarla.

Una vez que hemos encontrado una evidencia que creemos que sirve como prueba, lo primero que debemos hacer es obtener dicha evidencia, y seguidamente anotar toda la información relacionada con la misma. Para ello podemos usar un simple archivo de Excel.

Herramientas y automatización

Los tipos de evidencias que obtengamos van a definir qué tipo de herramientas utilizar.

Como norma general te recomiendo que utilices herramientas que automaticen estas tareas. Te ahorrarás trabajo y pérdidas de información.

Te recomiendo que uses OSIRT[84].

Osirtbrowser es una fantástica herramienta para guardar las evidencias de nuestra investigación. Está pensado para OSINT. Integra herramientas para capturas de pantalla, capturas de video y descargas completas de páginas web.

Algo muy útil es que automáticamente se asigna a la evidencia la fecha y el HASH, y todo queda almacenado en local.

Sin duda, es una herramienta a tener en cuenta, y de todas las que he probado, creo que es la más completa y enfocada a tareas de obtención para OSINT, y gratuita, como todo lo que recomiendo.

Es posible que tengas que usar otras herramientas para complementar la obtención de evidencias. No existe la herramienta perfecta, aunque OSIRT es

83. https://chrome.google.com/webstore/detail/save-to-pocket/niloccemoadcdkdjlinkgdfekeahmflj/reviews
84. http://osirtbrowser.com/

de las más completas.

En el caso de necesitar hacer una captura de pantalla de un sitio web o perfil social, sin duda mi recomendación es Nimbus Screenshot[85]. He probado muchas extensiones de captura de pantalla, y la única que ha podido con todo, hasta el momento, es esta.

Si necesitas descargar un sitio web completo, puedes usar Httrack[86]. Y si solo necesitas guardar una página única, puedes utilizar el método clásico de tu navegador "Archivo/Guardar página como".

En mi web tienes un artículo[87] muy completo con todas las herramientas de obtención que he encontrado. Elige la que más se adapte a tus gustos y necesidades.

Organización

Ya te he hablado de lo importante que es la organización. No es lo mismo guardar las evidencias en la carpeta de Descargas de tu PC, o en el escritorio, que crear un sistema de carpetas para cada caso, y que solo tengas que copiar y pegar este sistema cada vez que comienzas un caso.

Un ejemplo de sistema de carpetas podría ser algo así:

Una carpeta principal llamada *OSINT*, dentro otra carpeta llamada *CASO-NÚMERO/AÑO*, dentro tres carpetas llamadas *OBTENCIÓN, ANÁLISIS Y PRESENTACIÓN*.

Solo tendríamos que copiar la carpeta *CASO-NÚMERO/AÑO* en cada caso nuevo y ya tendríamos todo bien organizado.

85. https://chrome.google.com/webstore/detail/nimbus-screenshot-screen/bpconcjcammlapcogcnnelfmaeghhagj
86. http://www.httrack.com/
87. Herramientas de obtención de pruebas en Internet - https://ciberpatrulla.com/obtencion-pruebas-internet/

Presentación de las evidencias

Como ya hemos visto en la sección sobre la cadena de custodia, las evidencias tenemos que presentarlas en formato digital. Y para ello necesitamos soportes (CDs, DVDs, HHDs o SSDs y USBs), y en caso de necesitarlo, sobres para precintar y rotuladores permanentes. A mí me gusta poner mi firma y datos de identificación en los CDs.

Dependiendo del caso y del tamaño, usaremos unos u otros soportes de almacenamiento.

Crear un avatar

Introducción

En ocasiones vamos a necesitar disponer de un avatar para ocultar nuestra identidad real. Los motivos, para hacer esto, son diversos y legítimos. Ya hemos visto que para investigar dentro de canales cerrados, en Internet, necesitamos autorización judicial y actuar bajo la figura del agente encubierto informático, pero para investigar en canales abiertos y públicos no necesitamos autorización, pero sí necesitamos pasar desapercibidos.

La figura del agente de paisano tradicional, podemos trasladarla al mundo digital.

En Internet no existe ningún tipo de regulación en la que se hable de cuáles son los límites, dentro de sus funciones de prevención e investigación de los delitos, con los que debe regir una investigación dentro de canales públicos como son las redes sociales, donde no tiene ningún sentido que, como investigador, ponga mis datos personales y mi foto de perfil real.

Imagino que la jurisprudencia y alguna regulación futura, marcarán las pautas. De momento ya hay alguna sentencia sobre este tema, y lo deja bastante claro. Por ejemplo tenemos la Sentencia 39/2016 del Juzgado de lo Penal de Gijón[88]:

"*En las actuaciones dirigidas a la vigilancia, prevención y evitación de ilícitos en las redes informáticas cuya evidencia tiene lugar en fuentes abiertas en la web o canales no cerrados de comunicación, se viene sosteniendo que la ocultación de la condición de agente de la policía haciéndose pasar por un usuario más en la red, en principio no requiere*

88. Sentencia 39/2016 del Juzgado de lo Penal de Gijón - http://www.poderjudicial.es/stfls/TRIBUNALES%20SUPERIORES%20DE%20JUSTICIA/TSJ%20Asturias/DOCUMENTOS%20DE%20INTER%C3%89S/Jdo.%20Penal%20Gij%C3%B3n%206%20julio%202016.pdf

autorización judicial."

En Internet, los malos ocultan su identidad, y nosotros tenemos que aprender a hacerlo también para evitar poner en riesgo nuestro trabajo y a nosotros mismos.

En este capítulo, no te voy a hablar de navegar de forma anónima, sino de crear una identidad ficticia y que parezca real, y de cómo protegerte de terceros.

Ten en cuenta que navegar de forma anónima, por ejemplo utilizando Tor, puede dar información a terceros, e identificar nuestro navegador, viéndonos como usuarios sospechosos. Tor no lo usa mucha gente.

Vamos a ver cómo crear una identidad ficticia en un minuto; cómo ocultar tu IP; cómo cambiar la ubicación en la que te encuentras; cómo obtener números de teléfonos virtuales; y cómo navegar de forma segura por Internet.

Ocultar la IP

El primer paso que debemos realizar, como medida de protección, es ocultar nuestra IP para impedir ser rastreados o, incluso algo peor, ser atacados.

Para ello podemos usar algún servicio de VPN (Red Privada Virtual).

Lo ideal es usar un servicio de VPN que disponga IPs de España porque, si llegan a identificarnos, sería algo sospechoso que nuestra IP fuese China, de EEUU o de Bulgaria, ¿no crees?

Algunos servicios de pago, muy buenos, con IPs españolas son:

- https://nordvpn.com/es/
- https://www.expressvpn.com/es

- https://pro.cyberghostvpn.com/es_ES/
- https://www.goldenfrog.com/es/vyprvpn

También puedes usar (https://www.tunnelbear.com/) en su versión gratuita, la cual tiene IP española.

Si te da igual la ubicación de la IP puedes probar el plan gratuito de (https://protonvpn.com/), pertenece a Protonmail.

Otra opción es (https://hide.me/es/) que tiene un plan gratuito de hasta 2 GB.

Recuerda usar siempre la VPN para conectarte a todos tus servicios. En el momento que te conectes tan solo una vez, sin VPN, a tu cuenta de email o RRSS, lo más probable es que tu IP real quede registrada.

Identidad ficticia

Cuando tenemos que inventarnos un nombre, o nombre de usuario, o cualquier dato ficticio, y la imaginación no es nuestro fuerte, podemos recurrir a servicios online donde te facilitan esta labor.

Uno de los más conocidos es Fakenamegenerator.com[89].

Fakenamegenerator te genera un perfil con todos los datos necesarios para crear perfiles en redes sociales, como por ejemplo, nombre, dirección postal, nº de teléfono, email temporal, usuario y contraseña, tarjeta de crédito, símbolo del zodiaco, fecha de nacimiento, características físicas, altura, peso, etc.

Gracias a este servicio no tendremos que estrujarnos el cerebro pensando en inventarnos esos datos.

89. https://www.fakenamegenerator.com/

Entorno de trabajo virtual

Ya hemos visto qué es una máquina virtual y para qué podemos usarla. En este caso le vamos a dar otra utilidad, y es la de crear un entorno de trabajo exclusivo para nuestra identidad ficticia.

Podemos descargarnos una copia de Windows de prueba, preparada para usar en una máquina virtual, desde la página de Microsoft[90].

Con nuestra identidad virtual creada en Fakenamegenerator pasamos a crear un entorno de trabajo virtual, para aislar completamente nuestro sistema operativo nativo de todas las actuaciones que llevemos a cabo. Además, una vez que no necesitemos esta máquina virtual, solo tenemos que eliminarla y no quedará ni rastro de nuestra actividad en nuestro PC.

Vamos a utilizar los datos de nuestra identidad ficticia para crearnos la cuenta en el sistema operativo, de forma que no existan incongruencias entre nuestra identidad ficticia y los datos de usuario del Sistema Operativo.

Si en la identidad ficticia nos llamamos “Eddie” no tendría mucho sentido crear una cuenta de usuario llamada “Paco”.

También tendremos que instalar el navegador Chrome o Firefox, ya que en estos no vienen instalados por defecto.

Gestor de contraseñas

Te recomiendo que utilices un gestor de contraseñas. Es cierto que usar un gestor de contraseñas es como tener una caja fuerte, y eso tiene un riesgo, y es que, en el caso de que accedan a tu ordenador, estarás diciendo donde guardas todas tus contraseñas. Tendrás que valorar el nivel de riesgo al que te enfrentas para decidir si lo usas o no.

90. Obtener un entorno de desarrollo de Windows 10 - https://developer.microsoft.com/es-es/windows/downloads/virtual-machines

En nuestra labor vamos a utilizar contraseñas aleatorias y seguras, las cuales va a ser difícil recordar, y esta es la gran ventaja de los gestores de contraseñas.

Existen algunos servicios en la nube, pero si queremos darle un plus de seguridad, lo mejor es usar un programa de escritorio como KeePassXC[91].

Cambiar nuestra ubicación

Por diversos motivos es posible que necesitemos ocultar o cambiar nuestra ubicación en el navegador.

Los servicios de VPN nos permiten navegar cambiando nuestra IP real, siendo esta una capa importante de seguridad ante terceros, pero aun así no estamos cubiertos del todo.

A través del navegador se puede obtener nuestra ubicación exacta. Aunque por defecto tendrían que pedirnos permiso antes.

Para comprobar en Chrome cómo tenemos configurado la información de la ubicación que compartimos, puedes ir "*Configuración*" y, a continuación, "*Avanzada*". En la sección "*Privacidad y Seguridad*", haz clic en "*Configuración de contenido*" , y ahí podrás ver qué estás autorizando y qué no.

Si queremos cambiar la ubicación real en la que nos encontramos solo tenemos que instalar la extensión de Chrome Manual Geolocation[92], con la que podremos elegir la ubicación que queremos mostrar.

Una vez instalada, actívala, cambia la posición a donde quieras y entra en (https://html5demos.com/geo/), donde podrás comprobar cómo tu ubicación cambia según lo hayas configurado.

Con el paso de arriba ya tenemos cambiada nuestra ubicación por una ficticia

91. https://ssd.eff.org/es/module/c%C3%B3mo-usar-keepassxc
92. https://chrome.google.com/webstore/detail/manual-geolocation/jpiefjlgcjmciajdcinaejedejjfjgki

en nuestro PC, ¿pero qué pasa si necesitamos que haya congruencia entre nuestro PC y nuestro móvil?

Si por cualquier motivo necesitamos que la ubicación de nuestro PC y nuestro móvil sea la misma, podemos usar algunas apps que sirven para cambiarla:

Fake GPS Location Spoofer Free[93]

Fake GPS location[94]

Puedes buscar más en la Play Store, sólo tienes que poner *"GPS falsa"* en la caja de búsqueda.

Cuenta de email anónima

El siguiente paso es crear una cuenta de email (casi) anónima, en la que no dejemos ningún rastro que nos pueda identificar.

La idea no es crear una cuenta tipo Protonmail, ya que lo que queremos es crear un avatar creíble, y como te decía antes, usando TOR y Protonmail, igual levantamos sospechas.

La idea es crear una cuenta gratuita genérica, tipo Gmail, sin dejar rastros de nuestra IP o teléfono móvil de uso habitual, ni datos personales que nos puedan identificar (nombre, fecha nacimiento, etc.).

Podemos hacerlo en un sitio en el cual no utilicemos nuestra IP (un Wifi público), o a través de una VPN, al ser posible, con IP española.

Aviso: este método, en el momento de escribir este libro, funciona, pero, por motivos que desconozco, algunas veces pueden pedirte el número de teléfono.

93. https://play.google.com/store/apps/details?id=com.incorporateapps.fakegps.fre
94. https://play.google.com/store/apps/details?id=com.lexa.fakegps

Los pasos serían los siguientes:

1. Accedemos a Gmail con la opción del navegador Chrome "Nueva ventana de incógnito".

2. Entramos en "Crear cuenta"

3. Rellenamos los datos personales (ficticios) y le damos a siguiente.

4. En la siguiente ventana nos aparece la opción de introducir el móvil y un email alternativo, pero ahora nos aparece como datos opcionales.

Si no nos queda más remedio que usar un teléfono para activar el email, podemos usar números virtuales como Sonotel[95]. Este servicio tiene una prueba gratuita (siento decirte que para darte de alta aquí tienes que dar un número de teléfono). También podemos utilizar alguna aplicación de móvil como Hushed.com[96]. También existen servicios como el de Simore.com[97], en el que te venden adaptadores para agregar una segunda tarjeta SIM a tu móvil.

Existen dos servicios de email que no piden número de teléfono para registrarse, aunque no son tan conocidos, y pueden levantar sospechas. Estos servicios son mail.com[98] y gmx.es[99].

Como ves, es difícil registrarte en servicios sin dejar algún rastro de tu identidad, especialmente porque tarde o temprano te obligan a introducir un teléfono móvil. Lo que buscamos es crear un avatar lo más real posible, y eso nos impide el anonimato total.

Teléfono móvil

Ya hemos visto que podemos usar números de teléfono virtuales, o sistemas

95. https://sonetel.com/
96. https://hushed.com/
97. https://www.simore.com/es/
98. https://www.mail.com/mail/
99. https://www.gmx.es/mail/

para usar varias tarjetas SIMs. Incluso muchos modelos ya vienen con sistemas para trabajar con varias SIMs.

Para cerrar el círculo del avatar, debemos disponer de un teléfono móvil exclusivo para estas tareas, o algún sistema[100] que separe el teléfono móvil de trabajo del personal.

Cuentas en redes sociales

Crear un perfil ficticio en redes sociales tiene su complejidad. Si no quieres ser descubierto deberás ser creativo y detallista.

Para el registro, usaremos la cuenta de email creada en el paso anterior, y en el caso de que no nos quede más remedio que añadir un teléfono móvil, podemos usar el nº virtual contratado, aunque para el registro de RRSS no suele ser necesario añadir el nº de móvil (de momento).

Y ahora la pregunta del millón. ¿Qué fotos uso para mi perfil?

Si lo que queremos es crear una identidad ficticia no podemos usar nuestras propias imágenes, al menos que no nos identifiquen, ni nos ubiquen, ni tampoco coger imágenes de otros perfiles, primero, porque podría ser ilegal, y segundo, porque nos podrían cerrar la cuenta, y tiraremos todo el trabajo por la borda.

¿Entonces qué opciones te quedan?

La caracterización.

Te dejo una app muy buena, Faceapp.com[101] (ojo con la política de privacidad de esta app), aunque es posible que haya otras, u otros métodos. Sé creativo.

100. Cómo usar dos cuentas de WhatsApp en el mismo teléfono - https://www.xataka.com/basics/como-usar-dos-cuentas-de-whatsapp-en-el-mismo-telefono
101. https://www.faceapp.com/

Es conveniente eliminar los metadatos[102] a las imágenes que usemos, y aplicarles filtros, como el filtro espejo, este filtro dificulta las búsquedas inversas de imágenes en los buscadores, de las que te hablaré más adelante.

Antes de generar ningún tipo de contacto, es importante dar vida a nuestros perfiles con contenido, fotos y añadir amigos, de forma que no levantemos sospechas.

Si tenemos datos sobre qué gustos, ideología, edad, orientación sexual y aficiones tiene el investigado, es conveniente tenerlos en cuenta para crear un perfil lo más afín posible a él.

Un buen método de acercamiento es el de conseguir hacer amigos o seguidores de personas de su red social, de forma que sienta que somos alguien de cierta confianza.

Te dejo un buen artículo detallado de pasos que puedes dar en la creación de la cuenta (https://es.wikihow.com/crear-un-perfil-de-Facebook-falso).

102. Cómo eliminar el rastro de los archivos que compartes - https://computerhoy.com/paso-a-paso/software/como-eliminar-rastro-archivos-que-compartes-17847

Buscadores

Introducción

Google, Bing o Yahoo son buscadores que muestran los resultados de todo el contenido que indexan en Internet.

Utilizando las búsquedas avanzadas de dichos buscadores o algunos comandos específicos, podemos llegar a conseguir información bastante sorprendente.

Un error muy común es quedarse solo con los primeros resultados. Existen estudios[103] que dicen que las páginas web que aparecen a partir de la tercera página de resultados son como si no existieran para los usuarios que buscamos en Internet.

Para tener éxito en una búsqueda no puedes quedarte en los primeros 30 resultados, tienes que profundizar. En la siguiente sección te explicaré cómo funciona Google, el rey de los buscadores. Y verás que no todo está en Google, aunque esté en Internet.

Es muy importante tener en cuenta que no solo existe Google, aunque será el que más usemos, y que en ocasiones puede que un contenido haya sido borrado de Google y aún permanezca en otro buscador.

El funcionamiento de los buscadores es similar entre ellos, pero los algoritmos son diferentes, por lo que los resultados también lo son. Google te mostrará unos resultados y otros buscadores arrojarán resultados muy diferentes.

---

103. Si estás en la segunda página de Google no existes - https://www.apasionadosdelmarketing.es/si-estas-en-la-segunda-pagina-de-google-no-existes/

Este capítulo es algo largo, pero te aviso que es muy importante, especialmente la parte de Google y en especial un artículo de mi blog que te recomiendo en la siguiente sección.

En todos los años que he pasado con temas relacionados con Internet, si algo he aprendido es que, lo simple siempre es mejor.

Puedes tirarte semanas intentando poner en marcha un sofisticado script o aprendiendo a utilizar las decenas de funcionalidades de un gran software, o probando cada semana una nueva novedad que promete soluciones fantásticas y darte cuenta que, muchos de estos programas o scripts, utilizan los mismos buscadores que tú y, si hubieses hecho la búsqueda directamente, a mano, hubieses llegado a la misma conclusión y en mucho menos tiempo. Con esto no digo que haya que dejar de usar todos estos programas, pero es importante valorar cuál es el método más efectivo en cada caso.

Google

Por desgracia, no existe una herramienta que haga todo. ¿O sí?

Es probable que la primera idea que se te pase por la cabeza, a la hora de buscar algo en Internet, sea utilizar un buscador, probablemente el más usado, Google.

Google se ha convertido en el Rey de Internet. Todo pasa por sus manos.

¿Todo pasa por sus manos? La respuesta es: No. No podemos hacer OSINT solo con Google. En esta sección te voy a contar qué puedes hacer con Google y qué no.

¿Cómo funciona Google?

Todos conocemos Google, lo usamos a diario. ¿Pero sabemos cómo funciona?

Google es un **índice** de enlaces. Si Google desapareciera, Internet y sus webs

seguirían existiendo, aunque lo echaríamos bastante de menos.

Su funcionamiento se basa en recorrer Internet mediante sus robots[104] (arañas). Va pasando de una web a otra a través de los enlaces que contienen los sitios web, y de esa forma va añadiendo a su índice dichas URLs.

Google no almacena el contenido, pero sí una versión actual de la URL que ha añadido a su índice, la cual la guarda en su caché, de la que te hablaré más abajo.

¿Qué contenido indexa Google?

Google no solo indexa páginas webs.

Es cierto que, en los resultados de las búsquedas que hagas, te va a mostrar, principalmente, URLs a archivos web, es decir, HTML, PHP o ASP, pero Google es capaz de indexar todo tipo de archivos a su índice.

Esto es bueno tenerlo en cuenta para hacer búsquedas específicas de determinados archivos o dentro de ellos. Como, por ejemplo, buscar texto dentro de un DOC o un PDF.

Con el operador filetype:, puedes hacer que solo se muestren resultados de un tipo de archivo concreto en la Búsqueda de Google. Por ejemplo, si introduces "*filetype:doc Madrid*", sin las comillas, solo verás archivos DOC que contengan el término "Madrid".

Estos son los tipos de archivo que Google es capaz de indexar en su índice:

Adobe Flash (.swf)

Formato de documento portátil de Adobe (.pdf)

PostScript de Adobe (.ps)

104. Robot de Google - https://support.google.com/webmasters/answer/182072

Formato web de diseño de Autodesk (.dwf)

Google Earth (.kml, .kmz)

Formato de intercambio GPS (.gpx)

Hancom Hanword (.hwp)

HTML (.htm, .html y otras extensiones de archivos)

Microsoft Excel (.xls, .xlsx)

Microsoft PowerPoint (.ppt, .pptx)

Microsoft Word (.doc, .docx)

Presentaciones de OpenOffice (.odp)

Hojas de cálculo de OpenOffice (.ods)

Texto de OpenOffice (.odt)

Formato de texto enriquecido (.rtf)

Gráficos vectoriales escalables (.svg)

TeX/LaTeX (.tex)

Formato de texto (.txt, .text y otras extensiones de archivos), incluido el código fuente de los lenguajes de programación habituales:

Código fuente básico (.bas)

Código fuente C/C++ (.c, .cc, .cpp, .cxx, .h, .hpp)

Código fuente C# (.cs)

Código fuente Java (.java)

Código fuente Perl (.pl)

Código fuente Python (.py)

Lenguaje de marcas inalámbrico (.wml, .wap)

XML (.xml)

¿Qué contenido no puede indexar Google?

Google, aunque ya le gustaría, no puede con todo. Hay cosas que se le escapan. Aunque ya se ha encargado de que se le escape lo menos posible. ¿A qué me refiero?

Google no es capaz de indexar todos los contenidos de servicios que estén protegidos por contraseñas o sean privados.

Por ejemplo, tus emails, servicios como Dropbox, OneDrive, perfiles en redes sociales que tengan restringido el acceso, etc.

Cuando digo que Google se ha encargado de tener acceso a estos servicios, no me refiero a que pueda entrar a tus cuentas privadas, que no puede. Me refiero a que Google ha conseguido hacerse un gran hueco dentro de todos estos servicios, entre otros, con la prestación de los servicios como Gmail, Google Drive, Google +, Chrome, Google Analytics, y ya si ya hablamos de Android…

Caché de Google

Como te comentaba más arriba, Google guarda una versión en su caché[105] de todas las URLs que indexa.

La caché de Google tiene mucha importancia para nosotros. ¿Por qué?

105. Ver páginas web en caché en los resultados de la Búsqueda de Google - https://support.google.com/websearch/answer/1687222?hl=es

Porque podemos tener acceso a una copia de dicha URL con unos días de antigüedad.

En el caso de que accediendo a la URL original, no encontremos lo que estamos buscando porque haya desaparecido, la caché de Google nos muestra una versión más antigua de dicha URL, donde igual, dicho contenido sí aparece todavía.

El uso más habitual es cuando nos encontramos con que dicha URL ya no es accesible, o nos da error 404 (el contenido no se encuentra), o el contenido ha sido modificado.

Para acceder a la caché de Google se puede hacer de dos formas:

Mediante la pestaña que aparece al lado derecho del resultado de búsqueda, representada con un triángulo con el vértice hacia abajo, o utilizar este operador: escribe *"cache:"* delante de la dirección URL del sitio web que quieras. Ejemplo: (*cache:ciberpatrulla.com*)

En el resultado de la caché de google aparece la fecha en la que Google indexó dicho contenido.

¿Cómo impedir que Google indexe un contenido?

El propietario de un sitio web puede decirle a Google que no quiere que indexe su web o blog, y aunque no lo creas, Google hace caso, o al menos no lo muestra en sus resultados.

Pero, ¿por qué iba alguien a querer no aparecer en Google?

Pueden existir varios motivos por los que un propietario de un sitio web no quiera que su contenido aparezca en el índice de Google.

Puede querer ocultar datos personales o sensibles; puede querer ocultar contenido irrelevante; ocultar secciones sensibles del sitio; o como técnica

Es importante tener en cuenta que no todo lo que Google muestra de una web es todo el contenido existente de esta, puede haber más contenido oculto a Google, pero accesible si navegamos por la estructura de dicho sitio web.

¿Cómo se le da la orden a Google de que no indexe un contenido?

Existen dos formas de hacerlo:

1. Mediante el archivo robots.txt[106].

2. Mediante las metaetiqueta "robots[107]"

No voy a profundizar en cómo implementarlo, porque me saldría del objeto de este libro, si te interesa el tema, puedes buscar en San Google, pero sí quiero explicarte qué te puedes encontrar dentro del archivo robots.txt para que puedas interpretarlo y, de esta forma, saber si el propietario del sitio web ha querido ocultar URLs de su web.

Lo primero que tienes que hacer para acceder al archivo *robots.txt* es añadir el nombre de este archivo a la URL del dominio que te interese (ejemplo: https://nombrededominio.com/robots.txt). Prueba con cualquier dominio.

Lo normal es que todas las webs tengan este archivo, pero te puedes encontrar con alguna que no lo use.

Dentro del archivo *robots.txt* puedes encontrar las siguientes órdenes:

User-agent: *** (Hace referencia al buscador al que quieres dar la orden. En este caso, con el asterisco, estás haciendo referencia a todos los buscadores).

Disallow: /wp-admin/ (Con el comando *Disallow*, estás diciendo que los buscadores no indexen todo el contenido que hay dentro del directorio */wp-*

106. Cómo bloquear URLs con robots.txt - https://support.google.com/webmasters/answer/6062608?hl=es
107. Especificaciones de la metaetiqueta "robots" y de la cabecera HTTP "X-Robots-Tag" - https://developers.google.com/search/reference/robots_meta_tag

admin/).

Allow: /index.html (Con el comando *Allow*, estás diciendo que quieres que los buscadores indexen este contenido).

Accediendo al archivo *robots.txt* e interpretándose, podemos encontrar contenido que Google no muestra, pero sí existe.

Anuncios de Google

No viene de más recordar que Google vive de la publicidad (entre otras cosas), y que algunos de sus resultados, cuando hacemos una búsqueda, son anuncios publicitarios relacionados con nuestra búsqueda.

Lo normal es que estos no tengan ningún interés para lo que estamos buscando.

