Wildlife Conservation Society

EL PACCT
EUROPA ↔ LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

ALIANZA POR LA FAUNA SILVESTRE Y LOS BOSQUES.

Manual para la iniciación en la investigación del tráfico de fauna silvestre y otros delitos contra el medio ambiente a través de internet

Edita: Programa EL PAcCTO
Calle Almansa 105
28040 Madrid (España)
www.elpaccto.eu

Con colaboración de:

Autor:

Ramón González Gallego
Jefatura del SEPRONA – Guardia Civil

Edición no venal

4 de abril de 2022

Este documento ha sido elaborado con la financiación de la Unión Europea. Su contenido es responsabilidad exclusiva de su autor, del programa EL PAcCTO y WCS, y no refleja necesariamente las opiniones de la Unión Europea.

Índice

Índice de Tablas

Índice de Ilustraciones

ACRÓNIMOS

API: Interfaz de Programación de Aplicaciones.

CITES: Convención sobre el Comercio Internacional de Especies Amenazadas de Fauna y Flora Silvestres.

EL PAcCTO: Europa Latinoamérica Programa de Asistencia contra el Crimen Transnacional organizado.

IP: Dirección IP.

OSINT: Inteligencia de fuentes abiertas - Open Source Intelligence en inglés.

UNODC: Oficina de las Naciones Unidas contra la droga y el delito.

URL: Localizador de Recursos Uniforme - Uniform Resource Locator.

VPN: Red Privada Virtual - Virtual Private Network en inglés.

WCS: Wildlife Conservation Society.

INTRODUCCIÓN

En octubre de 2020, la Conferencia de las Partes de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), realizó un llamado a los Estados miembros a recoger en sus ordenamientos jurídicos al delito medioambiental como delito de carácter grave, con base en la alarma que supone que este tipo de delitos se esté convirtiendo en uno de los más lucrativos, y señalando la preocupación que suponen estos ilícitos para el mantenimiento del medio ambiente.

Este hecho es sin ninguna duda, un reconocimiento a escala mundial sobre un fenómeno que se ha visto crecer enormemente en los últimos años: el delito contra el medio ambiente, particularmente el tráfico de fauna silvestre. Sin duda, esto debe de ponernos en alerta y alejarnos de ese pensamiento preconcebido que ha imperado durante años de que este tipo de delitos "son delitos menores que carecen de gravedad y/o sofisticación". Sin embargo, estamos nada más lejos de la realidad.

Hoy en día, en el ámbito del delito contra la fauna silvestre, no es difícil encontrar que un hecho delictivo no se limita a un espacio cercano a donde se localiza el crimen, sino que involucra a varias personas o grupos, ubicados en continentes distintos, que consiguen mover los especímenes - vivos, sus partes o derivados a través de transportes intercontinentales, obteniendo enormes beneficios. Estos beneficios ilegales cada vez con más frecuencia se incardinan dinero que mezclan procedencia lícita e ilícita, con mecanismos de lavado de capitales exactamente iguales a los presentes en otros tipos delictivos. Por supuesto, no es extraño en absoluto encontrar ofertas en Internet relativas a especies animales o vegetales protegidas, venta de documentos CITES falsificados, entre otros.

Estos supuestos, ya no son una excepción. Por ello, las unidades especializadas en la lucha contra el tráfico de fauna silvestre y otros delitos medioambientales requieren fortalecer sus procedimientos de investigación para abordar esta nueva problemática, de forma tal que se pueda abordar el control y disuasión de la conducta a lo largo de la cadena de suministro, iniciando desde el cierre de las transacciones de compraventa que se surten con el uso del internet.

El presente Manual ha sido elaborado en coordinación y financiación entre el programa europeo EL PAcCTO y la organización Wildlife Conservation Society, junto a un experto del SEPRONA de España; y tiene por objetivo ser una guía práctica para la iniciación, formación y especialización de los cuerpos de control en América Latina en la investigación del tráfico de fauna silvestre que se comete con el uso de Internet, pudiendo ser empleado también en la investigación de otros delitos contra el medio ambiente en el ciberespacio en lo que fueren compatibles.

CONFIGURACIÓN DE EQUIPOS

El primer paso para adentrarse en la búsqueda de indicios relacionados con los delitos contra la fauna silvestre y otros delitos contra el medio ambiente en Internet es configurar nuestro material de trabajo, es decir, nuestros equipos informáticos. A estos efectos, vamos a dejar claro desde el principio un axioma que se repetirá a lo largo de este manual. Hay muchas opciones, configuraciones y parámetros en la búsqueda en fuentes abiertas en Internet; algunas opciones son claramente mejores que otras, pero en la gran mayoría de los casos, habrá varios recursos para solventar un mismo problema, cada uno con pros y contras. ¿Cuál de esos recursos es el mejor? La respuesta es sencilla: el que mejor se adapte a los gustos, necesidad y experiencia personal del usuario. En este manual, se exponen diferentes opciones para un mismo problema y se dan recomendaciones para su solución, pero la palabra final sobre cómo solventarlo, qué herramienta utilizar o qué metodología implementar debe basarse en la experiencia y necesidad del usuario y su organización.

Teniendo esto en cuenta, pasemos a enumerar en primer lugar las necesidades en materia de software y de hardware para la realización de labores de inteligencia de fuentes abiertas (Open Source Intelligence – OSINT, por sus siglas en inglés).

Hardware y software

Definamos en primer lugar qué equipo informático debemos utilizar y qué herramientas de software debe de tener instaladas.

En lo que refiere al equipo informático, la primera pregunta que surge es qué tipo de ordenador debemos utilizar con base en su gama (baja, media o alta). Aquí la respuesta sí es categórica: las herramientas para la realización de labores de OSINT no requieren de equipos informáticos especialmente potentes. La única excepción la constituyen herramientas avanzadas de OSINT para obtención y tratamiento de enormes cantidades de datos. Estas herramientas no son objeto de este manual, por lo que podemos desechar la necesidad de equipos de gama alta. Por lo tanto, con un equipo de gama media o baja (es decir, sin componentes informáticos como procesador, memoria RAM o tarjeta gráfica, de última generación) seremos capaces de realizar todas las labores necesarias.

La siguiente pregunta en materia de hardware puede basarse en qué opción es mejor entre un PC de sobremesa o un portátil. En este caso, la respuesta también es en principio simple: ai el usuario pertenece a una unidad de análisis o de obtención de inteligencia, la mejor opción será un PC de sobremesa, pues tendrá mejores prestaciones técnicas a menor coste, sin que el problema de que la falta de movilidad afecte al trabajo rutinario. Si por el contrario el usuario pertenece a una unidad operativa, con desplazamientos habituales fuera de su base de operaciones, la mejor opción es un ordenador portátil.

Como recomendaciones adicionales en materia de hardware, siempre es conveniente contar con una unidad de almacenamiento de respaldo para la realización de copias de seguridad. Esta unidad puede ser el clásico disco duro portable, o algo más actualizado como una unidad de almacenamiento en línea (local o en la nube). En lo relativo a la conectividad, la situación ideal es la de realizar la conexión a Internet por cable de red, pues aporta mayor velocidad y estabilidad a la navegación, carga y descarga de archivos.

En relación con las necesidades de software la primera duda que puede aparecer es sobre qué sistema operativo es el más idóneo para la realización de labores de OSINT. La propuesta que se hace en este manual es el uso de Windows 10 como sistema operativo principal. El motivo es simple: Windows 10 es objetivamente el sistema operativo más utilizado en el mundo (por lo que basar en él este manual hace que su aplicación llegue más fácilmente a un mayor número de usuarios), y por tanto es para el que más aplicaciones se desarrollan, con una interfaz de uso más agradable para los usuarios. Dicho lo cual, cualquier sistema operativo (Windows, macOS o sistemas basados en UNIX) cuenta con herramientas suficientes para la obtención de información en Internet, por lo que la elección con base en las preferencias del usuario siempre será la mejor opción.

El resto de las herramientas esenciales de software para la recopilación de inteligencia en Internet constituyen en sí mismas una categoría, pues tienen

relación con la seguridad propia a la hora de realizar estas actividades.

Seguridad propia

Este manual tiene por objeto dar una formación de base para la realización de actividades de obtención de información en Internet relativa a tráfico de fauna silvestre y otros delitos contra el medio ambiente. Ahora bien, nunca debemos de pensar que, porque estemos realizando operaciones en Internet, probablemente desde nuestra oficina, en un entorno que consideramos seguro, no estamos expuestos a peligros y amenazas tan serias o graves como si nos adentráramos en un entorno real. De hecho, es necesario hacer una observación que a veces obviamos: la realización de actividades OSINT no es un monopolio de las fuerzas policiales. Los delincuentes llevan a cabo este tipo de actividades, cada vez con mayor frecuencia y detalle. Así que de igual forma a que nosotros vamos a intentar encontrar información en Internet sobre actividades delictivas, ellos pueden llegar a detectar nuestras actividades y ejecutar labores de contra vigilancia. Para evitar que esto suceda, se recomienda que se ejecuten las siguientes medidas preventivas:

Uso de Red Privada Virtual (Virtual Private Network o VPN)

La conexión normal a Internet está expuesta a varias vulnerabilidades. En primer lugar, la información que se envía a través de esta no está sometida específicamente a un cifrado que la haga ilegible, y, en segundo lugar, cada vez que realicemos una conexión a una página o servicio web, en los servidores de dicha web o servicio se reflejará nuestra IP real de conexión. Esta información puede exponer extremos tales como, en los casos menos graves, la ciudad en la que nos encontramos, o en los casos más graves, nuestra identidad o la de nuestra agencia.

Esta problemática la solucionan las VPNs, las cuales cifran la información que se transmita a través de nuestra conexión a Internet y, además, reflejan una IP de conexión distinta a la nuestra durante nuestra navegación. Las VPNs y algunos aspectos del uso de VPNs se encuentran regulados en algunas jurisdicciones según los territorios, por lo que el usuario deberá actuar de conformidad con la legislación nacional relativa al uso de VPNs.

Hay infinidad de VPNs disponibles en el mercado, versiones gratuitas o de pago. Las versiones gratuitas tienenlimitaciones en varios aspectos tales como de limitación a la cantidad de navegación diaria que se puede realizar a través de esta (medida en Megabytes o Gigabytes), o limitación en la elección del país origen de la IP que refleje la navegación. La elección se debe de realizar con base en criterios económicos y/o de idoneidad de las características propias de cada una de ellas, y de los intereses de cada agencia. Sin embargo, en relación a su uso y popularidad, a modo de ejemplo se recomiendan las siguientes VPNs:

- NordVPN, ubicada en https://nordvpn.com/es/
- ExpressVPN, ubicada en https://www.expressvpn.com/es

Los desarrolladores de VPN actualizan sus tecnologías en diferentes intervalos, por lo cual los usuarios deberían mantenerse actualizados con los avances y nuevas funcionalidades y revisiones de los diferentes VPN regularmente.

Uso de Máquinas virtuales

Con las VPNs se protege la salida de información desde nuestra conexión a Internet, pero sigue existiendo una vulnerabilidad en la entrada de contenido, es decir, en la descarga de información de Internet.

Toda navegación web es susceptible de sufrir procedimientos de infección por Malware[1]. En determinadas ocasiones es fácil evitar sufrir estas infecciones, y en otras es difícil darse cuenta de ellas. Igualmente, en la gran mayoría de las ocasiones las infecciones serán de piezas de Malware de gravedad baja tales como el Adware[2] , pero otras pueden ser más severas, que espíen nuestra navegación, el uso de nuestro equipo informático o que dañen nuestros ficheros informáticos.

La forma más sencilla de evitar estas vulnerabilidades es el uso de máquinas virtuales. Una máquina virtual nos permite instalar un sistema operativo dentro de nuestro sistema operativo. De forma sencilla, nos permite tener otro equipo informático distinto dentro de nuestro equipo informático. Esta capacidad nos ofrece dos grandes ventajas: primero, no nos tenemos que preocupar de que la máquina virtual se infecte. Las máquinas virtuales están pensadas para poder ser devueltas de forma sencilla a un estado anterior, por lo que, en caso de sufrir una infección, basta con devolver la máquina virtual a un estado anterior pre-infección. Por otro lado, usando las

1 Programa malicioso, referente a cualquier tipo de software que hace acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

2 Adware es software no deseado, diseñado para mostrarnos anuncios publicitarios. Más información en https://es.malwarebytes.com/adware/

máquinas virtuales exclusivamente para navegación, y no teniendo en ellas documentación sensible, es imposible que por una infección de Malware un delincuente tenga acceso a información importante. Adicionalmente, por la infección de una máquina virtual es prácticamente imposible que se contagie al sistema operativo principal, por lo que tampoco se debe temer este extremo.

En segundo lugar, nos permite tener las capacidades de varios sistemas operativos, de forma sencilla, en un solo equipo informático. Expliquemos esto con un ejemplo: probablemente nuestro equipo principal use un sistema operativo Windows 10, por ser el más utilizado por la mayoría de la población. Sin embargo, es posible que para determinadas tareas deseemos utilizar otro sistema operativo, como Linux para determinadas herramientas de obtención, o MacOS para tareas de edición de vídeo. Con las máquinas virtuales puedo tener un sistema operativo principal Windows10 para mi labor habitual, y contar con máquinas virtuales con los sistemas operativos Linux y MacOS para aquello que considere necesario (e incluso una máquina virtual con otro Windows10 exclusivamente para navegación web peligrosa, por ejemplo).

Actualmente los dos programas más utilizados para la configuración y uso de máquinas virtuales son:

- VirtualBox, disponible en https://www.virtualbox.org/wiki/Downloads.
- VMWare, disponible en https://www.vmware.com/es/products/workstation-player/workstation-player-evaluation.html.

La principal diferencia entre estos dos productos radica en que VirtualBox es una herramienta de código libre y gratuita, mientras que VMware, aunque tiene una versión gratuita, es de código cerrado y de pago.

Perfiles en redes sociales

Uno de los objetivos de este manual es dar a conocer cómo obtener información de diferentes redes sociales que pueden ser de interés en el transcurso de una investigación. Pero hemos de tener claro que esta relación de obtención de información no es unilateral: al igual que nosotros podemos obtener información sobre usuarios de redes sociales, el resto de los usuarios de esa red social puede obtener información sobre nosotros. Este hecho se ve magnificado por el propio funcionamiento de las redes sociales.

Pondremos un ejemplo para entender el riesgo de exposición. Imaginemos que hemos localizado un objetivo en redes sociales, y lo monitorizamos de forma activa; se esta forma, obtenemos información sobre él. La bilateralidad de este intercambio de información se manifiesta en el hecho de que es muy posible que, si visitamos su perfil de forma frecuente, más tarde o más temprano le aparezca al objetivo el perfil que estemos utilizando en redes sociales como sugerencia de amistad.

Este riesgo es grave, y nos deja deducir una consecuencia inmediata. Jamás, salvo excepciones de auténtica gravedad o urgencia, debemos realizar labores de investigación de perfiles en redes sociales utilizando nuestro perfil particular. La recomendación es la creación de perfiles específicos, con trasfondos neutrales (o de interés, esto puede variar en función del marco legal de cada país y se explicará más adelante) en relación con la temática delictiva que se esté investigando; y tantos perfiles como sea necesario.

A este respecto, hay varias páginas web que, en teoría, ayudan a la creación de perfiles falsos generando biografías ficticias, nombres falsos, correos electrónicos de usar y tirar, fotografías de personas ficticias, y otros recursos. Como norma general, NO se recomienda el uso de este tipo de páginas web, máxime si se sospecha que el delincuente toma medidas de seguridad, pues estos datos ficticios son fácilmente identificables.

Uso de contraseñas seguras

E es necesario mantener, como mínimo, una cuenta por cada red social en la que queramos realizar labores de obtención de información. Eso supone tener que manejar un gran volumen de cuentas, lo que a su vez repercute en tener que mantener un control sobre un gran volumen de contraseñas o passwords.

Es política de seguridad básica mantener contraseñas complejas (con mayúsculas, minúsculas, números y símbolos, y longitud superior a los 10 caracteres), e individualizadas (no repetir la misma contraseña para distintas plataformas) lo que acaba suponiendo en tener que gestionar, si queremos hacerlo correctamente, un gran volumen de contraseñas complejas.

La solución sencilla para mantener un correcto control de cuentas y contraseñas, y de la calidad de estas, es el uso de un programa de gestión de contraseñas. Estos programas generan y almacenan contraseñas seguras de forma automática, haciendo que para el usuario solo sea necesario recordar una contraseña maestra, que es la que da acceso a todo el "llavero" de contraseñas de las diferentes cuentas.

Vistas las distintas opciones que existen para este tipo de programas, se recomienda el uso de Keepass (disponible en https://keepass.info/), pues es un programa de código abierto, totalmente gratuito, fácil de manejar, y que cubre todas las necesidades de forma satisfactoria en lo que refiere a generación y almacenamiento de contraseñas.

TERMINOLOGÍA DE BÚSQUEDA

El principal error con respecto a la realización de OSINT es pensar que se puede encontrar todo de todo en Internet con un simple comando. No todo está en Internet, y lo que está, no siempre es sencillo de encontrar. La realización de actividades de búsqueda en internet no puede hacerse de forma aleatoria o caprichosa. Debe de seguir una pauta o metodología, que normalmente se plasma en un documento estratégico denominado Plan de obtención.

El primer paso de este plan consiste en definir qué queremos encontrar.

