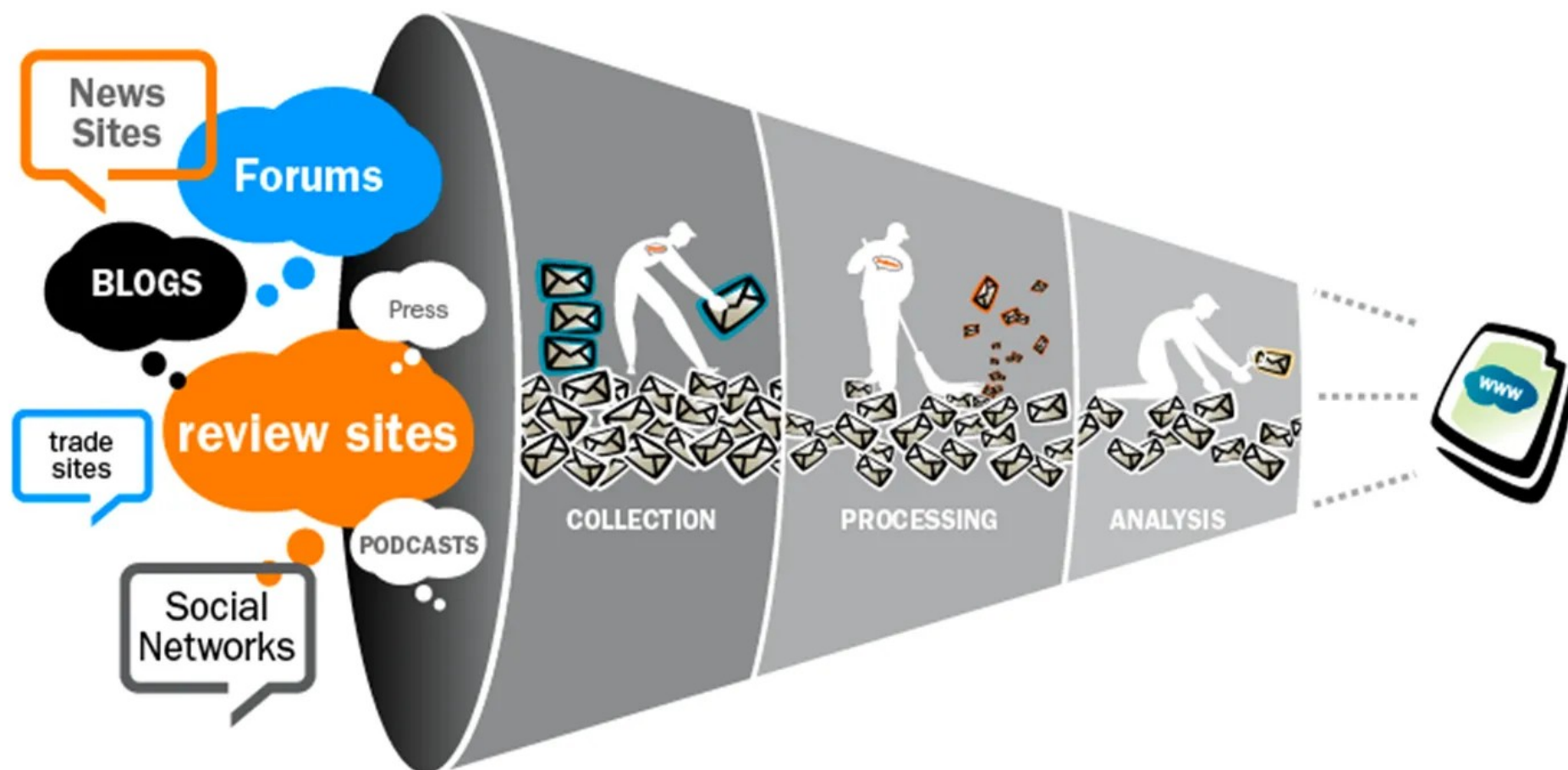


Técnicas y herramientas para OSINT



Contenidos

- 1.Introducción.
- 2.Reconocimiento web.
- 3.Análisis de ficheros.
- 4.Hacking con buscadores.
- 5.Reconocimiento de emails.
- 6.Reconocimiento de dominios e IPs.
- 7.Búsqueda de información en leaks.
- 8.Frameworks para OSINT.
- 9.Otras herramientas para OSINT.

Introducción

- ▶ En la presentación anterior vimos dos tipos de técnicas de recolección de información:
 - **Técnicas pasivas:** no dejan huella.
 - **Técnicas activas:** dejan huella.



Técnicas pasivas
(no interactuamos
directamente con
el objetivo).



Técnicas poco
comprometedoras
(interactuamos
con el objetivo, de
forma parecida a
como lo haría un
usuario normal).



Técnicas muy
comprometedoras
(interactuamos
con el objetivo de
una forma que
delata nuestras
intenciones).

Introducción



GIVE ME SIX HOURS TO CHOP DOWN
A TREE AND **I** WILL SPEND THE FIRST
FOUR SHARPENING THE AXE,

- ABRAHAM LINCOLN

Introducción

- ▶ **Clasificación de técnicas y herramientas:**
 - Reconocimiento web.
 - Análisis de ficheros.
 - Hacking con buscadores.
 - Reconocimiento de emails.
 - Búsqueda de información en leaks.
 - Frameworks para OSINT.

Reconocimiento web

- ▶ Descarga de sitios web.
- ▶ Acceso a versiones anteriores.
- ▶ Testigos online.



Reconocimiento web

- ▶ **Descarga de sitios web.** Obtener una copia local de todos los ficheros del sitio.
 - Subdominios e IPs.
 - Direcciones de correo.
 - Palabras clave.
 - Indicios de configuración del servidor y la aplicación.
 - Limitado al código de cliente.
 - **TIP: los comentarios html pueden contener información relevante.**

Reconocimiento web

► Descarga de sitios web. Herramientas:

- **HTTrack**. Recrea la estructura en modo local y es navegable offline.
- **Cyotek WebCopy**. Semejante al anterior.
- **wget**. No modifica los enlaces, posiblemente la copia más fiel al original.

```
$ wget \  
  --recursive \  
  --no-clobber \  
  --page-requisites \  
  --html-extension \  
  --convert-links \  
  --restrict-file-names=windows \  
  --domains website.org \  
  --no-parent \  
  www.website.org/tutorials/html/
```

<https://www.linuxjournal.com/content/downloading-entire-web-site-wget>

<https://gist.github.com/mikecrittenden/fe02c59fed1aeebd0a9697cf7e9f5c0c>

Reconocimiento web

- ▶ **Acceso a versiones anteriores.** Consultar el estado de una web en una determinada fecha.
 - Revisar información que se ha podido eliminar.
 - La revisión de cambios puede ofrecer indicios de cambios en la configuración del servidor o software.
 - Solo estará disponible la parte visible accesible por el cliente sin autenticación.
 - No es una copia continua, sino discreta, por lo que no es posible revisar todos y cada uno de los cambios.

Reconocimiento web

► Acceso a versiones anteriores. Herramientas:

- [Wayback Machine](#). Servicio de archive.org (desde 1996) que realiza capturas de sitios a lo largo del tiempo de forma automática mediante un crawler.
- [Archive.is](#). Semejante al anterior, pero las capturas se realizan bajo demanda. Es menos probable encontrar capturas de nuestro objetivo.
- **Caché de los buscadores**. A través de los resultados del buscador o en el sitio [cachedview.com](#).

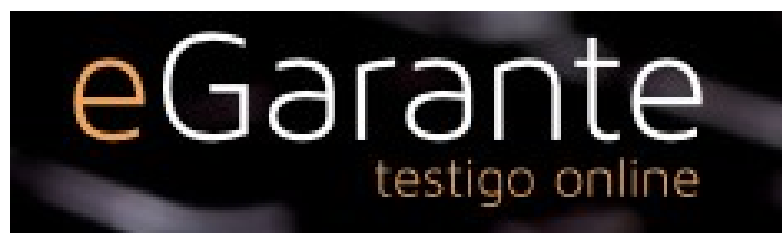


Reconocimiento web

- **Testigos online.** Sirven para certificar el contenido de una web, de modo que si desaparece, sirva como prueba de que ha existido.