Estos se pueden diferenciar fácilmente del resto de resultados, ya que muestran un pequeño texto de "Anuncio" al lado de los mismos.

Posicionamiento en Google y penalizaciones

Cuando realizamos una búsqueda en Google, este nos devuelve un resultado, a veces acertado, otras no tanto.

¿Te has parado a pensar qué criterio usa Google para mostrarte un resultado y no otro?

Google utiliza un algoritmo de calificación del contenido que muestra los resultados basándose en la relevancia de los mismos, es decir, intenta que, el resultado de la búsqueda, sea lo más relevante posible en relación a lo que estás buscando. Para conseguir esto, Google tiene en cuenta muchos factores, puede que más de 200[108].

108. Los 200 factores que Google tiene en cuenta para posicionar tu página - https://www.quondos.com/factores-seo-posicionamiento-web-google/

En ocasiones, webs muy relevantes para tu búsqueda no van a salir en primeras posiciones.

Esto puede ser por varios motivos.

Porque sea una web nueva y Google aún no haya decidido que se merece salir en los primeros resultados o, puede ser, que dicha web haya sufrido una penalización de Google por no cumplir con sus directrices y la haya mandado al fondo de los resultados.

¿Por qué me cuentas todo este rollo Julián?

No quiero ser pesado, pero, lo que te quiero decir es, que no te quedes en los primeros resultados. Quizás lo que buscas no esté entre ellos, y se encuentre en páginas interiores de Google. A veces hay resultados relevantes escondidos en páginas interiores de los resultados de búsqueda.

Para evitar tener que pasar horas revisando resultados puedes usar la búsqueda avanzada de Google y operadores booleanos y sus combinaciones (Google Dorks), de esto te hablo en la siguiente sección.

Búsqueda avanzada de Google

Google cuenta con opciones avanzadas para realizar búsquedas.

Cuando la cantidad de resultados que nos muestra por una determinada búsqueda es muy grande, puede venirnos bien utilizar la búsqueda avanzada y las distintas posibilidades que nos ofrece este buscador.

A continuación, te dejo el acceso a guías de cómo buscar en Google y a su búsqueda avanzada, tanto de sitios webs como de imágenes:

- Cómo buscar en Google (Básico)[109]

109. https://support.google.com/websearch/answer/134479?hl=es&ref_topic=3081620

- Cómo buscar imágenes en Google (Básico)[110]
- Búsqueda avanzada de Sitios Web[111]
- Búsqueda avanzada de Imágenes[112]
- Filtrar los resultados de búsqueda[113]
- Búsqueda inversa de imágenes[114]

Acotar búsquedas en Google

Google admite algunos operadores para hacer búsquedas acotadas sobre el tema que nos interesa.

No añadas espacios entre el símbolo o la palabra y el término de búsqueda. La búsqueda *site:ciberpatrulla.com* funciona, pero la búsqueda *site: ciberpatrulla.com*, no.

Técnicas habituales de búsqueda

- **Excluir palabras** de la búsqueda: escribe "–" delante de la palabra que quieras excluir de la búsqueda. Por ejemplo: *gato grande -rueda*.
- Buscar una **concordancia exacta**: escribe la palabra o la frase que quieras encontrar, de forma exacta, entre comillas. Por ejemplo: *"blog sobre OSINT"*.
- Buscar mediante **comodines** o términos desconocidos: escribe "*" en la palabra o en la frase donde quieras incluir el marcador de posición. Por ejemplo: *"el * más caro de Madrid"*.
- Limitar la búsqueda a un **intervalo de números**: escribe ".." entre dos números. Por ejemplo: *coche €5000..€10000*.

110. https://support.google.com/websearch/answer/112511
111. https://www.google.es/advanced_search
112. https://www.google.es/advanced_image_search
113. https://support.google.com/websearch/answer/142143?hl=es&ref_topic=3081620
114. https://support.google.com/websearch/answer/1325808

- **Combinar** búsquedas: escribe "*OR*" entre las consultas de búsqueda. Por ejemplo: *dirección OR domicilio*.
- Buscar en **un sitio concreto**: escribe "*site:*" delante del sitio o del dominio en el que quieras buscar. Por ejemplo: *site:ciberpatrulla.com*.
- Buscar en **sitios web similares**: escribe "*related:*" delante de una dirección web que ya conozcas. Por ejemplo: *related:ciberpatrulla.com*.
- Ver la versión en **caché de Google** de un sitio web: escribe "*cache:*" delante de la dirección del sitio web.

Si quieres aprender como un experto a buscar en Google, tienes que leer mi artículo sobre búsquedas avanzadas en Google (https://ciberpatrulla.com/buscar-google/).

Buscar en modo incógnito

Google es muy cotilla, y está constantemente guardando información de todo lo que hacemos en su buscador.

En ocasiones y dependiendo de cómo configuremos el navegador, Google nos puede mostrar anuncios personalizados en base a nuestro historial de búsquedas, incluso resultados de búsqueda basados en usos anteriores del buscador.

Si necesitas que los resultados de las búsquedas sean los más naturales posibles, es conveniente que las realices con el modo incógnito del navegador y/o desautenticado. Revisa que no estés conectado a ninguna cuenta de Google mientras navegas.

Alertas de Google

Google dispone de un servicio de alertas llamado Google Alerts[115].

El servicio consiste en enviarte un email cada vez que encuentre resultados nuevos sobre un tema que tú le especifiques.

115. https://www.google.com/alerts

Por ejemplo, podemos usarlo para que nos avise cuando aparece en Google nuestro nombre y apellidos, o nuestros teléfono, o DNI, o los datos de otra persona, o cualquier dato que se nos ocurra. De esta forma no tendremos que hacer las búsquedas nosotros, este servicio lo hará automáticamente.

Google Trends

Google Trends[116] es otro servicio de Google, que en este caso da información de la tendencia que tiene determinada búsqueda.

Por ejemplo, si queremos saber qué tendencia tiene en Google la búsqueda "Indonesia", nos mostrará una gráfica del número de búsquedas para ese término.

Haciendo inteligencia con esta información podemos llegar a obtener algunas conclusiones sobre determinados hechos.

Como ves Google tiene un gran potencial para hacer OSINT, aunque también tiene sus limitaciones, que no son pocas.

Otros buscadores

Bing

Ya sabes lo que opino de Google, que va a ser el buscador que más uses con diferencia, pero existen otros buscadores, y algunos con opciones que Google no tiene y muy buenas.

Por ejemplo Bing[117], el buscador de Microsoft, nos da la posibilidad de averiguar cuántos sitios web se encuentran alojados bajo una misma IP.

El buscador Bing no tiene tanta flexibilidad como Google para hacer búsquedas, pero sí tiene algo muy útil, y es este operador que nos muestra todos los dominios alojados en una misma IP: *ip:xxx.xx.xx.xx*

116. https://trends.google.es/trends/
117. https://www.bing.com/

Como veremos en el capítulo sobre cómo hacer OSINT en sitios web, este operador tiene mucho valor para nosotros, así que, apúntatelo.

Buscadores alternativos a Google

Podría hacer un capítulo entero solo hablando de todos los buscadores que existen, y qué hace cada uno, pero no creo que sea práctico.

Te dejo un enlace a Inteltechniques (https://inteltechniques.com/osint/menu.search.html) donde podrás hacer búsquedas en varios buscadores a la vez. Puedes probar algunos operadores y combinaciones de estos, aunque no te funcionarán en todos.

También existe un buscador que te facilita mucho buscar en varios a la vez, se llama Instya (http://www.instya.com/).

Buscadores especializados

Además de los típicos buscadores genéricos, existen multitud de buscadores muy específicos para determinados objetivos.

Estos son algunos de los buscadores especializados:

Shodan (https://www.shodan.io/): ayuda a localizar diversas tecnologías incluyendo webcams, impresoras, dispositivos VoIP y routers, entre otras cosas.

NameCHK (https://namechk.com): es una herramienta que permite comprobar si un nombre de usuario está disponible en multitud de servicios online.

Tineye (https://www.tineye.com): es un servicio de búsqueda inversa de imágenes. Añadiendo una imagen a este servicio nos muestra si esta imagen se encuentra en algún sitio de Internet.

Pipl (https://pipl.com): en base a diferentes criterios como nombres,

direcciones de correo o teléfonos, estos buscadores buscarán en bases de datos de Internet si existen coincidencias.

Páginas blancas (http://www.paginasblancas.es/): las páginas blancas son un clásico que no debes dejar de lado. Aportan mucha información.

Buscadores personalizados

Existe una manera de optimizar las búsquedas de forma que nos ahorraremos tiempo, buscando en varios servicios a la vez, y pudiendo elegirlos a nuestro gusto y necesidades.

Google nos da la opción de crear buscadores personalizados. Puedes crearte tu propio buscador de Google personalizado para que haga búsquedas en los sitios que tú prefieras y no lo haga en toda la web.

Por ejemplo este buscador personalizado[118] busca a la vez en varias redes sociales, excluyendo el resto de webs de Internet.

Para crear un buscador personalizado solo tienes que entrar aquí (https://cse.google.com/cse/). El proceso es muy sencillo.

Te dejo un vídeo donde explica cómo crearlo y qué utilidades tiene (https://youtu.be/B6LSmsJ4QhI).

118. https://cse.google.com/cse?cx=001580308195336108602:oyrkxatrfyq&q=palabra%20a%20buscar&oq=palabra%20a%20buscar&gs_l=partner-generic.12...127617.130896.1.132258.0.0.0.0.0.0.0.0..0.0.gsnos%2Cn%3D13...0.3264j1064174j15..1ac.1.25.partner-generic..0.0.0.#

Archivo Web

Introducción

Internet tiene una peculiaridad, y es que, el contenido que se publica es muy difícil de eliminar, incluso si se elimina la fuente original.

Si tienes un blog o un perfil social y decides en algún momento dar de baja dichos servicios o borrar determinado contenido, es muy probable que, ese contenido, haya sido indexado por servicios que se dedican a archivar todo el contenido de la web, unos de forma manual y otros automáticamente.

¿Por qué son importantes estos servicios a nivel OSINT?

Los archivo web son una fuente muy importante para recuperar contenido que ha sido eliminado, y no solo eso, además nos permiten "certificar" que dicho contenido es el que aparece en el archivo. Lo pongo entre comillas, porque no tengo claro que podamos incluirlo como un tercero de confianza para certificar contenido de Internet, pero sí estoy seguro que aporta valor probatorio a la hora de presentar una evidencia.

Internet Archive

Internet Archive (https://archive.org/index.php) es una biblioteca digital sin ánimo de lucro, cuyos objetivos son guardar una copia de la totalidad del contenido indexable de internet. El objetivo es como el de cualquier biblioteca, que el contenido perdure y sea accesible.

Qué contenido almacena Internet Archive

Podemos encontrar distintas versiones de la misma página web de forma

cronológica. Podríamos hacer un viaje al pasado y ver la evolución de un sitio web a lo largo del tiempo.

Internet Archive es capaz de guardar de forma indefinida páginas web y documentos que han desaparecido de la fuente original.

Cómo guarda el contenido Internet Archive

El contenido de Internet es añadido a la biblioteca de forma automática mediante los bots del propio sistema, que rastrean Internet en busca de contenido nuevo. Además dispone de un formulario para enviar contenido de forma manual por parte de cualquier usuario.

Cómo hacer las consultas en Internet Archive

Para consultar el contenido que nos interesa solo tenemos que copiar y pegar la URL del mismo en la caja de búsqueda de Internet Archive. Si tiene contenido almacenado de dicha URL te mostrará en un calendario todas las capturas que ha hecho de esa URL a lo largo del tiempo en sus distintas versiones.

Si te creas una cuenta de usuario podrás subir contenido, almacenar tus favoritos y realizar colecciones de contenidos.

Es una herramienta que estoy seguro que vas a utilizar mucho.

Puedes usar los enlaces directos de Aware-Online (https://aware-online.com/academy/osint-tools/onderzoek-naar-internet-archieven/) que te facilitarán las búsquedas.

Es importante que tengas en cuenta que las páginas que almacena Internet Archive pueden ser eliminadas[119] por sus titulares. Es importante que si vas a utilizar una URL almacenada en este servicio como evidencia, tomes las

119. Cómo eliminar una web de archive.org - https://www.apasionadosdelmarketing.es/como-eliminar-una-web-de-archive-org/

correspondientes capturas y actúes conforme a lo que ya hemos visto sobre las evidencias, porque si solo aportas la URL, corres el riesgo de que el contenido sea eliminado de dicho servicio.

En el caso de no tener éxito con Internet Archive puedes probar con otra alternativa, no tan conocida, pero que pueden salvarte del apuro: (http://archive.is/).

Webs

Introducción

En este capítulo voy a hablarte de las diferentes opciones de las que dispones para identificar al administrador de un sitio web. En muchas ocasiones te vas a encontrar con sitios web que ocultan todo tipo de datos personales con el objetivo de no ser identificados. En ocasiones va a ser por privacidad y, en otras, porque saben que están cometiendo actos ilegales.

Sitio Web

En esta sección vamos a ver qué opciones tenemos para identificar al administrador de un sitio web dentro del contenido del propio sitio.

Aviso legal

Suponiendo que el sitio web que estamos investigando tenga todo adecuado a la legislación, el primer sitio donde podemos dirigirnos es a la sección *Aviso Legal*. La LSSI[120] establece la obligación de que todo particular con un sitio web, que preste servicios que den lugar a una contratación o venta on-line, o reciba algún beneficio económico directo o indirecto, está obligado a identificarse, reflejando el nombre o razón social, domicilio y email. La sección de *Aviso Legal* suele ser accesible mediante un enlace en el pie de página de los sitios web, junto con las *Políticas de Privacidad* y las *Políticas de Cookies*, las cuales también podemos revisar por si aportan algún dato más.

120. LSSI - Obligaciones de los ciudadanos - http://www.lssi.gob.es/ciudadanos/Paginas/ciudadanos.aspx

Formularios de contacto

Otra sección que podemos revisar es la de *Contacto* o *Quiénes somos*. En muchas ocasiones esta sección solo dispone de un formulario de contacto, pero a veces puede mostrarnos la dirección de email o algún otro dato de interés. Igualmente, en el caso de que lo creamos pertinente, podemos enviar un email mediante ingeniería social, utilizando este formulario. Si tenemos suerte y nos contesta, obtendremos la dirección de email desde la que recibimos la respuesta.

Documentos alojados

Ya hemos visto que no todo lo que está visible es lo que se encuentra en Internet. En un sitio web pasa lo mismo. Podemos buscar documentos (PDF, DOC, PPT) dentro del sitio web, que, a simple vista, no están visibles.

Para localizar este tipo de documentos podemos usar combinaciones de operadores para buscar en Google, como por ejemplo:

site:dominio.com filetype:pdf

Esta búsqueda nos devolverá todos los archivos PDF alojados en dicho sitio web.

¿Qué podemos hacer con estos archivos?

En muchas ocasiones este tipo de archivos contienen metadatos[121], firmas o datos personales. Igualmente, mediante la propia lectura del documento podemos obtener información de interés. También podemos analizar los metadatos de dicho archivo utilizando herramientas como (http://exif.regex.info/exif.cgi). Con el análisis de los metadatos podemos obtener diversa información, como autor del documento y fecha de creación.

121. Definición de Metadatos - https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Archivo_electronico/pae_Metadatos.html#.W2vzeNgzZaY

También podemos automatizar este proceso con la herramienta FOCA[122] (Fingerprinting Organizations with Collected Archives). Se trata de una herramienta que encuentra metadatos e información oculta en los documentos que examina. Los documentos los busca utilizando los buscadores Google, Bing y DuckDuckGo. Antes de descargar el fichero realiza un análisis completo de la información descubierta a través de la URL. También existe la posibilidad de añadir ficheros locales para extraer la información EXIF de archivos gráficos.

Te dejo una pequeña guía de uso[123] y un vídeo tutorial (https://www.youtube.com/watch?v=PK1ECI0gAV0).

Imágenes y vídeos

Las imágenes y vídeos alojados en un sitio web pueden aportarnos información, además de la propia información del propio contenido que estamos visualizando, la que podemos extraer de los metadatos. Las imágenes y los vídeos tienen una peculiaridad, y es que pueden llegar a guardar en los metadatos información del dispositivo desde donde se obtuvo y, en algunos casos, hasta la geolocalización, en el caso de que el dispositivo disponga de ella y la tenga activada.

Analizar el sitio completo

Ya hemos visto cómo analizar un sitio web de forma online, aunque es cómodo, tiene sus limitaciones, ya que encontrar todo el contenido nos puede llevar mucho tiempo. Disponer del sitio web en local nos facilita la exploración.

Podemos analizar un sitio web de forma completa descargándolo en nuestro PC. Para ello podemos usar herramientas como (http://www.httrack.com/). Una vez descargado obtendremos la web completa con toda la estructura de

122. FOCA - https://elevenpaths.com/es/labstools/foca-2/index.html
123. Rastreando ubicaciones reales en los metadatos de las fotografías con FOCA - https://blog.elevenpaths.com/2016/05/rastreando-ubicaciones-reales-en-los.html

directorios, y con todos los archivos.

URLs eliminadas

Un problema con el que nos podemos encontrar es con que la URL a la que queremos acceder haya sido eliminada, o que el contenido que estamos buscando ha sido modificado. Si necesitamos acceder a versiones anteriores de una página web o recuperar un contenido eliminado podemos usar Internet Archive (https://archive.org/index.php) como vimos en el capítulo anterior, o podemos utilizar la opción de visualizar la caché de Google, como vimos en esta sección.

Texto plagiado

En ocasiones los administradores de sitios web disponen de más de un sitio, e incluso, pueden llegar a utilizar los mismos artículos o partes de ellos para generar contenido en los otros sitios. Igualmente pueden haber compartido dicho texto en redes sociales.

Utilizando los operadores de Google podemos localizar contenido plagiado o compartido en otros sitios. Para ello podemos usar búsquedas de este tipo:

Búsqueda en todo Internet: "*texto que queremos encontrar en otros sitios*"

Búsqueda en una Red Social en concreto: *site:twitter.com* "*texto que queremos encontrar en otros sitios*"

Con estas búsquedas, introduciendo el texto entre comillas, le decimos a Google que busque el texto exacto en otros sitios de Internet.

Whois

Hasta hace poco tiempo, realizando una consulta Whois a la base de datos donde se registran los datos de los titulares de los dominios, podíamos

obtener bastante información de los titulares de los mismos, salvo que esta consulta se encontrara oculta, opción que algunos administradores contratan con las empresas de intermediación para proteger la privacidad de sus datos personales.

Con la llegada del nuevo Reglamento General de Protección de Datos[124] las cosas han cambiado, y las consultas Whois a las bases de datos de titulares de dominios ya no muestran mucha información sobre datos personales, por lo que las cosas se complican para identificar a los titulares de las páginas web. Aun así te enseñaré algunos servicios para ver los históricos de dichas bases de datos, donde podremos encontrar información de interés.

Para hacer este tipo de consulta podemos utilizar alguna de los servicios online que existen para ello. Como por ejemplo (https://whois.icann.org).

Tenemos que tener en cuenta la extensión del dominio. Por ejemplo si es un *.es* debemos hacer la consulta en una base de datos específica (http://www.dominios.es/dominios/).

Como te decía antes, un método que podemos usar para seguir obteniendo información de interés cuando usamos el Whois, es usar los históricos. Existen registros de los cambios que ha sufrido un dominio en la base de datos de los registrantes, de forma que no nos mostrará información actual, pero sí información de los cambios de titular o datos de contacto. Estos datos nos pueden ayudar para continuar con la investigación.

Si queremos ver el historial de estos cambios podemos usar servicios como los de (https://domainbigdata.com/), (https://whoisology.com) o (https://www.whoxy.com/). Otro servicio bastante bueno es (https://community.riskiq.com/home), aunque hay que registrarse, te aseguro que merece la pena.

124. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). - http://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Si tienes problemas para identificar en la consulta Whois la empresa de alojamiento web (Hosting) donde se encuentra alojada el dominio, puedes usar este servicio (https://www.whoishostingthis.com/), el cual te dirá en qué empresa se encuentra alojado. Saber la empresa que aloja dicha web nos servirá para ponernos en contacto con ella en el caso de necesitar requerir información del titular de dicha web.

Consulta Whois inversa

Hacer una consulta Whois está muy bien si queremos saber la información sobre un solo dominio.

¿Pero qué pasa si queremos saber todos los dominios asociados a una cuenta de email, a un nombre, un número de teléfono o a personas con cuentas de email corporativas que tienen dominios registrados?

Ahora verás cómo conseguir esta información fácilmente.

Para conseguir esto vamos a usar un servicio de consulta inversa de Whois (https://viewdns.info/). Entre todas sus opciones se encuentra una para este cometido. Por ejemplo, si queremos saber en cuántos dominios se usa una cuenta de email concreta o un nombre concreto, solo tenemos que buscarlo aquí (http://viewdns.info/reversewhois/).

Se nos puede dar el caso de que no tengamos los datos completos. Por ejemplo, que solo dispongamos del dominio del email corporativo, o de los apellidos, sin el nombre. Para solucionar esto podemos usar comodines (**apellidos* o **@dominio.com*) de esta forma nos mostrará todas las coincidencias con esos apellidos, o todos los dominios asociados a cuentas de email corporativas.

Otro servicio online para hacer consultas Whois inversas es (https://www.whoxy.com/reverse-whois/).

En un artículo de Ciberpatrulla te explico cómo interpretar el resultado de la

consulta Whois (https://ciberpatrulla.com/whois-osint/).

IP/DNS

Todos los nombres de dominio, cuando realizamos una petición desde nuestro navegador, se transforman, de forma invisible para nosotros, en una IP. Por ejemplo Google, en el momento de escribir este libro, tiene asignada la IP: 172.217.17.3. Esta transformación la realizan los DNS[125] (Domain Name Server).

Cuando hacemos una petición en nuestro navegador escribiendo, por ejemplo, Google.com en la barra de direcciones, los ISP realizan una consulta DNS[126] para solicitar los servidores de nombres asociados con el dominio que hemos solicitado. Todo este proceso es invisible para nosotros. Si no existieran los DNS, tendríamos que escribir la IP para llegar a Google.

En realidad los nombres de dominio se utilizan para simplificar el acceso a sitios web, aunque no serían necesarios, porque con solo disponer de la IP podríamos acceder a ellos. Si utilizas la IP de Google 172.217.17.3, podrás comprobar que te lleva al buscador sin haber usado el dominio.

De forma muy genérica, todo servidor que aloja páginas web tiene asignada una IP. Estas páginas web pueden estar en un servidor dedicado para ellas solas o compartirlo con otras páginas web. Dentro de un mismo servidor, puede haber alojados decenas de sitios web, los cuales pueden pertenecer al mismo titular o no. Cuando hay más de un titular compartiendo servidor, se le llama *Servidor Compartido*[127], y cuando es usado por un solo titular, se le llama *Servidor Dedicado*[128].

¿Qué pasa si dentro del servidor hay más de un sitio web con la misma

125. Cómo funciona el DNS - https://blog.smaldone.com.ar/2006/12/05/como-funciona-el-dns/
126. Cómo se dirige el tráfico de Internet a su sitio web o aplicación web - https://docs.aws.amazon.com/es_es/Route53/latest/DeveloperGuide/welcome-dns-service.html
127. Alojamiento compartido - https://es.wikipedia.org/wiki/Alojamiento_compartido
128. Servicio de alojamiento dedicado - https://es.wikipedia.org/wiki/Servicio_de_alojamiento_dedicado

IP?

Al entrar mediante la IP, lo normal es que nos muestre la primera página configurada en ese servidor. Pero eso no quiere decir que sea la única web que hay dentro.

¿Cómo se consigue la IP de un servidor web?

Para saber la IP del servidor donde se encuentra alojado el sitio web podemos usar varios métodos. Podemos utilizar herramientas de nuestro propio PC, como indica este artículo (https://www.solvetic.com/tutoriales/article/4397-como-conocer-direccion-ip-pagina-web/), o podemos utilizar servicios online como este (https://viewdns.info/reverseip/).

¿Cómo se consiguen los DNS?

Para saber que DNS está utilizando un dominio podemos usar servicios online como este (https://viewdns.info/dnsrecord/).

¿Qué información podemos obtener con la IP o con los DNS?

Una vez que hemos obtenido la IP podemos utilizarla para realizar búsquedas inversas, como por ejemplo buscar qué otros dominios usan la misma IP. Esto podemos consultarlo utilizando el buscador Bing mediante el operador *ip: (ip:xxx.xxx.xx.x)*. También podemos usar servicios online como (https://dnslytics.com/reverse-ip).

Existe un servicio online (https://securitytrails.com/) que nos da mucha información, y en concreto, cuando arroja el resultado buscado por un dominio, en el bloque "*NS Records*", haciendo clic en los números que aparecen al lado de los DNS, nos mostrará todos los dominios que usan estos DNS, y que por lo tanto comparten servidor.

Es importante tener en cuenta que compartir servidor no quiere decir que dichas webs sean del mismo titular. Habría que analizar cada dominio y valorar si guardan relación con el investigado. En la siguiente sección te

cuento un método que podemos utilizar para conseguir encontrar otros sitios web relacionados con el investigado.

¿Qué sucede si la web que investigamos usa un CDN[129]?

Muchos administradores web utilizan servicios de CDN en sus proyectos web, esto les reporta muchos beneficios, sobre todo en cuanto a velocidad y rendimiento. Un ejemplo de este tipo de redes CDN es CloudFlare[130].

Uno de los "beneficios" en cuanto a criterios de seguridad se refiere que aporta utilizar un CDN es que, al situarse delante del servidor donde tenemos alojado el sitio web, la IP que muestra es la suya y no la de nuestro servidor web, por lo que oculta la IP real. Esto es beneficioso para evitar ataques, pero perjudicial si queremos averiguar la IP real para llevar a cabo una investigación.

Podemos utilizar algunos métodos y herramientas para averiguar la IP real de un sitio si se encuentra oculto detrás de un CDN, como por ejemplo: Crimeflare (http://www.crimeflare.com:82/cfs.html).

Además te dejo un artículo con varios métodos para intentar descubrir la IP real (https://backtrackacademy.com/articulo/como-detectar-la-ip-real-de-un-sitio-en-cloudflare).

Tecnologías usadas

Descubrir qué tecnologías utiliza un sitio web puede abrirnos nuevos caminos de investigación. En la actualidad, la mayoría de los sitios web utilizan sistemas de gestión de contenidos (CMS), como Wordpress[131] o Joomla[132], los cuales utilizan a su vez plugins de terceros para ampliar las

129. ¿Qué es un CDN y cómo utilizarlo en una Web de WordPress? - https://www.webempresa.com/blog/cdn-wordpress.html
130. https://www.cloudflare.com/es-es/
131. https://es.wikipedia.org/wiki/WordPress
132. https://es.wikipedia.org/wiki/Joomla

funcionalidades que tienen por defecto estos sitios.