Definir qué queremos encontrar se traduce, de forma resumida y en el caso del tráfico de especies específicamente, en un diccionario de términos que queramos "atacar". Estos términos, principalmente, tendrán relación con especies que sean de nuestro interés (bien por el grado de amenaza de la especie, por su valor económico o por su relación con nuestro país o zona de interés, entre otros). La redacción de este diccionario es algo que debe de realizar cada agencia, pues los intereses varían en función de los parámetros descritos anteriormente. A continuación, se enumeran los pasos que deben de ser tenidos en cuenta para crear - y mantener actualizados - nuestros diccionarios, detalles que en caso de ser omitidos puede acarrear que estemos dejando fuera del ámbito de nuestras búsquedas resultados valiosos para nuestro plan de obtención. Los pasos son:

1. Identificación de las especies de interés, incluyendo nombre común y científico.
2. Inclusión de términos coloquiales con relación a las especies introducidas. En este caso, nos referimos a diminutivos o argot empleado por los delincuentes. Se recomienda revisar y actualizar constantemente los términos.
3. Inclusión de todas aquellas palabras con respecto a estas especies que denominen partes suyas o derivados que puedan ser objeto de interés y, por tanto, de tráfico ilegal.
4. Traducción de todo lo anterior a inglés obligatoriamente, y a cualquier otro idioma que por la idiosincrasia de la investigación pueda ser de interés.
5. Inclusión de errores ortográficos normales que puedan ocurrir de forma habitual con respecto a todos los términos anteriores (por ejemplo, un término formal sería búho, y un término ortográficamente incorrecto pero habitual es bú o). A pesar de que estos errores pueden ser aceptados por los buscadores habituales, y reinterpretados hacia el término correcto, es mejor no dejar nada a la interpretación del software.

A continuación se detallan algunas consideraciones sobre terminología utilizada en el estudio "Comercio en línea de fauna silvestre: análisis de plataformas y especies comercializadas en Bolivia, Colombia, Ecuador y Perú" elaborado por Wildlife Conservation Society (WCS, 2022).

Términos y estrategia de muestreo

Cuando las búsquedas son multi país, se recomienda utilizar términos de búsqueda asociados a especies priorizadas para los países seleccionados. Cada una de las combinatorias o ecuación de búsqueda estará compuesta por el nombre común o nombre científico de la especie. Se sugieren el uso palabras claves que incluyen: verbos como comprar, vender, querer, buscar y sustantivos, relacionados al conocimiento o experiencia de cada país sobre la demanda y/u oferta de la especie, pudiendo ser la divisa o moneda local (incluyendo su símbolo) o el nombre de un lugar en específico.

Tabla 1. Modelo de priorización de especies y palabras clave

Nro	Grupo	Especies	Palabras clave
1	Tortugas **Tortoise – turtles** *(Tortugas acuáticas - semi acuáticas – terrestres)*	*Podocnemis unifilis* (taricaya, terecay) *Podocnemis expansa* (charapa) *Chelus fimbriata* (mata mata) *Chelonoidis carbonarius* (morrocoy) *Chelonoidis denticulata* (motelo) *Chelonoidis chilensis* (peta) *Chelonoidis* sp. *Rhinoclemmys* sp.	Tortuga; huevos; mascota; carne; caparazón; acuario; tortugario; tortuga acuática; tortuga enana; peta; juvenil morrocoy; tortuga; huevos; mascota; carne caparazón; acuario; tortugario; peta; galápagos
2	Caimanes, cocodrilos y lagartos **Lizards** **Caiman and crocodiles**	*Melanosuchus niger* (caimán negro) *Caiman yacare* (lagarto)	lagarto; caimán; piel; cabeza; artesanía; negro; cuero; huevo
3	Boas **Boas**	*Boa constrictor* *Corallus* sp. *Epicrates* sp.	Boa; mascota; serpiente grande; artesanía; piel serpiente; piel; cuero; esqueleto
3	Ranas **frogs**	*Oophaga histrionica* (rana arlequín) *Oophaga lehmanni* (rana dardo)	Rana arlequín, terrario, mascota, rana dardo
4	Guacamayos – **Guacamayas** **Macaw**	*Ara rubrogenys* (paraba de frente roja) *Ara macao* (guacamayo escarlata) *Ara glaucogularis* (guacamayo barbazul) *Ara ararauna* (guacamayo azul y amarillo)	Paraba; plumas; mascota; papagayo; parabas; loro; corona
5	Loros – pericos, periquitos **Parrots** **Parakeets**	*Psittacara erythrogenys* (loro cabeza roja) *Brotogeris jugularis* (perico real) *Brotogeris versicolurus* (perico ala amarilla) *Amazona ochrocephala* (loro frentiamarillo) *Amazona farinosa* (loro farinoso) *Brotogeris* sp. (pihuicho, perico) *Aratinga mitrata* (cotorra mitrada) *Aratinga weddellii* (perico cabeza gris) *Aratinga acuticaudata* (perico corona azul)	Loro, hablador, exótico, mascota, plumas, jaula, corona, perico, periquito
6	Monos – titi **Marmoset** **Monkey**	*Saimiri sciureus* (mono ardilla) *Sapajus apella* (mono cachudo) *Cebuella pygmaea* (tití pigmeo)	Mono, mascota, mico, barizo, mono pequeño; martín

Respecto a la familiaridad con la dinámica de la oferta y/o demanda, por ejemplo los grupos de redes sociales/ foros, se recomienda recolectar información o "investigar" tan lejos como sea productivo, tomando notas sobre el esfuerzo (tiempo), enlaces adicionales explorados, grupos específicos investigados, material útil y enlaces producidos, hasta llegar a información específica potencialmente accionable, registrando meticulosamente esa información.

Tabla 2. Algunos términos asociados a partes de fauna silvestre en 2 idiomas usados en redes sociales y otras plataformas.

English	Español
Head	Cabeza, trofeo
skull, cranium	Cráneo, calabera, calavera
Teeth, canine, fangs	Dientes, caninos, colmillos
Whiskers	Bigotes, pelos
Paws	Patas, pies, manos, pata, pie, mano, piches en aves
Claws	Garras, uñas, garra, uña,
Bones	Huesos, hueso, esqueleto
Genitals,penis	Genitales, pene, testículos, órganos, genitales, huevos, tanates, pico, chile, miembro
Paste, glue,oil,butter	Pasta, manteca, mantequilla, aceite, grasa, sebo, goma, ungüento, pomada, pegamiento, ungüento, crema de untar
Liquor	Licor, vino, guaro Alcohol
Jewelry	Joyería, arete, collar, dije, collar, amuleto, joya, joyas, pulsera, brazalete
Hide, skin	Piel, cuero, piel, pellejo, tapete, alfombra, taxidermia,
Tail	Cola, rabo
Meat	Carne
Soup	Sopa
Amulet	Amuleto

USO DE BUSCADORES

Existen numerosos buscadores en Internet a disposición de los usuarios. La principal clasificación de estos buscadores se realiza en función de la precisión de su algoritmo de búsqueda, lo que finalmente acaba traduciéndose en una clasificación de estos buscadores en base a la compañía desarrolladora del algoritmo. Así, en esta primera diferenciación, hay tres grandes motores de búsqueda: Yahoo, Bing y Google. No se pueden considerar a estos buscadores como iguales: Yahoo es un motor venido a menos desde sus mejores tiempos, y Bing, a pesar de contar con una compañía tan potente como Microsoft detrás, tampoco alcanza grandes cotas de un mercado claramente copado por Google. Según datos de Statcounter[1], Google ha realizado un 92% de las búsquedas en el último año a nivel mundial, frente al 2,48% de Bing y el 1,5% de Yahoo.

Una segunda clasificación de los motores de búsqueda sería según la región geográfica en la que se realice la búsqueda. En este caso, si se estudian los datos de la región asiática[2], aparecen los motores de búsqueda Baidu (eminentemente chino) con un 2,84% de las búsquedas, y Yandex (eminentemente ruso) con un 1,8% de las búsquedas. No obstante, estos datos pueden estar afectados por la falta de transparencia de las comunicaciones en Internet provenientes de Rusia y China, pudiendo ser su uso superior al mostrado. En cualquier caso, conviene tomar nota de ambos buscadores como muy relevantes en mercados tan importantes como estos dos citados países.

Finalmente, una última clasificación de los motores de búsqueda surgiría por sus características técnicas y, en este caso específico, por el mayor respeto a la privacidad de los navegantes. En este caso, conviene citar a Duckduckgo, con un 0,63% de las búsquedas mundiales, como principal referente.

Definido el escenario del mercado de los buscadores a nivel mundial, y sus características diferenciadoras, es normal lanzarse la pregunta: ¿cómo es posible que Google obtenga tanta preferencia? Probablemente se deba a la suma de tres factores:

- Los usuarios perciben los resultados del algoritmo de Google como mejores.
- Los usuarios perciben el buscador como más atractivo visualmente y/o más amigable hacia el usuario.
- La experiencia de usuario en la optimización de búsquedas de Google.

Y he aquí uno de los aspectos claves: la optimización en las búsquedas de Google en función de la experiencia de usuario. Cuando utilizamos esta expresión, nos referimos a cómo Google cambia los resultados que nos arroja cuando realizamos una búsqueda en función de las búsquedas que hayamos realizado previamente. Todos aquellos que hemos utilizado Google de forma frecuente (lo cual corresponde con la amplia mayoría de la población) hemos experimentado este proceso, cuyo exponente más vistoso es la presencia de anuncios sobre una temática buscada anteriormente, pero que en lo que refiere a las búsquedas como tal, se observa sobre todo cuando buscamos algo, elegimos un resultado que no es el primero (quizás sea el cuarto o quinto resultado), y volvemos a realizar la misma búsqueda posteriormente. Más tarde o más temprano ese cuarto o quinto resultado pasará a ser el segundo o incluso el primero que Google nos arroje[3].

Pues bien, la experiencia de usuario puede considerarse como un problema o como una ventaja. En puridad, si lo que queremos es realizar búsquedas individuales, no afectadas por parámetros externos distintos a los términos buscados, la experiencia de usuario es un problema, y debe de corregirse (utilizando búsquedas en modo incógnito, por ejemplo, de forma conjunta con la eliminación de cookies y del historial de navegación). Ppara los fines de este documento, vamos a verlo como una ventaja, y vamos a utilizar la optimización de búsquedas de Google a nuestro favor, así que en este manual vamos a aprender a configurar y usar Google para nuestras búsquedas. No se entrará en detalle sobre el uso del resto de buscadores, salvo para referir que Bing y Yahoo son opciones similares disponibles; que Baidu debe de tenerse en cuenta si realizamos búsquedas relacionadas con el entorno chino y Yandex con el ruso; y que Duckduckgo está específicamente diseñado para aportarnos mayor privacidad.

1 https://gs.statcounter.com/search-engine-market-share

2 https://gs.statcounter.com/search-engine-market-share/all/asia

3 Startpage.com busca en Google pero no tiene la misma trazabilidad y tiene más opciones de privacidad que Google. Además, distintos navegadores pueden producir resultados diferentes, así que es útil usar más de uno y comparar los resultados. Usualmente empleamos Google a través de Startpage y DuckDuckgo. En buscadores de imágenes, Bing tiene mucho más resultados y es más sencillo de filtrar y explorar, en comparación con Google images. Bing fue recomendado por un entrenador en OSINT.

Configuración de Google

A la hora de utilizar Google para nuestras búsquedas vamos a intentar que el motor detecte nuestro interés en ámbitos concretos como el tráfico de especies en particular para que, al realizar búsquedas, priorice los resultados en función de estos intereses. Para ello, debemos de tener en consideración lo siguiente:

- Debemos de crear una cuenta de Google específica para su uso en el ámbito profesional. La creación de una cuenta de Google es gratuita, y se puede hacer desde la siguiente URL : https://accounts.google.com/signup/v2/webcreateaccount?flowName=GlifWebSignIn&flowEntry=SignUp
  Los motivos de crear una cuenta específica son simples. Por un lado, evitamos realizar búsquedas con nuestras cuentas particulares. Por otro lado, está cuenta puede ser transferida o prestada a otro usuario de nuestra misma unidad o grupo, para que sea utilizada por más personas, y recibir el beneficio de la experiencia de usuario.
- No debemos de realizar NUNCA búsquedas que no estén relacionadas con una investigación sobre estas temáticas. Si realizamos búsquedas sobre otros términos, como otras temáticas delictivas completamente ajenas o, incluso peor, sobre ámbitos particulares y personales, estaremos contaminando la experiencia de usuario, y haremos que Google tome en consideración factores externos a aquellos de nuestro interés a la hora de arrojarnos resultados.
- No obstante, hemos de ser conscientes de que la actividad de una cuenta de Google puede ser supervisada en su totalidad sobre el usuario, en lo que refiere a los términos buscados, navegación, localizaciones. Para ello, basta con ingresar en la URL https://myaccount.google.com/, e inspeccionar los campos “Datos y privacidad” y posteriormente “Configuración del historial”. Ahí encontraremos información sobre nuestra actividad en la web, aplicaciones, geolocalizaciones y uso de YouTube . (Ilustración 1).

Al ingresar en cualquiera de esos tres campos, podremos elegir qué información queremos borrar para que no sea tenida en cuenta. Podemos incluso borrar todo el historial de búsquedas de una cuenta y toda su actividad (Ilustración 2).

Ilustración 1. Actividad de una cuenta de Google.

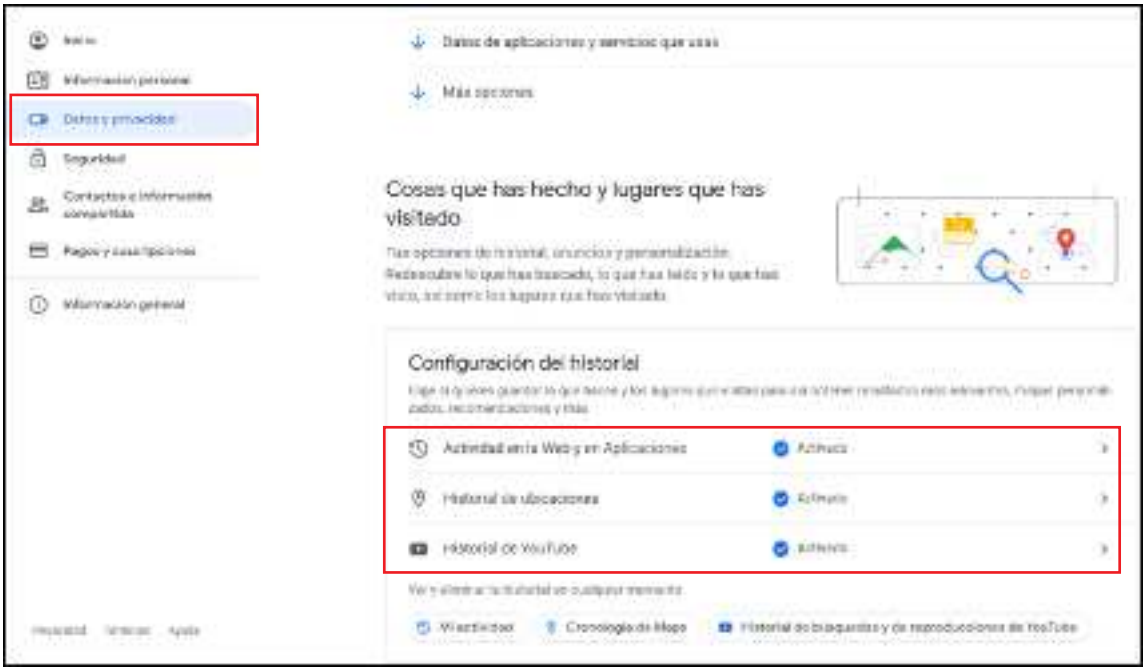
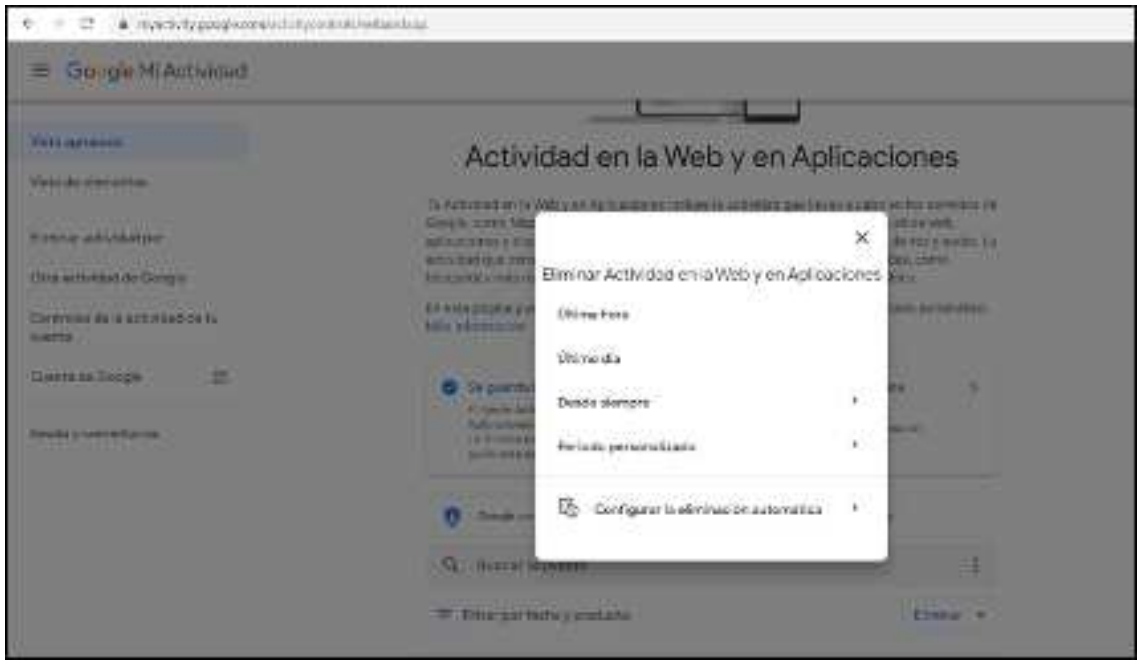