Herramientas:

- **eGarante.** Es un servicio online que certifica pruebas de contenido en tres servicios: email, web y entrega de documentos. Dispone de acceso limitado para uso personal y versiones de pago para uso profesional.
- **Save the Proof.** Similar al anterior, incluye la certificación de una sesión de navegación de hasta 15 minutos, certificación de tweets y otras herramientas.



<https://www.osi.es/es/actualidad/blog/2017/03/09/testigos-online-y-obtencion-de-pruebas-te-explicamos-su-utilidad>

Análisis de ficheros

- ▶ Identificación de formatos.
- ▶ Extracción de información textual.
- ▶ Búsqueda de información en ficheros.
- ▶ Análisis de metadatos.



Análisis de ficheros

- ▶ **Identificación de formatos.** En qué formato está almacenado un fichero. Dos enfoques:
 - La **extensión del fichero**. Es fácil de interpretar pero es fácil de modificar por los usuarios. Vía de ataque común (Ej. virus I Love You: "*LOVE-LETTER-FOR-YOU.txt.vbs*").
 - El **número mágico**. Valor único y constante en la cabecera del fichero. Es más difícil de interpretar pero su modificación es más compleja.
 - Se consulta con cualquier editor hexadecimal (*hexdump -C archivo | head*).
 - Comando ***file***.
 - Listado de números mágicos en [Wikipedia](#).

Análisis de ficheros

► Extracción de información textual.

- Para realizar búsquedas de contenido en un conjunto de ficheros grande.
- Si no se encuentra en un formato adecuado, será necesario usar herramientas para pasarla a un formato manejable.
 - <https://cloudconvert.com/>
 - Comando ***pdftotext***.

```
entreunosyceros@18-04:~/Escritorio$ ls
pdf-entrada.pdf
entreunosyceros@18-04:~/Escritorio$ pdftotext -layout pdf-entrada.pdf pdf-salida.txt
entreunosyceros@18-04:~/Escritorio$ ls
pdf-entrada.pdf  pdf-salida.txt
entreunosyceros@18-04:~/Escritorio$
```

<https://ubunlog.com/pdftotext-convierte-pdf-texto/>




Análisis de ficheros

► Extracción de información textual.

- OCR (*Optical Character Recognition*) en imágenes.
 - **Tesseract**. Desarrollado originalmente por HP, es código libre desde 2005. Dispone de **proyectos creados por la comunidad** como entornos gráficos, servicios online y aplicaciones móviles.
 - **EasyOCR**. Librería de python con una comunidad muy activa. Disponible **demo online**.
 - **GOOCR**. Programa con licencia GNU, comenzó su desarrollo en el 2000. Sin actualizaciones desde 2018.

Análisis de ficheros

- **Extracción de información textual.**
 - OCR (*Optical Character Recognition*)

image			
result	<p>'Reduce your risk of coronavirus infection:', 'Clean hands with soap and water', 'or alcohol based hand rub', 'Cover nose and mouth when coughing and', 'sneezing with tissue or flexed elbow', 'Avoid close contact with anyone with', 'cold or flu like symptoms', 'Thoroughly cook meat and eggs', 'No unprotected contact with live wild', 'or farm animals', 'World Health', 'organization'</p>	<p>'เส้นทางลัด', 'เพชรบุรี'</p>	<p>'du 1er', 'Mairie', 'Palais du', 'LOUVRE', 'LES ARTS DÉCORATIFS', 'Musée du LOUVRE', 'Théâtre', 'du PALAIS-ROYAL'</p>

Demostración de funcionamiento de EasyOCR

Análisis de ficheros

► Búsqueda en ficheros:

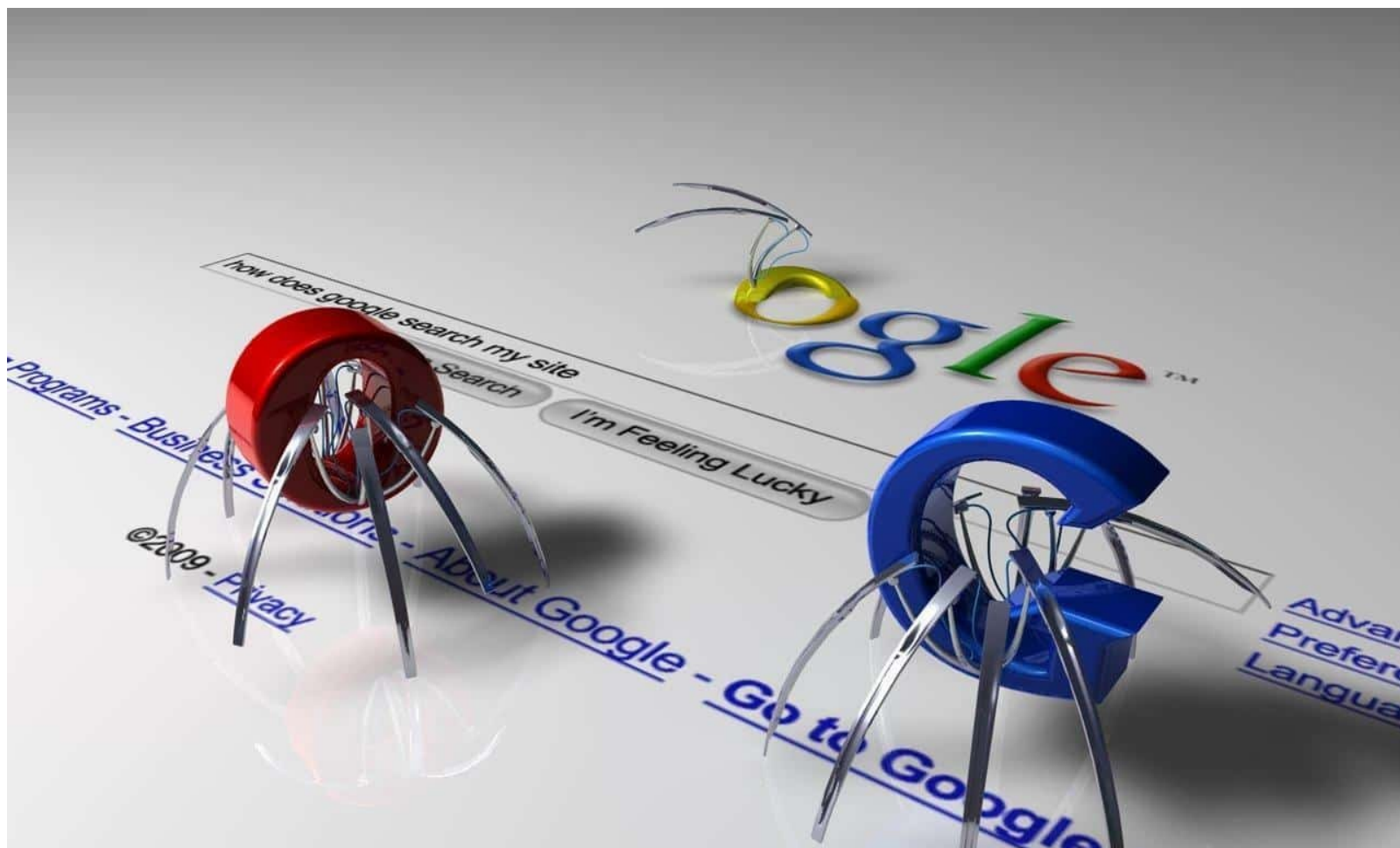
- Herramientas:
 - **grep**. Línea de comandos.
 - DocFetcher.
 - Midnight Commander y similares.
- Expresiones regulares:
 - Ej: Búsqueda de números de DNI en cualquier fichero txt: `grep "[0-9]{7,8}[\-]?[a-zA-Z]" *.txt`
 - Ej: **Búsqueda de vulnerabilidades** en repositorios: [1] [2]
 - GitHub ya incorpora escáner de código para el análisis de vulnerabilidades.
 - Ayuda con expresiones regulares:
 - <https://regexr.com/>
 - <https://regexper.com/>
 - <https://www.regextester.com/index.php>

Análisis de ficheros

- ▶ **Análisis de metadatos.** Pueden contener información relevante para el análisis y procesado. Por ejemplo, coordenadas GPS de una imagen, el software empleado en un fichero *.doc*, etc.
 - **Foca:** Herramienta opensource desarrollada por ElevenPath para el análisis de metadatos de ficheros.
 - **Metagoofil:** permite extraer metadatos de documentos públicos para obtener direcciones de correo del personal de una empresa, software empleado en la creación de documentos, etc.
 - **Exiftool:** herramienta para la consulta y modificación de metadatos.
 - **Script para el análisis de metadatos.** Desarrollado por sweepatic.