Averiguar qué gestor de contenidos y qué plugins utiliza un sitio web puede servirnos para encontrar asociaciones con otros sitios web pertenecientes al mismo titular. En el caso de que un mismo administrador gestione varios sitios web de su propiedad, lo normal es que utilice plataformas y plugins similares.

Igualmente podemos encontrar la utilización de servicios de plataformas externas, como por ejemplo, sistemas de email marketing o plugins de pago, los cuales, para ser usados, han tenido que registrarse en el servicio o comprar el plugin, por lo que nos permitiría disponer de otra fuente de donde solicitar información, mediante el requerimiento a estas empresas de los datos personales del titular.

Podemos usar esta herramienta online para obtener esta información (https://builtwith.com/).

Código fuente

Visualizar el código fuente de un sitio web nos puede facilitar información que a simple vista está oculta.

Por ejemplo, podemos encontrar información de interés en los nombres de las imágenes; en las etiquetas html[133] de las imágenes (alt y tittle); en las etiquetas de los enlaces (title); y en las etiquetas de información del sitio, por poner algunos ejemplos.

133. Alt y Title – Diferencias y Obligaciones - https://ayudawp.com/alt-y-title-diferencias-y-obligaciones/

Códigos de seguimiento

Google Analytics

Un dato de mucho interés para nosotros dentro del código fuente es el código de Google Analytics. Los administradores de sitios web usamos sistemas de estadísticas para saber cuántos visitantes tenemos, entre otras cosas. Uno de los sistemas de estadísticas más populares es el de Google. Para poder obtener las estadísticas de un sitio web mediante este sistema se añade al código del sitio un código de seguimiento que facilita Google.

¿Cómo se encuentra el código de Google Analytics?

En la sección anterior hemos visto cómo analizar qué tecnologías usa un sitio web, y entre ellas nos puede mostrar que usa Google Analytics. Si un sitio web utiliza Google Analytics, el código de dicho sistema se muestra en algún lugar del código fuente de un sitio web. Solo tenemos que entrar en el código fuente y buscar un código parecido a este:

"*<script async src="https://www.googletagmanager.com/gtag/js?id=**UA-117266785-1**"></script> <script>window.dataLayer = window.dataLayer || []; function gtag(){dataLayer.push(arguments);} gtag('js', new Date()); gtag('config', '**UA-117266785-1**');</script>*"

Y buscar la ID de seguimiento, que en el ejemplo es: **UA-117266785**.

El número que va después del último guion hace referencia al número de orden asignado a dicho sitio web al crear el código de seguimiento, es decir, si tenemos una cuenta de Google Analytics, y añadimos un sitio web para seguir las estadísticas, el sistema asigna un número a ese sitio web, en este caso el nº 1, y según vayamos añadiendo más sitios web, nos irá asignando un

número de orden (2, 3, 4…), por lo tanto, teniendo en cuenta este detalle, si el código de Google Analytics muestra algo así (-8), quiere decir que ese código de seguimiento es usado por al menos 8 sitios web.

Google Adsense

Otro código que tenemos que tener en cuenta es el de Google Adsense (la plataforma de publicidad para webmasters de Google). Dicha plataforma facilita a los webmasters incluir publicidad en sus sitios web a cambio de una remuneración por clics en los banners. Para mostrar los banners publicitarios en tu sitio web tienes que incluir un código que te facilita la plataforma y, al igual que con Google Analytics, dicho código dispone de una ID asociada a una cuenta de Adsense. Los webmasters suelen usar una misma cuenta de Adsense para todos sus sitios web, por lo que realizando una búsqueda inversa de dicho código, sabremos de cuántos sitios web es titular o administrador.

Antes de entrar en detalles sobre este código de seguimiento, quiero señalar que, para darse de alta en Google Adsense hay que dar datos de facturación reales, por lo que si detectamos en un sitio web que utiliza esta plataforma, una forma de obtener los datos del titular es mediante el requerimiento a Google de esta información.

El código que debemos buscar es similar al siguiente, siendo la ID el valor marcado en negrita **ca-pub-123456789**:

*<script async src="http://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js"></script> <Script> (adsbygoogle = window.adsbygoogle || []).push({ google_ad_client: "**ca-pub-123456789**", enable_page_level_ads: true }); </script>*

Para facilitarte el trabajo puedes usar algunos servicios online que harán esta búsqueda por ti. Como por ejemplo (https://www.sitesleuth.io/) o (http://

pub-db.com/), aunque con este último tienes que tener en cuenta que guarda un registro de las consultas y las hace públicas, pudiendo levantar sospechas al investigado si detecta que se está analizando su sitio web.

Aquí te he puesto algunos de los ejemplos del potencial que tiene el estudio del código fuente de un sitio web, pero va a depender del sitio web, porque cada uno tendrá su peculiaridad.

Si queremos explorar otras opciones de búsqueda podemos usar otro tipo de buscadores para ello, como por ejemplo (https://publicwww.com/).

Truco: podemos usar (https://archive.org/index.php) para buscar antiguas versiones de una web y buscar códigos de seguimiento antiguos.

Correlación de dominios

En esta sección vamos a ver cómo correlacionar todos los nombres de dominio que pueden tener relación de una única persona u organización de nuestro interés. Para ello buscaremos posibles subdominios relacionados con el dominio principal, y también dominios, que sin tener relación con el dominio principal, pueden pertenecer a la misma persona u organización.

Subdominios

Los subdominios o dominios relacionados pueden ser de mucha importancia ya que, si bien el dominio principal puede estar muy protegido, con todas las medidas de ocultación, es posible que en los subdominios o webs relacionadas haya bajado la guardia, y sea en estos donde podamos encontrar información de interés.

Podemos encontrar subdominios de un sitio web usando algunos Google Dorks, como por ejemplo:

site:dominio.com (mostrará todas las URLs del dominio).

site:.dominio.com* (mostrará todos los subdominios indexados y todas las URLs de estos).

site:.dominio.com -www* (mostrará todos los subdominios indexados, excepto el subdominio *www.)*

Estos operadores no funcionan en todos los buscadores, pero el operador *site:dominio.com* suele funcionar en bastantes, por lo que te recomiendo que busques en más buscadores y no te quedes solo en Google.

También podemos usar servicios online como (https://findsubdomains.com/). Este servicio nos mostrará todos los subdominios de forma sencilla, y sin ruido.

Dominios relacionados

Encontrar dominios relacionados es algo más complejo que encontrar subdominios. No existe una lógica en la que basarnos para encontrarlos. Para encontrar dominios relacionados podemos usar búsquedas inversas partiendo de algún dato del que dispongamos o hayamos encontrado en las consultas Whois, como por ejemplo una dirección de email.

Para realizar este tipo de búsqueda podemos utilizar servicios como (https://viewdns.info/reversewhois/) donde, a partir del nombre o email que dispongamos nos dirá si existen más dominios con esos datos.

En el caso de encontrar dominios relacionados, podemos realizar de nuevo la búsqueda de subdominios de los mismos, de esta forma aumentaremos las opciones de encontrar información.

Herramientas SEO

Otra fuente de obtención de información son las herramientas de análisis

SEO[134] (Search Engine Optimization). Las cuales se utilizan para estudios relacionados con el posicionamiento de páginas web en el ranking de los buscadores.

Estas herramientas pueden darnos información muy útil para nuestra investigación, por ejemplo, podemos saber desde qué webs están enlazando a dicho sitio, y analizar dichos sitios web por si guardan algún tipo de relación; podemos ver qué otros sitios web están catalogados en la misma temática, y guardan relación estrecha con este, por si queremos ampliar la investigación a otros sitios similares por algún motivo; podemos obtener información sobre la popularidad del sitio web y cuantas visitas tiene, que nos puede dar una perspectiva de la influencia que puede tener dicho sitio, incluso, la procedencia de estas visitas, que nos puede servir para analizar estas fuentes, como por ejemplo si la procedencia de las visitas es de redes sociales, pudiendo investigar de qué perfiles sociales están enlazando a dicho sitio web y si estos tienen relación directa con él.

Te dejo algunos de estos servicios:

- SimilarWeb (https://www.similarweb.com):
- Moz Link Explorer (https://moz.com/link-explorer)
- SEMRush (https://www.semrush.com)
- Moonsearch (http://moonsearch.com)
- Keyhole (https://keyhole.co/)

Extraer enlaces

Analizar los enlaces dentro de un sitio web nos puede dar información relevante, no solo porque nos llevarán a otras partes del sitio web para

134. Posicionamiento en buscadores - https://es.wikipedia.org/wiki/Posicionamiento_en_buscadores

analizar sino, a otros sitios web externos o a cuentas de redes sociales asociadas al sitio web.

Un detalle importante puede aparecer en cualquier página del sitio web. Podemos navegar por la página web e ir haciendo clic en cada enlace que veamos, pero este método puede hacernos pasar algún enlace por alto. Para facilitarnos esta labor existe una extensión de Chrome que nos extrae todos los enlaces de la página que estamos visualizando, la extensión es Link Grabber[135].

Si lo que necesitamos es obtener todos los enlaces de un sitio web completo podemos utilizar una herramienta gratuita, algo antigua, y con un sitio web que asusta un poco, pero que funciona perfectamente. La herramienta se llama Xenu (http://home.snafu.de/tilman/xenulink.html).

Emails del dominio

La mayoría de los sitios web disponen de cuentas de emails asociadas a sus respectivos dominios. En el caso de que la búsqueda dentro del sitio web no haya sido fructífera en este aspecto, podemos utilizar diversos métodos y herramientas que nos pueden sugerir posibles cuentas de email asociadas a un dominio concreto.

Aquí te dejo algunas de estas herramientas:

-**Hunter** (https://hunter.io/) dispone de un buscador de direcciones de email de diversas empresas.

-**Email Permutator** (http://metricsparrow.com/toolkit/email-permutator/) dispone de un formulario en el que introduciendo un nombre y un dominio te sugiere diversas combinaciones de posibles cuentas de email.

-**Email-Format** (https://email-format.com/) muestra ejemplos de cómo

135. https://chrome.google.com/webstore/detail/link-grabber/caodelkhipncidmoebgbbeemedohcdma

generan de forma automática las cuentas de email corporativas de muchas empresas, sirve para dar ideas de cómo buscar una posible cuenta de email.

-The Harvester (https://github.com/laramies/theHarvester) es una herramienta que, entre otras opciones, busca emails relacionados con un dominio en concreto. Dicha herramienta viene instalada en los sistemas operativos Buscador y Kali Linux.

Te estarás preguntando cómo vas a saber cuál de todas esas cuentas puede ser la válida. No te preocupes, no es necesario que envíes un email a todas esas cuentas preguntando si hay alguien al otro lado.

Una vez que hemos obtenido las posibles cuentas de email asociadas al dominio, podemos verificarlas y comprobar que dicha cuenta existe y es 100% funcional. Para ello podemos usar herramientas online como (https://tools.verifyemailaddress.io/) o (https://hunter.io/email-verifier).

Certificados SSL

Los certificados SSL[136] pueden servirnos para obtener información del titular de un sitio web.

SSL (Secure Sockets Layer), es una tecnología para mantener segura una conexión a Internet y para proteger cualquier información confidencial que se envía entre dos sistemas (por ejemplo, un sitio web de compras y un navegador) e impedir que terceros lean y modifiquen cualquier dato que se transfiera, como datos personales, datos bancarios o datos de acceso, como usuarios y contraseñas.

Podemos saber si un sitio web usa esta tecnología fijándonos en la barra de direcciones de nuestro navegador. Una vez que estamos visualizando el sitio web en cuestión, podemos comprobar que aparece un candado de color verde

136. Todo lo que debe saber sobre certificados SSL - https://www.verisign.com/es_LA/website-presence/website-optimization/ssl-certificates/index.xhtml

al principio de la barra de direcciones, esto nos indicará que, dicho sitio, utiliza un certificado SSL.

Podemos hacer clic en el candado verde y seleccionar la opción de "Certificado" y visualizar la información que nos ofrece el mismo. En la información del certificado podemos encontrar datos como, por ejemplo, la empresa que ha contratado el certificado.

Puedes utilizar esta herramienta online (https://sslanalyzer.comodoca.com/) que te mostrará toda la información disponible en el certificado SSL.

Red Tor

Ya te he hablado de la red Tor y del objeto de dicha red, que no es otro que navegar de forma anónima. Al igual que los usuarios que navegan por dicha red, los sitios web de la misma también ocultan su IP, y como es lógico, ocultan todo tipo de dato personal que les pueda identificar, de forma que es sumamente complejo identificar al administrador que se encuentra detrás de un sitio web en la red Tor.

Uno de los métodos para identificar a alguien en la red Tor es conseguir ubicarlo geográficamente, ya sea con el análisis de conversaciones escritas o mantenidas con el investigado, o a través del análisis de imágenes o vídeos o cualquier otra información que nos pudiese dar algún tipo de dato de donde se pudiese encontrar.

Eduardo Casas[137], en su libro *La red oscura* [138] detalla cómo se detuvo a un pederasta, que compartía vídeos manteniendo relaciones sexuales con menores, analizando dichos vídeos de forma exhaustiva. El investigado tomaba todo tipo de medidas para evitar ser descubierto, una de ellas era utilizar la red Tor, así como encriptar el contenido de su ordenador y borrar

137. https://twitter.com/aguilaken?lang=es
138. libro La red oscura (Actualidad) (Spanish Edition) (Posición en Kindle823). La Esfera. Edición de Kindle - https://www.amazon.es/oscura-Actualidad-Eduardo-Casas-Herrer-ebook/dp/B01N2117ML

todo tipo de evidencias de las tarjetas de memoria.

"*Lo primero que llamó la atención era que estaba rodado en el amplio camarote de un barco, de forma más o menos circular y con una claraboya en el techo. La ausencia de objetos personales en las mesillas les condujo a pensar que tal vez no fuera de su propiedad, sino que lo tuviera alquilado o, más probablemente, que trabajase en él como mecánico. Eso lo dedujeron de las manos que, cuando se mostraban en pantalla, tenían alguna sustancia oscura bajo las cortas uñas, tal vez grasa. No eran manos delicadas. El individuo debía de dedicarse a algún trabajo manual y la reparación de yates le venía como anillo al dedo. Como en el interior de la península no hay demasiados mares, había que buscar por la costa. Otro detalle acotó más la búsqueda. En una de las escenas aparecía un fragmento de una gorra en la que se podía leer ca'n, es decir «casa de» en mallorquín, tal vez el nombre de un restaurante. Era suficiente. Un equipo se trasladó de inmediato a Palma, donde se coordinaron con la Brigada Provincial de Policía Judicial de la isla para rescatar con la máxima urgencia a las víctimas. Faltaban pocos días para la Semana Santa de 2011. Montaron tres subgrupos. Uno iría por los colegios con las fotos de los niños, puesto que en alguno debían conocerlos; el segundo acudiría a todos los concesionarios de venta de yates para tratar de localizar el modelo exacto y el tercero buscaría por los talleres de reparación de embarcaciones, donde intentarían encontrar al violador. El primer resultado positivo llegó de los vendedores de barcos: el camarote era el de un Rodman 56, uno de los modelos más comunes en nuestras costas. Ese camino iba a ser complicado. Los centros educativos tardaron dos días en dar resultados, cuando un centro para alemanes creyó reconocerlos y, tras algunas gestiones adicionales, al fin se consiguieron algunos apellidos. El problema era que ya no estudiaban allí y no aparecían empadronados en ningún lugar de las islas. Al menos ya tenían un nombre con el que trabajar, Holger Jaques, del que no tardaron en saber que tenía antecedentes en Alemania por estafador y en España había sido investigado en una operación contra la pornografía infantil del año 2007,*

Herrer, Eduardo Casas. La red oscura"

Como puedes ver en el relato anterior, cualquier detalle en una imagen o texto puede abrir una nueva vía de investigación.

Los sitios web de la red Tor no son accesibles desde los motores de búsqueda

tradicionales y aunque existen buscadores específicos para dicha red, como Tor2Web[139], Ahmia[140] o Torchtorsearchno[141], no son lo suficientemente eficaces. El motor de búsqueda para la red Tor más popular es DuckDuckGo (https://duckduckgo.com/). DuckDuckGo puede usarse para buscar en la red Tor y en la web superficial.

Flujo de trabajo

Puedes acceder al flujo de trabajo de Ciberpatrulla (https://ciberpatrulla.com/responsable-pagina-web/) el cual te ayudará a la hora de encontrar al responsable de un sitio web.

139. https://hss3uro2hsxfogfq.onion.to/
140. https://ahmia.fi/
141. http://www.torchtorsearch.com/

Twitter

Introducción

Sin duda Twitter es una de las redes sociales más usadas, aunque este no es el principal motivo por el que Twitter es muy importante a nivel OSINT.

Los motivos principales son:

-La mayoría de los perfiles son públicos. Es raro encontrar en Twitter un perfil privado.

-La API[142] **de Twitter es una de las que más información nos facilita.** El acceso a Twitter mediante su API y la flexibilidad que esta permite, fomenta la creación de aplicaciones muy útiles para llevar a cabo estudios, investigaciones y análisis.

-Multitud de herramientas para OSINT. En relación con lo anterior, para Twitter disponemos de decenas de herramientas externas, que conectadas mediante su API, nos permiten obtener valiosos informes de actividad de usuarios, conexiones entre ellos, tendencias, horas a las que se conectan, dispositivos desde los que lo hacen, etc.

Tip: Twitter tiene una peculiaridad en la forma que nos muestra la hora de publicación de un tweet. Cuando hacemos clic en un tweet, debajo de este nos muestra la fecha y la hora de publicación, pero la hora que mostrará variará dependiendo de si estamos conectados a Twitter o lo estamos visualizando como invitados. Si estamos conectados nos mostrará la hora según la zona horaria que hayamos configurado en nuestro perfil de Twitter, pero si lo hacemos como invitados nos mostrará la hora en Horario Estándar

142. Información sobre las API de Twitter - https://help.twitter.com/es/rules-and-policies/twitter-api

del Pacífico (PST), es decir, 8 horas menos que la hora UTC.

Buscando en Twitter

Twitter te da varias opciones para buscar resultados en su red. Podemos usar la caja genérica (https://twitter.com/search-home) con sus distintas opciones; podemos usar la sección de búsquedas avanzadas (https://twitter.com/search-advanced); o podemos utilizar operadores en la caja genérica y en la sección de búsquedas avanzadas.

Te dejo un artículo muy completo con explicaciones de todas las búsquedas que puedes realizar en Twitter (https://ciberpatrulla.com/osint-twitter/).

Estos son los operadores que puedes usar en la caja de búsqueda de Twitter:

- ***Twitter operadores***: buscará tanto "Twitter" como "operadores"
- ***"Twitter operadores"*** : buscará la frase exacta "Twitter operadores"
- ***Monitorizar OR Analizar*** : buscará "Monitorizar" o "Analizar" o ambos
- ***gato -coche***: buscará "gato" pero no "coche"
- ***#OSINT***: buscará el hashtag "OSINT"
- ***Email from:0ciberpatrulla***: buscará tweets que han sido enviados por "0ciberpatrulla" y que contienen la palabra "Email"
- ***to:0ciberpatrulla***: buscará tweets que han sido enviados a "0ciberpatrulla"
- ***@0ciberpatrulla***: buscará tweets donde ha sido mencionado "0ciberpatrulla"
- ***"curso OSINT" near:"Madrid"***: buscará tweets que contienen la frase

exacta “curso OSINT” y han sido enviados cerca de “Madrid”

- ***near:Madrid within:15km***: buscará tweets enviados en un radio de 15 km de “Madrid”

- ***Policía since:2018-05-26***: buscará tweets que contiene “policía” y se envió desde la fecha “2018-05-26” (año-mes-día)

- ***Madrid until:2018-05-18***: buscará tweets que contienen “Madrid” y se envió antes del día 2018-05-18

- ***geocode:40.453254,-3.688334,1km***: buscará tweets en esas coordenadas, con un radio de 1 kilómetro

- ***evento -deportivo*** `:)`: buscará tweets que contienen “evento” pero no “deportivo”, y con una actitud positiva

- ***turista*** `:(`: buscará tweets que contienen “turista” y con una actitud negativa

- ***agresión ?***: buscará tweets que contienen “agresión” y haciendo una pregunta

- ***accidente filter:links***: buscará tweets que contienen “accidente” y que enlaza a URLs

- ***Madrid source:twitterfeed***: buscará que contiene “Madrid” y se publicó a través de TwitterFeed.

Listas de Twitter

Las listas de Twitter[143] son grupos o colecciones de cuentas de Twitter. Sirven para organizar a tus amigos por temáticas, de forma que no tienes que leer

143. Cómo usar las Listas de Twitter - https://help.twitter.com/es/using-twitter/twitter-lists

todo el Time Line, sino acceder a la lista que te interesa en cada momento.

Cómo usar las listas para OSINT

Las listas de Twitter pueden ser públicas o privadas:

Una lista pública significa que cualquiera en Twitter puede ver tu lista y suscribirse a ella. Cualquier persona que añadas a esa lista recibirá una notificación de Twitter para informarle sobre ello y podrán comprobar que son parte de tu lista en la pestaña “Miembro de” dentro de la página de listas en su perfil.

Una lista privada sólo es visible para quien la crea. Cualquiera que añadas a una lista privada no será notificado y no sabrá que pertenece a dicha lista.

¿Empiezas a ver su utilidad?

Efectivamente, es lo que estás pensando. Una lista privada de Twitter te permite seguir a cualquiera sin que sepa que le sigues.

Puedes usarla para añadir perfiles afines o que tienen algún tipo de relación entre ellos. Solo tienes que entrar cuando lo necesites y ver de qué se está hablando.

Te dejo un vídeo sobre las listas de Twitter (https://youtu.be/fCGiHonRzFk).

Caso práctico

Te voy a poner un ejemplo de uso:

Imagina que tienes una lista con perfiles de usuarios pertenecientes a algún grupo, y del cual quieres seguir sus movimientos porque crees que pueden estar organizando alguna reunión.

Uno de los perfiles publica un tweet en el que dice "*en dirección a Madrid*". Más tarde aparece otro tweet de otro usuario diciendo "h*oy será un día que no*

olvidaremos". Igualmente aparece otro tweet de otro usuario "*esperando tomando una cerveza*", en el que se aprecia la zona, de forma que podemos identificar la localidad, e incluso la calle.

En la lista comienzan a publicar tweets, durante horas, que guardan cierta relación unos con otros, y de repente, durante tres horas se hace el silencio, y pasado ese tiempo comienzan a aparecer tweets, y uno de ellos dice "*la unión hace la fuerza. Volveremos a terminar lo que ha quedado pendiente*"

Así a simple vista no tienen por qué guardar ninguna relación unos tweets con otros, pero podría darnos información de que un grupo de personas se han organizado para ir a Madrid, con un objetivo, que conoceremos o no, y que durante tres horas han llevado a cabo.

Podemos anticiparnos a dicho acto o podemos contrastar sucesos en la zona con la información obtenida en los tweets.

Cómo seleccionar los integrantes de una lista

Imagina que quieres hacer una lista de personas que trabajan en una determinada organización. Lo normal es que no encuentres muchos perfiles en los que se haga mención a la organización a la que pertenecen. Es muy probable que los perfiles que dispongan estas personas no dispongan de información relacionada con dicha organización.

Podemos usar herramientas como Followerwonk (https://followerwonk.com/bio). Con esta herramienta podemos buscar fácilmente coincidencias en la biografía, como el nombre de una organización o una URL. Aunque la mayoría de los integrantes no hagan pública esta información, podemos tener suerte y encontrar que alguno de ellos sí lo haga.

Cómo configurar la lista privada

En Twitter, ve a *configuración*, arriba a la derecha, y haga clic en *Listas*. Haz clic

en *Crear nueva lista*.

Haga clic en *Privado*. Ahora agrega los perfiles que has encontrado con Followerwonk, o los perfiles que ya conozcas.

Una forma de hacer crecer esa lista es analizando los amigos de los perfiles que vayas encontrando. Un truco a tener en cuenta es acceder a los amigos de cada perfil, desplazarte hasta el final para ver los últimos amigos, los cuales serán los primeros que añadió, y que probablemente, serán las personas mas cercanas, amigos, familiares y compañeros de trabajo.

Geolocalización de Twitter

Twitter tiene la opción de geolocalizar[144] todos tus tweets. Esta opción viene deshabilitada por defecto en todos los perfiles, pero, en ocasiones, podemos encontrar contenido geolocalizado.

Existen herramientas para analizar Twitter en base a la ubicación, pero eso lo veremos más adelante, ahora me gustaría que entendieras cómo funciona.

Twitter, a través de la posición que le facilite nuestro móvil o nuestro PC, geolocalizará un determinado tweet de forma automática, siempre que tengamos la opción activada.

¿Cómo podemos usar la geolocalización de Twitter para OSINT?

Podemos analizar cuántos tweets existen en una determinada ubicación y en un día o fecha determinada, o podemos analizar si un usuario concreto ha enviado tweets geolocalizados.

Para el primero de los casos, necesitamos unas coordenadas de la ubicación concreta. Conseguir las coordenadas de un lugar es sencillo, podemos utilizar

144. Cómo agregar tu ubicación a un Tweet - https://help.twitter.com/es/using-twitter/tweet-location

Google Maps[145].

Lo primero que vamos a hacer es introducir en Google Maps la dirección que nos interesa, una vez que tenemos ubicada la dirección, con el botón derecho encima de la ubicación en el mapa, hacemos clic y en el menú contextual elegimos *"¿Qué hay aquí?"*. Ahora nos mostrará en la parte inferior una caja con las coordenadas del lugar.

Con los datos obtenidos nos vamos a Twitter y los introducimos en la caja de búsqueda.

Este es un ejemplo de una combinación que podemos usar en la caja de búsqueda de Twitter (sin las comillas):

"geocode:40.453254,-3.688334,1km until:2018-05-02"

Tranquilo, te voy a explicar qué significa todo esto:

***Geocode**:* es el operador que define que los datos que estamos introduciendo son coordenadas.

Radio: le hemos dicho que busque en un radio de 1 km.

Fecha: le hemos dicho que busque solo hasta la fecha indicada.

Puedes agregar muchas más instrucciones a esta búsqueda para filtrar aún más, reduciendo los resultados. Solo tienes que jugar con los operadores que te he dejado en la sección anterior.

Una vez que se muestran los resultados, podemos seleccionar qué contenido queremos que nos muestre, fotos, vídeos, o cualquier otro.