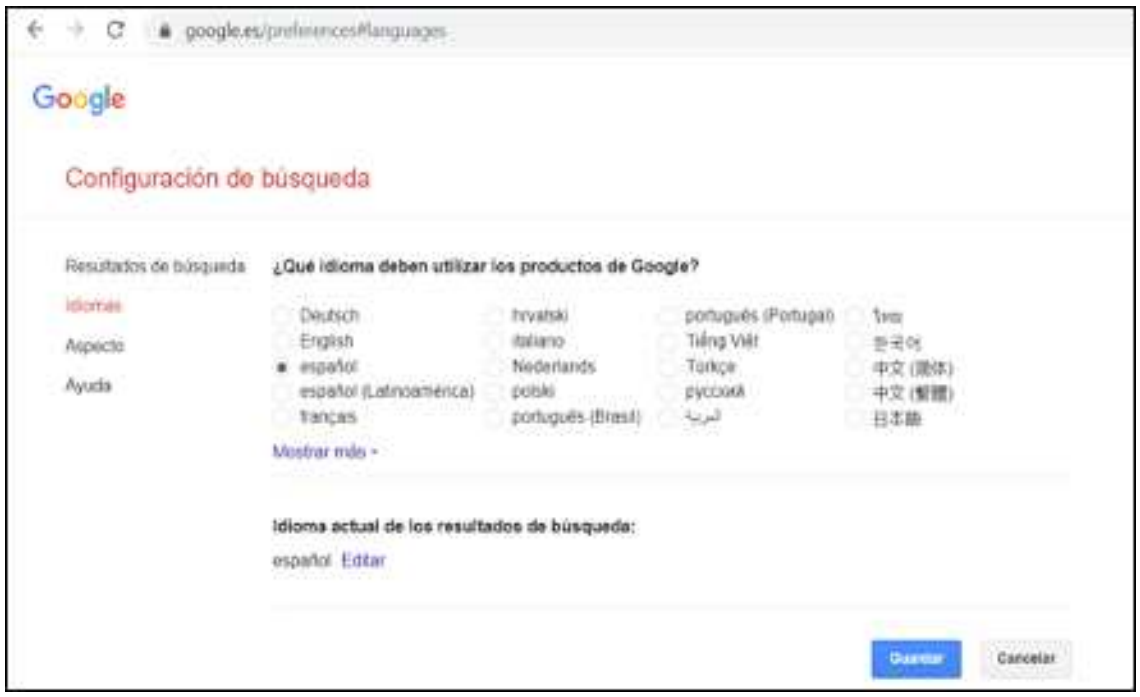
Ilustración 2. Eliminación de actividad de la cuenta de Google



- Después de crear una cuenta de Google para fines profesionales de búsqueda, hemos de configurar su uso ingresando en la URL https://www.google.es/preferences (entendamos que ".es" debe sustituirse por la terminación del país del usuario cada vez que aparezca una referencia similar a lo largo del presente manual). En esta página nos encontraremos con las siguientes casillas de personalización que son de interés.
    - En el apartado de "Resultados de búsqueda" son de interés los campos: "Activar búsqueda segura", el cual se recomienda que esté desactivado; "Resultados por página", el cual se recomienda que no sea superior a 20; "Autocompletar con tendencias de búsqueda", el cual debe contener la opción "Mostrar búsquedas populares"; y por último el apartado "Configuración de región". En este último campo debe de constar "Región actual", salvo que queramos ver los resultados que Google arroja sobre una zona geográfica concreta, en cuyo caso es recomendable cambiar al país que sea de interés.
    - El apartado "Idiomas" por defecto deberá figurar nuestro idioma nativo, pero en aquellos casos en los cuales estemos buscando términos en otro idioma, es recomendable cambiar el idioma a aquel que sea de nuestro interés.

Ilustración 3. Configuración de región en preferencias de Google.

Ilustración 4. Configuración de idioma en preferencias de Google.



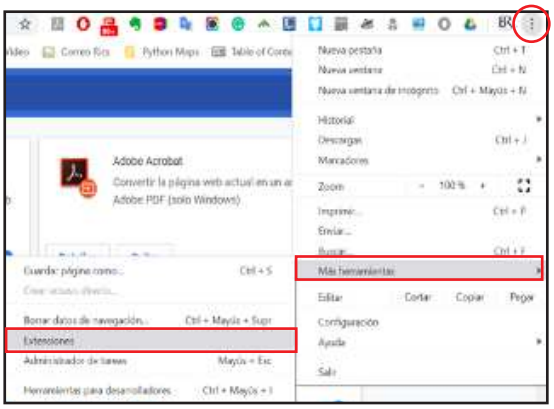
Comprendido todo lo anterior, ya estamos en disposición de entrar en el campo de la realización de búsquedas.

Habilitación de add-ons (Chrome) en modo incógnito.

Por default, los add-ons o extensiones de Google Chrome no se habilitan en modo incógnito. Para realizar su habilitación, ejecute los siguientes pasos.

1. Entre a la ventana de extensiones de Google Chrome. En la esquina superior derecha, presione sobre los tres (3) puntos verticales, del menú desplegable, seleccione “más herramientas” y luego “extensiones”. Se desplegará la ventana de extensiones.

Ilustración 5. Paso 1 para la habilitación de add-on (Chrome) en modo incógnito



2. Seleccionar la extensión de interés y hacer click en el botón de detalles.

Ilustración 6. Paso 3 para la habilitación de add-on (Chrome) en modo incógnito.

3. En las opciones que despliega, activar la opción de “Permitir en modo incognito”.

Ilustración 7. Paso 4 para la habilitación de add-on (Chrome) en

Ilustración 8. Títulos de las webs elpais.com, elmundo.es y amazon.

Realización de búsquedas con Google: Comandos de búsqueda

Para mejorar nuestras búsquedas en Google lo primero que tenemos que entender es dónde busca Google los términos que introducimos en el buscador. En este aspecto, Google busca los términos introducidos en los siguientes lugares:

- URL: Google busca los términos en la propia URL.
- Título de una página web: es la descripción que nos aparece sobre una web cada vez que generamos una pestaña nueva con ella. En la Ilustración 8 se puede ver un ejemplo de diferentes webs con sus títulos (para ver el título completo basta con dejar el cursor del ratón unos segundos encima de la pestaña pertinente).
- Cuerpo de la página web: esto es, el contenido de la página web.
- Multimedia: los vídeos, los audios y las imágenes presentes en una página web tienen, como archivos que son, nombres asociados. Sobre esos nombres asociados también se realizará la búsqueda de los términos que introduzcamos.
- Código fuente: el código fuente de una página web contiene parte de la programación de esta. Sobre esto, también se realizarán búsquedas de los términos. El código fuente de una web es visible pulsando clic derecho y seleccionando la opción "ver código fuente de la página" o similar, en la mayoría de los navegadores web.

Una vez que tenemos esto claro, se pasa a ejecutar comandos de búsqueda avanzados. En primer lugar, hay una versión más amigable de los comandos de búsqueda de Google accesible desde la URL https://www.google.es/advanced_search. En esta URL ya encontramos lo básico para poder realizar búsquedas más profundas. Pero, al objeto de comprender lo que sucede, es mejor explicar los diferentes comandos que utiliza el buscador, y posteriormente que cada usuario amolde este conocimiento a su gusto.

En segundo lugar, el objetivo de utilizar los comandos avanzados de Google es simple: disminuir (significativamente) el número de resultados que arrojan nuestras búsquedas, y conseguir que estos resultados tengan mayor calidad. Los comandos más relevantes son los siguientes:

- **Comando AND**: nos permite ejecutar una conjunción. Es decir, nos permite obtener resultados que contengan un término de búsqueda y otro, a la vez. Por tanto, es un comando que sirve de filtro. Por ejemplo: si introducimos la palabra leon (sin acento) en Google obtenemos lo siguiente:
  644 millones de resultados (Ilustración 9). Esto ocurre porque hay muchos resultados relevantes que contienen la palabra leon: la película el rey leon; el coche seat leon; la ciudad de León; y el animal. Si queremos obtener resultados que solamente se refieran a una de las categorías anteriores, basta con poner el comando AND y términos de esa categoría. Por ejemplo, si quiero buscar resultados del coche, haría: (Ilustración 10) Como vemos, los resultados han disminuido hasta 162 millones (Ilustración 10). Por supuesto, son todavía muchísimos resultados, pero con la introducción del comando hemos logrado recortar el número en un 75% aproximadamente. Además, todos los resultados que hemos obtenido contienen la palabra león y la palabra seat a la vez, por lo que la inmensa mayoría corresponderán a resultados que tienen que ver con el coche Seat Leon.
- **Comando -** : de uso similar a AND, el comando – nos permite filtrar resultados. En este caso, permite eliminar términos de nuestra búsqueda. Veámoslo con un ejemplo. Si busco el término jaguar, obtengo 357 millones de resultados, que van desde el animal, hasta el coche jaguar, y la serie de TV Jaguar. Sin embargo, si introduzco la búsqueda jaguar -serie -animal, aunque el número de resultados sigue muy similar (342 millones), la referencia a la serie de televisión y al animal han desaparecido, quedándome resultados sobre el coche Jaguar principalmente.

Ilustración 9. Resultado de la búsqueda del término leon

Ilustración 10. Resultado de la búsqueda leon AND seat

- **Comando “”**: podríamos denominarlo el comando literalidad. Nos permite buscar el término que se introduzca entre las comillas de forma literal, tal y como lo hayamos puesto.

Veamos un ejemplo. Antes hemos visto como la búsqueda del término leon (sin acento) nos daba 644 millones de resultados. Sin embargo, si buscamos “león” ocurre esto (Ilustración 11)

Ilustración 11. Resultados de la búsqueda “león”

Como vemos, la introducción del término ortográficamente correcto reduce a la mitad aproximadamente el número de resultados, y todos contienen la palabra león, y no león . ¿Para qué es especialmente útil este comando? Para la búsqueda de nicknames o apodos, pues muchos son similares a palabras reales, pero cambian quizás una “o” por un “0”. Si queremos buscar el apodo, y no palabras similares, la literalidad nos proporcionará resultados útiles.

- **Comando Cache**: a cuando vamos a ver una versión anterior de una página web, una forma de hacerlo es con el comando cache. Veamos un ejemplo. Si visito la web https://as.com/ meristation/ se observa lo siguiente (Ilustración 12):

Sin embargo, si introduzco en Google el comando cache:meristation.com, obtengo lo siguiente: (ilustración 13)

Se observa un anuncio de Google que nos avisa que la web era así a las 07:12 horas GMT del 27 de septiembre. Así que, por así decirlo, hemos viajado un poco al pasado. Aunque el contenido parece idéntico, de hecho, no lo es porque los temas que aparecen en el apartado “Temas del día” han variado. Es solo un ejemplo de cómo podemos ver modificaciones en una web (aunque hay mejores herramientas que veremos posteriormente).

Ilustración 12. Contenido de la web as.com/meristation el 27/09/20201 a las 11:30 horas.

Ilustración 13. Resultado del comando cache:meristation.com

- **Comando Filetype:** uno de los comandos más útiles sin duda. Nos permite restringir los resultados a tipos de archivo específicos. Es decir, si queremos obtener documentos de Microsoft Word, Excel, PDF... podemos filtrar sobre ese criterio. Veamos un ejemplo. Si buscamos Interpol en Google, obtenemos lo siguiente: (Ilustración 14)

Como vemos, obtenemos casi 22 millones de resultados. Sin embargo, supongamos que estamos haciendo un informe oficial, y lo que queremos son documentos u otros informes que hagan referencia a Interpol. Para ello, usamos el comando filetype:pdf Interpol, y obtenemos lo siguiente: (Ilustración 15)

Ilustración 14. Resultados de la búsqueda de Interpol en Google.

Ilustración 15. Resultados de búsqueda del comando filetype:pdf interpol

En primer lograr, observamos como el número de resultados ha descendido a 900.000, una reducción muy significativa. Por otro lado, todos los resultados ahora son exclusivamente documentos PDF relacionados con Interpol. Si quisiéramos buscar documentos de Word, usaríamos doc o docx; si queremos tablas de Excel, xls o xlsx; etc.

- **Comando Site:** el comando site nos permite filtrar los resultados en base a la página web en la que aparecen. Es especialmente útil para localizar anuncios de compra/venta. Veamos un ejemplo. Si realizamos una búsqueda sobre piel de león, obtenemos lo siguiente

Ilustración 16. Resultados de búsqueda de piel de león.

Es un número de resultados muy elevado, que contiene además mucho ruido (algunos resultados son canciones, cuentos, otros; los cuales son ajenos a la temática del tráfico de especies). Sin embargo, por inteligencia policial conocemos que la página web milanuncios.com es una de la más utilizada por los usuarios para actividades de compraventa (en España esta web es de facto una de las más utilizadas). Por tanto, realizamos la búsqueda site:milanuncios.com piel de león, y obtenemos lo siguiente:

Ilustración 17. Resultados de la búsqueda site:milanuncios.com piel de león.

Como vemos, el número de resultados ha disminuido enormemente, y además, solo nos ofrece resultados relativos a milanuncios.com. La observación de estos resultados nos ofrece algunos que, aparentemente, son candidatos a su investigación en mayor detalle:

Ilustración 18. Ejemplo de resultado obtenido al utilizar site:milanuncios.com piel de león.

- **Comando Link**: este comando nos permite obtener resultados que enlacen a una URL concreta. Como uso general podríamos utilizar link:milanuncios.com piel de león, siguiendo el ejemplo anterior, para encontrar resultados que enlacen a milanuncios.com y hablen sobre piel de león. Pero la verdadera utilidad de este comando es la siguiente. En la búsqueda anterior, site:milanuncios.com piel de león, hemos obtenido anuncios que pueden ser ilegales. Si cogemos la URL exacta de alguno de esos anuncios, y utilizamos link:URL (entendido URL como la URL exacta del anuncio sospechoso) Google nos arrojará resultados que enlacen a ese anuncio. En muchas ocasiones, los resultados serán nulos, pero en otras ocasiones puede que el anunciante haya enlazado al anuncio desde su cuenta en Facebook, o en Twitter, o en un foro, y de esta forma obtendremos perfiles relacionados con él

Con toda esta información, y teniendo en cuenta que se pueden concatenar varios de los comandos simultáneamente, podremos tener un manejo mucho más preciso de Google a la hora de realizar nuestras búsquedas.

Las ecuaciones de búsqueda pueden contener operadores booleanos para disminuir el sesgo en la búsqueda (por ejemplo: "Jaguar" es una marca de automóviles y cuyos resultados pueden incluirse en las búsquedas).

Tabla 3. Operadores booleanos Google, significado y uso

Operador Booleano	Significado/ Uso
OR, |	Equivalente a conjunción "o", Muestra resultados que contengan al menos uno de los términos usados en la ecuación de búsqueda. jaguar OR otorongo
" "	Busca las palabras exactas en una frase. "jaguar latinoamericano"
AND	Equivalente a conjunción "y". Muestra resultados que contenga ambos términos utilizados en la ecuación de búsqueda taricaya AND terecay
+	Busca páginas web que contengan todos los términos precedidos del símbolo +. También te permite incluir términos que, normalmente, se ignoran. +tortuga
-, NOT, AND NOT	Muestra resultados donde se excluyen el término precedido del operador. jaguar -autos
*	Muestra resultados que pueden omitir una o varios términos de búsqueda, así como variaciones de palabra con una misma raíz. taricaya*
"..."	Muestra resultados que incluyan los términos incluidos dentro del operador, en la misma frase, en el mismo orden. "huevo de taricaya"
site:	Muestra resultados obtenidos de en una página web determinada o concreta. site:www.wcs.org
intext:	Muestra resultados que en los textos contengan los términos de búsqueda utilizados
filetype:	Muestra resultados que contenga archivos relacionados con los términos de búsqueda utilizados. filetype:pdf
intitle:	Muestra resultados cuyo título contenga los términos de búsqueda utilizados. intitle:guacamayo

Tabla 4. Operadores boleanos Bing[1]

Operador	Definición	Ejemplo
+	Busca páginas web que contengan todos los términos precedidos del símbolo +. También te permite incluir términos que, normalmente, se ignoran.	Jaguar +colombia
AND o &	Busca páginas web que contienen todos los términos o frases.	Jaguar AND colmillo
NOT o -	Excluye las páginas web que contienen un término o frase.	Jaguar -auto
OR o |	Busca páginas web que contienen alguno de los términos o frases.	Tortuga or morrocoy
contains:	Mantiene los resultados en los sitios que tienen links a los tipos de archivos especificados	Para buscar sitios web que contengan links a archivos Windows Media Audio (.wma) music contains:wma.
ext:	Búsqueda de archivos por extensión.	Busqueda de archivos de word ext:docx.
filetype:	Busqueda solo de archivos de determinado tipo	Busqueda de archivos pdf filetype:pdf.
inbody:	Webpages que contienen el término de búsqueda en el contenido de la pagina	inbody:Tortuga
loc: o location	Retorna páginas ubicadas en la localización especifica (país)	Busqueda de páginas ubicadas en estados unidos loc:US Para una lista de los códigos de países utilizado por Bin visite Country, region, and language codes.