<https://medium.com/hacker-toolbelt/osint-metadata-collecting-for-reconnaissance-6b3ff18ddbfe>

Hacking con buscadores



Hacking con buscadores

► Clasificación de buscadores.

- Buscadores generalistas.
- Metabuscadores.
- Búsqueda inversa de imágenes.
- Buscadores en redes anónimas.
- Buscadores en redes sociales.
- Buscadores tecnológicos.

Hacking con buscadores

- ▶ Utilizamos la información pública indexada por los buscadores que está expuesta en los sitios web y otros servidores (*ftp*, etc).
 - La información se recopila por **arañas web** (*crawlers/spiders*) que recorren los sitios de Internet de forma periódica creando el índice del buscador.
 - El fichero **robots.txt** indica al *crawler* qué ficheros y directorios no deben indexarse.
 - ¡Información relevante para el pentest!

<https://www.elladodelmal.com/2011/07/hacking-driven-by-robotstxt.html>

Hacking con buscadores

► Buscadores generalistas: Google.

- https://www.google.com/advanced_search
- https://www.google.com/advanced_image_search
- Operadores útiles:
 - Concordancia exacta: *"el dilema de la ciberseguridad"*
 - Búsqueda con comodines: *"el * de la ciberseguridad"*
 - Operadores lógicos: *"dilema" AND "ciberseguridad"*
 - Restringir los resultados a un dominio: *site:dominio*
 - Buscar en el título: *intitle:"cadena"*
 - Buscar en la URL: *inurl:"cadena"*
 - Buscar en el texto de la web: *intext:"cadena"*
 - Buscar en la versión en caché: *cache:dominio*

Hacking con buscadores

► Buscadores generalistas: Google.

- Más operadores útiles:
 - Obtener información sobre una web: *info:dominio*
 - Páginas que incluyan un enlace: *link:url*
 - Buscar por extensión de archivo: *ext:pdf*
 - Negar un operador: *-ext:pdf*
 - Buscar fuentes parecidas: *related:dominio*

Hacking con buscadores

► Buscadores generalistas: Google.

- **Google Dorks**: determinadas búsquedas dejan al descubierto información relevante. Ejemplos:
 - *inurl:robots.txt intext:"disallow: /wp-admin" site:dominio*
 - *inurl:robots.txt filetype:txt "/INSTALL.mysql.txt"*
 - *filetype:sql password* (contraseñas de bases de datos Sql)
 - *"you have an error in your sql syntax" inurl:/events.php?id=* (búsqueda de errores en bases de datos Sql)
 - *index.of.dcim* (buscaríamos archivos indexados en paginas web de dispositivos de almacenamiento de teléfonos móviles)
- **Google Hacking Database** (GHDB). Recopilación de dorks útiles para pentesting.
 - **Pagodo**. Script para automatizar la búsqueda en GHDB.

Hacking con buscadores

► Otros buscadores generalistas:

- **Bing** <https://www.bing.com/>
 - Buscador de Microsoft, similar a Google.
- **Yahoo!** <https://www.yahoo.com/>
- **DuckDuckGo** <https://duckduckgo.com/>
 - Orientado a la privacidad (no rastrea a los usuarios).
- **Baidu** <https://www.baidu.com/>
 - Buscador chino
- **Yandex** <https://yandex.com/>
 - Buscador ruso.
- **Carrot2** <https://search.carrot2.org>
 - Búsqueda de información clasificada por temas/topics.

Hacking con buscadores

► Pruebas de Concepto y trucos.

- **Truco de la barra:** Se pueden obtener sitios web que se encuentran en puertos poco usuales.
 - Ejemplo. Encontrar sitios web que se encuentran en el puerto 9000: *site:/.es:9000/*.
- Hacer que el navegador indexe **búsquedas que contienen url maliciosas**, por ejemplo *SQL Injection*.
 - Buscadores como arma de destrucción.



Hacking con buscadores

► Fugas de información. Ficheros interesantes

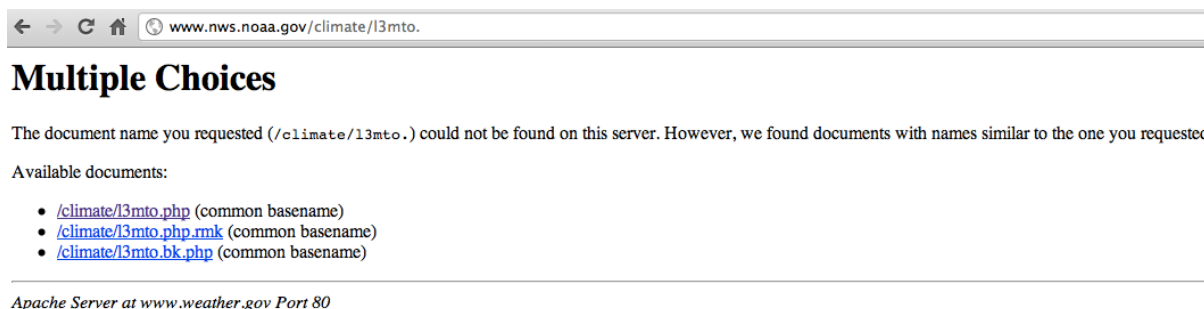
- **Ficheros *.listing***. Son creados por *wget* y contienen un *ls -la* (listado de directorios y archivos) de la carpeta donde se ha realizado el comando. Ofrece nuevas rutas que explorar. (*site:dominio inurl:.listing*)
- **Ficheros *DWSync.XML***. Similar al anterior, creados por *DreamWeaver*.
- **Ficheros *.DS_Store***. Generados por la aplicación *Finder* de Mac OS X.
- **Ficheros *thumbs.db***. Nombres de archivos y miniaturas, asociado a sistemas operativos Windows.
- **Ficheros *desktop.ini***. Archivos de configuración de una carpeta.
- **Archivos de *log***. Por ejemplo, búsqueda de archivos de *log* de servicios importantes (*WS_FTP.log*)
- **Ficheros *.login*, *.bashrc*, *.profile*, *.bash_profile***. Otra lista de ficheros que es posible comprobar si están públicos y pueden ofrecer información del equipo del usuario

<https://www.elladodelmal.com/2013/04/tecnicas-para-descubrir-los-ficheros-de.html>

Hacking con buscadores

► Malas configuraciones.

- **Listado de directorios.** Si el servidor no está bien configurado se puede navegar por el árbol de directorios (*"Index of"*).
- **Mensajes de error.** Los mensajes de error del servidor web (404) pueden ofrecer información de rutas internas.
- **Multiple Choices con Mod_Negotiation.** Este módulo de Apache devuelve un listado de posibles extensiones de archivos que sí existen en el servidor al introducir un fichero erróneo.
- **Directorios de usuarios con Mod_user_dir de Apache.** Se puede usar un diccionario para tratar de averiguar los directorios de tipo */~usuario* existentes.
- **Bug de IIS Short name.** En IIS 6 y 7, este bug permite enumerar los nombres de fichero acortados en Windows.
- **Shared hosting.** Si la web se encuentra en un hosting compartido, una vulnerabilidad en cualquiera de ellas puede comprometer a todas. Con el **operador ip en Bing** se mostrarían todos los sitios web de una determinada IP. También se puede emplear el [servicio Robtex](#) o [IP-Neighbors](#) (Ej: 216.239.38.21).