145. https://www.google.es/maps

TweetDeck

TweetDeck (https://tweetdeck.twitter.com/) es una herramienta oficial creada por Twitter para gestionar cuentas desde un solo panel de control. Se pueden controlar notificaciones, menciones, mensajes y la actividad en general de una o varias cuentas.

Se pueden agregar columnas al panel para realizar el seguimiento de hashtags, usuarios, actividad de otras cuentas. Te da la opción de activar alertas de escritorio con sonido para avisarte de las novedades en las búsquedas que le hayamos definido.

TweetDeck es una potente herramienta para OSINT.

TweetDeck te permite, desde su panel, ver todo lo que está sucediendo en la actualidad en base a los criterios que hayamos definido, como nombres de usuario, hashtag, palabras clave, listas y un sin fin de opciones más.

Lo primero que necesitas es tener una cuenta de Twitter creada, y estar conectado a ella. Ahora solo tienes que ir a TweetDeck, y directamente entrarás en el panel.

Cuando entras por primera vez, te aparecerá contenido de tu perfil de Twitter. Yo elimino todas esas columnas y creo las que necesito en base a mis criterios. Te sugiero que hagas lo mismo. Lo importante es tener un tablero con contenido útil, sin nada de ruido. El exceso de información es perjudicial. Lo ideal es tener una cuenta exclusivamente para hacer OSINT.

Te detallo algunas de las posibilidades de TweetDeck:

- Puedes configurar un tramo de fechas y hora.
- Seleccionar una área geográfica de los tweets.
- Excluir palabras clave.

- Seleccionar un usuario en concreto.
- Seleccionar un Hashtag.
- Puedes utilizar operadores y combinaciones de estos.

Si te interesa estar al día de un tema en particular, puedes monitorizar por un hashtag. El problema es la gran cantidad de información que puede mostrarte esta consulta. Para evitar morir de exceso de información puedes jugar con los filtros que te ofrece.

Filtros de las columnas

Haciendo clic en el icono para abrir los filtros de las columnas te muestra las siguientes opciones:

Tweet content: donde puedes seleccionar qué tipo de tweet quieres que aparezca en los resultados, con imágenes, sin ellas, con GIFs, con enlaces. Además puedes seleccionar qué palabras clave quieres que contenga el tweet, o cuáles no quieres que aparezcan. También puedes seleccionar si quieres que muestre retweets o no. Otra opción muy interesante es el rango de fechas en el que quieres que te muestre los resultados, y por último el idioma de los mismos. La opción de la fecha y el idioma no aparece cuando filtramos por usuarios.

Location: nos permite seleccionar una ubicación con un rango de distancia desde donde se han publicado dichos tweets. Esta opción no está disponible cuando la columna está filtrada por usuario.

Tweet authors: nos permite filtrar por todos los usuarios, especificar uno, tú mismo, usuarios verificados, o miembros de una lista.

Engagement: nos permite definir parámetros relacionados con la cantidad de retweets, me gusta o comentarios que debe contener el tweet para que aparezca en nuestra búsqueda.

Preferences: nos va a permitir definir si queremos recibir notificaciones sonoras o de escritorio y el tamaño del tweet. Las notificaciones nos pueden resultar muy útiles si no queremos estar constantemente revisando las novedades.

Como ves, el potencial de esta herramienta es increíble.

Es conveniente que no abuses de los filtros, porque podemos dejar contenido de interés sin recibir. Por ejemplo puede haber tweets con pocos comentarios o retweets y que tengan un gran valor para nuestra investigación.

Te dejo un vídeo donde se explica muy bien su funcionamiento (https://youtu.be/oSKpor2bCLs).

Herramientas para Twitter

Existen decenas de herramientas que, mediante su API, se conectan a Twitter y nos facilitan la obtención de información muy valiosa de esta red social.

He hecho una selección de las que creo que son imprescindibles, pero seguro que encontrarás muchas más, con funcionalidades varias, pero no es mi intención llenar las secciones de listados infinitos de herramientas.

TweetBeaver

(https://tweetbeaver.com/)

Se trata de una colección online de herramientas fantástica. Con TweetBeaver podemos:

- Conseguir la ID del perfil desde el nombre de usuario o viceversa
- Comprueba si dos cuentas se siguen

- Descarga los favoritos de un usuario
- Busca dentro de los favoritos de un usuario
- Descarga una cronología de usuarios
- Busca dentro de una línea de tiempo de usuarios
- Obtiene los datos de una cuenta de usuario
- Obtiene información de usuarios de forma masiva
- Descarga una lista de amigos de usuarios
- Descarga una lista de seguidores de los usuarios
- Encuentra seguidores comunes de dos cuentas
- Encuentra amigos comunes de dos cuentas
- Encuentra conversaciones entre dos usuarios

Como ves, TweetBeaver tiene mucho potencial para sacar diversas conclusiones en nuestras investigaciones. La curva de aprendizaje es casi inexistente y aporta información de mucho valor.

Tinfoleak

(https://tinfoleak.com/)

La versión online, en base al nombre de usuario que le pongamos, nos devolverá, vía email, un reporte[146] muy exhaustivo de dicho perfil.

Con la versión de escritorio[147] la cosa cambia. Tenemos tres opciones, buscar

146. Guía explicativa del reporte - https://www.isecauditors.com/herramientas-tinfoleak
147. https://github.com/vaguileradiaz/tinfoleak

por usuario, por Time Line o por coordenadas.

De un usuario podemos sacar toda esta información:

- Información básica de la cuenta
- Identificación de dispositivos, sistemas operativos, aplicaciones y redes sociales utilizadas
- Temáticas sobre las que opina el usuario
- Franjas horarias de mayor actividad, horarios de sueño
- Contactos del usuario y relaciones entre ellos (amigos, familia, compañeros…)
- Opinión del usuario sobre temáticas específicas
- Descarga de imágenes publicadas
- Geolocalización de tweets (incluyendo fotografías)
- Identificación de residencia habitual, lugar de trabajo y otras ubicaciones relevantes
- Predicción de ubicaciones futuras
- Análisis de metadatos
- Temáticas relacionadas con una palabra clave

A partir de las coordenadas:

- Usuarios que se encontraban en la zona, en un día y hora concreta
- Imágenes y vídeos de sucesos y eventos

A partir del Time Line global:

- Tweets sobre temas determinados que se publicaron en una fecha o periodo en concreto

Como ves, con toda esta información es fácil llegar a las conclusiones que estamos buscando.

En mi artículo sobre Tinfoleak encontrarás más información y guías para su instalación: (https://ciberpatrulla.com/tutorial-tinfoleak/).

Allmytweets

(https://www.allmytweets.net)

Una de mis favoritas. Sencilla, pero potente herramienta. Una vez conectados, nos mostrará todos los tweets del perfil que le digamos, de forma cronológica y en texto plano. Ideal para navegar rápidamente entre cientos de tweets y buscar tweets antiguos.

¿Qué se puede hacer con esta herramienta tan simple?

Una vez conectado y habiendo elegido el usuario que queremos analizar, inicia la opción 'Buscar' de tu navegador. Ingresa la palabra clave que desees buscar.

Te doy algunas ideas:

-'"feliz cumpleaños", "felicidades" para averiguar cuál es la fecha de nacimiento de un usuario.

-"te quiero" o "te amo", para encontrar relaciones.

-Puedes buscar por número de teléfono o por direcciones de correo electrónico.

Socialbearing

(https://socialbearing.com/)

Esta herramienta online ofrece un completo análisis de perfiles de twitter.

De esta herramienta puedo destacar:

- Búsquedas de Twitter en tiempo real, estadísticas y análisis
- Ver los principales influencers, menciones y hashtags
- Buscar líneas de tiempo de usuario, seguidores y amigos
- Tweets y mapa geolocalizados
- Exportar tablas y gráficos de Twitter
- Tablero de análisis personalizable

Este tipo de herramientas ponen a prueba tus dotes de analista, debido al volumen de información que pueden llegar a mostrarte.

Foller

(https://foller.me/)

Esta es otra plataforma online de análisis social sobre Twitter. Yo soy amante de lo simple, y esta herramienta cumple dicho cometido. Ofrece poca información, pero muy valiosa.

Followerwonk

(https://followerwonk.com/compare)

Este servicio online cuenta con varias herramientas, y una de ellas realiza comparaciones de tres perfiles de Twitter. Comparando varios perfiles de

Twitter podemos encontrar patrones en común entre ellos y encontrar relaciones.

Perfiles privados en Twitter

Los perfiles de Twitter se pueden configurar como privados. Va un poco en contra de la filosofía de esta red, pero la opción existe.

Puede darse el caso de que alguien se sienta investigado y decida poner en privado su perfil.

Configurar un perfil como privado conlleva lo siguiente:

- Para seguir un perfil privado tiene que ser aprobado por el administrador.
- Sólo los seguidores aprobados podrán ver los tweets.
- Otros usuarios no pueden retwittear los tweets de este perfil.
- Los tweets no aparecen en los buscadores como Google, sólo en las búsquedas en Twitter realizadas por usuarios aprobados.
- Las menciones no podrán ser vistas por los mencionados, a no ser que estos sean seguidores aprobados.
- Todo lo publicado mientras que la cuenta es pública ahora será privado y sólo los seguidores aprobados podrán verlo o buscarlo.
- Sólo podrán compartir enlaces permanentes en los tweets con los seguidores aprobados.

¿Qué opciones tenemos para obtener información de perfiles privados?

Lo primero que hay que tener en cuenta es que no se puede acceder de

ninguna manera a un perfil privado.

Podemos utilizar la herramienta TweetBeaver para determinar si dos usuarios se siguen mutuamente (https://tweetbeaver.com/mutualfollow.php).

Una vez que hemos identificado usuarios que siguen este perfil privado, podemos observar tweets dirigidos al perfil privado que nos pueden dar información relevante.

Usando la búsqueda de Twitter, podemos buscar todos los tweets que mencionan o van dirigidos a la cuenta privada.

Recuerda los operadores que vimos en la sección de búsqueda de Twitter.

Por ejemplo podemos usar el operador *@usuario* si queremos buscar menciones o el operador *to:usuario*, si queremos buscar tweets enviados a dicho usuario. Podemos añadir los filtros que necesitemos, como los de una fecha determinada.

Si bien los tweets del perfil privado no podremos verlos, podremos ver qué conversaciones está manteniendo con otros perfiles, y en base a las respuestas o tweets de estos perfiles públicos, podremos sacar conclusiones o contextos.

Otra opción para encontrar tweets de perfiles privados es buscar nombres de usuarios en los motores de búsqueda que tienen páginas en caché (como Google, Yandex y Bing) y probar suerte a la espera de que aparezca un resultado en caché con tweets.

¿Cómo es posible que aparezcan en los buscadores si son perfiles privados?

Hemos visto que si configuras un perfil como privado deja de ser indexado por los motores de búsqueda, pero si este perfil ha estado abierto al público en algún momento no muy lejano, es posible que dicho contenido siga apareciendo en los motores, y podamos verlo en las caché de los mismos.

Además, existen servicios de archivo web, como: (http://web.archive.org/) y

(http://archive.today/), que pueden tener guardados tweets privados de cuando eran públicos.

Facebook

Introducción

Facebook es una de las redes sociales más usadas, y donde más datos personales se comparten de forma pública. Se comparten fotos y vídeos con detalles de todo tipo; dónde y qué comemos y con quién; dónde viajamos; a qué eventos asistimos; cuáles son nuestras aficiones; quiénes son nuestros amigos, familiares, compañeros de trabajo, mascotas, vehículo, lugar de trabajo, ideología, etc.

Como investigador es una fuente con abundante información para perfilar a una persona, aunque he de decir que, me preocupa cómo compartimos alegremente nuestras intimidades sin conciencia de lo peligrosa que puede ser esta información en manos de terceros.

Estos son algunos de los ejemplos de información que podemos obtener para nuestra investigación de esta red social:

- Lugar de trabajo
- Saber quiénes son los compañeros de trabajo
- Saber quién es la pareja
- Saber quiénes son los familiares
- Saber quiénes son los amigos más cercanos
- Averiguar sus aficiones
- Averiguar futuros eventos a los que asistirá

- Averiguar lugares que visita habitualmente
- Centros donde ha estudiado
- Horas a las que publica
- Lugares desde donde publica
- Grupos a los que sigue
- Fecha de nacimiento
- Aniversarios
- Qué vehículos tiene
- Dónde suele ir de vacaciones

A diferencia de Twitter, en Facebook puedes encontrar todo tipo de perfiles, privados y públicos, y con distintos niveles de privacidad. Para Facebook no existen tantas herramientas OSINT como para Twitter, esto es debido a las restricciones de su API, pero aún así tenemos muchas opciones para extraer información. Puedes echar leer mi artículo sobre herramientas OSINT para Facebook (https://ciberpatrulla.com/herramientas-osint-facebook/).

Buscando en Facebook

En esta sección te voy a hablar de las opciones de búsqueda que tiene Facebook. Aunque voy a entrar en detalle sobre cómo funcionan las mismas porque creo que es importante entender su funcionamiento, decirte que, si no quieres aprenderte la teoría y quieres ir al grano, al final de la sección te he dejado herramientas que facilitan las búsquedas.

Facebook proporciona una barra en la parte superior del sitio web para realizar las búsquedas. Desde esta barra permite filtrar los resultados.

Facebook te permite buscar palabras y frases específicas. Puedes usar este tipo de búsquedas para buscar publicaciones hechas por un amigo determinado o para ver lo que se habla sobre un tema específico.

Si quieres sacar todo el potencial a la búsqueda de Facebook es conveniente que cambies el idioma de tu perfil a *Ingles (US),* ya que con esta configuración aparecen nuevas opciones de filtrado en la parte superior. Para ello tienes que ir a "*Configuración/Lenguaje* y cambiar la opción "*¿En qué idioma quieres usar Facebook?*".

Una vez cambiado el idioma podrás usar tres bloques para realizar las búsquedas:

1. La caja de búsqueda.

2. Debajo de la caja, una barra horizontal con filtros predefinidos (todo, posts, personas, fotos, vídeos, páginas, lugares, grupos, aplicaciones, eventos y enlaces).

3. Una barra lateral a la izquierda con un menú para filtrar los resultados. Este menú se personalizará con distintos filtros en base a qué filtro hayamos aplicado en la barra horizontal.

Tenemos que tener en cuenta que los resultados de las búsquedas estarán condicionados a la configuración de privacidad de los perfiles de Facebook, es decir, si un usuario tiene restringido el contenido solo para sus amigos o solo para él, no aparecerán resultados sobre ese contenido en las búsquedas que hagamos. Aún así, un usuario de Facebook puede aparecer etiquetado en una fotografía fuera de su perfil, o haber comentado un post de un amigo que tiene el perfil público, por lo tanto, aún teniendo la información privada, se pueden obtener datos con la suficiente relevancia para sacar conclusiones. A lo largo de esta sección veremos cómo hacerlo.

Caja de búsqueda

Podemos utilizar la caja de búsqueda para hacer combinaciones como estas:

- **Posts de una persona determinada:** NOMBRE posts from
- **Posts de un usuario sobre un asunto :** posts from NOMBRE-USUARIO about ASUNTO
- **Fotos realizadas en un lugar por personas de un lugar determinado:** Photos taken in LUGAR-FOTOS by people from LUGAR-PERSONAS
- **Vídeos grabados recientemente en un lugar:** Recent videos taken in LUGAR
- **Vídeos grabados en un lugar desde una fecha determinada:** Videos taken in LUGAR-VÍDEOS from FECHA-VÍDEOS (ejemp: december 2015)
- **Vídeos grabados en un lugar por personas de un lugar determinado:** Videos taken in LUGAR-VÍDEOS by people from LUGAR-PERSONAS

Recuerda introducir los parámetros de las búsquedas en inglés.

Tipos de búsquedas personalizadas

Aunque la caja de búsqueda nos puede resultar útil en determinados momentos, te voy a contar otro método que puedes utilizar para exprimir al máximo las búsquedas de Facebook.

Podemos utilizar URLs personalizadas para realizar búsquedas. Estas URLs tendrás que insertarlas o modificarlas en la propia barra de direcciones de tu navegador. Siempre comienzan con el prefijo (https://www.facebook.com/

search/), seguidas de números de ID y algunos operadores de búsqueda.

Hay dos tipos de búsqueda personalizada en Facebook; una de ellas utiliza los números de identificación o ID y la otra utiliza palabras.

Búsqueda con números de identificación de Facebook

Antes de nada voy a explicarte qué es la ID de Facebook y cómo conseguir este identificador que a simple vista no aparece.

Lo primero que tenemos que hacer cuando investigamos un perfil social en Facebook es conseguir la ID del mismo. La ID de un perfil o grupo de Facebook es única, sin embargo el nombre de usuario puede ser modificado. Es decir, un usuario puede cambiar su nombre de usuario, pero la ID permanecerá siempre asociada a ese perfil.

Para la obtención de la ID, podemos usar servicios online que nos facilitan la identificación de la misma, como por ejemplo (http://lookup-id.com/) o (https://findmyfbid.com/).

Este es un ejemplo de una cuenta de usuario con las distintas URLs, con el nombre de usuario y con la ID:

Con nombre de usuario: (https://www.facebook.com/Iker.Casillas/)

Con ID: (https://www.facebook.com/189956894367877)

Cuando hacemos búsquedas con el número de identificación, esta se ciñe exclusivamente al perfil que corresponde a dicha ID.

A continuación te voy a poner algunos ejemplos de posibles búsquedas que podemos hacer con las URLs personalizadas:

-Vídeos de Iker Casillas: (https://www.facebook.com/search/189956894367877/videos-of)

-Páginas que le gustan a Iker Casillas: (https://www.facebook.com/search/

189956894367877/pages-liked)

-Fotos de Iker Casillas: (https://www.facebook.com/search/189956894367877/photos-by)

-Fotos que ha comentado Iker Casillas: (https://www.facebook.com/search/189956894367877/photos-commented)

Más abajo te diré cómo exprimir estas búsquedas al máximo.

Buscando con palabras

Otra forma de buscar en Facebook es mediante palabras o combinación de estas. La búsqueda con palabras muestra resultados más genéricos, siendo menos precisa que si buscamos por la ID pero, a su vez, es más flexible.

Por ejemplo vamos a hacer una búsqueda de **personas que han visitado el Estadio Santiago Bernabéu**:

(https://www.facebook.com/search/str/Estadio%20Santiago%20Bernab%C3%A9u/places-named/visitors/intersect)

Ahora vamos a complicarlo un poco más, y le vamos a decir que nos muestre **personas que viven en Francia y que han visitado el Estadio Santiago Bernabéu**:

(https://www.facebook.com/search/str/Estadio%20Santiago%20Bernab%C3%A9u/pages-named/visitors/intersect/str/Francia/pages-named/residents/present/intersect)

Vamos a dar un paso más en la complejidad de la cadena de búsqueda y vamos a buscar **personas que se llaman Nicolás y Máxime, que viven en Francia y han visitado el Santiago Bernabéu**.

(https://www.facebook.com/search/str/Nicolas/users-named/str/Maxime/users-named/union/str/Estadio%20Santiago%20Bernab%C3%A9u/pages-named/visitors/intersect/str/Francia/pages-named/residents/present/

intersect)

Observa que al final de cada combinación aparece el parámetro */intersect*. Igualmente para añadir dos usuarios o más, hemos añadido el parámetro */union* después de la combinación.

Como ves, conociendo los parámetros que podemos añadir a las URLs, podemos generar consultas complejas con muchísimo potencial.

Si queremos asegurarnos que la búsqueda la realiza sobre un lugar concreto, tendríamos que obtener la ID de dicho lugar para evitar resultados genéricos de lugares parecidos. Por ejemplo, si queremos saber quién visitó Toledo, pero queremos asegurarnos que la búsqueda la realiza con Toledo de España y no con otras ciudades llamadas Toledo (que las hay), podemos usar la ID de la página oficial de dicha ciudad, en este caso (https://www.facebook.com/476373032416957).

Puedes profundizar en las combinaciones que puedes usar para buscar en Facebook en estos artículos:

En español (http://www.globograma.es/verificacion-digital-en-facebook).

En inglés (http://www.researchclinic.net/facebook/) o (https://netbootcamp.org/facebookpeoplesearchtips/).

Sitios web que facilitan las búsquedas

Todo lo que hemos visto hasta ahora es la teoría con algunos ejemplos, y como te decía, creo que es muy necesaria saberla y entenderla, pero para que no tengas que estar creando todas esas URLs te dejo varias webs que disponen de atajos para facilitarte esta labor.

- (https://stalkscan.com/)
- (https://inteltechniques.com/OSINT/facebook.html)

- (https://aware-online.com/academy/osint-tools/facebook-graph-search/)
- (https://netbootcamp.org/facebook.html)
- (http://graph.tips)
- (https://searchisback.com/)
- (https://lookup-id.com/facebooksearch.html)
- (http://fb-search.com/)

Tips de Facebook

Descubrir los amigos comunes en Facebook

En la sección anterior hemos visto las opciones de búsqueda que dispone Facebook, entre ellas existe la opción de descubrir qué amigos comunes tienen dos o más cuentas de Facebook, esta opción nos ofrece mucha información sobre las conexiones de dichos perfiles. Dicha opción solo estará disponible si al menos uno de los perfiles que estamos analizando no tiene oculta su lista de amigos, como así avisa el propio Facebook:

"*¿Quién puede ver tu lista de amigos?*
Recuerda que tus amigos controlan quién puede ver sus amistades en sus propias biografías. Si las personas pueden ver tu amistad en la biografía de otra persona, podrán verla en la sección de noticias y en otros lugares de Facebook, así como mediante la función de búsqueda. Si cambias el público a Solo yo, solo tú podrás ver tu lista de amigos completa en tu biografía. Las demás personas solo podrán ver vuestros amigos en común."

Vídeos significativos

Muchos usuarios son partidarios de compartir vídeos conmemorando determinados momentos especiales, como por ejemplo, cumpleaños,

aniversarios, resúmenes de sus biografías, etc. Analizar la sección de vídeos de los perfiles puede darnos información oculta en otras secciones del perfil. Podemos obtener la fecha de su cumpleaños; el aniversario de boda; la fecha en la que comenzó una amistad con otro usuario; un resumen de fotos, etc. Puedes buscar estos vídeos en la sección de vídeos de cada perfil.

Saber la hora exacta de una publicación

Si queremos saber la hora exacta en la que se publicó un determinado post o comentario es habitual encontrarse en Facebook la antigüedad de dichos mensajes (8 horas, 7 días, etc.) en vez de la hora exacta. Para saber la hora exacta podemos hacerlo colocando el cursor justo encima de dicho texto y nos mostrará la fecha y la hora exacta de dicha publicación, siempre coincidiendo con la zona horaria configurada en el ordenador desde el que se visualiza.

Cómo saber si una publicación ha sido editada

Facebook, a diferencia de Twitter, permite la edición de las publicaciones y de los comentarios. En los comentarios, en el caso de haber sido editado por su autor, aparece un mensaje de "Editado" de forma visible y desde el que podemos ver el historial de los cambios que se han realizado, sin embargo en los posts dicha opción se encuentra oculta dificultando saber a simple vista si una publicación ha sufrido modificaciones. Para saber si un post ha sido editado tendrás que hacer clic en los tres puntos que se encuentran en el ángulo superior derecho de la publicación y en el menú emergente aparecen varias opciones, pero la que nos interesa es "Ver historial de ediciones", si dicha opción no aparece es que no ha sufrido cambios desde su publicación.

Cómo saber si un perfil es falso

Te voy a dejar un checklist para que compruebes fácilmente si un perfil de Facebook es falso:

- La única foto que aparece es la del perfil
- No tiene publicaciones o son antiguas
- Sus gustos no parecen tener coherencia, sus amigos no parecen reales, no pertenece a ningún grupo
- Tiene pocos amigos o la mayoría son del sexo contrario
- No tiene información en la biografía
- La fecha de cumpleaños es muy genérica (01/01/2000, 31/12/2009)
- Aparecen en su muro mensajes de sus amigos preguntándole de qué se conocen, los cuales se encuentran sin respuesta
- No dispone de ningún juego (https://www.facebook.com/games)
- Foto de perfil de artistas o dibujos

Cómo descargar un video de Facebook

Si no quieres utilizar páginas online para descargar un vídeo de Facebook, puedes utilizar este método:

1. Abre el video que quiere descargar
2. Haz clic con el botón derecho encima de video y selecciona "Copiar URL del vídeo"
3. Pega la URL anterior en una pestaña nueva y cambia esto en la URL (www por mbasic)
4. Dale a Intro y haz clic en el video para que se reproduzca. Se abrirá una nueva ventana
5. Mientras se reproduce, haz clic en el botón derecho del ratón en el

video y selecciona "guardar vídeo"

También puedes utilizar la extensión de Chrome FBDown Video Downloader[148] para descargar los vídeos.

148. https://chrome.google.com/webstore/detail/fbdown-video-downloader/fhplmmllnpjjlncfjpbbpjadoeijkogc

Otras RRSS

Introducción

Twitter y Facebook, en la actualidad son las dos redes sociales que más usaremos para OSINT, pero existen otras, y también importantes. Además tenemos que tener en cuenta que muchos usuarios disponen de varias cuentas en redes sociales. Es común que alguien tenga una cuenta de Facebook, otra de Twitter, otra en Instagram y otra en LinkedIn.

En este capítulo he descartado las plataformas de WhatsApp, Telegram o similares, porque las considero aplicaciones de mensajería y no redes sociales. Estas las veremos en el capítulo de Teléfonos.

Youtube

YouTube (https://www.youtube.com) es una red social dedicada exclusivamente a compartir vídeos, siendo la relación entre usuarios algo diferente al resto de redes sociales, ya que, en esta red, existe alguien que administra un canal y sube los vídeos, los cuales son visualizados por usuarios, registrados o no, con la única interacción por parte de los usuarios que visitan dicho canal de la mera inserción de comentarios en los distintos vídeos compartidos.

Los vídeos de estos canales son compartidos de forma habitual en otras redes sociales por los propios usuarios, incluso en muchas ocasiones veremos estos vídeos incrustados en páginas webs o blogs. YouTube permite, mediante la inserción de un código[149] en un sitio web, visualizar sus vídeos en ellos sin

149. Insertar vídeos y listas - https://support.google.com/youtube/answer/171780?hl=es

que estén alojados en los mismos.

Identificar el usuario o canal YouTube

El primer paso para identificar al administrador de un canal de YouTube es dirigirnos a la sección "*Más información*" del propio canal. En esta sección es habitual añadir otras formas de contacto con el administrador, como pueden ser otros perfiles sociales o un email de contacto.