Realización de búsquedas por entidades

Saber utilizar Google realmente nos ayuda a profundizar en cómo obtener la información. Pero nos es necesario saber sobre qué se puede buscar información, es decir, sobre las entidades de búsqueda. Los datos sobre los que se puede buscar información de forma más eficaz son:

- Nombres y apellidos.
- Apodos o nicknames.
- Correos electrónicos.
- Teléfonos.
- Dominios web.
- Localizaciones.
- Empresas.

Cada una de estas entidades puede someterse a búsquedas en Google y, optimizando con los comandos anteriores, pueden arrojar resultados de interés. Ahora bien, a efectos de abordar estas búsquedas de forma integral, debemos de saber que cada entidad tiene páginas web o bases de datos específicas que facilitan información sobre ellas. A efectos de este manual, se efectuarán recomendaciones específicas sobre algunas:

1 Bing Images es una buena opción para búsqueda de imágenes, pero no para imágenes invertidas.

Recopilatorios generales de herramientas web.

Se recomienda el uso de los portales https://osintframework.com/ y https://intelx.io/. Ambos portales cuentan con multitud de herramientas para abordar los diferentes tipos de entidades de búsqueda. No obstante, se debe de tener en cuenta que algunas de las herramientas que suministran, en el momento del uso, puede haberse quedado obsoleta o haber directamente desaparecido.

Nombres y apellidos.

Como opción gratuita para la obtención de información en base a nombres y apellidos, se recomienda el uso de la web https://webmii.com. Como opción de pago, https://pipl.com sigue siendo una de las bases de datos más potentes en este sentido.

Correos electrónicos.

Se recomienda el uso de las plataformas https://leakedsource.ru/ y https://haveibeenpwned.com/. Ambas plataformas, permiten realizar búsquedas de correos electrónicos y, en caso de ser positivas, nos informarán de si dichas cuentas de correo electrónico han sido detectadas como vinculadas a algún servicio web o red social (en base a que hayan aparecido en listados de datos filtrados tales correos electrónicos. Estas filtraciones tienen su origen en la gran mayoría de los casos en ataques informáticos). En ocasiones, estas informaciones pueden llevarnos a encontrar una contraseña vinculada a esa cuenta de correo, la cual puede ser la actual o no. Sobra decir que **JAMÁS** se debe utilizar esa información para intentar acceder a la cuenta de correo o al servicio web vinculado **sin autorización judicial.**

Dominios web.

Para obtener información de dominios web existen innumerables páginas web, destacando por su uso who.is y https://whois.domaintools.com/. Esta última, cuenta con opciones de pago bastante útiles de cara a obtener información sobre el histórico de una página web. En https://www.riskiq.com/ también se encuentra bajo pago una excelente base de datos sobre registros web.

Empresas.

Como opción gratuita y de alcance global, se recomienda el uso de https://Opencorporates.com. Esta web permite obtener información de empresas de cualquier lugar del mundo en base a la información pública de los diferentes registros mercantiles a nivel mundial. Como opción de pago, la más conocida y utilizada probablemente sea la de https://www.dnb.com/.

Con esto, se concluirían las búsquedas en lo que se refiere a mecanización de texto en buscadores para la obtención de resultados. Pero todavía queda un aspecto totalmente diferente por cubrir: las búsquedas no en función de texto, sino de imágenes.

Búsquedas por imágenes

La realización de búsquedas en base a imágenes es siempre una práctica que se suele dejar de lado en favor de la más clásica búsqueda de términos. Sin embargo, la realización de este tipo de búsquedas ofrece varios resultados de extremo interés para la investigación.

Uno de los casos más típicos de delito medioambiental a través de Internet es la venta de especies protegidas, amenazadas o invasoras a través de portales web de compraventa. Dichos anuncios deben de contar con imágenes de la mercancía ofertada, para atraer la atención de potenciales compradores. Sin embargo, es bastante posible encontrarse anuncios que o bien no son ofertas reales, sino potenciales estafas, o bien utilizan imágenes de otros anuncios para no exponer información propia. Una de las mejores maneras de saber de antemano si nos encontramos ante uno de estos supuestos, es usar la búsqueda por imágenes. Si la imagen del anuncio objetivo aparece en muchos sitios web de distinto origen, podemos pensar que nos encontramos ante una estafa o ante el uso de elementos engañosos.

Conociendo entonces la utilidad de este tipo de búsquedas, queda resolver como se llevan a cabo. Hay muchos motores de búsqueda por imágenes, pero desde este manual se van a recomendar tres:

Google[1] : para acceder a la búsqueda por imágenes de Google, debemos acceder a la URL https://www.google.es/imghp. Nos encontraremos con la siguiente imagen:

Ilustración 19. Captura de pantalla de https://www.google.es/imghp

1 Bing Images es una buena opción para búsqueda de imágenes, pero no para imágenes invertidas.

Como vemos, en la barra de búsqueda aparece el icono de una cámara fotográfica. Si pulsamos en dicho icono, Google nos permitirá o bien realizar búsquedas pegando la URL de la imagen, o bien subir una imagen de nuestro equipo. Si subimos la imagen de un ordenador portátil, por ejemplo, Google nos devuelve los siguientes resultados.

Ilustración 20. Resultado de búsqueda por imágenes en Google.

Aquí se observa otra de las utilidades de la búsqueda por imágenes. Lo que para nosotros era simplemente un ordenador portátil, Google lo identifica con marca y modelo, además de identificar numerosas páginas web en las que dicho artículo concreto está a la venta. Es decir, la búsqueda nos puede ayudar a identificar extremos que nos pasan por alto.

Yandex: el buscador ruso cuenta con una búsqueda por imágenes. Funciona de forma muy similar a Google, permitiéndonos 3 métodos para realizar la búsqueda. Podemos subir la imagen, pegar la URL o pegar una imagen que tengamos en el portapapeles. Podemos acceder a este buscador desde la URL https://yandex.com/images/.

TinEye: uno de los buscadores dedicados exclusivamente a imágenes más antiguos y, por tanto, con mayor experiencia en el desarrollo de su algoritmo de detección. Nos permite realizar las mismas operaciones que Yandex para realizar la búsqueda. TinEye es accesible desde la URL https://tineye.com/.

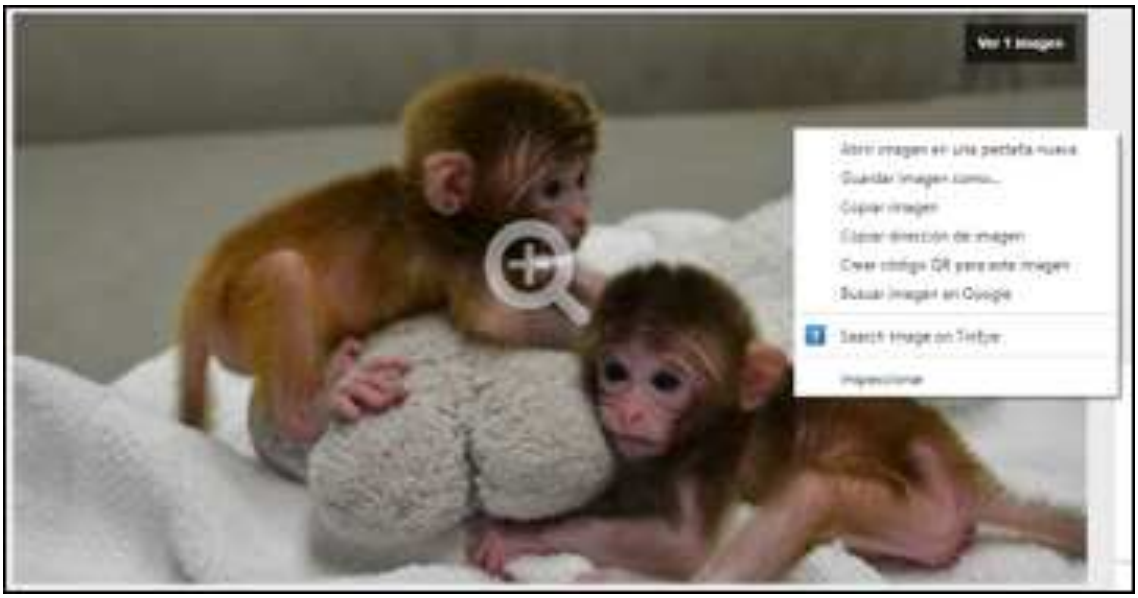
Una de sus características más relevantes es la existencia de una extensión de este buscador para Google Chrome. De esta forma, si usamos este navegador y queremos hacer una búsqueda de forma rápida, basta con instalar la extensión. Una vez instalada, basta con hacer clic derecho en la imagen, y nos aparecerá una opción que dice "Search image on TinEye". Pulsando, se ejecutará directamente la búsqueda de la imagen. Veamos un ejemplo.

Encontramos un anuncio de venta de monos en la URL https://www.casinuevo.com/mascotas/monos-titi-macho-y-hembra-acoruna-21071113145819447. El anuncio tiene la siguiente apariencia (Ilustración 21).

Si hemos instalado la extensión de TinEye para Google Chrome, disponible en la URL https://tineye.com/extensions, y hacemos clic derecho en la imagen, nos saldrá la siguiente opción (Ilustración 22).

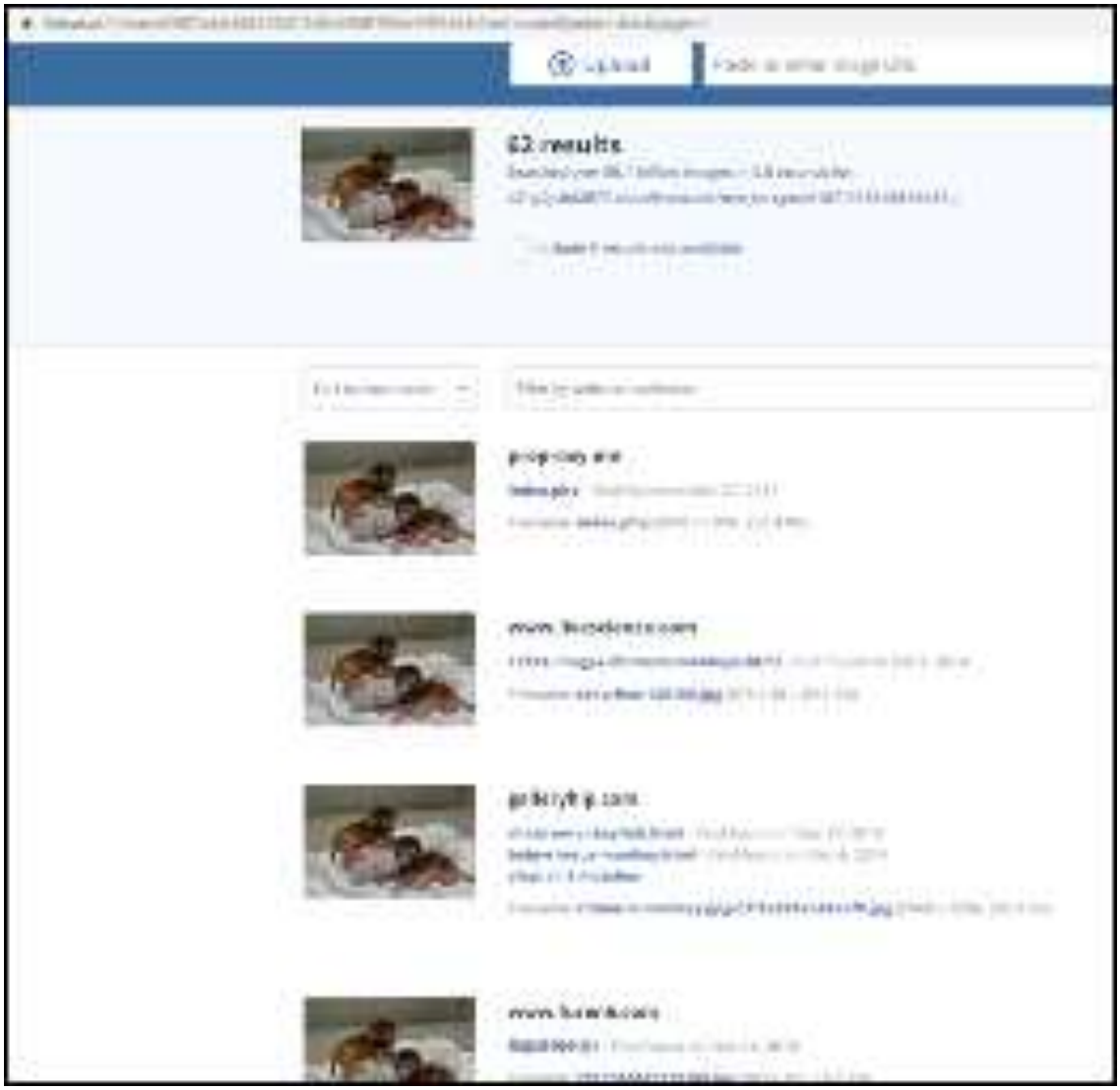
Ilustración 21. Captura de anuncio ubicado en https://www.casinuevo.com/mascotas/monos-titi-macho-y-hembra-acoruna-21071113145819447

Ilustración 22. Desplegable en Google Chrome con la extensión de TinEye.



Si pulsamos en la opción de TinEye, nos lleva a los siguientes resultados:

Ilustración 23. Resultados de la búsqueda con TinEye.



Como vemos, esta imagen no es única, sino que identificamos al menos 62 sitios web más en los que aparece esta imagen. Esto, como mínimo, nos hace saber que la imagen subida en el anuncio no es genuina y, por tanto, nos podemos encontrar ante una estafa, o ante un usuario que ha tomado medidas para no subir imágenes reales (porque puede ser que tema que se investiguen las mismas).

REDES SOCIALES

A continuación, hablaremos un poco de las diferentes redes sociales sobre las que es importante saber cómo obtener información, cómo contactar oficialmente con estas plataformas en un procedimiento judicial, y qué detalles específicos de interés tiene cada una de ellas. Dada la enorme cantidad de redes sociales existentes, nos centraremos en las tres más utilizadas en la actualidad: Facebook, Instagram y Twitter.

Las ecuaciones de búsqueda pueden ser utilizadas plataformas de motores de búsqueda, y/o en redes sociales como Facebook, Twitter e Instagram o sus equivalentes. Tener en cuenta que primer esfuerzo no solo proporcionará información sobre el comercio de las especies priorizadas de fauna silvestre, sino que también evaluará la eficacia relativa de las combinaciones de búsqueda de términos / plataforma, que se utilizará refinando búsquedas.

Según el último estudio de WCS (2021) los países andino-amazónicos evaluados, las redes sociales como Facebook e Instagram, seguidas de portales en línea de anuncios clasificados como Clasificados.st, Mil Anuncios, son los medios a través de los cuales se realiza el comercio online posiblemente ilegal de forma abierta o relativamente abierta.

Facebook

Desde su nacimiento en el año 2004, Facebook ha tendido a ser una red social de naturaleza familiar, especialmente diseñada para contacto con familiares y amigos. En estos 17 años que lleva de funcionamiento, muchos son los cambios que ha sufrido esta red social, tanto en su uso como en su estructura. Principalmente, estos cambios han tendido siempre hacia una mayor protección de la privacidad del usuario.

El principio fundamental de la privacidad en las redes sociales hoy en día ha sido en gran parte definido por Facebook, y consiste en la reciprocidad. Yo te veo si tú puedes verme a mí. Esto lo desarrollaremos a continuación. En Facebook existen básicamente dos tipos de perfiles: los particulares, de carácter privado, utilizados normalmente para las relaciones entre familiares y amigos. Y los públicos, de carácter profesional normalmente, abiertos a todo el mundo porque buscan la visibilidad en sus comunicaciones.

Con respecto a los perfiles particulares, debemos de tener claro que Facebook facilita casi una total invisibilidad del titular con respecto a extraños. Podemos elegir quien ve las publicaciones, quien puede enviar peticiones de amistad, si somos visibles a través de motores de búsqueda o no, e incluso si seremos visibles en Facebook mediante la búsqueda del correo electrónico o número de teléfono asociados a la cuenta o no. Como vemos, hay una amplia gama de opciones de privacidad.

Pero como primer hecho para tener en cuenta, es importante decir que lo referente a la búsqueda del correo electrónico o número de teléfono asociados a la cuenta es fácil de sortear. Imaginemos que tenemos un objetivo, del que sabemos que su número de teléfono es 111111111 y su correo electrónico es maildefacebook@gmail.com. Es cierto que si esta persona tiene perfil en Facebook y ha configurado su privacidad de forma que extraños no puedan hacer búsquedas en el motor de búsquedas de Facebook de su correo electrónico ni su número de teléfono, no vamos a encontrar nada en estas búsquedas. Pero para saber si ese número de teléfono o correo electrónico están asociados a una cuenta de Facebook, basta con intentar crearnos una cuenta en esta red social utilizando estos datos. Si la plataforma nos lo permitiera, sabríamos que ambos datos no están vinculados a una cuenta de Facebook. Pero si, al contrario, no nos lo permitiera, podemos concluir que dichos elementos sí están vinculados a esta red social. No seremos capaces de visualizar el perfil en primera instancia, pero podremos pedir información a Facebook, y/o podremos realizar gestiones para que dicho perfil nos agregue como amistad si creemos que esto nos puede merecer la pena.