<https://www.elladodelmal.com/2013/04/tecnicas-para-descubrir-los-ficheros-de.html>

Hacking con buscadores

► Buscadores personalizados:

- Google Programmable Search Engine
 - Google pone a su disposición su motor de búsqueda para que los webmaster puedan configurar un buscador a medida para ser usado por los usuarios.
 - Igualmente se puede emplear para preconfigurar búsquedas usando técnicas de [Google Hacking](#).

Búsqueda Programable [Previsualiza el nuevo panel de control.](#) [Previsualizar](#)

Nuevo motor de búsqueda

Introduce el nombre del sitio y haz clic en Crear para crear un motor de búsqueda para tu sitio. [Más información](#)

► Editar buscador

▼ Ayuda

- Centro de ayuda
- Foro de ayuda
- Blog
- Documentación
- Términos del Servicio
- Visitar el foro de ayuda y hacer una pregunta
- Enviar comentarios

Sitios web en los que buscar

Puedes añadir cualquiera de los elementos siguientes:

Páginas sueltas: [www.example.com/page.html](#)

Todo un sitio: [www.misitio.com/*](#)

Partes de un sitio: [www.example.com/docs/*](#) o [www.example.com/docs/](#)

Todo un dominio: [*.example.com](#)

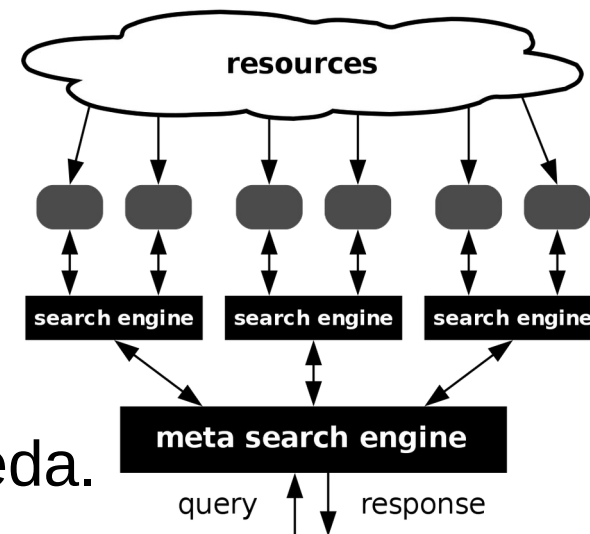
Idioma ⓘ

Nombre del motor de búsqueda

Hacking con buscadores

► Metabuscadores:

- SearX <https://searx.me/>
 - Metabuscador de código abierto.
 - Soporta hasta 70 motores de búsqueda.
 - Orientado a privacidad:
 - No comparte las IP ni el historial de búsquedas de los usuarios.
 - Permite realizar las búsquedas a través de Tor.
 - Puedes compilar e instalar tu propia instancia (mayor privacidad).
 - Alta programabilidad y personalización.
 - Listado de instancias públicas: <https://searx.space/>



Hacking con buscadores

► Metabuscadores:

- IntelligenceX <https://intelx.io/>
 - Metabuscador que emplea darknet, plataformas de archivos, leaks, etc.
 - La búsqueda trabaja con selectores (email, dominios, URLs, IPs, direcciones Bitcoin, IPFS hashes).
 - Dispone de un archivo histórico de datos (similar a Wayback Machine).
 - La versión libre está limitada.

	Public (not logged in)	Free (signed up)	Academia (universities & schools)
Selector Search	10 /day	50 /day	100 /day
Phonebook Lookups	5 /day	10 /day	25 /day
Alerts	×	×	10 included
Download	×	×	✓
Export (CSV, ZIP)	×	×	✓
API	×	Fair-use	Fair-use
Bulk Access	×	×	×
Extra Data Categories	×	×	×
Commercial Use	×	×	×
Data Categories	Public only	Public only	Pastes, Darknet, Whois
Preview Data Categories	Pastes, Darknet, Whois	Pastes, Darknet, Whois	Preview: Private Leaks

Hacking con buscadores

► **Búsqueda inversa de imágenes y vídeo:**

- Localiza los lugares donde aparece esa imagen o vídeo.
- Imágenes:
 - [TinEye](#). Buscador especializado de imágenes.
 - Búsqueda inversa en [Google Images](#).
 - Búsqueda inversa en [Yandex Images](#).
 - Extensiones del navegador ([search by image](#)).
 - [Berify.com](#). Servicio de verificación y robo.
- Vídeo:
 - Búsqueda inversa de vídeos en diferentes plataformas.
 - Guía avanzada de verificación de vídeo.

Hacking con buscadores

► Búsqueda en redes anónimas:

- Indexan contenido de la darkweb.
- Buscadores:
 - [Ahmia](#). Realiza búsquedas en Tor e I2P. Censura el contenido ilegal. Es posible realizar la búsqueda desde Internet.
 - [DarkSearch](#). Accesible desde Internet. Dispone de dorks y API libre.
 - [Dark.Fail](#). Orientado a investigadores, para comprobar la veracidad online de un sitio en Tor.
 - [Torch](#). Funciona sobre Tor y tiene indexadas un millón de páginas. Proporciona algunas opciones de personalización. No censura el contenido.
 - [Otros buscadores](#) que requieren el uso de navegadores específicos: Cancele, NotEvil, Kilos...

Hacking con buscadores

► Búsqueda en redes sociales:

- En la mayoría de los casos será necesario tener una cuenta para acceder a todos los datos.
- Estas búsquedas pueden ser útiles para **identificar relaciones** personales.
 - Aunque no se pueda acceder a los mensajes privados, se puede tratar de **pivotar a otras redes sociales**.
 - Ej. Si un contacto cercano de un usuario no tiene cuenta en una red social, podríamos intentar hacernos pasar por ese usuario en esa cuenta para realizar un ataque de phishing.
 - En LinkedIn los usuarios ponen su currículum completo. Se podría hacer una búsqueda de los empleados de una empresa. Completar los datos y opiniones de esos usuarios en redes sociales (Facebook, Twitter, Instagram...) y elaborar un grafo de relaciones entre esos empleados.

Hacking con buscadores

► Búsqueda en redes sociales:

- Búsqueda avanzada de Twitter . También disponible mediante operadores:
 - Publicaciones de una cuenta: *from:cuenta*
 - Publicaciones dirigidas a una cuenta: *to:cuenta*
 - Publicaciones que mencionan una cuenta: *@cuenta*



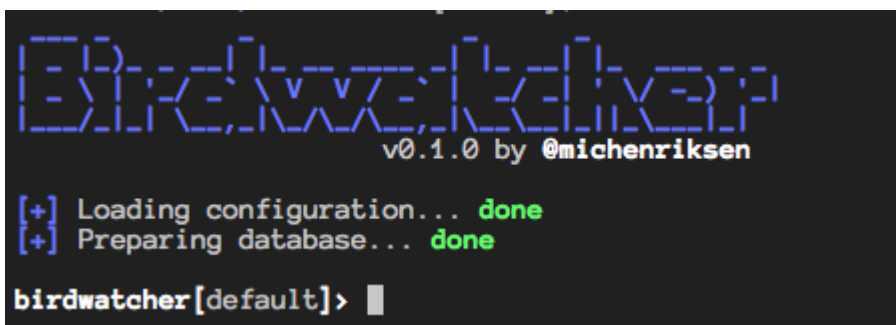
The image shows a screenshot of the 'Búsqueda avanzada' (Advanced Search) interface on Twitter. The interface is in Spanish and includes a 'Buscar' (Search) button in the top right corner. Below the title, there are several search filters:

- Palabras** (Words): A section with four options:
 - Todas estas palabras** (All these words): Example: 'qué pasa' - contains both 'qué' and 'pasa'.
 - Esta frase exacta** (This exact phrase): Example: 'hora feliz' - contains the exact phrase 'hora feliz'.
 - Cualquiera de estas palabras** (Any of these words): Example: 'gatos perros' - contains 'gatos' or 'perros' (or both).
 - Ninguna de estas palabras** (None of these words): Example: 'gatos perros' - does not contain 'gatos' and does not contain 'perros'.
- Estos hashtags** (These hashtags): Example: '#JuevesDeAntaño' - contains the hashtag #JuevesDeAntaño.
- Idioma** (Language): A dropdown menu currently set to 'Cualquier idioma' (Any language).