Para identificar el nombre de usuario que utiliza el administrador de un canal, e identificar el nombre e ID del canal podemos dirigirnos a la página individual de cada vídeo, y justo debajo del vídeo, en tu lado izquierdo, aparece una imagen de perfil, avatar o logo y justo al lado, un enlace con el nombre del Canal. Si hacemos clic en la imagen de perfil o copiamos la dirección del enlace de dicha imagen, veremos una URL como esta *(youtube.com/user/NOMBRE-DE-USUARIO)*, si hacemos la misma operación en el enlace del nombre del Canal accederemos a una URL como esta *(youtube.com/channel/ID-CANAL)*.

Una vez obtenido el nombre de usuario podemos intentar asociarlo con otros perfiles sociales a través de buscadores específicos o genéricos. Esto lo veremos en el siguiente capítulo.

Herramientas OSINT para YouTube

Si bien veremos herramientas, técnicas y métodos para la verificación y análisis de vídeos en otro capítulo, quiero dejarte algunas herramientas específicas para el análisis de canales y vídeos de YouTube.

- **Socialblade** (https://socialblade.com/): nos da estadísticas de los canales que le digamos

- **Yout** (https://yout.com/): servicio online para descargar vídeos de YouTube

- **Ytcomments** (http://ytcomments.klostermann.ca/): descarga los comentarios insertados en un vídeo
- **YouTube DataViewer** (https://citizenevidence.amnestyusa.org/): muestra los metadatos de un vídeo
- **Geo Search Tool** (https://youtube.github.io/geo-search-tool/search.html): búsqueda de vídeos por ubicación
- **Yasiv** (https://yasiv.com/youtube): muestra un gráfico de vídeos relacionados con una búsqueda

LinkedIn

LinkedIn (https://www.linkedin.com) es una red social para profesionales. Sin duda es una red a tener muy en cuenta a la hora de obtener información de un investigado. Quizás sea de las redes sociales donde más datos fiables vamos a encontrar ya que, en la mayoría, aparecerá un extenso currículum de la persona, así como las conexiones con posibles compañeros de trabajo.

Datos de LinkedIn

En el momento que conectamos con alguien en esta red social tendremos acceso a toda la información que disponga en su perfil. Es muy habitual encontrar datos como el teléfono, fecha de nacimiento y dirección de email, además de toda su historia profesional y formación académica. Para ello solo tenemos que entrar en dicho perfil y acceder al apartado "*Ver información de contacto*".

Si necesitas exportar todas tus conexiones para generar un listado de usuarios con todos sus datos de contacto, puedes hacerlo desde este enlace (https://www.linkedin.com/psettings/member-data). Una vez dentro seleccionas "*Solicitar archivo*" y te enviarán un email con un enlace de descarga en formato ZIP. Una vez descargado y descomprimido puedes abrir el archivo

Connections.csv y aparecerán tus conexiones con sus nombres, emails y otros datos de interés.

Búsquedas avanzadas en LinkedIn

Podemos realizar búsquedas genéricas desde la caja de búsqueda de esta red social. Los resultados obtenidos pueden filtrarse utilizando las distintas opciones que aparecen en la página de resultados, pero además podemos utilizar algunos operadores muy interesantes para realizar las búsquedas.

Podemos usar los siguientes operadores:

- **AND, OR Y NOT**
- **firstname**: busca por nombre
- **lastname**: busca por apellidos
- **company**: busca por compañía actual
- **school**: busca por centro educativo
- **title**: busca por actual puesto de trabajo

Imagina que nos interesa buscar solo trabajadores de una empresa determinada y excluyendo una ubicación determinada. Para ello podemos usar:

title:GERENTE AND company:MERCADONA NOT MADRID

No hay que olvidar las búsquedas avanzadas de Google. Los perfiles de LinkedIn son indexados por los buscadores, por lo que podremos hacer búsquedas directamente desde Google aunque no tengamos cuenta en LinkedIn, si bien no podremos ver el perfil en detalle, podremos acceder a un extracto del mismo en el resultado del buscador:

Ejemplo*: site:linkedin.com mercadona gerente NOT madrid*

Te dejo un sitio web muy útil para hacer combinaciones de búsquedas avanzadas en LinkedIn a través de Google (https://recruitin.net/).

Herramientas OSINT para LinkedIn

En Inteltechniques tienes algunas opciones bastante interesantes que facilitan las búsquedas en LinkedIn.

https://inteltechniques.com/osint/menu.linkedin.html

Instagram

Instagram es una de las joyas de la corona de las redes sociales y con una cuota de mercado en alza. Es posible que en mis nuevas ediciones de este libro dedique un capítulo entero a esta red social debido al protagonismo que está alcanzando.

No sé cuál es el éxito de esta red, pero muchos jóvenes se han pasado a ella. En alguna ocasión leí que el motivo de que los jóvenes prefieren esta red social, dejando incluso de lado los grupos de WhatsApp, es motivado por la privacidad, ya que pueden escapar mejor del control parental. Si un padre o madre revisase su móvil, debido al analfabetismo digital de estos, revisaría el WhatsApp, pero no la aplicación de Instagram. Ahí lo dejo.

Instagram fue pensada como una red social para compartir fotos. En la actualidad se pueden subir imágenes videos, loops, transmitir videos en vivo e historias.

Cómo obtener el ID de Instagram

Al igual que en otras redes sociales, Instagram permite cambiar el nombre de usuario desde el panel de usuario, por lo que corremos el riesgo de que este

sea cambiado y no podamos acceder al perfil en visitas posteriores. Para identificar correctamente un perfil de Instagram debemos obtener la ID, para ello podemos usar alguno de estos métodos:

Herramienta online (https://codeofaninja.com/tools/find-instagram-user-id): podemos usar este servicio online que introduciendo el nombre de usuario nos facilitará la ID del perfil.

Código fuente (https://www.instagram.com/NOMBRE-USUARIO/?__a=1): sustituyendo el nombre de usuario que aparece en mayúscula en la URL que te he dejado de ejemplo, accederás al código fuente del perfil. Ahora solo tienes que encontrar con el buscador la etiqueta "*profilePage*", y el número que sigue a esta etiqueta es la ID del perfil.

¿Cómo podemos acceder al perfil con la ID si han cambiado el nombre de usuario?

La verdad es que me ha costado encontrar la forma de realizar esta operación, ya que Instagram no lo facilita. Si sustituimos el nombre de usuario de la URL por la ID e intentamos acceder al perfil nos aparece una página de error, es decir, Instagram no nos permite acceder de forma inversa al perfil, solo lo permite mediante el nombre de usuario y no mediante la ID. Pero tranquilo, he encontrado una solución para ti:

Si añades en esta URL la ID del perfil que estás buscando te dirigirá al perfil con el nombre de usuario: (https://www.instagram.com/web/friendships/ID-PERFIL/follow/).

Buscar en Instagram

Instagram dispone de un buscador muy básico, sin opciones avanzadas, dificultando encontrar contenido concreto, por ejemplo por fecha o lugar. Podemos crear filtros por usuarios o por hashtags utilizando, en la caja de búsqueda, los símbolos de @ o # respectivamente (@USUARIO,

#HASHTAG).

También podemos realizar búsquedas, algo rudimentarias, en base a publicaciones por ubicación. Tienes que entrar en el siguiente enlace e ir navegando hasta encontrar la ubicación que más se acerque a tus necesidades:

Explorar por ubicación: (https://www.instagram.com/explore/locations/).

Buscar desde Google

Los perfiles de Instagram son indexados por Google, por lo tanto podemos utilizar las combinaciones de Google para encontrar contenido en Instagram, como por ejemplo:

site:instagram.com "PALABRA CLAVE"

site:instagram.com intitle:PALABRA CLAVE

site:instagram.com inurl:PALABRA CLAVE

Buscar dentro de cuentas privadas

Ya hemos visto en Facebook que, aunque protejamos nuestras cuentas, es posible que no tengamos el control absoluto y el contenido se encuentre en otras partes de la propia red o de Internet.

Si alguien decide hacer privada su cuenta en Instagram, solo los usuarios que apruebe podrán ver el contenido de dicho perfil. ¿Pero que pasa si ha publicado un mensaje de Instagram en otra red social? Pues qué podremos acceder a dicho contenido. Podemos utilizar esta combinación de operadores de Google para buscar contenido de un perfil de Instagram en otras partes:

"*instagram.com/p/*" "*NOMBRE*" (con las comillas incluidas)

site:twitter.com OR site:facebook.com "*instagram.com/p/*" "*NOMBRE*" (con las

comillas incluidas)

Cómo saber la hora de una publicación de Instagram

A diferencia de otras redes sociales, Instagram no muestra de forma visible la hora de una publicación. Para encontrar este dato tenemos que acceder a la publicación que deseemos y haciendo clic en los tres puntitos que aparecen abajo a la derecha debemos seleccionar la opción de "Código de inserción". Dentro de este código aparece esta información. Para visualizarlo podemos copiar y pegar el código en un archivo de texto y podemos buscar el parámetro "*datetime*=" que aparece al final del código, allí mostrará dos tipos de hora, la primera en UTC y la segunda en Hora Estándar del Pacífico.

Herramientas que facilitan la búsqueda en Instagram

Te dejo varios servicios online con herramientas que te ayudarán en la búsqueda y análisis de los perfiles de Instagram:

-Inteltechniques (https://inteltechniques.com/osint/instagram.html)

-Netbootcamp (https://netbootcamp.org/instagram.html)

-Stagram (https://web.stagram.com/)

Sitios de citas

De la mayoría de las redes sociales podemos obtener información sin disponer siquiera de una cuenta en ellas utilizando diversos métodos. Las redes sociales enfocadas a facilitar encuentros entre personas suelen tener un enfoque más privado y requieren que te des de alta para poder acceder a los

perfiles.

Podemos encontrar redes sociales como Badoo (https://badoo.com/) que nos permiten acceder a los perfiles sin tener cuenta creada utilizando su propio buscador (https://badoo.com/es/contactos/spain/) o mediante operadores de Google:

site:badoo.com NOMBRE

site:badoo.com/es/ intitle:NOMBRE intitle:LOCALIDAD intitle:EDAD

Te dejo un repositorio donde podrás encontrar infinidad de redes sociales y aplicaciones de citas, organizado por orientación sexual, gustos o intereses (https://start.me/p/VRxaj5/dating-apps-and-hook-up-sites-for-investigators).

Comunidades

Introducción

Los foros son uno de los sistemas de compartir información más antiguos de Internet. A pesar de la aparición de las redes sociales, los foros siguen siendo uno de los lugares preferidos para tratar temas de todo tipo, creando comunidades de miles de personas. En este capítulo te voy a dejar algunos de los mejores foros de Internet donde podrás encontrar información de todo tipo:

- **Alquiler** (http://alquiler.forosactivos.net/): foro dedicado al alquiler de vivienda, con secciones específicas sobre las subvenciones, las ayudas al alquiler, la RBE , o para poner en contacto arrendadores y arrendatarios.

- **Foromtb** (http://www.foromtb.com/): como el propio nombre indica, es un foro para interesados en el ciclismo de montaña.

- **ACB** (http://foros.acb.com/): foro dedicado a temas relacionados con el baloncesto español.

- **Htcmania** (https://www.htcmania.com/foro.php): foros sobre móviles.

- **Los Viajeros** (https://www.losviajeros.com/foros.php): foro sobre viajes con experiencias personales muy detalladas.

- **Burbuja** (https://www.burbuja.info/inmobiliaria/index.php): este foro apareció en la época de la Burbuja Inmobiliaria, de ahí su nombre, pero con el tiempo se ha convertido en un foro para debatir sobre cualquier tema.

- **Forocoches** (https://www.forocoches.com/): sin duda uno de los foros más conocidos, siendo el foro más grande en español. Para poder participar se requiere invitación.

- **4chan** (https://www.4chan.org/): tablón de anuncios y foro para tratar temas de todo tipo. Lugar peculiar y poco intuitivo. Te dejo una guía de uso[150].

- **Forobeta** https://forobeta.com/: foro de discusión acerca de bloggers, seo, monetización, hospedaje, wordpress, blogger, así como otros temas relevantes para los webmasters.

- **FP Informática** (http://www.fp-informatica.es/foro/): foro sobre los Ciclos Formativos de Grado Medio (SMR) y Superior (ASIR, DAM y DAW).

- **El Chapuzas Informático** (https://foro.elchapuzasinformatico.com/index.php): foro especializado en temas informáticos.

- **Tabloide** (https://tabloide.es/): según su propia definición, Tabloide es un Club de Caballeros.

- **Foros del Web** (http://www.forosdelweb.com/): foro especializado en el desarrollo web.

- **Cristalab** http://foros.cristalab.com/: foro de diseño y desarrollo web.

150. 4Chan: guía de uso y navegación, desde /r hasta lo más escondido - https://www.genbeta.com/web/4chan-guia-de-uso-y-navegacion-desde-r-hasta-lo-mas-escondido

Personas

Introducción

En este capítulo vamos a ver cómo obtener información de personas en base a algunos datos personales iniciales como su nombre y apellidos. Esta puede ser una labor compleja, ya que pueden aparecer multitud de resultados para una misma consulta, y si no disponemos de más información además del nombre, podemos investigar un objetivo equivocado. Para evitar esto es necesario recabar el máximo de información de la persona que validen la elección de alguno de los resultados que obtengamos.

Dónde buscar personas

Buscadores genéricos

El primer paso es buscar en los buscadores genéricos como Google o Bing, realizando búsquedas por su nombre e ir probando diversas opciones. Puedes ir probando con el nombre, luego nombre y apellidos, apellidos y después el nombre, nombre y apellidos y localidad, etc.

Buscadores de personas

Lullar (http://com.lullar.com/): este buscador, en base a una búsqueda por nombre de persona, te muestra una serie de resultados, con enlaces personalizados con dicho nombre, a otros servicios online o redes sociales donde podrás comprobar si existen perfiles o información de dicha persona.

Páginas Blancas (http://blancas.paginasamarillas.es/jsp/home.jsp): un clásico que no debemos olvidar y que nos puede dar mucha información,

como teléfono fijo y domicilio de la persona.

Pipl (https://pipl.com/): es uno de los buscadores de personas más conocidos.

Listas de Deseos

Las listas de deseos o las listas de bodas pueden ser una fuente de información muy valiosa. Es posible que tengamos conocimiento de que la persona investigada se haya casado recientemente o tenga previsto hacerlo.

¿Qué información podemos obtener de una lista de deseos?

Si sospechamos que la persona que estamos buscando se ha casado o tiene previsto hacerlo, podemos buscar en distintos servicios online que ofrecen la opción de crear una lista de bodas para los invitados. Estas listas disponen de un buscador para que los invitados encuentren a los novios. En dichas listas podemos encontrar información sobre nombre y apellidos de los novios, además de la fecha del evento.

En algunos casos, estos servicios también disponen de una página personal para los novios con información sobre el lugar de celebración y fotos del evento.

Estos son algunos de los servicios online donde podrás buscar listas de bodas:

- **Amazon** (https://www.amazon.es/gp/registry/wishlist/search.html)
- **El Corte Inglés** (https://www.elcorteingles.es/bodamas_ssl/invitados/celebrantes_acceso.asp?promo=01)
- **Calistaonelistadeboda** (http://calistaonelistadeboda.com/invitados)
- **Zankyou** (https://www.zankyou.es/event/invitados)
- **Ruevintage74** (https://www.ruevintage74.com/lista-de-bodas/)

(requiere registro)

- **Given2** (https://given2.com/es/buscar)
- **Bodabook** (https://www.bodabook.com/es/boda/soy-invitado)

También tenemos la posibilidad de hacer búsquedas en Google mediante el operador *site:* y el nombre de los novios para encontrar páginas personales de algunos de estos servicios:

Ejemplo: site:zankyou.com -www NOMBRE

Árboles genealógicos

Existen servicios online donde podemos crear nuestro árbol genealógico y donde, además, podemos consultar los árboles de otras personas:

-Geneanet (https://es.geneanet.org/)

-Familysearch (https://www.familysearch.org/)

Esquelas

Los servicios online para publicar esquelas pueden ofrecernos información tanto de la persona que buscamos, como de los familiares, así como del lugar de residencia, ya que en muchas ocasiones muestran el lugar donde se llevarán a cabo los distintos actos funerarios.

Rememori (https://www.rememori.com)

Generar emails a partir del nombre

Casi todos usamos variaciones de nuestro nombre a la hora de crear una cuenta de email. Una forma de averiguar el email de una persona es realizar distintas combinaciones del nombre que dispongamos al objeto de verificar posteriormente si dichas combinaciones de email existen, y pudiesen

pertenecer a la persona que buscamos, para ello podemos usar algunas herramientas que nos facilitan esta labor generando de forma automática diferentes combinaciones. Para ello podemos utilizar las herramientas de Inteltechniques (https://inteltechniques.com/OSINT/email.html).

En el capítulo de Emails veremos cómo verificar y buscar a personas en base a su email.

Flujo de trabajo

Puedes acceder al flujo de trabajo de Ciberpatrulla (https://ciberpatrulla.com/buscar-persona-nombre-apellidos/) el cual te ayudará a la hora de encontrar personas en Internet en base al nombre y apellidos.

Nicknames

Introducción

Los nombres de usuario o nicknames, a simple vista, pueden parecer que carecen de información de valor para una investigación, pero nada más lejos de la realidad. En ocasiones es posible encontrar a personas más fácilmente a través de sus nombres de usuario que de su nombre real. A continuación veremos cómo.

Identificar usuarios

Buscadores genéricos

¿Cuál es el primer paso que solemos dar todos para buscar algo en Internet? San Google.

Pues eso es lo que puedes hacer en primer lugar para intentar encontrar un nombre de usuario en Internet, buscar en Google.

Buscadores específicos

Además de los buscadores genéricos, como Google y Bing, existen otros buscadores más específicos para buscar nombres de usuario. Estos buscadores analizan las redes sociales y otros servicios en Internet en busca de coincidencias, y si existe una cuenta asociada a un Nick igual te lo dirá, aunque eso no garantice que dicha cuenta sea de la persona que buscamos.

La mayoría disponemos de varios perfiles en distintas redes sociales y, lo normal, es utilizar el mismo nombre de usuario en todas ellas, por tanto podemos realizar búsquedas en redes sociales en base al nombre de usuario

que dispongamos. Podemos hacerlo de forma manual o utilizar servicios que facilitan esta búsqueda como Namechk (https://namechk.com/).

Comprobaciones manuales

Además del paso anterior puedes hacer comprobaciones manuales de algunos perfiles sociales. Al final será el paso que tengas que dar, es la única forma de cerciorarse de que el perfil o servicio que has encontrado corresponde con el Nick que queremos identificar.

Posibles direcciones de email

Al igual que con los nombres, podemos usar los nicknames para hacer combinaciones de posibles cuentas de email de la persona que buscamos. Para ello podemos utilizar también las herramientas de Inteltechniques (https://inteltechniques.com/OSINT/email.html).

En el capítulo de Emails veremos cómo verificar y buscar a personas en base a su email.

Sitios que facilitan las búsquedas de Nicknames

Podemos acelerar el proceso de búsqueda de nombres de usuario utilizando los accesos directos y herramientas de estas dos webs:

-Aware-Online (https://aware-online.com/academy/osint-tools/gebruikersnamen/)

-Inteltechniques (https://inteltechniques.com/osint/menu.user.html)

Flujo de trabajo

Puedes acceder al flujo de trabajo de Ciberpatrulla (https://ciberpatrulla.com/identificar-personas-nombre-usuario-nick/) el cual te ayudará a la hora de encontrar personas en Internet en base al nombre de usuario.

Emails

Introducción

Cuando estamos buscando información en Internet en base a una dirección de email, tenemos que tener en cuenta algunos aspectos previos propios de las direcciones de email. El origen del email determinará algunos pasos previos en el análisis y la búsqueda de información. Podemos haber obtenido una dirección de email de forma casual, realizando búsquedas en fuentes abiertas o podemos haberlo obtenido porque nos han aportado una dirección de email desde la que han recibido un mensaje.

En el segundo caso es conveniente acceder a las cabeceras técnicas del email[151] recibido, para analizar la procedencia. Analizando las cabeceras[152] del email, comprobaremos que dicha cuenta de email es real y no ha sido suplantada[153]. Verificar este detalle nos puede evitar seguir caminos que no conducen a ninguna parte o que nos llevan a objetivos equivocados.

Obtener información con un email

Buscadores genéricos

Como siempre, hemos de realizar búsquedas en los buscadores genéricos como Google, donde pueden aparecer diversos resultados.

Utilizando los operadores de Google podemos hacer todas las combinaciones

151. Rastrear un correo mediante sus cabeceras completas - https://support.google.com/mail/answer/29436?hl=es
152. Herramientas forense para ser un buen CSI. Parte LI: Forense de emails - https://www.flu-project.com/2014/07/herramientas-forense-para-ser-un-buen.html
153. Herramientas forense para ser un buen CSI. Parte LII: Forense de emails - https://www.flu-project.com/2014/07/herramientas-forense-para-ser-un-buen_24.html

que se nos ocurran.

Estos son algunos ejemplos:

"*nombreusuario@email.com*"

"*nombreusuario@email.com*" *filetype:pdf OR filetype:doc*

"*NOMBREUSUARIO@hotmail.com*" *OR* "*NOMBREUSUARIO@gmail.com*" *OR* "*NOMBREUSUARIO@yahoo.com*"

Posibles direcciones de email

Aunque en el último ejemplo del paso anterior no hayamos tenido suerte buscando en Google con variaciones de servicios de email (Hotmail, Gmail, Yahoo, etc.), no quiere decir que no puedan existir cuentas de email asociadas a dichos servicios. Podemos hacer otra comprobación y es verificar que dicha cuenta existe.

Para hacer esta comprobación podemos usar servicios como el siguiente:

Mailtester (http://mailtester.com/testmail.php).

Buscar en Gmail

Si la cuenta que queremos identificar es de Gmail podemos obtener información de dicho contacto simplemente simulando el envío de un email. Para ellos solo tenemos que entrar en nuestra cuenta de Gmail y comenzar el proceso de envío de un email, sin llegar a hacerlo. Una vez que tengamos introducida la dirección de email de envío en la casilla *Para:*, solo tenemos que colocar el cursor encima de la misma y nos mostrará el nombre que utilizar para esa cuenta de email.

Buscar en buscadores de personas

Como hemos visto en otras guías, podemos utilizar buscadores específicos para buscar personas, ya sea por su nombre, teléfono o, como este caso, por su email.

Puedes probar en Pipl (https://pipl.com/).

Buscar en Redes Sociales

Con motivo de algún que otro escándalo sobre datos de usuarios de redes sociales[154], y con la entrada en vigor, este año, del nuevo RGPD[155], las plataformas de redes sociales han restringido el acceso a determinados datos que, hasta hace poco, cualquiera podía obtener de forma sencilla. Me estoy refiriendo a, mediante una simple búsqueda, saber por su email si una persona disponía de una cuenta en una red social. Esto ya se ha acabado, aunque no del todo. Se ha acabado utilizando el método habitual, pero podemos hacerlo entrando por la puerta de atrás.

Podemos usar los propios buscadores de las redes sociales para encontrar emails publicados, por los propios usuarios, en los post enviados por ellos mismos. Podemos hacer búsquedas dentro de la red social como las siguientes:

"*mi email es DIRECCIÓN EMAIL*"

"*te dejo mi email*" *DIRECCIÓN EMAIL*

En el caso de tener suerte y que aparezca publicado la dirección de email que nos interesa podremos asociarla con ese perfil social.

Te dejo un artículo de Ciberpatrulla donde explico algunos métodos alternativos para comprobar si una cuenta de email está asociada a varios perfiles sociales (https://ciberpatrulla.com/buscar-personas-rrss-email/).

Buscar por nombre de usuario

Como hemos visto en el capítulo sobre cómo identificar personas por su nombre de usuario (Nick), podemos hacer búsquedas solo del nombre de usuario del email, en las que podemos encontrar perfiles en RRSS u otras cuentas de emails alternativas del mismo propietario.

---

154. Facebook intercambia información de los usuarios con entidades bancarias en EE UU - https://elpais.com/tag/caso_cambridge_analytica/a
155. GDPR/RGPD: qué es y cómo va a cambiar internet la nueva ley de protección de datos - https://www.xataka.com/legislacion-y-derechos/gdpr-rgpd-que-es-y-como-va-a-cambiar-internet-la-nueva-ley-de-proteccion-de-datos

El nombre de usuario de un email es el que aparece justo antes de la @ (ejemplo: *NOMBREUSUARIO@email.com*). Podemos seguir los pasos que hemos visto para buscar con los nicknames usando solo esta parte del email.

Búsquedas inversas de Whois

Cuando hacemos las consultas Whois a la base de datos donde se almacena la información de los propietarios de un sitio web, no solo podemos hacerlas por el nombre de dominio, también podemos hacerla por nombre, por número de teléfono o por el email. Para ello podemos usar servicios online que nos permiten realizar este tipo de consultas, como Whoxy (https://www.whoxy.com/).

Buscar en servicios de Currículums Vítae

Internet está repleto de servicios online para buscar trabajo y enviar nuestro CV. Solo tienes que hacer algún tipo de búsqueda en Google del tipo "buscar Currículums" y te mostrará decenas de servicios. Algunos de estos servicios te permiten buscar dentro de estos CV al objeto de encontrar posibles candidatos para puestos de trabajo. Una peculiaridad de estos servicios es que en los CV que envían lo usuarios suelen aparecer todos los datos de contacto del mismo (nombre, dirección, número de teléfono, etc.), además de toda la experiencia laboral y académica.

Puedes entrar en algún servicio como el que te dejo a continuación y hacer búsquedas por dirección de email:

Indeed (https://www.indeed.es/reclutamiento/buscar-candidatos).

Verificar la opción de recuperar contraseña

Podemos utilizar un método muy sencillo, que no es otro que el de usar la opción de "*¿Has olvidado la contraseña?*" que nos suelen ofrecer todos los sitios donde necesitamos conectarnos mediante usuario y contraseña. La forma que tienen de ayudarnos a recuperar la contraseña olvidada es la de enviarnos una nueva a nuestro email o un enlace desde donde podemos cambiarla.

Nosotros no queremos recuperar la contraseña, solo saber si el email está

asociado a un perfil social o servicio online, y tampoco queremos terminar todo el proceso de recuperación de la contraseña, porque podría llegarle un email a la persona que estamos investigando.

En nuestro caso necesitamos dos cuentas de email, una que sabemos que no se está usando en dicha red social y la otra, la que queremos verificar.