Dicho esto, es importante por supuesto saber cómo se realizan las peticiones de información a Facebook de forma oficial. Para realizar cualquier consulta, debemos de acudir al portal para Fuerzas de Seguridad que tiene Facebook, ubicado en la URL https://www.facebook.com/records/login/. En dicho portal, se nos solicitará la identificación de oficial del caso, qué tipo de delito se está investigando, y se nos permite adjuntar documentación de respaldo a la petición (documentos oficiales policiales, mandamientos judiciales, comisiones rogatorias internacionales…).

Básicamente, hay dos tipos de peticiones que se pueden realizar: Peticiones de preservación de datos y peticiones para la obtención de datos. Las peticiones de preservación de datos tienen por objeto impedir que la información desaparezca. En base a las diferentes leyes de conservación de datos en Internet presentes en cada país, los proveedores de servicios en Internet tienen la obligación de almacenar la información que sirva para la identificación de sus usuarios durante un determinado periodo de tiempo. En España, por ejemplo, la información se almacena durante un año. Todo aquello que tenga antigüedad superior a un año, es susceptible de no poder ser rastreado, puesto que las compañías no tienen obligación de guardar la información sobre sus usuarios en periodos superiores. Si en el transcurso de una investigación en España observáramos, por ejemplo, un anuncio de compraventa de especies protegidas de hace 11 meses en Facebook, nos encontramos en peligro de que dicha información desaparezca. En un mes hasta la caducidad del dato, es posible que no tengamos tiempo suficiente para obtener la autorización judicial necesaria para conseguir dicha información. Pues bien, para eso existen las peticiones de preservación de datos. Enviando a través de esta plataforma un documento oficial policial en el que se informe de sobre qué perfil o página queremos preservar la información, Facebook conservará los datos durante un periodo adicional de 30 días, prorrogables.

En segundo lugar, están las peticiones para la obtención de datos. Como regla general, Facebook facilitará los datos de registro de sus usuarios y las conexiones al perfil o página objetivos (es decir, nos dará correo electrónico, teléfono, nombre y demás datos aportados durante el registro, y las conexiones IP realizadas a esa cuenta con fecha y hora) siempre que se aporte una orden judicial valida en el país desde el que se curse la petición. En caso de necesitar datos que suponen un acceso más intenso a la privacidad del perfil, como pueden ser los mensajes enviados a través de la mensajería de esta red social, Facebook puede requerir una comisión rogatoria internacional a las autoridades de Estados Unidos.

Si se quiere profundizar en el funcionamiento del portal de Facebook, y en qué información posee la red y cómo solicitarla, se recomienda la lectura del siguiente documento, ubicado en la URL https://netzpolitik.org/wp-upload/2016/08/facebook-law-enforcement-portal-inofficial-manual.pdf. Es una guía no oficial elaborada por el detective James Williams de Sacramento, muy completa.

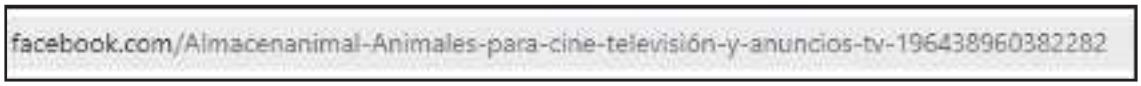
Al e utilizar la guía veremos que, a la hora de identificar perfiles o páginas de Facebook de forma inequívoca, se establecen tres criterios: la cuenta de correo electrónico vinculada (la cual puede que no conozcamos); la URL del perfil; y el USER ID. Este USER ID es una especie de número de identificación único para cada usuario.

Hay varias formas de obtener este número de identificación. Veámoslo con un ejemplo. Imaginemos que estamos investigando la compraventa de animales protegidos a través de Facebook, y que localizamos esta página (Ilustración 24).

Ilustración 24. Captura de pantalla de Almacenanimal en Facebook.

Pues bien, en algunas ocasiones, si observamos la URL, encontraremos este número de usuario al final de esta, como se puede ver a continuación:

Ilustración 25. URL del sitio con el número de usuario (USER ID)



En este caso concreto, el USER ID de esta página es 196438960382282. Sabremos que es correcto si al introducir Facebook.com/196438960382282, nos lleva directamente a la página que estábamos investigando.

Sin embargo, observemos por ejemplo la página del Real Madrid C.F. En este caso, la URL es https://www.facebook.com/RealMadrid. Como vemos, no hay rastro del número de identificación. En estos casos, para conocer el número basta con acceder al código fuente de la página, como aprendimos ya anteriormente, y realizar una búsqueda en el mismo utilizando el parámetro "profile_id". Al hacerlo, nos aparecerá lo siguiente:

Ilustración 26. Código fuente de la página en Facebook del Real Madrid C.F.

Como vemos, ahora sí obtenemos el número de usuario, o USER ID, siendo este 19034719952. De nuevo, podemos comprobarlo introduciendo la URL Facebook.com/19034719952 en nuestro navegador, y esto nos llevará a la página del Real Madrid C.F.

Este número de identificación es muy importante, o solo porque nos permite identificar perfiles de forma inequívoca, y realizar peticiones de información a Facebook de forma oficial;sino también porque este dato es necesario para la realización de búsquedas más complejas.

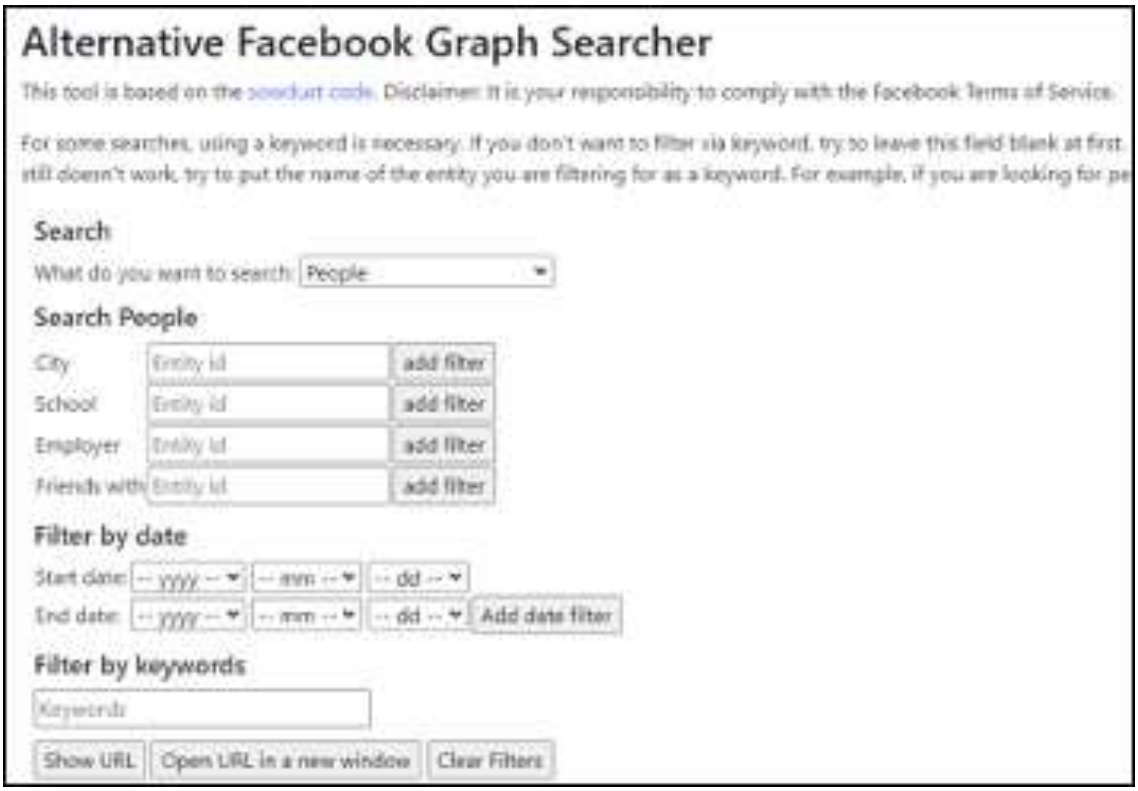
Como hemos dicho al principio, Facebook ha evolucionado mucho en lo que refiere a la privacidad de sus usuarios. Anteriormente, era más sencillo localizar información a través de su motor de búsqueda, pero cada vez e s más complicado. Como herramienta enfocada a la localización de información en Facebook, la más amigable probablemente sea https://intelx.io/tools?tab=facebook. Esta herramienta nos permite hacer búsquedas avanzadas. Las más interesantes son, en primer lugar, aquellas relativas a localizar posts de un usuario determinado en los que se hable de un término concreto. Por ejemplo, queremos saber si un objetivo en una investigación está hablando sobre loros. Pues para ello, usamos el siguiente campo.

Ilustración 27. Búsqueda en Facebook usando Intelx.io

Como vemos, nos pide que introduzcamos el término a buscar, y el usuario, introduciendo el USER ID, motivo por el cual este dato es tan relevante.

Además, la herramienta nos permite buscar personas, posts, eventos, páginas, fotografías y vídeos, pudiendo aplicar filtros que nos permitan acotar resultados. En el caso, por ejemplo, de la búsqueda de personas, podemos filtrar por ciudad, empresa, escuela o universidad, o sus amistades, como se ve a continuación.

Ilustración 28. Búsqueda de personas en Facebook usando intelx.io



Como vemos, siempre es necesaria la introducción del USER ID de aquellos elementos que queramos utilizar como filtro.

Una vez encontrado un perfil que pueda ser de interés para la investigación, debemos de recordar que, salvo que esté abierto a todo el mundo (lo cual es cada vez más extraño), no vamos a poder observar nada, salvo que nos acepte como amistad. Esa aceptación es objeto de un tema muy distinto, como es el uso del agente encubierto. No obstante, si es necesario remarcar una cuestión. Aunque el perfil esté abierto, NUNCA debemos visitarlo con nuestros propios perfiles particulares. Como ya expusimos cuando hablamos de la seguridad propia, visitar el perfil de un sospechoso con nuestro perfil particular puede resultar en que acabemos apareciendo como sugerencia de amistad, extremo de gran peligro que debemos evitar.

Instagram

Creada en 2010, Instagram puso de moda el concepto de red social donde primaba la fotografía. Dada su popularidad, fue adquirida por Facebook. Esto implica que cualquier tipo de petición de información que podamos tener de Instagram, se realiza a través del mismo portal ubicado en la URL https://www.facebook.com/records/login/. Los tipos de peticiones, datos a suministrar, requisitos, entre otros son exactamente los mismos.

Hay que tener en cuenta que realmente Instagram y Facebook difieren solo en lo que proporcionan al usuario, y en el tipo de usuario por tanto que atraen, pero su funcionamiento es muy similar. Por tanto, prácticamente todo lo escrito para Facebook es aplicable a Instagram.

De esta manera, sigue existiendo un USER ID. Para localizarlo, deberemos ir al código fuente del perfil, y realizar una búsqueda utilizando el parámetro “profilepage_”. De esta manera, encontraremos la sucesión numérica que se corresponde con el identificador de usuario. Veamos un ejemplo. Entramos al perfil de Instagram del Real Madrid C.F. Para encontrar su número de identificador, entramos al código fuente, y ejecutamos la búsqueda citada, obteniendo el siguiente resultado.

Ilustración 29. Localización de USER ID en Instagram del Real Madrid C.F.

La secuencia numérica posterior a "profilePage_" es el identificador de Instagram.

En Instagram sí es más habitual encontrar perfiles abiertos al público, puesto que en esta red social el objetivo es dar a conocer actividades diarias o extraordinarias. Como herramientas, para la descarga de perfiles y sus archivos vinculados (fotografías, vídeos, stories…) podemos recomendar Toolzu, accesible desde la URL https://toolzu.com/downloader/instagram/photo/.

Desde esta página web basta con entrar en la pestaña correspondiente, introducir el nombre del usuario del que queramos obtener los archivos, y se procederá a la descarga.

Ilustración 30. Captura de pantalla de Toolzu.com

Por último, son muchas las preguntas respecto a que se puede obtener de las imágenes en Instagram. La respuesta es que de dichas imágenes solo se puede obtener las imágenes como tal. Los metadatos ExifF[1] de las imágenes son borrados al subirse a Instagram para no hacerlos accesibles a cualquier usuario.

Twitter

Creada en 2006, Twitter es una red social muy distinta a Instagram y Facebook. Aunque tiene opciones de configuración de su privacidad muy similares a estas dos, Twitter es la red social del mensaje. El objetivo primero de los usuarios de esta plataforma es lanzar su mensaje, y que este tenga la potencialidad de llegar a cualquier otra persona del mundo que use Twitter. Es un altavoz de indudable potencia. Por tanto, lo normal en esta red social es que los perfiles de los usuarios sean abiertos, y accesibles para cualquiera. Esto

1 Exif: Exchangeable image file format (en español, Formato de archivo de imagen intercambiable. Disponible en: https://es.wikipedia.org/wiki/Exchangeable_image_file_format#Visualizar_Exif

permite estudiar los tweets (los mensajes posteados en esta red social) y el resto de las actividades de los usuarios con mayor facilidad, retrayéndonos periodos de tiempo muy significativos en algunos casos.

Entrando en detalle en el terreno de la privacidad, Twitter permite de nuevo administrar si quieres ser encontrado por aquellas personas que introduzcan tu número de teléfono o tu correo electrónico. Nuevamente, esta medida puede ser evitada o sorteada intentando crear una cuenta con esos datos, para verificar si ya están vinculados o no a una cuenta en esta red social. Por otro lado, Twitter no establece el principio de reciprocidad per se. Existe la opción de proteger la cuenta, de forma que tus tweets solo sean visibles por las personas que te siguen, pero son muy pocos los usuarios que seleccionan esta opción.

En Twitter, no existe un número de usuario como hemos visto en Facebook o Instagram, sino que el parámetro clave para poder realizar seguimiento a un perfil es el nombre de usuario. En esta red social, los nombres de usuario empiezan por el carácter "@", seguido del propio nombre. Ese nombre, por ejemplo @ejemplomanual, es el parámetro clave para la identificación de un usuario en esta red social.

Twitter es la red social que cuenta con mayor número de recursos que pueden apoyar los esfuerzos de búsqueda.

A través de la opción de "búsqueda avanzada" se pueden realizar búsquedas de forma similar a como se realiza en Google o Bing. Para acceder a la búsqueda avanzada, ingrese desde una cuenta de Twitter a twitter.com/search-advanced?lang=es

Para incluir geolocalización en su búsqueda, ingrese en la barra de búsqueda, las palabras clave que desee buscar, más la instrucción geocode:latitude,longitude,radius, por ejemplo, geocode:37.776692537,-122.4167751122,50km

Ilustración 31. Inlcusión de geolacalización en la búsqueda relacionada a Twitter.

Una plataforma interesante de apoyo de búsqueda en Twitter, una vez se ha identificado un usuario específico, es https://followerwonk.com/analyze. Permite analizar por los usuarios que siguen la cuenta y los que siguen la cuenta, esto puede ser útil a la hora de determinar vínculos.

Otra herramienta para perfilar usuarios de Twitter es https://tinfoleak.com/ la cual presenta información de la cuenta como su imagen, las aplicaciones, otras redes sociales vinculadas, etc.

Ilustración 32. Captura de pantalla de https://tinfoleak.com/ para identificar perfiles de Twitter

Ilustración 33. Remisión de la información de la cuenta (@) buscada al correo insertado en la parte inferior.

El reporte es remitido vía correo electrónico a la dirección provista en la parte inferior de la página.

Otra herramienta para análisis iniciales de cuentas de Twitter es SOCIALBEARING.COM. Despliega estadísticas básicas de la cuenta de Twitter

Con respecto a cómo se realizan las peticiones de información de forma oficial a Twitter, nuevamente, hay un portal específico, ubicado en la URL https://legalrequests.twitter.com. La forma de funcionamiento es muy similar a Facebook: se pueden realizar preservaciones de información en caso de que los datos se encuentren próximos a caducar, se facilita la información de registro y conexión con un mandamiento judicial del país correspondiente, y se requieren comisiones rogatorias para acceder al contenido de los mensajes directos entre usuarios y otros datos de mayor intimidad. Se puede encontrar

Ilustración 34. Captura de pantalla de SOCIALBEARING.COM usada para ver estadísticas de las cuentas.

más información a este respecto en la URL https://help.twitter.com/es/rules-and-policies/twitter-law-enforcement-support#20.

Al igual que en Facebook, NUNCA debemos realizar indagaciones en un perfil sospechoso con un perfil particular, para no aparecer como sugerencia de amistad y mantener la seguridad propia.

Finalmente, lo que cambia radicalmente con respecto a Facebook son las herramientas disponibles para obtener información. Hay una enorme cantidad de programas y webs que ofrecen posibilidades de obtención de información en Twitter, de las cuales vamos a destacar tres en concreto: Tinfoleak, Socialbearing y Omnisci.

En primer lugar, la herramienta de extracción de información por excelencia en Twitter es Tinfoleak, la cual tiene dos versiones: una versión a través de servicio web, y otra versión consistente en la ejecución del software Tinfoleak. La versión web es accesible a través de https://tinfoleak.com/, y nos permite obtener información de un usuario. Para ello, debemos introducir el usuario, y un correo electrónico propio. A ese correo electrónico, se nos remitirá un informe completo sobre la actividad del usuario objetivo.