Hacking con buscadores

► Búsqueda en redes sociales:

- OSINT Frameworks para Twitter.
 - [Birdwatcher](#). Herramienta en línea de comandos desarrollada en Ruby. Es necesario disponer de API Key de desarrollador de Twitter.
 - [Tafferugli](#). Herramienta de análisis en entorno web.
 - [Tinfoleak](#). Desarrollada por Vicente Aguilera (presidente de OWASP Spain). Recientemente, disponible a través de un servicio web.



Hacking con buscadores

► Búsqueda en redes sociales:

- OSINT Frameworks para Twitter.
 - [Twint](#) (*Twitter Intelligence Tool*). Herramienta desarrollada en Python, de código abierto y tiene la ventaja de que no se necesita darse de alta como desarrollador en Twitter, por lo que no se necesita clave de la API.
 - Vídeo: [Automatizando Twint desde cero](#) (Carlos Loureiro)

Hacking con buscadores

► Buscadores tecnológicos:

- No indexan el contenido, sino los servicios conectados a Internet (cabeceras, pantallas de login, etc.).
- Permiten identificar las tecnologías utilizadas (tipo y versión del software).
- Otros metadatos que se pueden obtener: localización geográfica, nombre del host, sistema operativo, etc.
- Buscadores:
 - **Shodan.** <https://www.shodan.io/>
 - **Censys.** <https://censys.io/>
 - **Spyse.** <https://spyse.com>
 - **Zoomeye.** <https://www.zoomeye.org/>. Disponible un API y CLI en Python.

Hacking con buscadores

► Buscadores tecnológicos. Shodan:

- Es un servicio “fremium”:
 - Sin usuario: búsqueda básica.
 - Cuenta gratuita: búsqueda con operadores y uso básico de la API.
 - Distintos niveles de pago: operadores avanzados, límite de búsquedas mayor, monitorización de IPs.

Freelancer \$59/month	Small Business \$299/month	Corporate \$899/month
LOGIN TO SUBSCRIBE	LOGIN TO SUBSCRIBE	LOGIN TO SUBSCRIBE
<ul style="list-style-type: none">✓ Up to 1 million results per month *✓ Scan up to 5,120 IPs per month✓ Network Monitoring for 5,120 IPs	<ul style="list-style-type: none">✓ Up to 20 million results per month *✓ Scan up to 65,536 IPs per month✓ Network Monitoring for 65,536 IPs	<ul style="list-style-type: none">✓ Unlimited results per month *✓ Scan up to 327,680 IPs per month✓ Network Monitoring for 327,680 IPs
<ul style="list-style-type: none">✓ Access to most filters✓ Allows paging through results✓ Basic access to the Streaming API✓ Commercial Use	<ul style="list-style-type: none">✓ Access to most filters✓ Allows paging through results✓ Basic access to the Streaming API✓ Commercial Use	<ul style="list-style-type: none">✓ Access to all filters✓ Allows paging through results✓ Basic access to the Streaming API✓ Commercial Use
<ul style="list-style-type: none">✓ E-Mail support	<ul style="list-style-type: none">✓ E-Mail support✓ Vulnerability search filter	<ul style="list-style-type: none">✓ Premium Support✓ Vulnerability search filter✓ Bulk IP Lookups✓ Tag Search Filter✓ Complementary Membership Upgrades

<https://account.shodan.io/billing>

Hacking con buscadores

► Buscadores tecnológicos. Shodan

- Algunos operadores interesantes:
 - country: ES
 - city: “Granada”
 - hostname: ieszaidinvergeles.org
 - net:217.116.18.19
 - os: windows
 - port:8333
 - port:8333 | port:8332
 - title:”Zaidin Vergeles”
 - html:”comentario en html”
 - vuln:CVE-2014-0160 (disponible en planes de pago avanzados)

<https://github.com/lothos612/shodan>

<https://twitter.com/i/events/924862201667702784?lang=ga>

Hacking con buscadores

► Buscadores tecnológicos. Shodan

The screenshot displays the Shodan search engine interface. At the top, the search bar contains 'city:granada country:es'. Below the search bar, there are navigation tabs: Exploits, Maps, Images, Share Search, Download Results, and Create Report. The main content area is divided into several sections:

- TOTAL RESULTS:** 35,914
- TOP COUNTRIES:** A world map with a red dot indicating the location of Granada, Spain.
- TOP CITIES:** A list of cities with their respective result counts: Granada (35,564), Beas de Granada (264), Alhama de Granada (63), and La Granada (23).
- TOP SERVICES:** A list of services with their respective result counts: HTTP (4,040), DNS (2,584), Modem Web Interface (2,209), HTTPS (1,914), and SSH (1,199).
- TOP ORGANIZATIONS:** A list of organizations with their respective result counts: 24 Shells (7,283), Vodafone Spain (3,933), Telefonica de Espana (3,394), Orange Espana (3,054), and Telmi Telecom S.L. (2,554).
- TOP OPERATING SYSTEMS:** A list of operating systems with their respective result counts: Playstation 4 (97), MikroTik RouterOS 6.45.8 (55), Ubuntu (47), Debian (42), and Raspbian (34).
- TOP PRODUCTS:** A list of products with their respective result counts: 88-82-195-55 (97), 88-82-195-55-jetnet.es (55), and Jetnet Wimax S.A. (47).

On the right side of the interface, there are detailed search results for specific IP addresses:

- 62.151.13.72:** Orange Espana, Added on 2021-02-02 10:18:14 GMT, HTTP/1.1 404 Not Found, Content-Length: 0.
- 195.76.174.123:** Telefonica de Espana, Added on 2021-02-02 10:14:19 GMT, HTTP/1.1 302 Found, Date: Tue, 02 Feb 2021 10:14:18 GMT, Server: Apache/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.2k-fips PHP/7.2.22, X-Powered-By: PHP/7.2.22, Expires: Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform, Pragma: no-cache, Location: https://signon.thomson.com.
- 192.168.1.1:** ServHosting Networks S.L., Added on 2021-02-02 10:14:42 GMT, HTTP/1.0 200 OK, Date: Tue, 20 Jan 1970 20:30:43 GMT, Server: Boa/0.93.15, Connection: close, Content-Type: text/html.
- 88.82.195.55:** Jetnet Wimax S.A., Added on 2021-02-02 10:17:05 GMT, HTTP/1.1 200 OK, Content-Type: text/html, Accept-Ranges: bytes, ETag: "2010596279", Last-Modified: Thu, 03 Aug 2017 03:55:36 GMT.

Hacking con buscadores

► Buscadores tecnológicos. Shodan

- Ejemplo: **Shodan Ship Tracker**. Sistemas vSAT. Muestran en tiempo real el posicionamiento de embarcaciones.