Ahora solo tenemos que comenzar el proceso de recuperación de la contraseña y nos pedirá un email, donde introduciremos las dos direcciones de email y comprobaremos si el aviso que muestra es diferente en caea caso. Si es diferente sabremos que el queremos verificar está asociada a dicho servicio.

Otro dato que a veces aparece cuando utilizamos la opción de recuperar la contraseña es el número de teléfono asociado, aunque solo suele mostrar un par de dígitos, normalmente los dos últimos, salvo en el caso de PayPal que llega a mostrar hasta 5 cifras, la primera y las cuatro últimas. Aunque aparentemente no nos ofrezca mucha información nos puede servir para abrir nuevos caminos de búsqueda.

Buscar en bases de datos de servicios comprometidos

Los hackeos de servicios online[156] están a la orden del día. Existe un gran negocio detrás del robo de estas bases de datos. Algunas de estas bases de datos terminan siendo públicas y podemos buscar en ellas coincidencias con la cuenta de email que estamos buscando.

Estos son algunos de los servicios que podemos utilizar para realizar las búsquedas:

- Haveibeenpwned (https://haveibeenpwned.com/)
- Ghostproject (https://ghostproject.fr/)
- Weleakinfo (https://weleakinfo.com/)

156. Descubren a la venta base de datos con 1.400 millones de contraseñas de Netflix, YouPorn y otros servicios - https://www.fayerwayer.com/2017/12/descubren-la-venta-base-de-datos-con-1-400-millones-de-contrasenas-de-netflix-youporn-y-otros-servicios/

- Inteltechniques (https://inteltechniques.com/osint/pastebins.html)
- Netbootcamp (https://netbootcamp.org/pastesearch.html)

Herramientas que facilitan las búsqueda

Te dejo dos enlaces con herramientas que te facilitarán las búsquedas:

-Ciberpatrulla (https://ciberpatrulla.com/links/) (Emails)

-Inteltechniques (https://inteltechniques.com/osint/email.search.html)

-Inteltechniques (https://inteltechniques.com/osint/iframe/docs.both.html)

Flujo de trabajo

Puedes acceder al flujo de trabajo de Ciberpatrulla (https://ciberpatrulla.com/identidad-persona-correo/) el cual te ayudará a la hora de encontrar personas en Internet en base a su dirección de email.

Teléfonos

Introducción

En este capítulo veremos qué información podemos obtener a partir de un número de teléfono, y en especial en lo relacionado a número de teléfonos móviles, ya que estos son los que más habitualmente nos vamos a encontrar.

Existen servicios online que nos ofrecen la posibilidad de, a partir de un nombre y de una localidad, encontrar solo titulares de línea de telefonía fija, mostrando incluso el domicilio del mismo, pero si queremos hacer la búsqueda inversa, es decir, a partir de un número de teléfono fijo o móvil encontrar a su titular, no existe dicha posibilidad.

Para asociar un número de teléfono con un usuario tendremos que usar las fuentes abiertas y otras técnicas que a continuación veremos.

Obtener información con un número de teléfono

Buscadores genéricos

Como siempre, antes de hacer búsquedas más complejas, podemos usar nuestro querido Google y utilizar los operadores para hacer búsquedas avanzadas. A continuación te dejo dos combinaciones de búsqueda, solo tienes que cambiar los ceros por el nº que quieras buscar y añadir cuantas combinaciones se te ocurran:

"*000000000*" *OR* " *000000000*" *OR* "*-000000000*" *OR* "*34 000000000*" *OR* "*+34 000000000*"

"000000000" OR "000-000-000" OR "000.000.000" OR "000 000 000"

Buscar en redes sociales

En ocasiones los propios usuarios publican sus números de teléfono en los mensajes o tweets en las redes sociales. Podemos hacer búsquedas del tipo: *"mi número de teléfono es 000000000"; "mi móvil es 000000000"; "llamarme al 000000000"*.

Verificar la opción de recuperar contraseña

Al igual que hemos visto para los emails, podemos usar la opción de *"¿Has olvidado la contraseña?"* que nos suelen ofrecer las redes sociales y otros servicios online en los que hayamos utilizado un número de teléfono para conectarnos a la cuenta.

En nuestro caso necesitamos dos números de teléfono móvil, uno que sabemos que no se está usando en dicha red social y otro el que queremos verificar.

Ahora solo tenemos que comenzar el proceso de recuperación de la contraseña y nos pedirá un número de teléfono móvil, donde introduciremos los dos números y comprobaremos si el aviso que muestra es diferente en cada caso. Si es diferente sabremos que el número que queremos verificar está asociado a dicho servicio.

Servicios de búsqueda inversa

Existen algunos servicios online que ofrecen cierta información de identificación de números móviles. Aunque suele ser solo el nombre, y no completo, para un investigador puede ser un dato más que suficiente para abrir nuevas líneas de investigación.

Aquí te dejo algunos de ellos:

-Whocalld (https://whocalld.com)

-Opencnam (https://www.opencnam.com)

-**Truecaller** (https://www.truecaller.com)

-**Sync** (https://sync.me/)

Aviso: al instalar las aplicaciones móviles Truecaller y Sync en tu dispositivo incluirán automáticamente todos tus contactos en su base de datos. Si necesitas trabajar con estas aplicaciones es recomendable usar un emulador y/o un número de teléfono exclusivo para ello. En el próximo capítulo veremos cómo trabajar con emuladores.

Buscadores específicos

Existen ciertos servicios online que, introduciendo determinados datos personales, nos pueden dar bastante información. No solo puedes buscar por nº de teléfono, también por nombre o email. Uno de los más conocidos es: Pipl (https://pipl.com).

Buscar en Webs de anuncios

Los servicios online para publicar anuncios son una fuente importante de información, nos pueden dar nombres, direcciones, vehículos, emails, fotos del interior de la vivienda y número de teléfono de contacto.

Podemos hacer una búsqueda en algún servicio de anuncios online y probar si este teléfono se encuentra público. No todas las webs de anuncios muestran este dato públicamente, y no todas te dejan realizar búsquedas con este filtro. Tan solo he encontrado una web de anuncios que lo hace, y es Milanuncios (https://www.milanuncios.es/).

Cuando publicamos un anuncio, lo normal es incluir fotografías del producto anunciado, dichas imágenes, junto con el anuncio, pueden haber sido indexadas por Google Images, y estas pueden estar relacionadas con el número de teléfono publicado en el anuncio, por lo que no está de más buscar el número de teléfono en Google Images.

Averiguar a qué operador corresponde un teléfono

Saber el operador donde se ha contratado un número de teléfono nos ayudará

en el caso de que tengamos que solicitar la información del abonado a dicha compañía. Podemos buscar la compañía utilizando servicios como (https://www.peoplecall.com/), en el que, además, podremos averiguar si ha sido portado a otra compañía.

Obtener información de aplicaciones de mensajería

Un truco que es posible que ya hayas usado con anterioridad es el de crear un contacto en tu agenda del móvil con el número de teléfono que te interesa identificar, de esta forma podrás acceder a la información pública que dispone en las aplicaciones de mensajería como WhatsApp, en la que podremos ver la foto de perfil y cualquier otro dato que tenga visible. Igualmente si realizamos la misma operación con la aplicación Messenger de Facebook podremos saber si dicho número de teléfono está asociado a un perfil de Facebook. Puedes hacer pruebas con cuantas aplicaciones de mensajería se nos ocurra.

Al igual que te comentaba más atrás, es recomendable que esto se haga con teléfonos exclusivos para esta tarea o a través de emuladores, como veremos en el siguiente capítulo.

Buscar en listas de spam

Existen servicios en Internet que recopilan números de teléfono denunciados por realizar spam. Dichas bases de datos suelen ser alimentadas por los propios usuarios que sufren llamadas indeseadas, en las que además de añadir el número, comentan sus experiencias. No viene mal consultarlas por si el número que buscamos se encuentra en alguna de estas bases de datos.

Algunos de estos servicios son: Quienhallamado (http://www.quienhallamado.es/) o Listaspam (https://www.listaspam.com/).

Herramientas que facilitan las búsqueda

Puedes usar la sección de herramientas de Ciberpatrulla donde encontrarás herramientas y servicios online donde buscar números de teléfono:

-Ciberpatrulla (https://ciberpatrulla.com/links/) (Teléfonos)

-Inteltechniques (https://inteltechniques.com/osint/iframe/docs.both.html)

Flujo de trabajo

Puedes acceder al flujo de trabajo de Ciberpatrulla (https://ciberpatrulla.com/averiguar-titular-telefono-movil/), el cual te ayudará a encontrar información a partir de un número de teléfono.

Emulación

Introducción

En capítulos anteriores te he hablado de las posibilidades que nos ofrecen algunas aplicaciones de redes sociales. Con ellas podemos obtener información de una persona agregando sus datos de contacto a nuestra agenda, y en algunos casos vamos a necesitar disponer de un dispositivo móvil en el que sincronizar nuestros contactos y poder así acceder a información de interés.

Para realizar estas tareas es conveniente utilizar números de teléfonos exclusivos, pudiéndose usar en un smartphone o una tablet, pero además podemos utilizar un emulador donde poder ejecutar de forma virtual un dispositivo Android en un PC y así proteger nuestra privacidad y ahorrar costes. Un emulador nos ofrece la posibilidad de cambiar nuestra ubicación GPS real de forma mucho más sencilla que un dispositivo móvil.

A continuación veremos cómo hacerlo.

Cómo instalar un emulador Android

Te pego la definición de emulador[157] de la Wikipedia:

"*En informática, un emulador es un software que permite ejecutar programas o videojuegos en una plataforma (sea una arquitectura de hardware o un sistema operativo) diferente de aquella para la cual fueron escritos originalmente. A diferencia de un simulador, que solo trata de reproducir el comportamiento del programa, un emulador trata de modelar de forma precisa el dispositivo de manera que este funcione como si*

157. Definición de Emulador - https://es.wikipedia.org/wiki/Emulador

estuviese siendo usado en el aparato original."

En nuestro caso el software que vamos a utilizar está pensado para poder ejecutar un sistema operativo móvil Android en nuestro PC de la misma forma que lo usaríamos en un smartphone o tablet.

Qué emulador usar

Para nuestras investigaciones vamos a usar el emulador Genymotion (https://www.genymotion.com/fun-zone/) para configurar un dispositivo virtual Android. Genymotion es compatible con los sistemas operativos Microsoft Windows; macOS y Linux.

Genymotion es un emulador muy popular, especialmente utilizado por desarrolladores de aplicaciones, pero, además dispone de una versión gratuita para uso personal y pensada principalmente para instalar juegos.

Para ejecutar dispositivos virtuales, tenemos que instalar Oracle VM VirtualBox. No te preocupes que te voy a dejar guías para su instalación y configuración.

Guías de instalación

-Vídeo tutorial (español) (https://www.youtube.com/watch?v=72JQPComCqM)

-Tutorial (español) (https://securityhacklabs.net/articulo/instalacion-y-configuracion-de-genymotion-un-emulador-de-android-para-linux-windows-y-mac)

-Tutorial (inglés) (https://www.bellingcat.com/resources/how-tos/2018/08/23/creating-android-open-source-research-device-pc/)

-Guía oficial Genymotion (inglés) (https://docs.genymotion.com/latest/Content/01_Get_Started/Get_started.htm)

DNIs

Introducción

El número del documento nacional de identidad (DNI), es un dato único para cada persona y que al contrario que el nombre, no se puede repetir. Aunque parezca increíble, si disponemos de un número de DNI, son muchas las fuentes en Internet que podemos utilizar para buscar información, y la mayoría son webs oficiales.

Dónde buscar por DNI

Buscadores genéricos

Cómo en todos los casos, el primer sitio donde podemos dirigirnos es a los buscadores genéricos, como Google, donde podemos utilizar combinaciones de búsquedas como la siguiente:

DNI OR D.N.I. "00000000" OR " 000000000" OR "00000000A" OR " 000000000A" OR "000000000-A" OR "000000000 A" OR " 000000000 A" OR "00.000.000A" OR "00.000.000-A" OR "00.000.000 A"

Boletines oficiales

Los boletines oficiales son una fuente para obtener datos personales muy valiosa. En estos boletines aparecen diariamente publicaciones de todo tipo, como embargos, notificaciones de sanciones administrativas, adjudicaciones, y muchos otros actos que requieren de la publicación en dichos boletines.

Para realizar las búsquedas en estos sitios tenemos que utilizar términos exactos por DNI. Tenemos que introducir el DNI tal cual está publicado, de lo

contrario no lo mostrará en los resultados de la búsqueda. Es conveniente probar varias combinaciones, como por ejemplo:

00000000A, 00000000-A, 00.000.000-A, 00.000.000G

El boletín oficial del estado dispone de un servicio en el que podremos guardar nuestras búsquedas para futuras consultas de alertas y además, podemos crear alertas para que nos avise cuando aparezca alguna publicación con contenido de nuestro interés.

Te dejo los enlaces a los buscadores de los boletines:

- **Todo el BOE** (https://www.boe.es/buscar/boe.php)
- **BOE (Multas, embargos)** (https://www.boe.es/tablon_edictal_unico/notificaciones.php)
- **TESTRA (Multas)** (https://sede.dgt.gob.es/es/aplicaciones/testra-sin-certificado.shtml)
- **BORNE (Registro mercantil)** (https://www.boe.es/anuncios/anborme.php)
- **Boletines autonómicos** (https://www.boe.es/legislacion/enlaces/boletines_autonomicos.php)
- **Boletines provinciales** (https://www.boe.es/legislacion/enlaces/boletines_provinciales.php)
- **Alertas del BOE** (https://www.boe.es/a_la_carta/)
- **Boletines municipales**. Podemos acceder a las webs oficiales de los ayuntamientos y consultar sus boletines oficiales. Para acceder al boletín de algún ayuntamiento en particular solo tienes que escribir en la caja de búsqueda de Google "*Boletín Oficial del Ayuntamiento de NOMBRE AYUNTAMIENTO*" (sin comillas).

Buscar en curriculums vitae

Ya hemos visto en el capítulo sobre teléfonos cómo buscar en servicios online

de búsqueda de trabajo. Estos servicios también los podemos usar para buscar por DNI.

Verificar la opción de recuperar contraseña

El DNI no es un dato que solamos utilizar para darnos de alta en servicios online, normalmente utilizamos una dirección de email o un número de teléfono móvil, pero existen algunos servicios en los que el DNI es obligatorio para identificarse, como pueden ser los servicios bancarios.

Al igual que sucede con algunas redes sociales, si utilizamos la opción de "recuperar la contraseña" en estos servicios, e introducimos el DNI, nos proporcionará alguna información, por ejemplo si tiene una cuenta en dicho banco, o algunos dígitos de la tarjeta de débito asociada, o los últimos números del teléfono móvil asociado.

Vehículos

Introducción

En el transcurso de una investigación podemos encontrar información sobre un vehículo, ya sea un automóvil, un barco, una moto de agua, una avioneta o el número de un vuelo determinado. En el siguiente capítulo vamos a ver qué información podemos obtener a partir de estos datos y qué servicios o métodos podemos utilizar para obtenerla.

Información sobre vehículos

Buscadores genéricos

Podemos empezar buscando en los buscadores genéricos utilizando los datos que dispongamos, ya sea matrícula o número VIN.

En el caso de que no dispongamos de todos los datos de la matrícula podemos utilizar asteriscos como en este ejemplo "**0AAA*" (sin comillas).

Además de los buscadores genéricos puedes probar en sitios web sobre coches, como páginas de anuncios o en foros especializados.

Buscar en sitios oficiales

En España podemos hacer algunas consultas muy genéricas de forma gratuita y algunas más detalladas pagando una tasa. En el caso de los automóviles, podemos obtener un informe muy simple y gratis en el que nos muestra la marca y modelo, fecha de matriculación y tipo de combustible que utiliza

dicho vehículo, pero si necesitamos un informe completo del vehículo[158], hay que pagar una tasa de 8,5€.

Puedes acceder a dicho servicio aquí (https://sede.dgt.gob.es/es/tramites-y-multas/tu-coche/informe-de-vehiculo/).

Al igual que hemos visto en el capítulo de DNIs, podemos utilizar los tablones de anuncios oficiales para realizar búsquedas por matrícula de un vehículo para comprobar si existe algún tipo de publicación relacionada. Algunos de estos tablones son:

TESTRA (Multas) (https://sede.dgt.gob.es/es/aplicaciones/testra-sin-certificado.shtml)

Tablón edictal (https://www.boe.es/tablon_edictal_unico/notificaciones.php)

En el caso de que, además de la matrícula, dispongamos del número de DNI del titular, podemos obtener el número de identificación del vehículo (VIN) utilizando la herramienta de la Junta de Andalucía (http://www.juntadeandalucia.es/economiayhacienda/apl/surweb/modelos/modelo621/621.jsp). Puedes probar esta herramienta con tu propio vehículo y tu DNI.

Números de identificación del vehículo

Si el dato del que disponemos es el número de identificación de un vehículo (VIN[159]), podemos obtener información sobre el tipo de vehículo, marca, modelo y algunas características del mismo. Para realizar esta consulta podemos utilizar herramientas como la de Vin-info (https://es.vin-info.com/).

Información sobre aviones

Los aviones civiles también disponen de matrícula, y podemos consultar algunos registros para obtener información del titular, ya sea empresa,

158. Cómo saber los datos del titular de un coche - https://www.dieselogasolina.com/guias/como-saber-titular-coche.html
159. Qué es el número VIN - https://es.vin-info.com/que-es-un-vin

particular o compañía aérea.

Además podemos hacer un seguimiento en vivo de determinados vuelos utilizando algunos servicios online como el de AENA (http://www.aena.es/csee/Satellite/infovuelos/es/) o el de Flightaware (https://es.flightaware.com/live/).

Información sobre barcos

Me ha costado bastante encontrar información sobre registros de barcos, y en realidad no he encontrado (que no quiere decir que no exista) un registro público online. El mundo marítimo tiene su peculiaridad y para que entiendas un poco qué información podemos obtener de una matrícula de un barco y a dónde dirigirnos en caso de necesitarlo te dejo este artículo (https://www.exponav.org/los-registros-de-los-buques-y-las-listas/).

Existe un Registro de Matrícula en cada Distrito Marítimo y un Registro Central llevado por la Dirección General de la Marina Mercante.

Los barcos deben estar matriculados, en uno y sólo uno, de los Registros de Matrícula de Buques de cada provincia. Estos Registros de Matrícula de Buques, son públicos y de carácter administrativo. Cada Capitanía Marítima dispone de su propio Registro de Matrícula el cual está a cargo del Capitán Marítimo correspondiente de la Provincia. Aquí te dejo un listado de las capitanías y distritos marítimos (https://www.fomento.gob.es/marina-mercante/capitanias-maritimas/relacion-entre-capitanias-y-distritos-maritimos).

Si necesitas obtener información de una embarcación en vivo, puedes utilizar el servicio online Marinetraffic (https://www.marinetraffic.com/), ideal si queremos saber la ubicación exacta de una embarcación.

Empresas

Introducción

En este capítulo vamos a ver de qué opciones disponemos para obtener información de una empresa a través de Internet de forma pública. Va a depender de los objetivos que persigamos para elegir las fuentes a consultar. Podemos tener interés en saber quién es el responsable de una empresa; podemos querer saber quiénes son sus empleados o podemos tener interés en información de la organización interna de la misma. A continuación veremos dónde dirigirnos en cada caso.

Información sobre empresas

Registros oficiales

Si queremos obtener información básica de una empresa, lo mejor es dirigirnos al registro mercantil, donde podremos obtener los datos del responsable además del CIF y domicilio de la empresa, entre otra información.

Para obtener esta información podemos utilizar servicios como el de Libreborme (https://libreborme.net/).

También podemos utilizar los buscadores de los boletines oficiales donde podemos encontrar información de interés, ya sea de litigios, embargos, resoluciones o de cualquier otra índole. En la sección *Empresa/Profesional* del repositorio de Ciberpatrulla (https://ciberpatrulla.com/links/) podrás encontrar todos los enlaces a estos servicios.

Buscadores genéricos

Google no puede faltar dentro de las recomendaciones para buscar información de una empresa. Podemos realizar búsquedas simples o utilizar las combinaciones que ya hemos visto en capítulos anteriores. En este artículo puedes encontrar ejemplos de muchas combinaciones de búsqueda en Google (https://ciberpatrulla.com/buscar-google/).

Google Groups

Google Groups (https://groups.google.com/forum/) es una fuente muy importante de información que no se suele utilizar mucho. Podemos buscar por el dominio del email de la empresa (*@dominio)* y, en el caso de que existan grupos relacionados con dicha empresa, puede mostrarnos conversaciones con personal de la misma. No voy a poner ejemplos, pero te sorprendería todo lo que hay indexado y en abierto en esta red.

Servicios de pastebin

Podemos hacer consultas en los servicios de pastebin. En ocasiones puede publicarse información de interés sobre una empresa. Para ello podemos utilizar el buscador personalizado de Inteltechniques (https://inteltechniques.com/osint/pastebins.html). Podemos buscar por dominio de email, por nombre de la empresa, o por cualquier otro dato asociado a la misma.

Sitio web de la empresa

Prácticamente todas las empresas disponen de página web, aunque todavía hay rezagados que no se han subido al tren digital. Si la empresa que estamos investigando dispone de un sitio web, podemos revisarlo en busca de información. Puedes consultar el capítulo sobre Webs, donde encontrarás muchos consejos para obtener información de un sitio web.

LinkedIn

LinkedIn te permite encontrar información de empleados de una empresa y

qué cargo tienen dentro de ella, pero no solo obtendremos información de sus empleados, también obtendremos la información que estos compartan, de forma pública, de su empresa. Puedes consultar el capítulo sobre Otras RRSS y en la sección de LinkedIn encontrarás trucos para obtener información de esta red social.

Reseñas en buscadores

Las reseñas en los buscadores es otra fuente de información. En estos servicios podemos obtener información de la experiencia de los clientes e, incluso, podemos obtener respuestas de los responsables de la empresa. Uno de los sistemas más conocidos es el del propio buscador Google.

Si realizamos una búsqueda en Google por el nombre de una empresa, es muy probable que aparezca un resultado destacado de la misma, donde obtendremos la información de contacto, así como horarios de apertura y cierre, y en muchas ocasiones aparecerán reseñas de clientes.

Ofertas de trabajo

Podemos obtener información de ofertas de trabajo publicadas por una empresa en servicios online o en su propia web. Podemos utilizar LinkedIn Jobs (https://es.linkedin.com/jobs), o cualquier otro servicio que conozcamos. También podemos utilizar Google para encontrar todos los anuncios indexados en este buscador.

Este es un ejemplo de una posible combinación de búsqueda en Google:

"EMPRESA" intext:oferta de trabajo OR intext:puestos de trabajo OR intext:oferta de empleo

Redes sociales

Los perfiles sociales de una empresa pueden ser una fuente complementaria donde obtener información, incluso puede darse el caso que la empresa no disponga de sitio web pero si cuente con perfiles sociales. La metodología para investigar en redes sociales ya la hemos visto en capítulos anteriores.

Imágenes

Introducción

Las imágenes digitales pueden proporcionar mucha más información de la que aparece en la propia imagen. En este capítulo vamos a ver cómo acceder a información oculta de una imagen analizando los metadatos de la misma. Además veremos que pasos seguir para verificar si una imagen ha sido manipulada y también cómo podemos averiguar el lugar desde donde se tomó dicha imagen cuando esta información no está disponible en los metadatos.

Verificación de imágenes

Antes de comenzar a investigar a partir de una imagen es conveniente realizar algunas comprobaciones[160] con el fin de analizar si la imagen es real, si es actual y verificar que la ubicación es la correcta.

Como se muestra en esta guía de verificación de imágenes (https://es.firstdraftnews.org/wp-content/uploads/sites/2/2017/08/FDN_verificationguide_photos_ES.pdf), antes de comenzar debemos responder a varias preguntas:

-¿Estás mirando la versión ORIGINAL?

-¿Sabes QUIÉN captó la foto?

-¿Sabes DÓNDE se tomó la foto?

-¿Sabes CUÁNDO se tomó la foto?

-¿Sabes POR QUÉ se tomó la foto?

160. Así que quieres llevar a cabo una investigación en fuentes abiertas - https://es.globalvoices.org/2015/10/24/asi-que-quieres-llevar-a-cabo-una-investigacion-en-fuentes-abiertas/

Asegurándonos de haber respondido adecuadamente a estas preguntas podremos comenzar la investigación con la certeza de que la fuente es fiable y no terminar en un callejón sin salida.

Análisis forense de imágenes

Si tenemos dudas de si una imagen es real o no[161], podemos utilizar algunas herramientas de análisis forense de imágenes que nos ayudarán a determinar si ha sido modificada.

Fotoforensics

Por su sencillez de uso, por ser gratuita y por encontrarse online, he elegido como herramienta de análisis de imágenes Fotoforensics (http://fotoforensics.com/). Esta herramienta lo que hace, entre otras cosas, es resaltar detalles que a simple vista no se aprecian. Para ello utiliza el análisis de nivel de error (ELA), el cual permite la identificación de las áreas dentro de una imagen que se encuentran en diferentes niveles de compresión. Con las imágenes JPEG, toda la imagen debe estar más o menos al mismo nivel. Si una sección de la imagen está en un nivel de error significativamente diferentes, entonces es probable que indique una modificación digital[162].

Este es un ejemplo en el que se aprecia perfectamente la modificación de una imagen utilizando el análisis ELA (http://fotoforensics.com/analysis.php?challenge=1&id=9d40f53a05ca7cc7932ccc09b260312e9e3372c3.208035).

Con Fotoforensics, además del análisis ELA, podemos obtener los metadatos, información básica de la imagen, su valor HASH y mucha más información. Te dejo varios enlaces por si te interesa profundizar en esta herramienta y en el análisis forense de imágenes:

161. Manipulación de las fotografías a lo largo de la historia - http://pth.izitru.com/
162. Análisis básico de la veracidad de una imagen - https://es.linkedin.com/pulse/an%C3%A1lisis-b%C3%A1sico-de-la-veracidad-una-imagen-marcos-gutierrez

-Fotoforensics (Tutorial) (http://fotoforensics.com/tutorial.php)

-Fotoforensics (Ejercicios prácticos) (http://fotoforensics.com/messages.php?challenge=1)

-Blog sobre análisis forense de imágenes (http://www.hackerfactor.com/blog/)

InVID

InVID[163] es una extensión de Chrome que nos ayuda a la hora de verificar y analizar imágenes. Te dejo un video tutorial para que veas las posibilidades que ofrece (https://youtu.be/nmgbFODPiBY?t=5m16s).

Búsqueda inversa de imágenes

Uno de los pasos que podemos dar para obtener información de una imagen es realizar una búsqueda inversa en Internet. Podemos comprobar si una imagen determinada se encuentra publicada en sitios web o redes sociales.