Ilustración 35. Captura de pantalla de tinfoleak.com

Esta versión puede llegar a servir completamente para la investigación de objetivos, aunque limita la información a lo relativo a los 200 últimos tweets. Si queremos más funcionalidad, debemos usar el software de Tinfoleak. Está disponible en la URL https://github.com/vaguileradiaz/tinfoleak, teniendo una versión para Linux y otra versión para Windows. Para usar cualquiera de estas versiones, es necesario que tengamos cuenta de desarrollador en Twitter (el alta como desarrollador en Twitter se realiza a través de la URL https://developer.twitter.com/en). Esto nos permitirá obtener acceso a la API[1] (Interfaz de Programación de Aplicaciones) de Twitter. Con la información que se genera, debemos de configurar los datos de Consumer_key, Consumer_secret, Access_token y Access_token_secret en el archivo tinfoleak.conf. Una vez hecho esto, debemos de instalar Python[2] en nuestro equipo, y ya podremos ejecutar tinfoleak.exe para usar el programa. Al hacerlo, observaremos una pantalla similar a esta.

1 Más información sobre que es una API en https://www.xataka.com/basics/api-que-sirve

2 Python es uno de los lenguajes de programación más utilizados. Tinfoleak se ejecuta en Python, motivo por el que es necesaria su instalación.

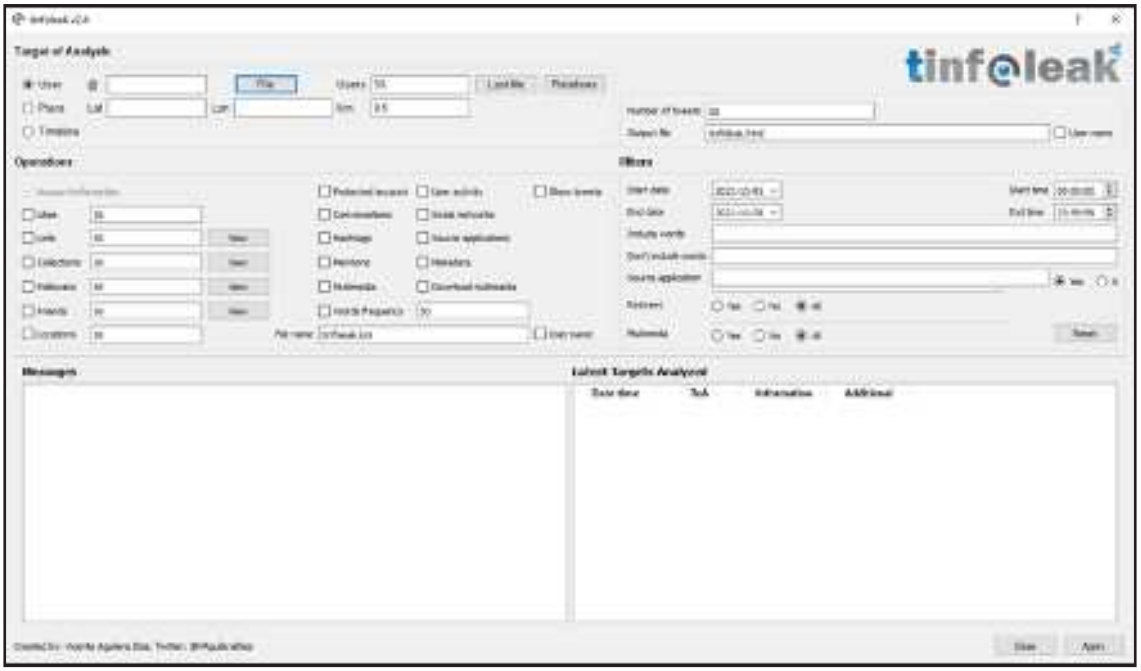
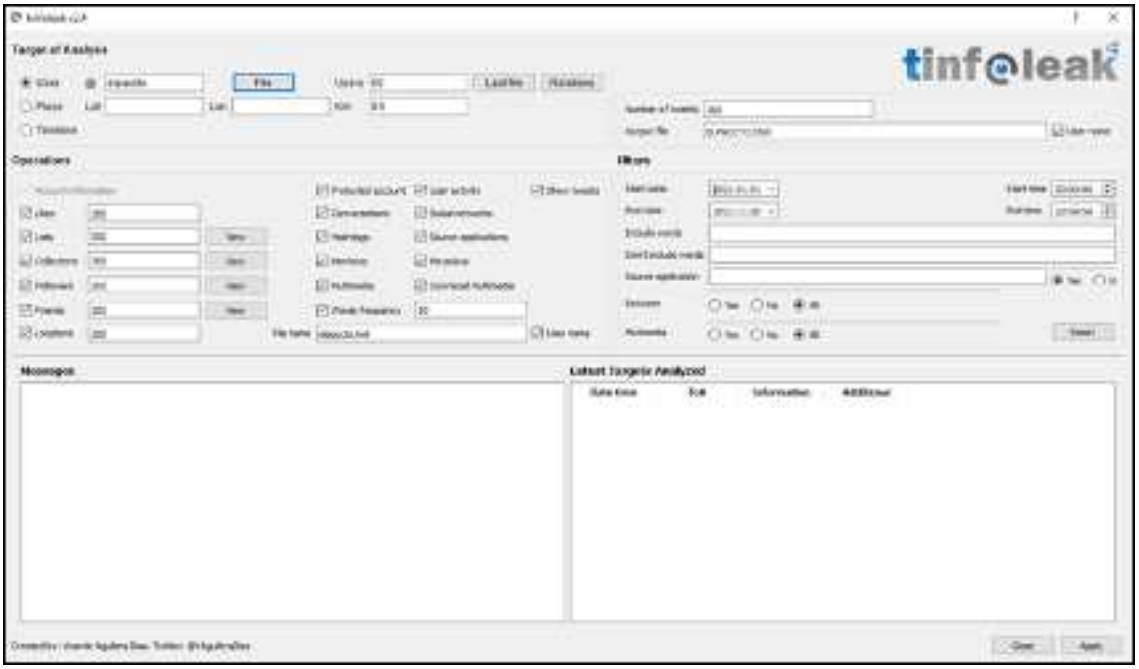


Ilustración 36. Captura de pantalla de la interfaz de Tinfoleak.

El uso del programa no es complicado. En la parte superior izquierda, en el área "Target of Analysis" podemos elegir qué tipo de objetivo tenemos. Podemos estudiar a un usuario, o como novedad con respecto a la aplicación web, podemos estudiar un término o un rango de fechas. A la derecha de esta área, debemos introducir el número de tweets que queremos estudiar sobre el término, rango de fechas o usuario objetivo. Debe de tenerse cuidado con el número de tweets, pues la práctica revela que intentar obtener información de más de 2.000 tweets, resulta en que Twitter bloquea el acceso al interpretar esta consulta como un ataque o conducta sospechosa. Igualmente, aquí podemos elegir el nombre que queremos darle al fichero de informe que se generará. En la parte inferior izquierda, están las opciones adicionales de obtención de información. Como se ve, podemos elegir si queremos obtener información sobre los "Me gusta", listas, seguidores, amigos... Por último, en la parte inferior derecha, podemos aplicar filtros a la búsqueda. Se puede filtrar básicamente por fechas y palabras.

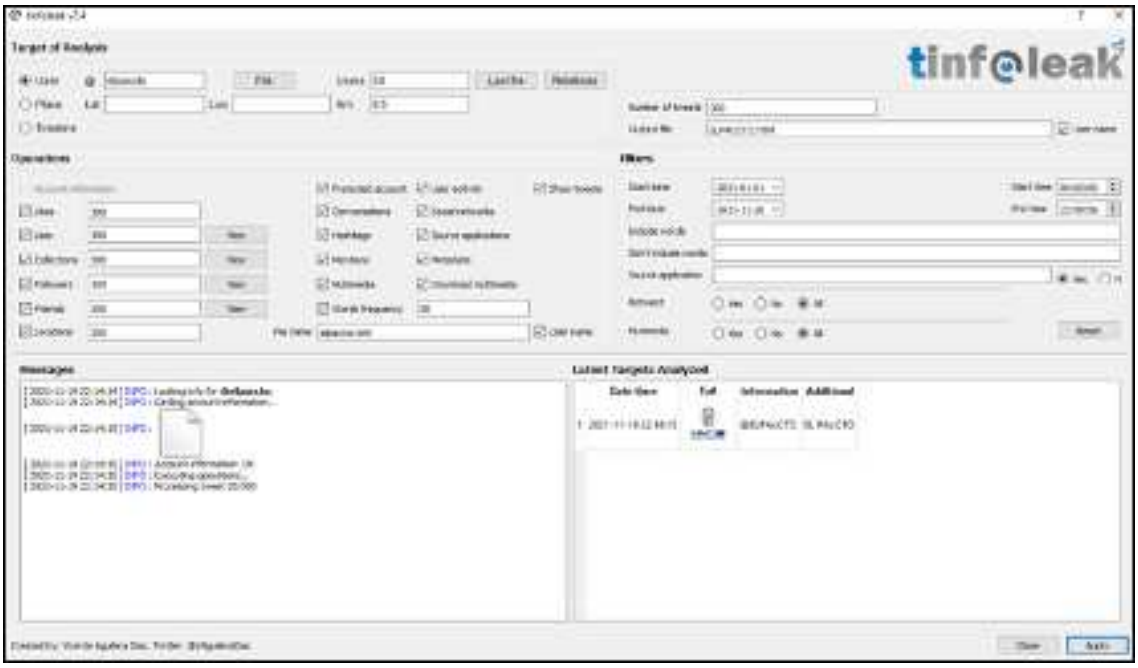
Veamos un ejemplo con la cuenta de El PAcCTO en Twitter. Para ello, introducimos el nombre de usuario, y configuramos la búsqueda para estudiar los últimos 300 tweets, aplicando todas las opciones de obtención de información adicional, y generando un informe llamado ELPACCTO.html. A continuación, se adjunta imagen de cómo se configuraría la herramienta para esta búsqueda.

Ilustración 37. Uso de Tinfoleak para estudiar los últimos 300 tweets de @ELPACCTO en Twitter.



Una vez configurada la herramienta, damos Aplicar o "Apply", y se empieza a ejecutar la búsqueda, la cual puede tardar bastante, dependiendo de la cantidad de información que hayamos requerido. A continuación, se adjunta imagen de la herramienta ejecutando la búsqueda.

Ilustración 38. Ejecución de Tinfoleak



Al finalizar la búsqueda, en la carpeta "Output_reports", encontraremos el informe con el nombre que le hayamos dado. El informe es muy pormenorizado, detallado y probablemente extenso (en función de la cantidad de información que hayamos requerido), pero nos dará un conocimiento profundo del usuario objetivo. La cabecera del informe tiene la siguiente apariencia.

Ilustración 39. Informe generado por Tinfoleak sobre @ELPACCTO.

Es posible que, para algunas personas, el uso o la instalación de Tinfoleak sea problemático. Para solucionar este posible problema, o para tener una interfaz más agradable y amigable, podemos utilizar Socialbearing, accesible desde la URL https://socialbearing.com/. Esta web nos permite búsquedas por términos o usuarios, y nos ofrece los resultados de forma agradable y atractiva. Sigamos con el ejemplo, y ejecutemos una búsqueda de ELPAcCTO. Los resultados que obtenemos son los que se observan en la siguiente imagen.

Ilustración 40. Resultado de búsqueda en Socialbearing sobre @elpaccto.

No solamente aporta estos resultados, sino que más abajo en la página se observa una nube de palabra y hashtags más utilizados, y la captura de los tweets. Estos datos, se pueden exportar inmediatamente a un fichero .csv, que es manejable con Microsoft Excel. Como se ve, es una herramienta similar, no tan exhaustiva, pero si más sencilla de manejar.

Por último, vamos a examinar la herramienta de Omnisci, accesible desde la URL https://www.omnisci.com/demos/tweetmap. Esta herramienta tiene un objetivo más estratégico. Cuando accedemos a la URL, vamos a observar un mapa del mundo y en la parte inferior, una barra que marca un intervalo temporal y diferentes idiomas. A continuación, se adjunta imagen de la página web al acceder.

Ilustración 41. Captura de pantalla de omnisci.com/demos/tweetmap

Podemos seleccionar que rango de tiempo queremos estudiar, y que idiomas queremos observar y, en el buscador superior, podemos realizar filtros por palabras clave. Imaginemos que queremos observar los tweets ocurridos en español, entre el 1 de junio de 2021 y el 1 de julio de 2021 que contengan la palabra "lagarto". Al ejecutar la búsqueda de esta forma, obtenemos los siguientes resultados.

Ilustración 42. Búsqueda en Omnisci de tweets utilizando el término "lagarto" entre el 1 de junio y el 1 de julio de 2021, en español.

Esta búsqueda ha localizado, y geolocalizado, 635 tweets en español usando dicho término. Además, si queremos ver los tweets en concreto de una zona, podemos hacer zoom, y pinchando en sus representaciones, podemos ver el contenido concreto del tweet. Como se ha dicho, esta herramienta es muy útil a nivel estratégico para saber si se está hablando de un tema concreto en una zona determinada.

MARKETPLACES O SITIOS DE COMPRA Y VENTA

A la hora de luchar contra los delitos contra el medio ambiente en Internet, hay que distinguir entre páginas abiertamente delictivas, y páginas legales que contienen contenido delictivo. En el caso de las primeras, suelen ser obvias porque todo lo que en ellas se vende o anuncia tiene prohibida o restringida su venta. Estas páginas son las más interesantes para investigar, pero también es difícil encontrarlas, puesto que conocen de su carácter ilícito y están configuradas para no aparecer en búsquedas en Google u otros motores de búsqueda. Además, a la hora de tratar con estas páginas web hay que considerar siempre que los titulares no solo no van a colaborar, sino que abiertamente van a hacer todo lo posible por dificultar cualquier investigación sobre las mismas.

Por otro lado, tenemos las páginas legales que albergan contenido ilegal. Ejemplo de este tipo de páginas web son las grandes plataformas a nivel mundial de compraventa, como Ebay, Amazon o Alibaba. Estas plataformas no se dedican a actividades ilegales, pero los usuarios postean anuncios de naturaleza ilegal por lo que ofrecen. Es cierto que estas grandes compañías cada vez tienen mejores algoritmos de funcionamiento que hacen que la presencia de anuncios de venta ilícitos sean cada vez menores, no obstante todavía es relativamente sencillo encontrar objetos prohibidos a la venta en estas webs. Estas grandes plataformas de compraventa en Internet son un buen punto de partida para aquellas personas que estén empezando a investigar delitos contra el medio ambiente en Internet, puesto que estas compañías guardan registros de toda la actividad y colaboran con las fuerzas de seguridad. Veamos algunas particularidades de cada una de ellas.

En el estudio realizado por WCS (2021) para los países andinos - amazónicos, se encontranron resultados productivos en diferentes sitios de anuncios clasificados que incluyen los marketplaces como: Clasificados.st, MilAnuncios, Posot.class, SitioAnuncios, Evisos, OLX, Mercado Libre y otros, por lo que es importante considerar diversas plataformas de “compra y venta” de uso frecuente en los países donde se desarrollen las búsquedas.

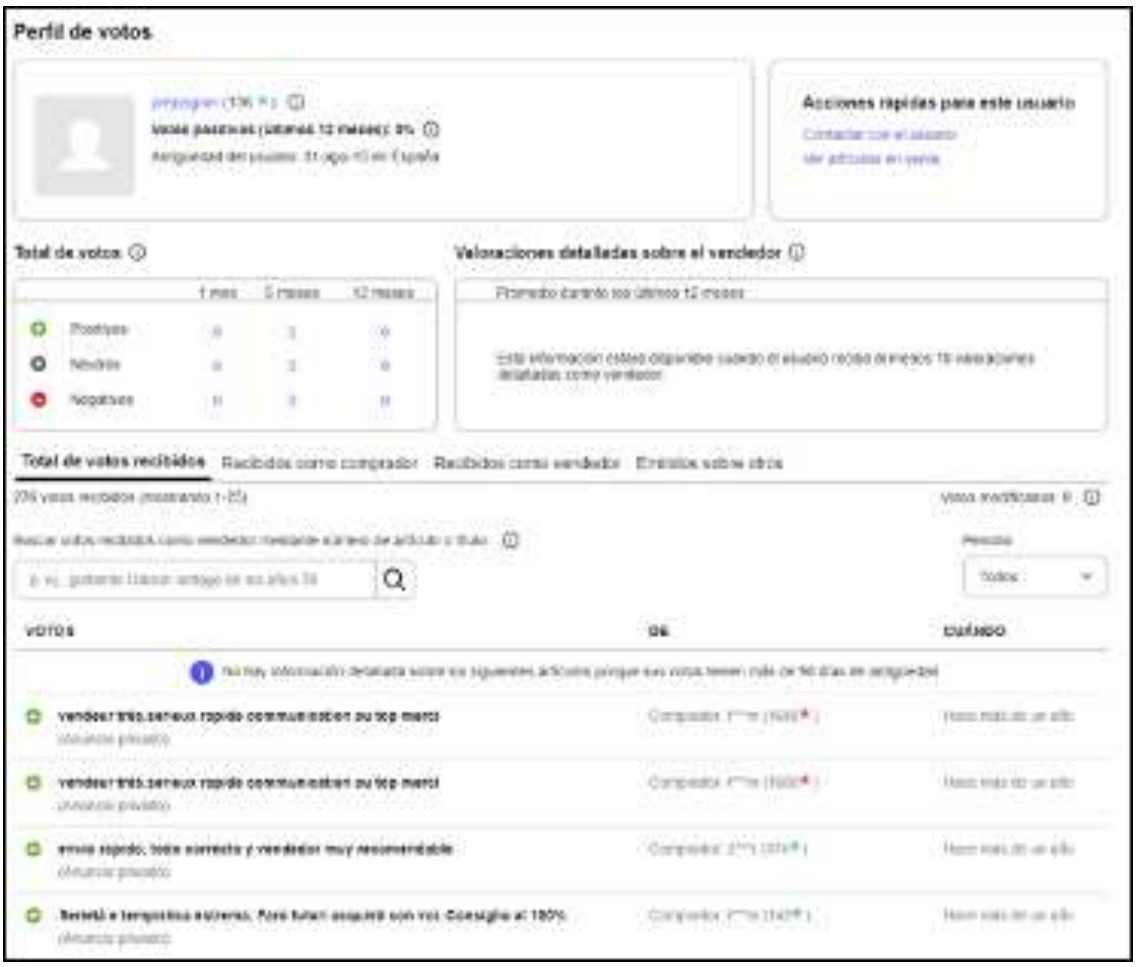
Ebay

Ebay (ebay.com) es una plataforma de compraventa basada en la subasta. Es de las más antiguas que existen. En primer lugar, para obtener información de Ebay deben de hacerse las peticiones a través del portal para fuerzas de seguridad, el cual requiere un registro previo, y que está accesible desde la URL https://le.corp.ebay.com/LEPortal_CommunitiesLogin?country=es_ES.