<https://twitter.com/x0rz/status/887240903995400192>

Hacking con buscadores

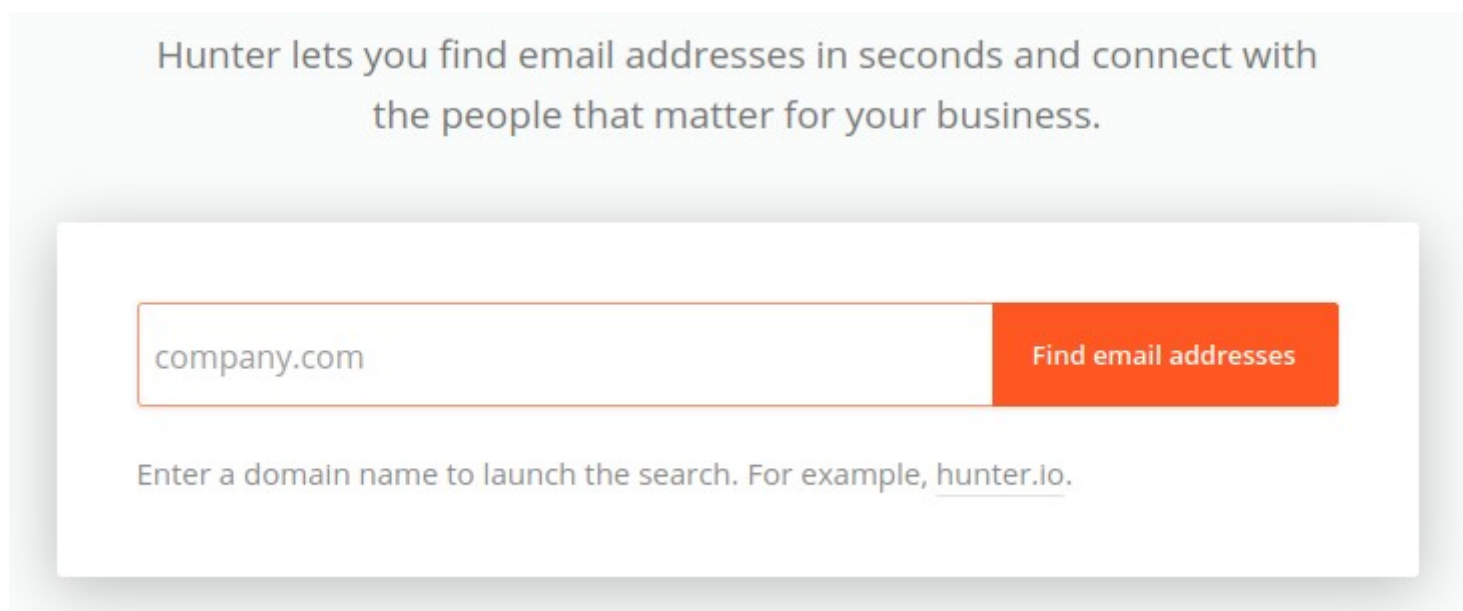
► Buscadores tecnológicos. Spyse

- Permite buscar a partir de dominios, IP, tecnologías, certificados SSL/TLS, y otras.

The screenshot displays the Spyse search engine interface. At the top, a search bar contains the domain 'ieszaidinvergeles.org' with a dropdown menu set to 'Domain'. Below the search bar, there are buttons for 'Add Search Parameter', 'API Request', and 'Download'. The results section shows '4 results'. The first result is for 'ieszaidinvergeles.org' with a status of '200 LOW'. It includes details like 'Title: 301 Moved Permanently', 'Final url: https://www.ieszaidinvergeles.org', 'Alexa rank: 9348801', 'Registrar: 1&1 IONOS SE', and 'Issuer Org: DigiCert Inc'. It also shows 'DNS Records' (A, MX), 'WHOIS', and 'SSL/TLS' tabs. The second result is for 'www.ieszaidinvergeles.org' with a status of '200 MEDIUM'. It includes details like 'Title: IES Zaidin Vergeles', 'Final url: https://www.ieszaidinvergeles.org', and 'Scanned on 2021-05-20'. It also shows 'DNS Records' (A, AAAA) and 'SSL/TLS' tabs. The third result is for 'informatica.ieszaidinvergeles.org' with a status of 'N/A'. It also shows 'DNS Records' and 'SSL/TLS' tabs. On the right side, there is a world map and a list of 'Top Countries' (Germany, Spain), 'Top HTTP Status Codes' (200 OK), and 'Top Title' (IES Zaidin Vergeles, 301 Moved Permanently).

Reconocimiento de emails

- ▶ **Hunter.** Buscador web y extensión de Chrome para búsqueda de emails dentro de un dominio.



Reconocimiento DNS e IPs

- ▶ Información de ***whois***.
 - Información asociada al registro de un dominio.
 - Podemos encontrar direcciones IP, subdominios, servidores DNS, servidores de correo, datos de contacto administrativo, ...
 - Con anterioridad a la entrada en vigor del RGPD la información pública disponible era mucho mayor.
 - Consultas mediante línea de comandos (*whois*) o servicios web (<https://whois.domaintools.com/>).

Reconocimiento DNS e IPs

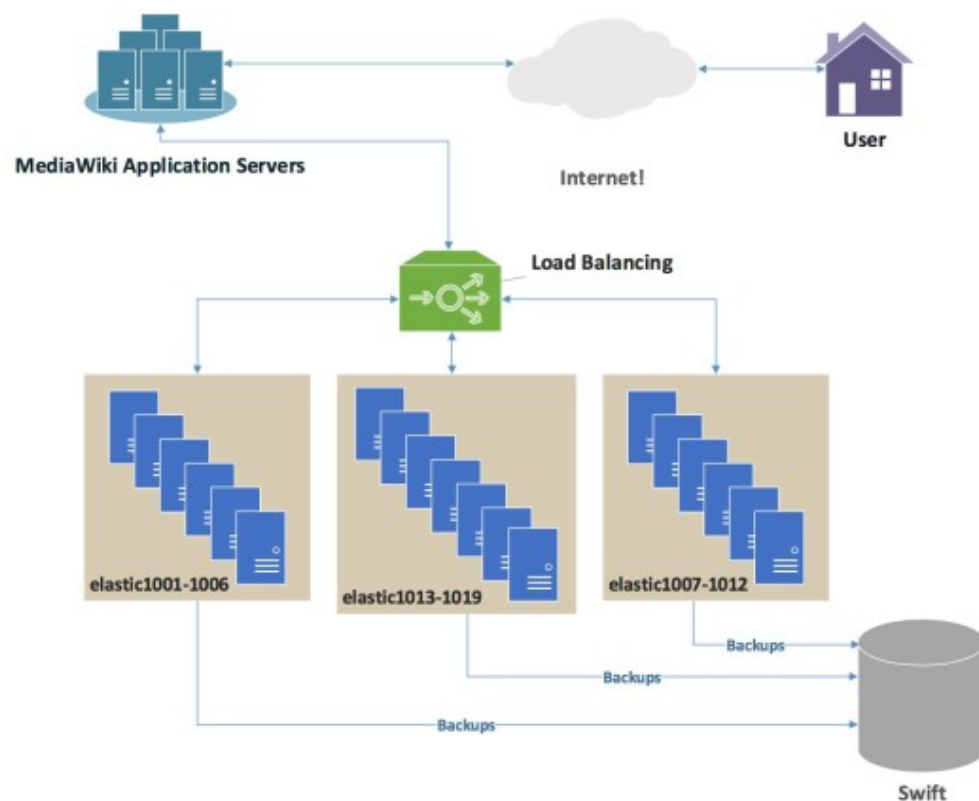
► Reconocimiento de IPs.

- Averiguar la IP de un dominio (**IP lookup**):
 - Comando **ping** → Se comunica con el objetivo.
 - Comando **host** → Consulta los servidores DNS.
 - Comando **dig** → Consulta los servidores DNS.
- Geolocalización de una IP:
 - <https://www.ip-adress.com/>
 - API para geolocalización de IP. <https://ip-api.com/>

Reconocimiento DNS e IPs

► Detectar equilibradores de carga.