¿Cómo podemos hacer este tipo de búsquedas?

Para ello solo tenemos que subir una imagen o pegar la URL que queremos comprobar en alguno de los servicios que te voy a dejar más abajo. Estos sitios realizan una búsqueda en Internet mostrando resultados de sitios que también contienen dicha imagen, desde los que podremos obtener más información relacionada con esta.

- **Google Images** (https://www.google.es/imghp?hl=es&tab=wi)
- **Bing Images** (https://www.bing.com/images/) (Debes cambiar la región en la configuración del buscador, elige *Estados Unidos – Inglés*)

163. InVID - https://chrome.google.com/webstore/detail/fake-video-news-debunker/mhccpoafgdgbhnjfhkcmgknndkeenfhe?hl=en

- **Yandex Images** (https://www.yandex.com/images/)
- **Tineye** (https://www.tineye.com/)
- **Baidu Images** http://image.baidu.com/

Nota: estas herramientas no son infalibles y tienen sus limitaciones. Una de ellas es que no son capaces, de momento, de identificar imágenes a las que se les hayan realizado algunas modificaciones, como por ejemplo el efecto espejo, es decir, voltear la imagen horizontalmente. En el caso de una imagen de un rostro, el lado derecho del rostro pasaría a ser el izquierdo.

En el caso de que la imagen se encuentre publicada en alguna red social como Instagram, podemos realizar una búsqueda inversa utilizando la ID de la URL de dicha imagen. En el caso de Instagram, la ID de una imagen se localiza en la parte señalada en este ejemplo en negrita (*instagram.com/p/**Bni3itVnMah**/*). Las búsquedas las podemos realizar tanto en buscadores genéricos, como dentro de otras redes sociales, como Facebook o Twitter.

Imagen de perfil

Muchos de nosotros utilizamos la misma imagen de perfil en varias redes sociales. Ya hemos visto que realizando una búsqueda inversa de una imagen podemos encontrarla en otros sitios de Internet. Si hacemos esta misma operación con la imagen de perfil de una red social es posible que localicemos otros perfiles sociales de la misma persona.

Lo mismo podemos hacer con la imagen de perfil de WhatsApp de un objetivo. Si disponemos de su teléfono, podemos, utilizando la imagen de perfil de esta aplicación, realizar una búsqueda inversa en Internet y obtener sus perfiles sociales.

Metadatos

Cada vez que realizamos una fotografía con un dispositivo digital (ya sea una cámara digital, smartphone o tablet) se añaden una serie de datos (metadatos[164]) a la propia imagen, como por ejemplo:

- Fecha y hora en la que se hizo la fotografía.
- Características del dispositivo desde el que se tomó la misma.
- En el caso de tener activada la localización GPS en el dispositivo también guardará las coordenadas exactas de donde se realizó dicha fotografía.
- Los ajustes de la cámara, como velocidad ISO, velocidad de obturación, distancia focal, diafragma, balance de blancos, tipo de lente, etc.
- Marca y modelo de la cámara o teléfono inteligente.
- Nombre del programa utilizado para editar la foto.

Hay que tener en cuenta varios aspectos sobre esta característica, uno de ellos es que los metadatos son fácilmente alterables. Cualquiera puede modificarlos[165] o borrarlos[166], por lo que estos datos deben ser contrastados con otras fuentes de información para verificar que no han sufrido ninguna manipulación. Otro aspecto a tener en cuenta es que la mayoría de las redes sociales y aplicaciones de mensajería móvil eliminan estos metadatos cuando subimos o compartimos imágenes a través de ellas.

A continuación te dejo algunas herramientas para analizar los metadatos de una imagen:

---

164. Metadatos en las fotografías: Exif e IPTC (I) - https://aprendofotografia.wordpress.com/2016/06/05/15a-metadatos-en-las-fotografias/
165. Cómo geolocalizar dónde se hizo una fotografía - https://computerhoy.com/noticias/imagen-sonido/como-geolocalizar-donde-hizo-fotografia-75601
166. Qué son y cómo borrar los metadatos de una foto en Windows 10 - https://www.xataka.com/basics/que-son-y-como-borrar-los-metadatos-de-una-foto-en-windows-10

-Regex (http://exif.regex.info/exif.cgi)

-Readexifdata (https://readexifdata.com/)

-Pic2map (https://www.pic2map.com/)

Geolocalizar una imagen

Ya hemos visto que a través de los metadatos podemos obtener la ubicación exacta de una fotografía, pero este dato no siempre va a estar disponible en los metadatos, por lo que, para verificar la ubicación real de una fotografía, deberemos utilizar métodos de observación, así como realizar comprobaciones con otras fuentes de información.

Examinando la imagen al detalle encontraremos pistas que pueden ayudarnos a identificar la ubicación y momento en que la fotografía fue tomada:

- Matrículas de los vehículos
- Condiciones climáticas
- Paisajes
- Anuncios publicitarios
- Vestimenta
- Señales de tráfico
- Edificios
- Reflejos en cristales o espejos
- Decoración y mobiliario de la vivienda
- Naturaleza (plantas)

- Mobiliario urbano
- Ortografía

Identificar lugares

Mediante la utilización de mapas, servicios online y algunas redes sociales, podemos llegar a identificar o verificar la ubicación de una fotografía[167].

-Google Earth (https://www.google.com/earth/): podemos utilizar esta herramienta para visualizar una determinada zona con vista aérea, que nos puede ser muy útil si queremos identificar una fotografía tomada desde la ventana de un edificio y así ubicar dicho edificio e incluso la altura desde donde se tomó.

-Google Maps (https://www.google.com/maps/): una opción muy interesante de Google Maps es la de buscar lugares cercanos a una ubicación concreta. Por ejemplo si queremos saber cuántas farmacias se encuentran cerca de un punto concreto del mapa solo tenemos que realizar una búsqueda en Google Maps y una vez que nos muestre el punto concreto que le hemos señalado, hacemos clic en la opción "*Sitios Cercanos*" y ahora podremos volver a hacer una nueva búsqueda por alguna palabra clave que nos interese, como por ejemplo: farmacias, restaurantes o peluquerías. Ahora nos mostrará las coincidencias que existen cerca del punto señalado. Te dejo un vídeo tutorial con algunos consejos de uso (https://www.youtube.com/watch?v=aWi51a7WbSw).

-Mygeoposition (http://es.mygeoposition.com/): con esta herramienta podemos obtener las **coordenadas** de un punto en concreto en un mapa.

-Foursquare (https://es.foursquare.com): en este servicio podemos visualizar **imágenes realizadas por usuarios** en hoteles, restaurantes, zonas

167. Reflejos de vidrio en imágenes + OSINT = Ubicación más precisa - https://ioactive.com/glass-reflections-in-pictures-osint-more-accurate-location/

de ocio y zonas turísticas.

-Tripadvisor (https://www.tripadvisor.es/Attractions): podemos obtener **fotografías realizadas por usuarios** en hoteles, restaurantes y zonas de ocio y turismo

-Instagram "*site:https://www.instagram.com/explore/locations/ hotel palace madrid*": mediante esta búsqueda en Google (sin las comillas), encontraremos **fotografías de un lugar concreto**, en este caso el hotel The Westin Palace Madrid, compartidas por los propios usuarios o perfiles oficiales en Instagram.

-Facebook (https://www.facebook.com/search/str/141270646560/users-checked-in/intersect): con esta búsqueda de Facebook estamos buscando **usuarios que han estado en un determinado sitio**, en este caso en el hotel The Westin Palace, Madrid y que pueden haber compartido fotografías del mismo.

-Facebook (https://www.facebook.com/search/141270646560/photos-in/): con esta búsqueda obtendremos **fotografías de usuarios realizadas en un determinado lugar**, en este caso en el hotel The Westin Palace Madrid.

-Facebook (https://www.facebook.com/search/str/plaza%20mayor%20madrid/photos-keyword): con esta búsqueda obtendremos **fotografías etiquetadas por usuarios sobre un determinado lugar**.

-Facebook (https://www.facebook.com/search/str/plaza%20mayor%20madrid/stories-keyword): con esta búsqueda obtendremos **posts que hablan sobre un determinado lugar** y que pueden contener fotografías del mismo.

-Facebook (https://www.facebook.com/search/str/plaza%20mayor%20madrid/pages-named/visitors/intersect): con esta búsqueda estamos buscando **personas que han visitado un determinado**

lugar y pueden haber compartido alguna fotografía del mismo.

También podemos utilizar **páginas de reservas** de alojamientos, restaurantes para identificar establecimientos a través de su ubicación o fotografías.

Identificar edificios de una ciudad

En ocasiones podemos visualizar una determinada zona en la que la única información de la que disponemos es de algunos edificios de la zona. Para identificar estos edificios y obtener información de los mismos, podemos utilizar algunos servicios online como los siguientes:

-Skyscraperpage (http://skyscraperpage.com/): base de datos de edificios de todo el mundo donde nos ofrece información de fecha de construcción, características del edificio, así como la finalidad del mismo (oficinas, hotel, etc.).

-Emporis (https://www.emporis.com/): base de datos de edificios de todo el mundo parecida a la anterior.

Identificar idioma

Podemos encontrarnos con texto dentro de la imagen, el cual puede estar en algún idioma que no podemos identificar, como japonés, chino, ruso, etc. Existen algunas aplicaciones móviles que, haciendo una fotografía a dicho texto, pueden identificar el idioma del texto y traducirlo al idioma que le digamos. Te recomiendo la aplicación Microsoft Traductor (https://translator.microsoft.com/), disponible para cualquier SO móvil.

Averiguar condiciones climáticas

Imagina que nos encontramos con una fotografía que supuestamente ha sido tomada en una fecha determinada, y en ella aparece un día radiante de sol, con esta herramienta podemos averiguar qué condiciones climáticas había en un lugar, fecha y hora determinada, y verificar si coincide con lo que muestra

una determinada fotografía.

-Accuweather (https://www.accuweather.com): consultar las condiciones climáticas en una zona y fecha determinada.

-Ogimet (http://www.ogimet.com/ranking.phtml): valores meteorológicos por zonas.

Averiguar la hora en la que se tomó la fotografía

Si queremos averiguar la hora a la que se tomó una fotografía, podemos utilizar la información de la posición del Sol en ese momento y comprobar las sombras de la imagen[168]. Para ello podemos utilizar herramientas como **Suncalc** (http://suncalc.net) para averiguar la posición del sol en una fecha y lugar determinado.

Identificar vehículos

Si queremos ubicar una fotografía a partir de los vehículos que aparecen en la misma, podemos fijarnos en las matrículas de estos. Puedes consultar **Matriculasdelmundo** (http://www.matriculasdelmundo.com/) donde encontrarás una gran base de datos de todas las matrículas de vehículos del mundo

Identificar país por las señales de tráfico

No debemos pasar por alto el tipo de señalización que aparezca en una imagen, nos puede dar muchas pistas de la localización de la misma. Puedes consultar la Wikipedia en este enlace (https://en.wikipedia.org/wiki/Comparison_of_European_road_signs#Warning) el cual contiene la tipología de las señales de tráfico según el país de origen.

168. ¿A qué hora exacta se tomó la fotografía del beso de Times Square? - https://www.muyinteresante.es/ciencia/preguntas-respuestas/a-que-hora-exacta-se-tomo-la-fotografia-del-beso-de-times-square-831439561276

Vídeos

Introducción

En este capítulo vamos a ver cómo acceder a información oculta de un vídeo analizando sus metadatos. Además veremos qué pasos seguir para verificar si un vídeo ha sido manipulado o no corresponde con los hechos descritos y también cómo podemos averiguar el lugar desde donde se grabó dicho vídeo.

El proceso de verificación de un vídeo[169] es similar al de las fotografías. Tendremos que responder a las mismas preguntas para determinar la validez del mismo.

Análisis forense de vídeos

Visualizar fotogramas

En ocasiones es necesario visualizar un vídeo fotograma a fotograma y encontrar detalles o incongruencias que reproduciendo el vídeo no se aprecian. Para ello podemos utilizar herramientas como Anilyzer (http://anilyzer.com) o Watchframebyframe (http://www.watchframebyframe.com/).

YouTube también nos permite visualizar los vídeos a cámara lenta, facilitando la observación de los detalles. Para acceder a esta opción tienes que ingresar haciendo clic en el icono de configuración que aparece en el mismo vídeo, y en la opción velocidad (speed) seleccionar la que más nos convenga.

Otra opción es utilizar Windows media. Para ello solo tienes que reproducir el vídeo con este reproductor y con el cursor encima del vídeo hacer clic con el botón derecho y seleccionar la opción "*Mejoras/Configuración de velocidad de*

169. Guía avanzada sobre verificación de contenido de video - https://gijn.org/2018/06/18/guia-avanzada-sobre-verificacion-de-contenido-de-video/

reproducción", ahora te aparecerán algunas opciones para configurar la velocidad del mismo.

InVID

Al igual que para las fotografías, InVID se puede utilizar para muchas operaciones con vídeos de YouTube o Facebook, como por ejemplo la lectura de los metadatos, visualizar los fotogramas del vídeo y realizar búsquedas inversas utilizando las miniaturas del vídeo.

Puedes ver el funcionamiento en estos videos tutoriales (https://youtu.be/nmgbFODPiBY) o (https://youtu.be/8Sy7RRnqvi4).

Averiguar la fecha y hora en la que se publica

Una herramienta muy sencilla para obtener la fecha y hora de publicación de un vídeo de YouTube, así como para obtener la ID del vídeo y para realizar búsquedas inversas es Amnestyusa (https://citizenevidence.amnestyusa.org/).

Descargar vídeos

Si necesitas descargar un vídeo al ordenador puedes utilizar alguno de los recursos que aparecen en este artículo (https://ciberpatrulla.com/descargar-videos/), seguro que no se te resiste ninguno.

Búsqueda inversa de vídeos

Buscar vídeos en Internet desde el PC

Hemos visto cómo hacer una búsqueda inversa de un vídeo de YouTube con la herramienta InVID utilizando las miniaturas de un vídeo, pero ¿qué podemos hacer si el vídeo no está alojado en Internet? ¿Cómo hacemos una búsqueda inversa de un vídeo que tenemos en nuestro ordenador?.

A veces puede llegarte un vídeo por email, en un pendrive, o a través de mensajería, no facilitándote la URL de donde lo han descargado (estas cosas

pasan). En este caso podemos hacer capturas de algunos fotogramas que creamos que pueden ser de interés y realizar una búsqueda inversa de dichas imágenes. Si este método falla, puedes subir el vídeo completo a un canal de YouTube propio y después hacer las comprobaciones con InVID o YouTube DataViewer (https://citizenevidence.amnestyusa.org/). Es conveniente que si utilizas un canal propio configures los vídeos que subas en modo "*Oculto*", si los configuras como privados no podrás verificarlos con estas herramientas y si los configuras como públicos cualquiera podrá encontrarlos en tu canal.

Búsqueda manual de vídeos

Cuando la búsqueda inversa de vídeos no ha dado resultados podemos llevar a cabo búsquedas manuales por los términos o palabras clave que creamos puedan llegar a identificar el vídeo en Internet. Para ello puedes utilizar los métodos que ya hemos visto en otros capítulos para buscar en Google u otros buscadores utilizando combinaciones de operadores, o puedes buscar dentro de las propias plataformas de vídeos online aplicando algunos filtros. Puedes leer este artículo con ideas e instrucciones de cómo y donde buscar vídeos en Internet (https://www.bellingcat.com/resources/how-tos/2017/10/17/conduct-comprehensive-video-collection/).

Buscar vídeos relacionados

Además de la propia búsqueda de YouTube podemos utilizar esta herramienta: Yasiv (https://yasiv.com/youtube). Con la que podemos realizar búsquedas por los términos que creamos convenientes y nos mostrará todos los vídeos relacionados con esa búsqueda en forma de grafo, lo que nos facilitará encontrar vídeos de interés de forma muy visual.

Buscar por ID del vídeo

En muchas ocasiones un vídeo puede haber sido compartido en otras webs o redes sociales, y una forma de buscarlo es utilizando como término de búsqueda dentro del buscador genérico o el de las redes sociales la ID del

vídeo (ejemplo: **1VgnhJKbK04**), la cual la podemos obtener ingresando la URL del vídeo en YouTube DataViewer.

vidIQ Vision for YouTube

VidIQ Vision for YouTube[170] es una extensión de Chrome que nos ofrece unas estadísticas muy detalladas del vídeo que estamos visualizando. Con esta extensión podemos comprobar si el vídeo ha sido compartido en otras redes sociales, como Facebook o Twitter, mostrándonos las URLs de donde se ha compartido. Igualmente dispone de otra característica muy útil como la de filtrar los comentarios del vídeo por diversos criterios, facilitándonos encontrar, dentro de vídeos con volúmenes altos de comentarios, lo que estamos buscando.

Herramientas que facilitan las búsquedas inversas de vídeos

Puedes utilizar las herramientas preconfiguradas para realizar búsquedas inversas en varios buscadores a la vez de Inteltechniques (https://inteltechniques.com/osint/reverse.video.html).

Metadatos

Al igual que en las fotografías, en los vídeos podemos analizar los metadatos incluidos en ellos, como por ejemplo la fecha, hora y dispositivo con el que se grabó, además de detalles de codificación del vídeo. Puedes utilizar herramientas online como Get-metadata (https://www.get-metadata.com/).

170. vidIQ Vision for YouTube - https://chrome.google.com/webstore/detail/vidiq-vision-for-youtube/pachckjkecffpdphbpmfolblodfkgbhl?hl=es

Geolocalizar un vídeo

Para geolocalizar un vídeo[171] podemos seguir las pautas que hemos visto para las fotografías, añadiendo pautas propias de los vídeos como el análisis del idioma, dialecto, acento, jergas o cualquier otra característica que nos ofrezca el audio y que nos pueda dar pistas de la región donde ha sido grabado.

Las redes sociales son una fuente importante donde buscar vídeos por ubicación. Podemos encontrar contenido relacionado con el vídeo del que disponemos, ayudándonos en la verificación del lugar donde fue grabado, además de aportarnos información complementaria.

Para ello podemos usar algunas búsquedas en Facebook como las siguientes:

Facebook (https://www.facebook.com/search/141270646560/videos-in/): con esta búsqueda obtendremos **vídeos de usuarios realizadas en un determinado lugar**, en este caso en el hotel The Westin Palace Madrid.

Facebook (https://www.facebook.com/search/str/plaza%20mayor%20madrid/videos-keyword): con esta búsqueda obtendremos **vídeos etiquetados por usuarios sobre un determinado lugar**.

Además podemos hacer búsquedas en zonas concretas a través de YouTube utilizando herramientas como (https://youtube.github.io/geo-search-tool/search.html) o (https://mattwright324.github.io/youtube-geofind/location).

Igualmente hemos visto en Twitter e Instagram cómo buscar contenido en base a la ubicación, pudiendo encontrar también vídeos de interés.

171. Una guía para principiantes para geolocalizar videos - https://www.bellingcat.com/resources/how-tos/2014/07/09/a-beginners-guide-to-geolocation/

Geolocalización e IPs

Introducción

La geolocalización es una técnica dentro de una investigación que utilizaremos para identificar la ubicación real de un objetivo. En realidad no existe un procedimiento por el cual se pueda ubicar un dispositivo de forma exacta a través de la posición GPS del mismo sin que haya autorización previa del usuario. Para conseguir ubicar a un objetivo utilizaremos toda la información que vayamos obteniendo y analizando.

Hasta ahora hemos visto cómo obtener información en buscadores, analizar perfiles sociales, así como imágenes y vídeos. Toda esta información, en su conjunto, será la que utilizaremos para definir la localización.

También hemos visto cómo utilizar aplicaciones móviles y de escritorio para cambiar nuestra ubicación real. Este método podemos usarlo para encontrar perfiles sociales de los objetivos cerca de nuestra ubicación, como por ejemplo con redes sociales como Facebook donde podemos usar la opción "*Amigos cerca*[172]", o en aplicaciones de citas en las que podemos configurar búsquedas en base a una determinada distancia de nosotros.

Redes sociales que geolocalizan a los usuarios

Hemos visto como Twitter, Instagram o Facebook ofrecen contenido en base a la ubicación compartida por los usuarios. Hay que tener en cuenta que la ubicación es un dato que ya prácticamente no se comparte de forma voluntaria y que por defecto suele venir desactivada en todas estas redes sociales, por lo que tendremos que recabar esta información del propio

172. ¿Cómo uso "Amigos cerca"? - https://www.facebook.com/help/iphone-app/291236034364603?helpref=related&ref=related

contenido compartido por los usuarios, por ejemplo dentro del texto del mensaje compartido, lugares etiquetados, personas etiquetadas y cualquier otro dato que podamos observar que nos ofrece información de la ubicación.

Geolocalizar a familiares, amigos o compañeros de trabajo

Una fuente de información que siempre tenemos que tener en cuenta es el círculo social del objetivo, ya que este puede no haber compartido información sobre su ubicación pero su círculo social sí. Para ello tenemos que identificar a familiares, amigos y compañeros de trabajo y realizar un análisis de sus perfiles con el objetivo de encontrar información sobre la ubicación, ya sea del lugar de trabajo, vivienda habitual, lugares de ocio, hobbies, hoteles donde se alojaron, etc.

IPs

Uno de los métodos más fiables para obtener la ubicación de alguien es a través de la obtención de la IP desde la que se conecta a Internet. Debemos tener en cuenta que el objetivo puede estar conectado detrás de un Proxy, un servicio de VPN, un establecimiento público (biblioteca, cafetería, etc.) o incluso, estar utilizando la conexión wifi de otra persona sin consentimiento de esta, no mostrando su IP real, por lo que siempre debemos cotejar con otra información que dispongamos la posible ubicación encontrada a través de la IP.

A continuación veremos cómo podemos obtener la IP desde donde se conecta un objetivo, a qué prestador de servicios de Internet[173] (ISP) pertenece dicha IP y cómo podemos ubicar dicha IP en una zona geográfica concreta.

173. Proveedor de servicios de Internet - https://es.wikipedia.org/wiki/Proveedor_de_servicios_de_Internet

Geolocalización de direcciones IP

En la actualidad las direcciones IP son asignadas de forma aleatoria y dinámica a los usuarios por los ISP para identificar la conexión de los dispositivos en Internet. Que una IP se asigne de forma dinámica significa que no siempre es la misma y que puede cambiar en cualquier momento, por lo tanto es importante reseñar de forma exacta la fecha y la hora en la que hemos obtenido dicha IP.

Precisión de geolocalización de direcciones IP

La precisión con la que se geolocaliza un dispositivo a través de la IP puede variar entre un 50% o un 98%. Para ubicar una determinada IP podemos utilizar algunos servicios que veremos más abajo, los cuales son capaces de obtener la localización física de una IP. Sin embargo, estos servicios no ofrecen ubicaciones exactas porque la dirección que realmente está registrada en la IP es una dirección aproximada. Es probable que a cada IP se le asigne una zona geográfica y cuando tu proveedor te asigna una IP, te asigne una que corresponde con tu zona, aunque en ocasiones este dato puede no ser del todo correcto, pero aun así, a nosotros nos ofrece una información muy valiosa. Piensa que Internet está globalizado, y conseguir ubicar a alguien en una localidad ya es logro.

Cómo obtener la IP de un dispositivo

Ya hemos visto en la sección de Protección de Datos que podemos obtener la dirección IP de un dispositivo, y ahora vamos a ver qué opciones disponemos para su obtención.

Existen algunas herramientas online que nos facilitan obtener la IP de un dispositivo a través del envío de un enlace. Estos sistemas generan enlaces personalizados para camuflar nuestras intenciones. Por ejemplo, podemos utilizar una URL a una noticia, fotografía o vídeo e introducirlas en estas herramientas, las cuales nos generarán otra URL nueva, siendo esta URL la

que tenemos que enviar a nuestro destinatario. Una vez que el destinatario haga clic en este URL le enviará al contenido inicial que hemos elegido (noticia, foto o vídeo) y en el camino habremos obtenido la dirección IP, dispositivo desde el que se conecta (PC o Móvil) y navegador utilizado.

A continuación te dejo dos herramientas y tutoriales de uso:

- **Iplogger (https://iplogger.org/)**
    - Tutorial (https://www.redeszone.net/2017/04/22/iplogger-recopilar-informacion-usuarios/)
    - Vídeo Tutorial (https://www.youtube.com/watch?v=BBMANeRN04A)
- **Grabify (https://grabify.link)**
    - Tutorial (https://www.redeszone.net/2017/04/17/grabify-ip-logger-te-permitira-saber-la-ip-y-otros-datos-de-los-usuarios-que-pinchen-en-el-enlace/)
    - Vídeo Tutorial (https://www.youtube.com/watch?v=kthkKtEu3Y0m)

Otro método de obtener la IP es a través del envío de un email sin necesidad de enviar ningún enlace para que el destinatario haga clic. Este sistema nos asegura que con el simple hecho de abrir el email podremos obtener la IP desde donde se ha conectado. Para ello podemos utilizar herramientas como **Whoreadme** (http://whoreadme.com), con la que podemos enviar emails asociando una cuenta de correo propia, a este servicio, de forma que cuando el receptor abre el email obtenemos su IP. Existen algunas limitaciones con esta herramienta, por ejemplo, cuando el receptor abre el email desde la versión web de los gestores de correos, en el caso de Gmail, nos aparecerá la IP del servidor proxy de Gmail y no del receptor, pero en el caso de que el receptor abra el email desde una aplicación móvil o cliente local desde su PC, nos mostrará la IP real del receptor. Igualmente si el receptor abre el email

desde la versión web le aparecerá un aviso como este: "*a través de mxsvr.net*". Detalle que debemos tener en cuenta si no deseamos que sepa que le estamos rastreando.

Por último podemos utilizar las URLs obtenidas en los servicios Iplogger y Grabify e incrustarlas dentro del código html del email que vamos a enviar, permaneciendo oculto a los ojos del receptor, de forma que al abrir el email obtengamos su IP sin necesidad de que haga clic en ningún enlace. Para ello insertamos un código html que lo que consigue es cargar una imagen invisible dentro del cuerpo del email que enviamos. Para añadir html a un email en Gmail puedes seguir los pasos de este vídeo tutorial (https://www.youtube.com/watch?v=h14c3c1Lrss).

Cómo geolocalizar una dirección IP

Una vez que hemos obtenido la IP, podemos obtener la ubicación, asociada a la misma, usando alguna de estas herramientas:

Para ello solo debemos introducir la IP que hemos obtenido y nos mostrará toda la información disponible sobre la misma.