En segundo lugar, es importante saber que se puede obtener información sobre los vendedores. Los vendedores en Ebay reciben votos en función de la satisfacción o no de los compradores. Pulsando en un vendedor, y examinando los votos, podemos saber en qué país está afincado el vendedor, y tener una noción de si lo que vende es auténtico, y hacia qué país o países está realizando sus ventas. Veamos un ejemplo (ilustración 43).

Como ejemplo hemos cogido un usuario, prejosgom, al azar. Podemos ver como se dio de alta en la plataforma en el año 2015, aparece como residente en España, teniendo mayoritariamente votos positivos (por lo que, en principio, lo que vende es lo esperado), y reseñas en español, francés e italiano, por tanto, vinculación con estos países y/o con individuos que hablan estos idiomas.

Ilustración 43. Perfil de votos en Ebay del usuario prejosgom



Amazon

El gigante de la compraventa a nivel mundial.. Debe de decirse que es difícil encontrar especies animales protegidas a la venta en Amazon, aunque sí es más sencillo encontrar especies vegetales, más desconocidas para el público en general. Las peticiones a Amazon de información oficial deben de realizarse a través de su portal para fuerzas y cuerpos de seguridad, ubicado en https://ler.amazon.com/us, y que requiere de registro previo.

Por otro lado, nuevamente, es posible obtener información sobre el vendedor. Imaginemos que el siguiente anuncio, fuera sobre una pieza de marfil ilegal.

Ilustración 44. Anuncio de venta de pieza de marfil (imitación) en Amazon

A la derecha, debajo de la fecha prevista de entrega, aparece un enlace titulado "Ver detalles". Si pulsamos en este, nos lleva a la siguiente información (ilustración 45).

Esta información nos permite conocer la valoración global del vendedor, y datos para intentar ubicar el país del que procede y realizar gestiones a partir de ellos.

Ilustración 45. Datos del vendedor del anuncio anterior.

Alibaba

El gigante chino de la compraventa constituye la excepción a todo lo anterior. Aunque su presencia y uso a nivel global cada vez es mayor, su nivel de colaboración es bajo. Cualquier petición de información que se les quiera realizar debe de ser a través de comisiones rogatorias de investigación, y dado que es una empresa china, sometida a las leyes y procedimientos de dicho país, es difícil que dicha comisión se ejecute. No obstante, tienen un formulario para la petición de datos con carácter de urgencia (https://docs.alibabagroup.com/assets2/pdf/Emergency_Law_Enforcement_User_Information_Disclosure_Request_Form.pdf), el cual debe de ser remitido por correo electrónico a la dirección enforcementenquiry@alibaba-inc.com.

ASEGURAMIENTO DE LA PRUEBA

Todo lo anterior no vale absolutamente de nada si no somos capaces de recoger todas las evidencias de nuestra navegación y plasmarlas correctamente en un informe destinado a la Fiscalía y a la autoridad judicial.

Cuando no se tiene experiencia en este terreno, es normal entrar en pánico y no saber cómo afrontar este tipo de informes. La forma más sencilla de definir cómo acometerlos es narrando los hechos, con la mayor exactitud posible.

En estos informes se debe de informar sobre nuestra navegación, aportando información sobre extremos tales como:

- Fecha y hora del inicio de nuestro "ciber patrullaje".
- Identificación del agente o de los agentes que realizan la actividad.
- En caso de utilizar software para la obtención de algún tipo de información, exponer su nombre y versión.
- URLs exactas en las que se encuentra contenido sospechoso de ser delictivo.
- Fecha y horas de la visualización de esas URLs (tengamos en cuenta que el contenido en Internet es extremadamente cambiante, y por tanto situarlo temporalmente es muy importante).
- Capturas de pantalla de cualquier tipo de evidencia que queramos plasmar visualmente en el informe. Es recomendable que las capturas de pantalla tengan la máxima resolución posible, y que se observe la URL (para dejar constancia de la ubicación del contenido). Igualmente, debe de informarse de la fecha y hora de obtención de esa captura.
- Debe anexarse al informe una copia de todos los archivos informáticos que hayamos considerado de interés durante el informe. Sobre este extremo hablaremos más en detalle a continuación.

A la hora de redactar nuestro informe, vamos a estar haciendo referencia constantemente a la presencia de páginas web, imágenes o vídeos, principalmente, potencialmente delictivos. Es por eso por lo que a continuación vamos a ver como almacenar esta información de la mejor manera posible.

Adicional a ello, se sugiere considerar completar diversas fichas de datos, por ejemplo:

1. Un archivo Excel individual y que posteriormente será compilada para la revisión y análisis de las diferencias observadas por país/idioma/observador, de ser el caso.
2. Un archivo Excel para el registro de cada búsqueda realizada, debe contener la echa, Código del Observador, Tiempo destinado para la búsqueda, Ecuación de búsqueda, Plataforma, Resultados totales, productivos e improductivos por cada plataforma. Esto es necesario para refinar la metodología (enfatizar/descartar términos, buscadores o plataformas), para informar la eficacia de las ecuaciones de búsquedas y las plataformas web utilizadas.

Almacenamiento de páginas web, imágenes y videos

Imaginemos que nos encontramos ante uno de los casos más habituales como hemos visto: un anuncio de compraventa aparentemente ilícito. Queremos trasladar esta información a nuestro informe. Una de las formas de hacerlo es mediante la realización de una captura de pantalla del anuncio. Para ello, podemos hacer uso de la herramienta "Recortes" integrada en Windows, la cual nos permite seleccionar el área de interés que queramos capturar, o podemos pulsar la tecla Imprimir Pantalla y pegar la captura (y posteriormente recortarla si así quisiéramos). Cualquiera de estas formas es correcta a la hora de llevar a nuestro informe el contenido ilícito visionado.

Sin embargo, las capturas de pantalla pueden ser puestas en tela de juicio dada su fácil manipulación. Por ello, debemos de tender a aportar evidencias más sólidas. En este caso, lo mejor es añadir archivos con mayor integridad, como son los relacionados con el contenido entero o parcial de la propia página web. Para ello disponemos de dos opciones. En

primer lugar, todos los navegadores dan la opción de descargar el archivo .HTML y los asociados de una web. Por poner un ejemplo concreto, Google Chrome permite hacer esto acudiendo a "Opciones" → "Más herramientas" → "Guardar página como...".

De esta forma, aparecerá una ventana para elegir como queremos almacenar la información. Podemos seleccionar la opción de guardar la web en un archivo único tipo .HTML, tal y como se ve en la siguiente imagen.

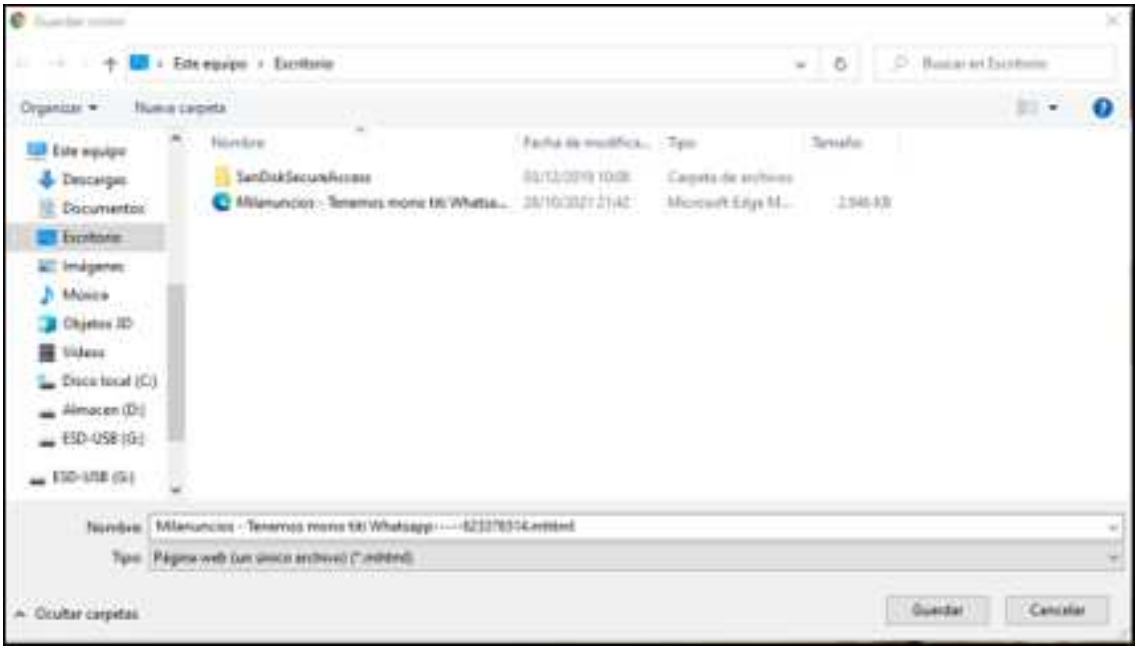
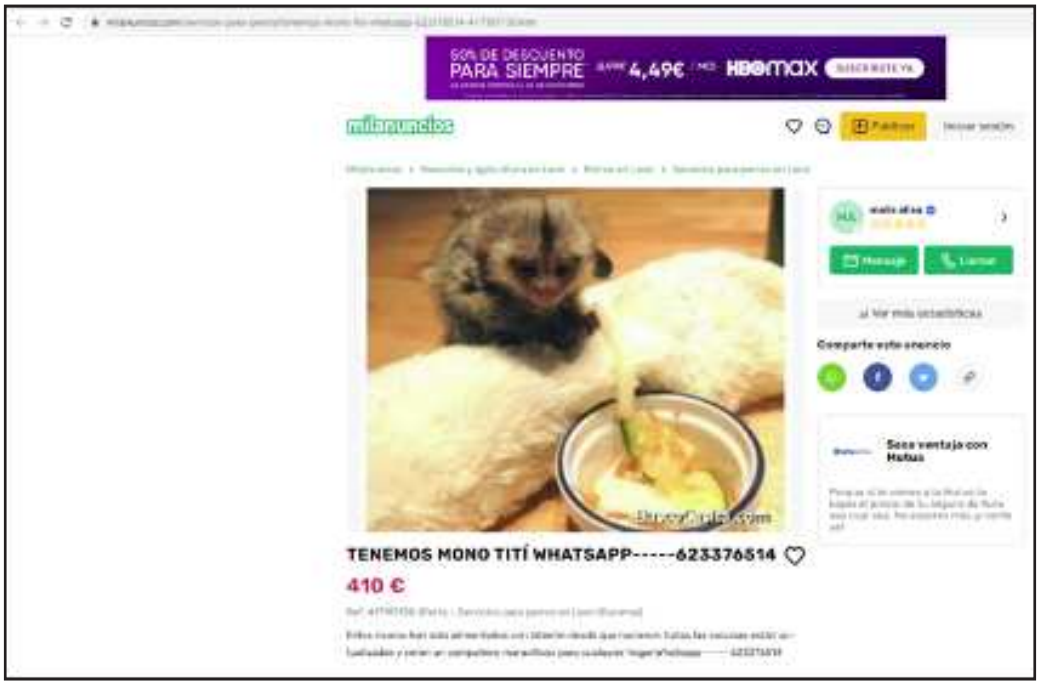


Ilustración 46. Ventana para almacenamiento de web en Google Chrome.

De esta forma, guardamos la evidencia para su visualización posterior de forma casi idéntica a la navegación convencional. Esto podemos comprobarlo con el siguiente ejemplo. En la primera imagen, observamos el anuncio tal y como lo veríamos en Internet. La siguiente imagen, es la visualización del archivo .MHTML descargado. Este hecho se evidencia en la URL presente en las dos imágenes. La primera es un URL de una página web. La segunda, es la ruta de almacenamiento en nuestro equipo del archivo .MHTML.

Ilustración 48. Anuncio visualizado desde el archivo .MHTML asociado.



La segunda opción disponible es usar un software para descargar la página web al completo. Hay muchos programas disponibles para la realización de esta función. Para este caso, vamos a utilizar HTTRACK.

El proceso es muy sencillo. Generamos un proyecto y una ruta para la descarga, introducimos la URL que queramos descargar, y se ejecuta la descarga.

Ilustración 49. Pantalla de inicio de HTTRACK

Ilustración 50. Selección de proyecto y ruta de descarga de HTTRACK

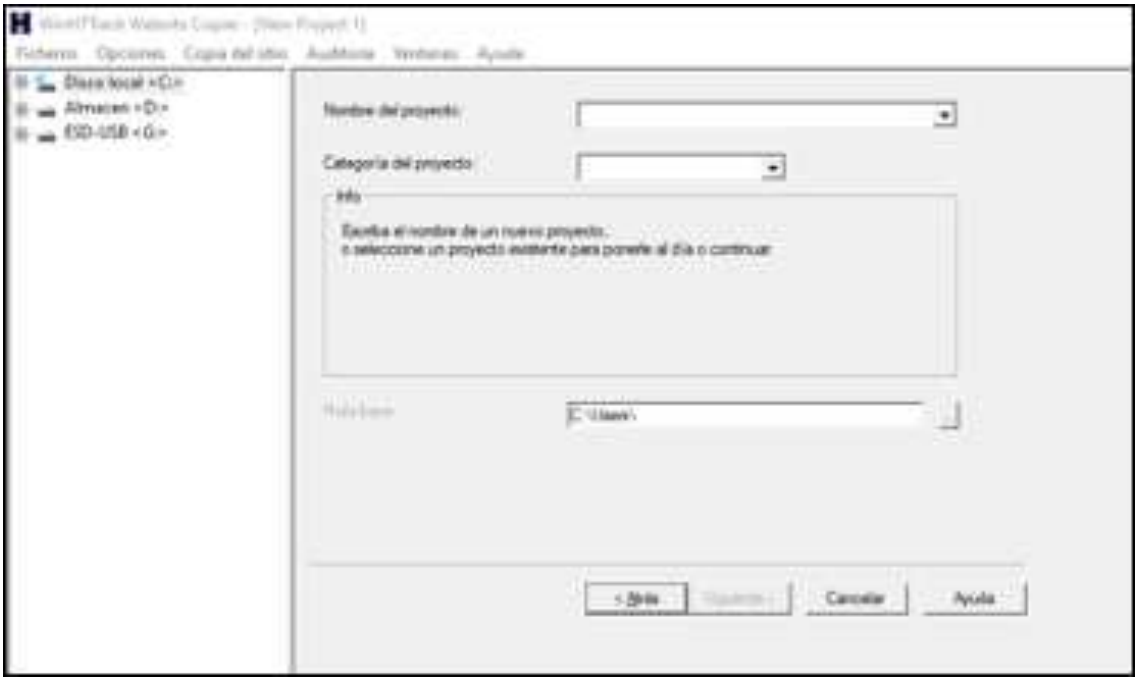


Ilustración 51. Introducción de URL a descargar.

Con estos dos mecanismos logramos almacenar la información de páginas web de una forma más fiable que con simples capturas de pantalla.