- Distribuyen las peticiones entre varios servidores para mantener la calidad del servicio.
- En web suelen operar:
 - En la capa de transporte (TCP/UDP LB)
 - En la capa de aplicación (HTTP LB, **DNS LB**)



<https://medium.com/martinomburajr/distributed-computing-tcp-vs-http-s-load-balancing-7b3e9efc6167>

Reconocimiento DNS e IPs

- Detectar equilibradores de carga.
 - Si un dominio se resuelve a múltiples IPs es probable que esté usando balanceo de carga.

```
(kali㉿kali)-[~]  
$ dig howtogeek.com  
  
; <<>> DiG 9.17.19-1-Debian <<>> howtogeek.com  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 19461  
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags;; udp: 65494  
;; QUESTION SECTION:  
;howtogeek.com.                IN      A  
  
;; ANSWER SECTION:  
howtogeek.com.                3183    IN      A      151.101.66.217  
howtogeek.com.                3183    IN      A      151.101.2.217  
howtogeek.com.                3183    IN      A      151.101.194.217  
howtogeek.com.                3183    IN      A      151.101.130.217  
  
;; Query time: 4 msec  
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)  
;; WHEN: Wed Dec 08 05:30:04 EST 2021  
;; MSG SIZE  rcvd: 106
```

<https://www.howtogeek.com/663056/how-to-use-the-dig-command-on-linux/>

Reconocimiento DNS e IPs

- ▶ Detectar equilibradores de carga.
 - **Load Balancing Detector** (*lbd*). El comando *dig* o *host* no siempre son fiables.

```
(kali㉿kali)-[~]
$ dig google.com

; <<>> DiG 9.17.19-1-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 44370
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;; udp: 65494
;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                157     IN      A      216.58.209.78

;; Query time: 60 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Wed Dec 08 05:30:57 EST 2021
;; MSG SIZE rcvd: 55
```

```
(kali㉿kali)-[~]
$ lbd google.com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
    Written by Stefan Behte (http://ge.mine.nu)
    Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:
    gws
    NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 10:33:33, 10:33:33, 10:33:34, 10:33:34, 10:33:34, 10:33:34, 1
0:33:34, 10:33:35, 10:33:35, 10:33:36, 10:33:36, 10:33:36, 10:33:36, 10:33:37, 10:33:37, 10:33:37, 10
:33:38, 10:33:38, 10:33:38, 10:33:39, 10:33:39, 10:33:39, 10:33:39, 10:33:40, 10:33:40, 10:33:40, 10:
33:40, 10:33:41, 10:33:41, 10:33:41, 10:33:41, 10:33:41, 10:33:42, 10:33:42, 10:33:42, 10:33:42, 10:3
3:42, 10:33:43, 10:33:43, 10:33:43, 10:33:43, 10:33:43, 10:33:44, 10:33:44, 10:33:44, 10:33:44, 10:33
:44, 10:33:45, 10:33:45, 10:33:45, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< Expires: Fri, 07 Jan 2022 10:33:45 GMT
> Expires: Fri, 07 Jan 2022 10:33:46 GMT

google.com does Load-balancing. Found via Methods: HTTP[Diff]
```


Reconocimiento DNS e IPs

- ▶ Protecciones de dominios (CDNs).
 - Un **Content Delivery Network** (CDN) es una red de servidores distribuidos que ofrece diferentes ventajas para servir tráfico web de forma más rápida además de proteger contra ataques DDoS entre otros.
 - Ejemplo de CDNs:
 - CloudFlare.
 - Akamai.
 - Imperva.

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

Reconocimiento DNS e IPs

- ▶ Protecciones de dominios (CDNs).
 - Hay diversas técnicas y herramientas para tratar de obtener la IP original aunque no siempre tendrán éxito. Ejemplos:
 - Configurar CloudFlare para el dominio principal pero no para los subdominios (*ftp*, *mx*, *cpanel*...).
 - Enviando un email al objetivo y analizando las cabeceras de la respuesta ([email tracer](#)).
 - Lecturas recomendadas:
 - [Bypassing CloudFlare WAF with the origin server IP address](#)
 - [Uncovering CloudFlare](#).
 - [Bypassing CloudFlare for long-running tasks without exposing your IP address](#)

Reconocimiento DNS e IPs

► Protecciones de dominios (CDNs).

– Algunas herramientas en línea de comandos:

- [CloudFlair](#). Requiere registro y configurar API Key de Censys.
- [CloudMare](#). Puede realizar consultas a través de Shodan y Censys.
- [CloudFail](#).
- [CloudIP](#). Script en Bash

```
(kali@kali)-[/opt/Cloudmare]
$ python3 Cloudmare.py

CloudMare [2.1.10.11]
Automatic CloudProxy and Reverse Proxy bypass tool
#####

usage: Example: python Cloudmare.py -u site.com
Cloudmare.py: error: missing a mandatory option (-u, --url). Use -h for basic and -hh for advanced help
```

```
CloudIP
By: R4v3N & TAPE TOP-HAT-SEC

> Checking connectivity..
> Internet connection found..proceeding
> Enter Domain Name without the www. [top-hat-sec.com] : 
```

Reconocimiento DNS e IPs

- ▶ **Reverse IP Lookup:** Descubrir otros dominios alojados en el mismo servidor (shared hosting).
- ▶ **Escaneo de subdominios** (*Forward DNS Lookup*). Descubrir subdominios que no están indexados en los DNS mediante fuerza bruta y diccionario. *Fierce*, [Knock](#), ...).
- ▶ **Enumeración DNS.** Obtener datos del dominio (subdominios, servidores de correos, rangos de IP, etc.) mediante consultas a los servidores de nombres.
- ▶ **Reverse DNS Lookup.** Buscar subdominios asociados a una dirección IP.
- ▶ **DNS Zone transfer.** Mecanismo de copia de registros entre servidores DNS. Una mala configuración puede exponer datos internos.

(ver documento Reconocimiento DNS)

Reconocimiento DNS e IPs

```
(kali@kali)-[/opt/knock]
$ sudo python3 knockpy.py ieszaidinvergeles.org
```

Knockpy v5.2.0

local: 10757 | google: 0 | duckduckgo: 0 | virustotal: 0

Wordlist: 10757 | Target: ieszaidinvergeles.org | Ip: 217.160.0.64

11:58:29

Ip address	Code	Subdomain	Server
Real hostname			
(ctrl+c) 14.2%		cisco-capwap-controller.ieszaidinvergeles.org	
(ctrl+c) 14.3%		cisco-lwapp-controller.ieszaidinvergeles.org	
(ctrl+c) 27.1%		enterpriseregistration.ieszaidinvergeles.org	
217.160.0.64	404	ftp.ieszaidinvergeles.org	nginx
(ctrl+c) 33.8%		googlefffffffa5b3bed2.ieszaidinvergeles.org	
80.28.211.131	200	informatica.ieszaidinvergeles.org	nginx
(ctrl+c) 75.0%		savvis-admin-commondata.ieszaidinvergeles.org	
88.12.54.231	200	server.ieszaidinvergeles.org	Apache
217.160.0.64	200	www.ieszaidinvergeles.org	Apache
217.160.0.64	200	youtube.ieszaidinvergeles.org	ESF

11:59:18

Ip address: 3 | Subdomain: 5 | elapsed time: 00:00:48

Búsqueda de información en leaks

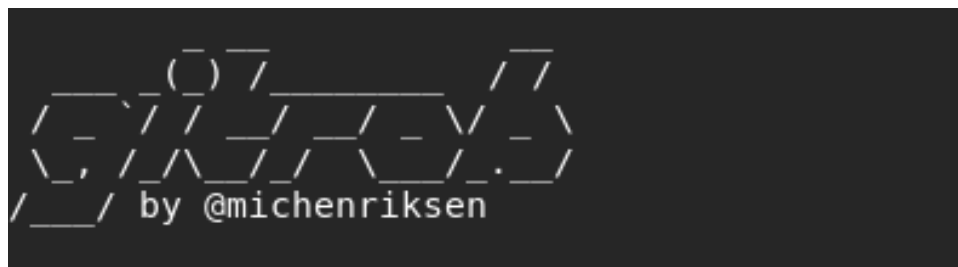
► Búsqueda de *leaks* en repositorios:

– Herramientas:

- **Gitrob**. Es una herramienta para buscar información sensible publicada en los repositorios de Github.