- **Maxmind** (https://www.maxmind.com/es/geoip2-precision-demo)
- **Ip-tracker** (https://www.ip-tracker.org)
- **Iplookup.flagfox** (https://iplookup.flagfox.net/)
- **Infosniper** (http://www.infosniper.net/)

Mapas

Unas de las herramientas más importantes para poder llevar a cabo tareas de geolocalización son los mapas. Por ello he querido añadir en este capítulo algunas herramientas que pueden facilitarte esta labor:

-Google Earth (https://www.google.es/intl/es/earth/index.html): realiza un viaje virtual a cualquier lugar del mundo. Explora el relieve, edificios 3D y otras imágenes. Busca ciudades, sitios y empresas locales. Puedes ver una guía de uso aquí: (https://support.google.com/earth/?hl=es#topic=7364681).

-Google Maps https://www.google.com/maps): Google Maps no solo ofrece vistas de calles, edificios y carreteras, además puedes ver imágenes de interiores de restaurantes, tiendas, museos, aeropuertos, centros comerciales, estadios y mucho más. Puedes ver una guía de uso aquí: (https://support.google.com/maps/answer/144349?hl=es).

-DualMaps (http://data.mashedworld.com/dualmaps/map.htm): esta herramienta muestra tres vistas del mapa de Google Maps a la vez (Street View, Satélite y normal).

-Instant Street View (https://www.instantstreetview.com): utiliza por defecto la vista Street View en todas las búsquedas que hagamos.

-Gpsvisualizer (http://www.gpsvisualizer.com/geocode): nos facilita las coordenadas de una dirección concreta.

-Mapillary (https://www.mapillary.com): crea mapas interactivos en base a imágenes compartidas por usuarios.

-Followyourworld.appspot (https://followyourworld.appspot.com/): este servicio nos notifica cambios en las imágenes de los mapas en un punto determinado. Muy útil si necesitamos estar informados de cuándo se actualiza la imagen de un punto concreto.

Dirección física

Introducción

Si disponemos del domicilio del objetivo podemos ampliar la información analizando algunas fuentes de información disponibles. A través del domicilio y utilizando algunas herramientas, podemos obtener información del interior de viviendas, locales, alrededores, así como fotos compartidas por usuarios. A continuación vamos a ver dónde obtener esta información.

Dónde buscar por domicilio

Búsqueda en Google

Podemos realizar búsquedas en Google utilizando la dirección como término de búsqueda, sin olvidar realizar búsquedas en Google Images, donde pueden aparecer muchos resultados de imágenes de dicho domicilio subidas a Internet.

Buscar en inmobiliarias

Las webs de compra-venta de viviendas puede ser un lugar idóneo para realizar búsquedas a partir de una dirección. Algunos de estos servicios ofrecen la posibilidad de buscar utilizando un mapa interactivo, por lo que será fácil encontrar la dirección concreta. Igualmente podemos usar el operador (*site:*) de Google para buscar en determinados servicios de compra-venta (ejemplo: "*site:idealista.es calle, localidad*") *(sin las comillas)*.

Servicios oficiales

Los servicios oficiales, como el registro de la propiedad[174], son una fuente de información pública pero de pago, donde podemos obtener información detallada del titular de una propiedad concreta a través de la dirección[175] de la misma.

Tampoco podemos olvidar los tablones de anuncios de los boletines oficiales como ya hemos visto en otros capítulos.

Mapas

Realizando búsquedas por dirección en mapas como Google Maps, podemos acceder a vistas de la zona en concreto, obteniendo panorámicas exactas del lugar. En el caso de querer ubicar exactamente una propiedad en base al número de la calle podemos utilizar la información del Catastro (https://www1.sedecatastro.gob.es/CYCBienInmueble/OVCBusqueda.aspx), ya que en ocasiones es difícil visualizar el número a través de los mapas tradicionales.

Aplicaciones de mensajería

Esta técnica ya la hemos visto en varios capítulos, y consiste en analizar perfiles sociales a través de aplicaciones de mensajería en base a la ubicación. Para ello solo tenemos que configurar nuestra ubicación para que nos sitúe en la dirección de interés y buscar perfiles cerca de ese domicilio.

Redes sociales

Una vez obtenida la dirección podemos conseguir las coordenadas de la misma y realizar búsquedas avanzadas en redes sociales, como Twitter, en busca de tweets ubicados en dicha dirección.

Puedes acceder al flujo de trabajo de Ciberpatrulla (https://ciberpatrulla.com/identificar-persona-ubicacion/), el cual te ayudará a

174. Registro Online - https://www.registradores.org/registroonline/home.seam
175. Problemas al pedir nota simple del Registro por la dirección - https://www.registrodirecto.es/blog/pedir-nota-simple-por-direccion/

encontrar información a partir de la ubicación del objetivo.

Monitorizar

Introducción

En este capítulo vamos a ver cómo podemos monitorizar eventos o sucesos en Internet, así como generar alertas por email para estar informados de novedades en base a criterios que nos interesen.

Para buscar información sobre sucesos, en muchas ocasiones recurrimos a Google, de hecho tiene muchísimo potencial a la hora de extraer información, pero esto no siempre es suficiente, y las redes sociales cubren una parte importante que el gigante buscador no puede.

Monitoreo y Alertas

Alertas

Podemos utilizar algunos servicios online para recibir alertas sobre determinado contenido publicado en Internet de nuestro interés. Lo normal es realizar una búsqueda manual en la fuente que nos interesa, y en el caso de no obtener resultados, podemos crear alertas para que el sistema siga repitiendo la búsqueda cada cierto tiempo y nos avise si, dicho contenido, aparece publicado en Internet, de forma que no tengamos que volver cada cierto tiempo a realizar la misma búsqueda de forma manual.

Alertas en buscadores

Ya te he hablado de GoogleAlerts, el sistema de alertas de Google. Con este sistema podemos crear cuantas alertas necesitemos para recibir los resultados en nuestro email. Algo que tienes que tener en cuenta es que las búsquedas que configuremos en este servicio soportan todos los operadores de

búsqueda[176] que hemos visto. Te dejo un vídeo tutorial sobre su uso (https://www.youtube.com/watch?v=qcCEu6oLBtg).

Otro servicio de alertas como el anterior es Talkwalker (https://www.talkwalker.com/alerts), con el que podemos crear también alertas de determinadas búsquedas, y en el que también podemos utilizar operadores booleanos. Te dejo un video tutorial sobre su funcionamiento (https://www.youtube.com/watch?v=yFyLmVKNg7o).

Alertas en redes sociales

Podemos generar alertas exclusivas para algunas redes sociales utilizando servicios específicos como Warble (https://warble.co/alerts) para Twitter, o podemos usar las alertas de Google añadiendo combinaciones de operadores como por ejemplo: "*término site:facebook.com*" (sin las comillas).

Alertas sobre cuentas comprometidas

Ya hemos visto en el capítulo de los emails que podemos utilizar algunos servicios específicos para buscar dentro de bases de datos de servicios online comprometidos. En el caso de que queramos estar informados de forma automática si una determinada cuenta de email se encuentra dentro de una de estas bases de datos, podemos utilizar sistemas de alertas como los siguientes:

-Haveibeenpwned (https://haveibeenpwned.com/): este servicio, además de poder buscar directamente en él, dispone de un sistema de alertas, al cual podemos acceder desde la opción "*Notify me*" que aparece en el menú superior.

-Hacknotice (https://hacknotice.com/): es un servicio de reciente creación enfocado a enviar alertas sobre cuentas de servicios online que han sido comprometidas.

Alertas en Pastebin

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, pero también es utilizado para compartir información

176. Cómo buscar en Google con un experto - https://ciberpatrulla.com/buscar-google/

comprometida, por lo que es un lugar que debemos consultar cuando estemos buscando datos personales, emails, teléfonos, etc.

Si queremos estar al día del contenido que se añade en estos sitios podemos crear alertas en sus propios servicios o configurar alertas de Google utilizando operadores personalizados, como veremos a continuación:

Pastebin (https://pastebin.com/alerts): este servicio de pastebin dispone de su propio sistema de alertas que te mantendrán informado cuando alguien añada contenido relacionado con tus alertas.

Si queremos configurar una alerta de Google para buscar en estos sitios, podemos utilizar combinaciones como este ejemplo "*término site:pastebin.com*" (sin las comillas).

Alertas boletines oficiales

Los boletines oficiales también disponen de un servicio de alerta para enviar por email cualquier novedad que haya relacionada con los términos que definamos. Para utilizar este servicio en el Boletín Oficial del Estado puedes dirigirte aquí: (https://www.boe.es/a_la_carta/).

Alertas Dark Web

Si necesitas estar al día de los sitios web nuevos que se crean en la Dark Web puedes utilizar el sistema de alertas de Hunchly (https://darkweb.hunch.ly/).

Alertas de cambios

En ocasiones vamos a necesitar supervisar cambios en algunos sitios web, los motivos pueden ser diversos, por ejemplo podemos querer saber cuándo un sitio web añade contenido nuevo o cuándo lo ha modificado. También podemos utilizarlo para que nos avise de cambios en perfiles sociales, como por ejemplo si cambia la foto de perfil, o su biografía. Para ello podemos utilizar servicios como Visualping (https://visualping.io/) o followthatpage (https://www.followthatpage.com/).

Creando paneles web

Disponer de una panel donde poder monitorizar redes sociales en tiempo real

nos puede ser de gran ayuda para estar informados de sucesos o eventos en una determinada zona, o para analizar la evolución en las redes sociales de un determinado acontecimiento y poder tomar decisiones al respecto.

A continuación vamos a ver algunas herramientas que nos ayudarán a tener toda esta información de forma rápida y ordenada.

-Tweet Deck (https://tweetdeck.twitter.com/): ya te he hablado de esta herramienta en el capítulo de Twitter. Sin duda una herramienta con mucho potencial, siendo el único límite tu imaginación.

-The One Million Tweet Map (https://onemilliontweetmap.com): es una herramienta muy interesante que nos permitirá visualizar tweets geolocalizados en un mapa. Podemos seleccionar la zona que nos interese y monitorizar qué se está compartiendo en dicho punto. Podremos realizar búsquedas especificando un término o un hashtag y encontrar rápidamente los resultados en el mapa.

-Mentionmapp (https://mentionmapp.com/): herramienta muy visual que muestra mediante un grafo las relaciones que existen en base a una búsqueda determinada, ya sea por hashtag o usuario. Muy útil para analizar quién habla sobre un tema y qué relaciones tiene.

-Followthehashtag (http://www.followthehashtag.com/): es un servicio muy completo que dispone de una búsqueda avanzada donde se pueden utilizar operadores booleanos, coordenadas e incluso fechas concretas.

-Twitonomy (http://www.twitonomy.com): es una completa herramienta de análisis de perfiles de Twitter, que podemos utilizar para analizar hashtags u otros perfiles que nos interesen.

-Instagram Locations (https://www.instagram.com/explore/locations/): con esta opción de Instagram podemos encontrar contenido compartido en base a una ubicación determinada, siendo útil si estamos analizando un suceso en una zona concreta. Si tienes dificultades para encontrar la ubicación que necesitas, puedes utilizar esta combinación en Google: "site:https://www.instagram.com/explore/locations/ UBICACIÓN" (sin las comillas).

Te recomiendo la lectura de un ejemplo sencillo de cómo monitorizar un

suceso o evento en Internet a través de las redes sociales. Puedes leer este artículo en Ciberpatrulla (https://ciberpatrulla.com/monitorizar-eventos-sucesos-internet/).

Software OSINT

Introducción

Hasta ahora hemos visto muchas técnicas de obtención de información, la mayoría de forma manual y otras utilizando herramientas online gratuitas. En este capítulo voy a hablarte de algunas herramientas, sin entrar en detalle ya que cada una de ellas podría dar para un capítulo o libro entero, y no son el objetivo de este libro, pero sí creo conveniente que conozcas de su existencia y qué pueden ofrecerte.

Muchos de estos scripts requieren tener instalado Python en tu PC para que funcionen correctamente y además se ejecutan a través de la consola del sistema operativo, por lo que si no estás familiarizado con Python y con la consola, no te resultará nada intuitivo. De ti depende decidir si te merece la pena profundizar en estas herramientas o llevar a cabo obtenciones manuales.

Puedes ver este vídeo tutorial sobre cómo instalar Python en Windows (https://www.youtube.com/watch?v=9fNKy9zOPkg).

Tinfoleak

Tinfoleak es una herramienta de código abierto que automatiza la extracción de información en Twitter. Permite obtener y analizar la información publicada con el fin de generar inteligencia útil, tanto de usuarios en concreto, como de acontecimientos en lugares específicos.

Tomando un identificador de usuario, coordenadas geográficas o palabras clave, Tinfoleak analiza la línea de tiempo de Twitter para extraer grandes volúmenes de datos y mostrar información útil y estructurada al analista de

inteligencia.

Puedes descargar Tinfoleak aquí (https://github.com/vaguileradiaz/tinfoleak).

Si quieres saber más sobre esta fantástica herramienta puedes leer este artículo de Ciberpatrulla (https://ciberpatrulla.com/tutorial-tinfoleak/).

Maltego

Maltego es un software para OSINT que se centra en la obtención de información de fuentes abiertas y la representación de esa información en un formato de gráfico. Maltego es una aplicación de pago en su versión completa, pero dispone de una versión gratuita. La vista en gráficos de la información recopilada permite analizar las relaciones entre objetivos y sus redes sociales. Cada resultado se puede transformar en un nuevo nodo, generando un árbol inmenso de datos que se puede relacionar y visualizar de diferentes formas.

Permite realizar búsquedas a partir de dominios, IPs, ubicaciones geográficas, correos, nombres, teléfonos, etc.

Puedes descargarlo desde su web (https://www.paterva.com/web7/downloads.php).

Te recomiendo el canal de Cylon Null para aprender a usarlo (https://www.youtube.com/channel/UCseLiPDQKBrKJfqtiHuH07w).

Spiderfoot

SpiderFoot es una herramienta de reconocimiento que consulta automáticamente más de 100 fuentes de datos públicas para recopilar inteligencia sobre direcciones IP, nombres de dominio, direcciones de correo electrónico, nombres y más. Simplemente hay que seleccionar el objetivo que deseas investigar, eliges qué módulos habilitar y luego SpiderFoot recopila

datos para desarrollar una comprensión de todas las entidades y cómo se relacionan entre sí.

Algunos módulos de SpiderFoot requieren o funcionan mejor cuando se suministran claves API. Tendrás que darte de alta en todos estos servicios para obtenerla. Te recomiendo que las guardes para futuros usos, porque lleva mucho tiempo darse de alta en todo estos sitios.

Puedes descargar esta herramienta en su propio sitio web (https://www.spiderfoot.net/index.html), además de acceder a mucha información de uso en inglés (puedes usar el traductor de Google como hago yo).

Datasploit

Datasploit está compuesto por varias herramientas que tienen la función de obtener información de varias fuentes, reuniendo en un solo lugar información relevante sobre un dominio, dirección de email, número de teléfono, nombre de una persona, etc.

Las herramientas se pueden utilizar mediante el símbolo del sistema o vía navegador, por lo que, una vez instalado y configurado, su uso es intuitivo.

Puedes descargarlo en Github (https://github.com/DataSploit/datasploit).

La guía más completa que he encontrado está en brasileño (https://www.oanalista.com.br/2017/10/14/osint-dados-pessoais-datasploit/).

Shodan

Shodan es un motor de búsqueda diferente, ya que busca dispositivos conectados a Internet, es decir, puede encontrar webcams, routers, cámaras de seguridad, FTPs públicos, etc.

La verdad es que yo no le he encontrado utilidad más allá de la propia

curiosidad del buscador, pero quién sabe si en algún momento puede ofrecer algún resultado que nos ayude en nuestra investigación.

La web de este buscador es: (https://www.shodan.io/).

Te dejo este vídeo de YouTube donde nos cuentan el funcionamiento de Shodan (https://www.youtube.com/watch?v=0phCROiqNV4).

También te recomiendo este artículo de Osintlatamgroup (https://www.osintlatamgroup.com/blog/obteniendo-informaci%C3%B3n-con-shodan).

TheHarvester

The Harvester es una herramienta para recopilar cuentas de correo electrónico, nombres de subdominio, Hosts, nombres de empleados de diferentes fuentes públicas (Motores de búsqueda, servidores de clave pgp, la red social LinkedIn y la base de datos de SHODAN).

The Harvester viene instalado en el sistema operativo Buscador, del que ya te he hablado.

Puedes ver su funcionamiento en este artículo de Osintlatamgroup (https://www.osintlatamgroup.com/blog/osint-cli-parte-i).

OSRFramework

OSRFramework es un conjunto de bibliotecas para realizar OSINT. Integra diferentes utilidades de investigación en fuentes abiertas orientadas a la identificación de usuarios en más de 200 plataformas diferentes.

La página de descarga en Github es (https://github.com/i3visio/osrframework).

Te dejo un vídeo tutorial de instalación y uso (https://www.youtube.com/watch?v=16JeQZbwZEA) y un taller de los creadores de esta herramienta, Félix Brezo Fernández y Yaiza Rubio Viñuela en Cybercamp 2015 (https://www.youtube.com/watch?v=dcLOtMKWO5k).

NodeXL

NodeXL Basic es una plantilla gratuita de código abierto para Microsoft® Excel® 2007, 2010, 2013 y 2016 que facilita el análisis de redes sociales, permitiendo visualizar y analizar las redes a través de grafos.

Instalar NodeXL es muy sencillo, no así su uso, que tiene una curva de aprendizaje media/alta. Funciona como una plantilla de hoja de cálculo incluida en la interfaz de Microsoft Excel. En la actualidad NodeXL ofrece dos paquetes: una versión gratuita y una versión profesional y solo está disponible para Windows.

Puedes descargarlo desde su página web (https://archive.codeplex.com/?p=nodexl).

Te dejo una guía de uso (http://inteligenciacomunicaciononline.blogspot.com/2017/07/analisis-de-redes-sociales-con-nodexl.html).

El informe

Introducción

Una vez que hemos realizado el análisis de toda la información obtenida y sacadas las conclusiones del mismo, solo queda plasmarlo en un informe. Sin duda esta fase es de vital importancia, todo nuestro trabajo puede no servir de nada si no lo sabemos plasmar adecuadamente. Debemos tener en cuenta que el informe, probablemente, esté dirigido a personas que carecen de conocimientos técnicos en la materia y que, incluso, los conceptos más básicos no sean comprendidos.

Es importante documentar todos los pasos que vayamos dando. Osirtbrowser te permite llevar un registro de todos los sitios que visitas. Si no encuentras algún dato, siempre puedes consultar el historial de navegación del caso creado.

Puedes ser buena idea que el informe sea revisado por terceros, tanto sin conocimientos en la materia como con ellos, pueden darte una visión más amplia e identificar detalles que faltan o no son compresibles.

Redacción del informe

En la redacción del informe es conveniente incluir una parte ejecutiva y una técnica, estando la primera destinada a explicar todo lo obtenido de forma comprensible, evitando utilizar terminología técnica, y en el caso de que no haya más remedio que usarla, incluir un glosario de términos.

Te dejo un artículo con muy buenos consejos para realizar un informe (https://segurint.wordpress.com/2012/02/15/analista-quiero-un-informe/).

Asistencia a Juicio

Es probable que después de realizar un informe técnico y darle traslado al juzgado correspondiente, este nos cite a la vista oral, donde debemos ratificarnos en lo presentado y donde pueden pedirnos aclaraciones sobre el mismo. No es raro encontrarse en una vista oral con preguntas mal formuladas o que son incomprensibles por parte del investigador, dado que quien formula la pregunta carece de conocimientos para poder hacerla de forma comprensible. En el caso de tener dudas, respecto a las preguntas formuladas, es conveniente parafrasearlas de forma que nos aseguremos que lo que vamos a responder está relacionado con la pregunta realizada y no provocar confusiones que pueden tener consecuencias en el proceso.

Informe simple

A continuación te dejo un ejemplo de informe de resultados muy simple y simulado. Ten en cuenta que cada caso es un mundo, y dependiendo de la complejidad del mismo, el informe requerirá más o menos nivel de detalle, pudiendo requerir mapas mentales, gráficos, presentaciones o cualquier otra forma de ampliar el informe y que llegue a ser comprensible.

———

INFORME RESULTADOS SENCILLO

OBJETIVO

En relación al asunto de referencia, se solicita al (cargo que ocupas) informe técnico sobre el perfil social de Facebook que a continuación se relaciona, al objeto de identificar el administrador del mismo, así como la obtención de las evidencias digitales necesarias al objeto de preservarlas ante una posible eliminación:

Perfil de Facebook (https://www.facebook.com/nombredeusuario) ID: XXXXXXXXXX

CONCLUSIONES

Que una vez analizado el perfil social de Facebook de interés, y habiendo realizado búsquedas en Internet en base a diversos criterios y en diferentes plataformas online, este (cargo que ocupas) concluye:

Que el administrador del perfil social es D. Nombre, Apellidos, con domicilio en_____, con dirección de email_____ y lugar de trabajo en_____.

PROCEDIMIENTO

-Análisis del perfil social de Facebook ID: XXXXXXXXXX: no se encuentran datos personales del administrador de forma pública en dicho perfil, no pudiendo acceder al contenido compartido de forma pública en el mismo al estar configurado como privado.

-Identificación de perfil personal de Twitter: a través de diversas búsquedas en Internet se localiza un perfil social de Twitter, en el que coincide el nombre de usuario y la foto de perfil con las que aparecen en el perfil de Facebook, mostrando en la biografía del mismo un enlace a un perfil social de LinkedIn.

-Identificación de perfil de LinkedIn: se analiza el perfil de LinkedIn, en el que aparecen diversos datos personales, como nombre y apellidos, lugar de trabajo, email de contacto, y municipio de residencia.

Las evidencias digitales de forma completa se adjuntan a este informe como anexo nº 1.

TERMINOLOGÍA Y ABREVIATURAS

ID: Identificación numérica y única

Y para que conste por medio de la presente, se hace constar que considerando el (cargo que ocupas) que no ha lugar a más actuaciones, se dan por concluidas las practicadas que constan de 2 hojas, a una sola cara, en las que se incluye: 1 Anexos-Anexo 1 con 1 hoja.

En Madrid a 05 de Julio de 2040

Firma:

_____

En el anexo se incluirán las URLs a los perfiles sociales, las IDs y todas las capturas con explicaciones y detalles del contenido presentado.

Las evidencias digitales deberán presentarse también en soporte físico (CD, DVD o HD), quedando reseñado en el anexo cada evidencia con nombre, descripción, fecha, hora de obtención y el valor HASH de las misma.

Bonus

Introducción

Antes de acabar el libro no podía dejarte sin un regalo. A continuación vas a encontrar un listado de extensiones para el navegador Chrome que te facilitarán mucho la vida en tus tareas de obtención. Esta selección de extensiones han sido todas probadas por mí, y todas son útiles, te facilitarán mucho el trabajo, tanto de análisis como de obtención.

Espero que lo disfrutes, me ha costado mucho reunir, probar y analizar todas estas herramientas.

Extensiones

Extensiones Chrome

1. 360social
2. Adblock Plus
3. AFS
4. Awesome Screenshot: Grabadora de video de pantalla
5. BOOL
6. BuiltWith Technology Profiler

7. Captura de página completa - FireShot
8. Capturador de Páginas Web-Screenshot Extension
9. Chameleon
10. Click&Clean
11. Click&Clean App
12. CrowdTangle Link Checker
13. Descargador para Instagram™ (+ Subir fotos)
14. Distill Web Monitor
15. DuckDuckGo Privacy Essentials
16. Email Extractor
17. EmailDrop – Extrae Correos Electrónicos Fácilmente
18. Facebook Meta Inspector
19. Fake Data - A form filler you won't hate
20. Fake video news debunker by InVID
21. FBDown Video Downloader
22. FBFriendsID
23. FirstDraftNewsCheck
24. Flash Video Downloader
25. Full Page Screen Capture

26. Full Page Screenshot
27. Google Search Filter
28. Hover Zoom
29. HTTPS Everywhere
30. Hunter
31. Image Tools
32. Intelligence Search
33. IP Address and Domain Information
34. LightShot (la herramienta de captura de pantalla)
35. Link Audit Checker, find invalid content.
36. Link Grabber
37. Maldito Bulo
38. Manual Geolocation
39. META SEO inspector
40. Nimbus Screenshot & Screen Video Recorder
41. OneTab
42. PageDash Web Clipper
43. Print Friendly & PDF
44. Privacy Badger

45. Prophet
46. RevEye Reverse Image Search
47. Sales Prospecting - Datanyze Insider
48. Save Page WE
49. Save to Pocket
50. Save To The Wayback Machine
51. Secret Revealer Social Advanced Search Engine
52. Session Buddy
53. SimilarWeb - Traffic Rank & Website Analysis
54. Snovio - Email Finder
55. Social Media Advanced Search - Find User Info
56. Stream Video Downloader
57. TabCopy
58. Tab Layouts - Arrange Tabs Into Layouts
59. The Great Suspender
60. Traductor de Google
61. Treeverse
62. TunnelBear VPN
63. uBlock Origin

64. uBlock Origin Extra
65. Unseen for Facebook
66. User-Agent Switcher for Google Chrome
67. Ver Imagen
68. Video Downloader professional
69. Video Downloader professional
70. vidIQ Vision for YouTube
71. Web Developer
72. WebRTC Leak Prevent Toggle
73. Who Is Hosting?

Y te estarás preguntando ¿cómo voy a instalar todas estas extensiones en el navegador? Yo me pregunté lo mismo cuando empecé a ir acumulándolas, pero tengo una solución fantástica: SimpleExtManager. Esta extensión gestiona todas las extensiones que tengas instaladas. Puedes organizarlas por grupos, pudiendo activarlas y desactivarlas por grupos o individualmente de forma muy sencilla.

Prácticas

Ya tienes muchas (no todas) herramientas e información para comenzar a investigar en Internet, pero antes de meterte a fondo puedes practicar lo aprendido en diversos sitios de Internet. Te dejo dos muy recomendados:

Sourcing.games (https://www.sourcing.games/) es un sitio con multitud de

juegos para practicar tus conocimientos en OSINT.

ATENEA (https://atenea.ccn-cert.cni.es/) es una plataforma de desafíos de seguridad informática compuesta por diferentes retos que abarcan diferentes campos, como Criptografía y Esteganografía, Exploiting, Forense, Networking y Reversing, y OSINT.

Ha sido desarrollada por el CCN-CERT, Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español.

Créditos

Autor

Si quieres saber más sobre mí puedes visitar mi página web (https://ciberpatrulla.com/sobre-mi/), o ponerte en contacto conmigo en ciberpatrulla.com@gmail.com.

Derechos de Autor

https://ciberpatrulla.com