Existe un tercer mecanismo de almacenamiento de páginas web. Hasta ahora, tanto las capturas de pantalla como la descarga de los archivos de la web se basan en un almacenamiento local en nuestros equipos de esa información. Pues bien, el tercer mecanismo es mediante un guardado de la página web en la nube. Nuevamente, son múltiples las plataformas que permiten hacer esto, pero por su interés vamos a utilizar específicamente archive.org. Si se acude a la URL https://archive.org/web/, nos encontraremos con lo siguiente:

Ilustración 52. Captura de pantalla de https://archive.org/web/

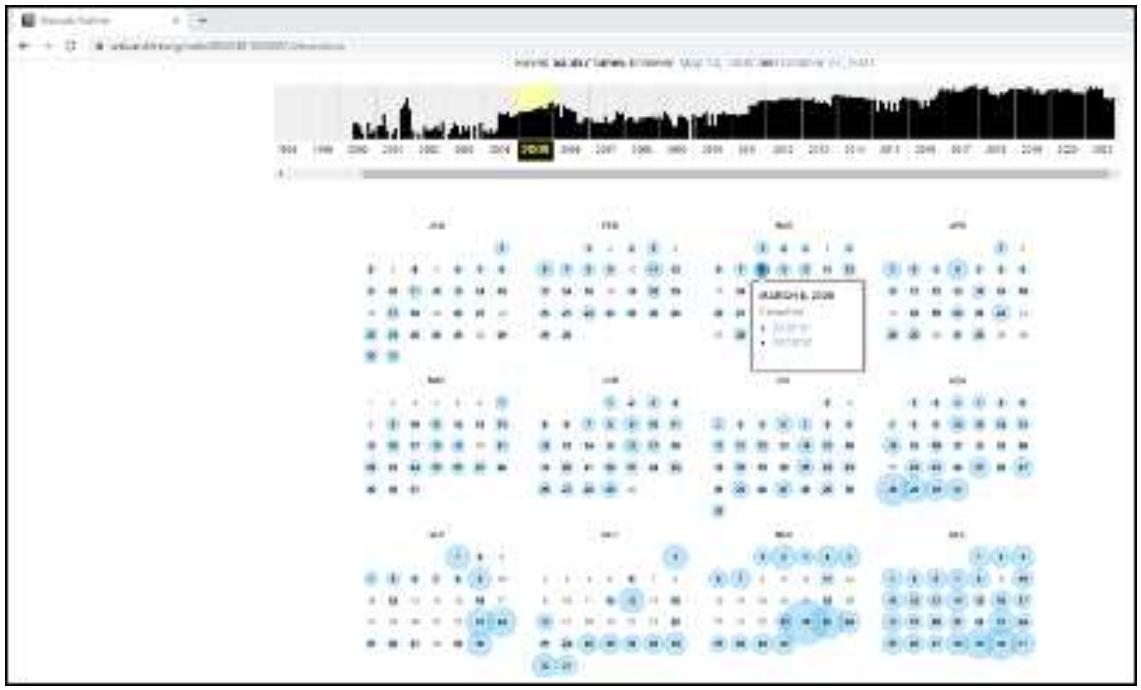
En esta página web tenemos dos opciones muy interesantes. En primer lugar, en la esquina inferior izquierda, aparece la opción "Save Page Now". Si introducimos una URL en dicho apartado, estaremos guardando en archive.org una copia exacta de la web tal y como sea en el momento de realizar el guardado. Si queremos acudir a esa copia, solo debemos buscar la URL que hemos guardado en el buscador presente en la parte superior central de la web.

En segundo lugar, esta página nos permite visualizar como eran las páginas web en el pasado. Archive.org y sus usuarios, realizan copias de las webs en diferentes momentos dependiendo de su interés y tráfico web. Si tenemos suerte, puede que encontremos una copia de una web que sea de interés para la investigación en otro momento temporal, con lo que pueden varias los datos presentes, contenido, etc. Veamos un ejemplo: si queremos conocer cómo era la página web elmundo.es el 9 de mayo del año 2005, acudimos al buscador e introducimos elmundo.es. y aparece lo siguiente:

Ilustración 53. Búsqueda de elmundo.es en archive.org/web

Observamos una línea temporal en la que se muestran los diferentes años en los que hay capturas de elmundo.es. Si acudimos al año 2005, observamos lo siguiente.

Ilustración 54. Copias de elmundo.es del año 2005 en archive.org/web.



Como vemos, de elmundo.es sí que hay copias relativas a el 9 de mayo del año 2005, puesto que esa fecha aparece rodeada con un círculo azul. Si hubiéramos elegido el 5 de mayo de 2005, no habría copia de ese momento específicamente. Cuando pulsamos en el día 9 de mayo, nos aparecen 2 copias de la web en función de la hora. Seleccionamos la segunda de ella, y obtenemos lo siguiente.

Ilustración 55. elmundo.es el 9 de mayo de 2005 en archive.org/web

Esta herramienta es muy útil para buscar información en el pasado de una página web.

Una vez que conocemos las diferentes posibilidades de almacenamiento de la información de una página web, pasaremos a las siguientes evidencias más habituales: imágenes y videos.

En lo que respecta a las imágenes, hay dos formas principales de almacenamiento de estas: realizar una captura de pantalla de la imagen, o descargar la imagen. La imagen, normalmente, la descargaremos utilizando el navegador web, realizando clic derecho sobre ella y pulsando la opción "Guardar imagen como...".

En lo que respecta a otros contenidos, como puedan ser archivos ofimáticos o similares, el procedimiento disponible es básicamente el mismo: o realizamos una captura, o descargamos el archivo pulsando "Guardar archivo como..." tras hacer clic derecho en nuestro navegador.

Este procedimiento, de cara al proceso judicial, cuenta con el problema de que es muy sencillo alterar imágenes. Tan sencillo como abrir cualquier programa de edición de imágenes y realizar los cambios (mejor realizados o peor realizados) que estimemos. Entonces, ¿cómo podemos aportar garantías fuertes sobre que la imagen que aportamos a la causa es la que figura en la web? La respuesta a esta pregunta es la función hash.

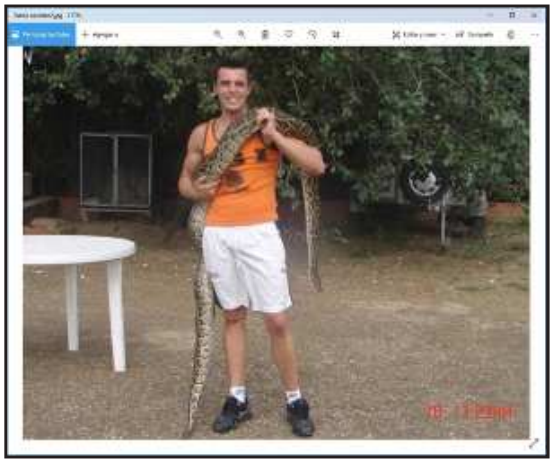
La función Hash

Definir con precisión técnica que es la función hash no es objeto de este manual, aparte de que hay mucha bibliografía sobre su funcionamiento específico disponible en interés. Pero para una primera aproximación, la función hash, como función matemática que es, depende de una variable que le suministremos, que en este caso será un archivo. Para cada archivo, proporciona un valor hash distinto. Y ese hash es único. Con cambiar lo más mínimo el contenido del archivo, cambiaría el valor del hash de una forma impredecible. Es una función no reversible, es decir, teniendo un valor hash no se puede obtener el archivo de procedencia.

Hagamos un ejemplo. Descargo una imagen cualquiera de internet. La imagen se descarga con el nombre "foto2.jpg" y es la siguiente:

Ilustración 56. Imagen "foto2.jpg" descargada de zooexoticoskiko.es

Ilustración 57. "casifoto2.jpg", modificando con un punto negro la mesa blanca.

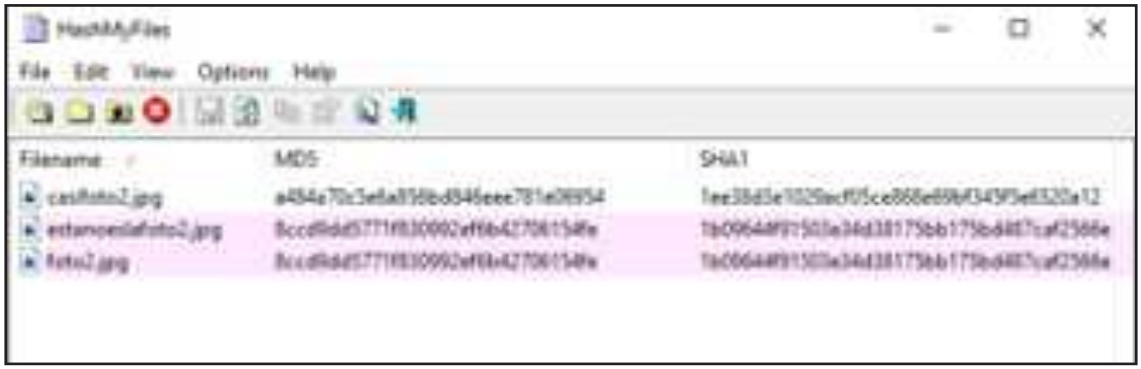


Una vez hecho esto, vamos a ver cómo funciona la función hash. Para ello, hago dos copias de la imagen. A una de ellas, simplemente se le cambia el nombre a "estanoeslafoto2.jpg". A la otra, se la cambia el nombre a "casifoto2.jpg", pero modificamos el contenido de la imagen añadiendo un punto pequeño de color negro a la mesa blanca que se observa en la imagen.

Pues bien, ahora que tenemos las tres imágenes para hacer la prueba, hallemos la función hash de cada una de ellas. Para ello, nos vamos a servir de la herramienta hashmyfiles, disponible en la URL https://www.nirsoft.net/utils/hash_my_files.html de forma gratuita.

Para hallar el hash de las tres imágenes, simplemente ejecutamos la herramienta, pulsamos en la opción "File" y "Add Files". Posteriormente, seleccionamos las tres imágenes. El resultado es el siguiente.

Ilustración 58. Obtención de hash mediante hashmyfiles.



Como vemos, la herramienta marca en color rosa los archivos "estanoeslafoto2.jpg" y "foto2.jpg", porque detecta que tienen el mismo hash, es decir, que son realmente el mismo archivo. Como vemos, cambiar el nombre del archivo no altera el resultado de la función hash. Sin embargo, el hash de "casifoto2.jpg" es totalmente distinto al hash de las otras dos imágenes, a pesar de haber realizado una modificación mínima. Esto prueba que cualquier modificación por pequeña que sea altera el hash de forma impredecible. En la imagen se muestra los dos tipos de hashes más comúnmente utilizados, MD5 y SHA1, pero existen hashes más complejos todavía.

La forma de utilizar la función hash a nuestro favor en las investigaciones es sencilla. Cada vez que descarguemos un archivo y lo incorporemos a la investigación, debemos obtener su hash. Si se cuestiona la integridad de la imagen, las partes y la autoridad judicial siempre podrán acudir a la fuente original, descargar de nuevo el archivo en cuestión, y comprobar que el hash coincide con el archivo aportado a la causa. Con este procedimiento, se aporta una garantía inequívoca a las investigaciones en Internet.

Por último, en lo que refiere a obtención de archivos de Internet, nos quedarían los archivos de video. La forma de proceder con estos archivos para su obtención es, en el fondo, muy similar al resto. En primer lugar, en algunos casos, se pueden realizar una o varias capturas de pantalla para aportar información sobre un vídeo. En segundo lugar, dependiendo de la plataforma donde se encuentre el vídeo, es posible que podamos descargar el archivo a través de nuestro navegador, realizando clic derecho y utilizando la opción "Guardar archivo como". Pero en las grandes plataformas de visionado, como Youtube o Dailymotion, esta opción no está disponible. Existen varios programas para la descarga de archivos de video en este tipo de plataformas, y en este manual vamos a ver el uso de la herramienta JDownloader, disponible en https://jdownloader.org/es/download/index.

Hagamos un ejemplo. Imaginemos que queremos descargar el video de Youtube sobre el tráiler de la película Dune, ubicado en la URL https://www.youtube.com/watch?v=n9xhJrPXop4.

Basta con tener ejecutado el programa Jdownloader y copiar la URL del vídeo en cuestión para que programa lo detecte como un video descargable, y nos aparecerá en la pestaña "Capturador de enlaces", tal y como se observa en la siguiente imagen.

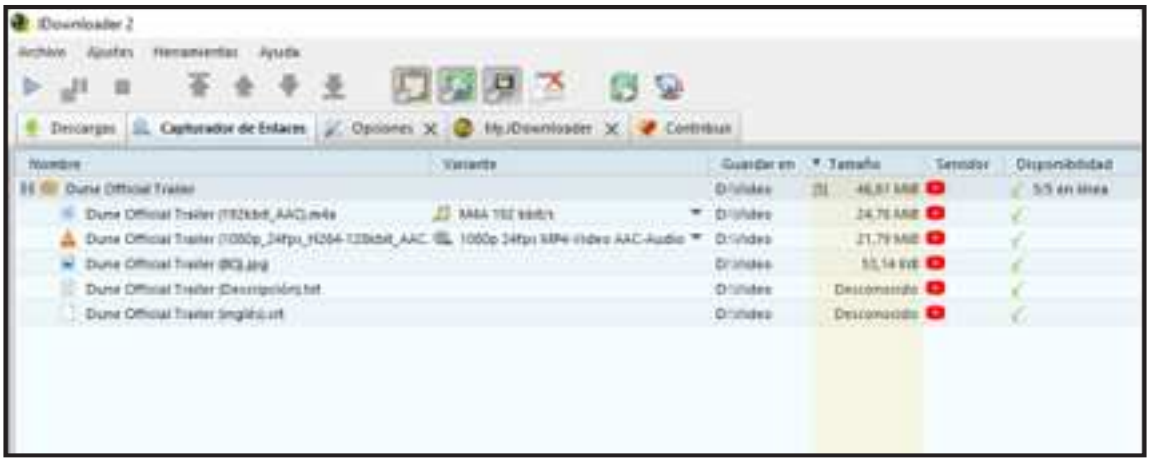


Ilustración 59. Uso de JDownloader para obtener el vídeo en https://www.youtube.com/watch?v=n9xhJrPXop4

Como se observa, la herramienta detecta 5 tipos de archivo: el video como tal, el archivo de audio, la imagen descriptiva del vídeo en Youtube, la descripción del vídeo en Youtube, y el archivo de subtítulos del video. Solo nos quedaría elegir que archivos queremos descargar, pulsando clic derecho y seleccionando "Añadir e iniciar descarga".

Sin embargo, hay portales de streaming que no permiten la descarga del contenido de video que se está produciendo en vivo y en directo. ¿Cómo podemos capturar ese contenido? La solución en este caso es el uso de herramientas de captura de escritorio, es decir, programas que permiten grabar lo que se está visionando en el escritorio como vídeo. Hay numerosas herramientas que permiten hacer esto: Camtasia, Hypercam, entre otras; incluso Windows 10 tiene integrada una función de grabación disponible pulsando la tecla de Windows y G a la vez.

Sobre este tipo de herramientas, hay dos consideraciones básicas que se deben de hacer. En primer lugar, el consumo de almacenamiento que realizan es muy elevado, por lo que debemos tener cuidado con no saturar las unidades de almacenamiento realizando grabaciones largas sin razón.

En segundo lugar, y mucho más importante, no circunscribamos el uso de este tipo de herramientas de grabación al almacenamiento de evidencia de emisión en vídeo en vivo. Es muy recomendable realizar grabaciones de aquellas sesiones de ciber patrullaje que consideremos de interés para la causa. De esta forma, podremos entregar en video a la autoridad judicial todo el proceso, de manera que se verá sin género de duda el contenido ilícito y su procedencia. La forma de realizar estas sesiones de grabación debe de ser muy similar a la de realizar nuestros informes, de forma que se informe de los agentes actuantes, hora de inicio de la actuación, se vayan narrando los hallazgos que se realicen, las URL implicadas, todas las acciones que se realicen con archivos, tales como descarga o similar, y hora de finalización de las actuaciones. Ni que decir tiene que de esta forma también se consigue que procesos técnicos complejos de búsqueda y obtención de evidencias en Internet, sean mucho más fáciles de entender para las autoridades fiscales y judiciales.

Así pues, y como resumen de este capítulo, se puede concluir que conseguiremos una integridad de las evidencias mucho mayor mediante la realización de informes integrales, en los cuales se detalle minuciosamente nuestras acciones en Internet, sin limitarnos a la obtención de capturas de pantalla, sino también aportando los archivos descargados, aportándolos como anexos al informe en un DVD o USB. Todos los archivos descargados deben ir acompañados de su hash, para garantizar la originalidad de estos. Es muy recomendable grabar la actuación con herramientas de captura de escritorio, y facilitar dicha grabación para todavía mayor garantía. Si se cumplen estas recomendaciones, es imposible que nos encontremos con problemas de integridad de nuestras evidencias, salvo que ejecutemos incorrectamente una cadena de custodia.

ANEXO. Documentos de referencia

- WCS 2021. Comercio en línea de fauna silvestre: análisis de plataformas y especies comercializadas en Bolivia, Colombia, Ecuador y Perú. Programa Contra el Tráfico de Vida Silvestre (CTVS) en Andes- Amazonía-Orinoquía (AAO).

EL PAcCTO
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

EL PAcCTO es un programa de cooperación internacional financiado por la Unión Europea que persigue promover la seguridad ciudadana y el Estado de derecho en América Latina a través de una lucha más efectiva contra el crimen transnacional organizado y de una cooperación fortalecida en la materia. Cubre los siguientes países: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Uruguay y Venezuela. Es la primera vez que un programa regional europeo trabaja en toda la cadena penal para fortalecer la cooperación a través de tres componentes (cooperación policial, cooperación entre sistemas de justicia y sistemas penitenciarios) con cinco ejes transversales (cibercrimen, corrupción, derechos humanos, género y lavado de activos).

ALIANZA POR LA FAUNA SILVESTRE Y LOS BOSQUES.

EL PAcCTO
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

Wildlife Conservation Society