<https://www.hahwul.com/2020/01/18/how-to-find-important-information-in-github/>

<https://medium.com/@pig.wig45/setting-up-gitrob-and-using-it-to-find-leaking-repository-of-an-employee-in-a-hackerone-private-e4c40da1bc8>



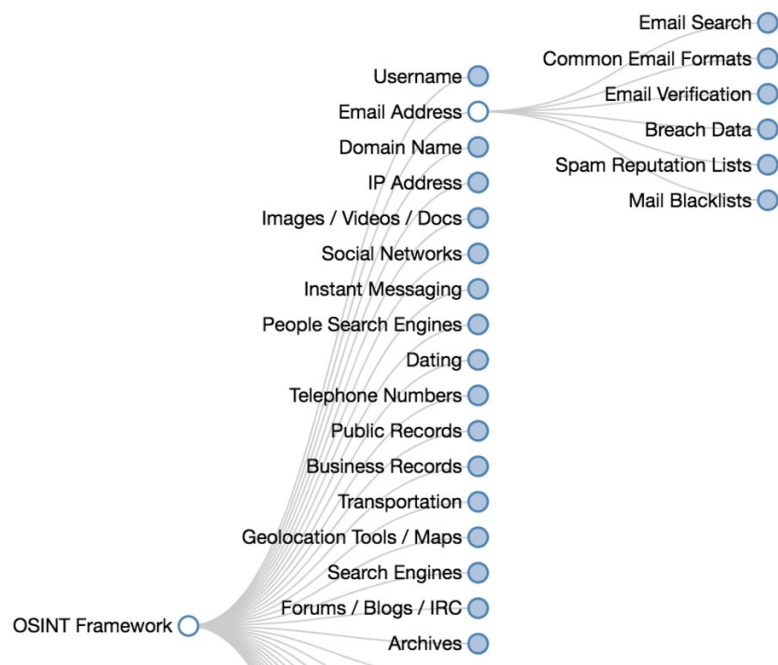
Búsqueda de información en leaks

► Búsqueda de credenciales y correos comprometidos:

- [Have I been pwned](#). Verifica si un email ha sido comprometido. Permite crear alertas.
- [Dehashed](#). Servicio similar al anterior, orientado a empresas, con API y operaciones complejas.
- [GhostProject](#). Dispone de diferentes opciones de pago y API.
- <http://pwndb2am4tzkvold.onion>. Buscador de leaks en la red Tor.
- [H8Mail](#). Herramienta en línea de comandos para la búsqueda de emails y leaks usando diferentes servicios.
- [WhatBreach](#). Similar al anterior.
- Sitios empleados para publicar fugas de información: AnonPaste, Pastebin, PasteHTML, Pastie.
 - [Pastenum](#). Herramienta en línea de comandos que automatiza las búsquedas en estos servicios. Desarrollada inicialmente por Corelan Team.
 - Ej. Google dork: *site:pastebin.com "gmail.com"*

Frameworks para OSINT

- ▶ Herramientas integradas para realizar investigaciones OSINT. Facilitan la generación de inteligencia.
- ▶ **OSINT Framework**. Web que recopila herramientas clasificadas por categorías.



<https://www.elladodelmal.com/2016/05/osint-framework-donde-buscar-datos-de.html>

<https://ciberpatrulla.com/osint-framework/>

<https://www.flu-project.com/2016/08/osint-framework-lidera-tu-revolucion.html>

Frameworks para OSINT

- ▶ **OSR Framework** (*Open Source Research Framework*). Desarrollado en Python. Desarrollada por Félix Brezo (@febrezo) y Yaiza Rubio (@yrubioseco), analistas de ElevenPaths.
- ▶ Dispone de diversos módulos para búsqueda de información.
 - **mailfy.py**. Módulo para automatizar búsqueda de emails.
 - **phonefy.py**. Módulo para encontrar información de un número de teléfono ha sido vinculado a prácticas de spam.
 - **usufy.py**. Módulo para verificar si existe un nombre de usuario en más de 300 plataformas
 - **searchfy.py**. Módulo para encontrar perfiles en RRSS con un nombre como entrada.
 - **alias_generator.py**. Generador de nicknames a partir de la información del objetivo (útil para tratar de averiguar posibles cuentas de correo, etc.).
 - **checkfy.py**. Adivina posibles emails basándose en una lista de nicknames y un patrón.
 - **domainfy.py**. Busca dominios que se resuelven a partir de una palabra o nickname.
 - **OSRF Console**. Módulo que ofrece una interfaz similar a la consola de metasploit (*msfconsole*).

Frameworks para OSINT

- **The Harvester.** Herramienta para recopilar emails, nombres, dominios, IPs, a través de multitud de servicios.
 - Se encuentra preinstalada en Kali Linux.
 - Algunos servicios requieren que se configure la API KEY de desarrollador.

```
Usage: theharvester options

-d: Domain to search or company name
-b: data source: google, googleCSE, bing, bingapi, pgp
    linkedin, google-profiles, people123, jigsaw,
    twitter, googleplus, all

-s: Start in result number X (default: 0)
-v: Verify host name via dns resolution and search for virtual hosts
-f: Save the results into an HTML and XML file
-n: Perform a DNS reverse query on all ranges discovered
-c: Perform a DNS brute force for the domain name
-t: Perform a DNS TLD expansion discovery
-e: Use this DNS server
-l: Limit the number of results to work with(bing goes from 50 to 50 results,
    google 100 to 100, and pgp doesn't use this option)
-h: use SHODAN database to query discovered hosts
```

Frameworks para OSINT

- ▶ **FOCA** (*Fingerprinting Organizations with Collected Archives*).
 - Herramienta open source utilizada principalmente para encontrar metadatos e información oculta.
 - Los archivos se obtienen a través de búsquedas en Google, Bing y DuckDuckGo.
 - Dispone de herramientas de descubrimiento de servidores (DNS Search, resolución IP, PTR Scanning, DNS Prediction, Robtex...).
 - Tiene un market de plugins para extender la funcionalidad.
 - Solo en entornos Windows.



Frameworks para OSINT

- ▶ **Maltego**. Desarrollada por la empresa sudafricana Paterva, posiblemente la herramienta de OSINT más potente.
 - Preinstalado en Kali Linux.
 - Posibilidad de añadir nuevas transformadas e integrar servicios (Ej. [Shodan](#), [nmap](#)) y programar nuestras propias transformadas.
 - [Tutorial de Maltego](#) en Youtube para principiantes.

Frameworks para OSINT

► Maltego.

- Dispone de una versión para la comunidad de uso libre y versiones de pago con funcionalidad avanzada.

Maltego Desktop Client - Community Edition	Data Integration	Deployment & Infrastructure	Support & Services	Learning & Training
<ul style="list-style-type: none"> ✓ Standard Transforms Included ✓ Only 12 results per Transform ✗ Upto 64,000 results per Transform ☹ 	<ul style="list-style-type: none"> ✓ Access to OSINT Standard Transforms ✓ Paid access to selected partner Transforms ✓ CaseFile Entities ✗ Integration to own data sources ☹ ✗ Enterprise on-premise integrations ☹ ✗ Own API keys for Standard Transforms ☹ 	<ul style="list-style-type: none"> ✓ Uses Maltego Community Cloud (the public Maltego Transform server and collaboration servers) for Standard and Community Transforms ✗ Traffic routed via the Maltego Enterprise Cloud ☹ ✗ Dedicated cloud instance available ☹ ✗ Traffic routing via regional servers in the USA and EU ☹ ✗ On-premise deployment ☹ 	<ul style="list-style-type: none"> ✓ E-mail support ✗ Phone and priority support ☹ ✗ Onboarding and guided deployment ☹ ✗ Integration and Transform writing services ☹ 	<ul style="list-style-type: none"> ✓ Online documentation ✓ Free learning resources ✗ Optional access to on-demand courses ☹ ✗ In-person training available ☹

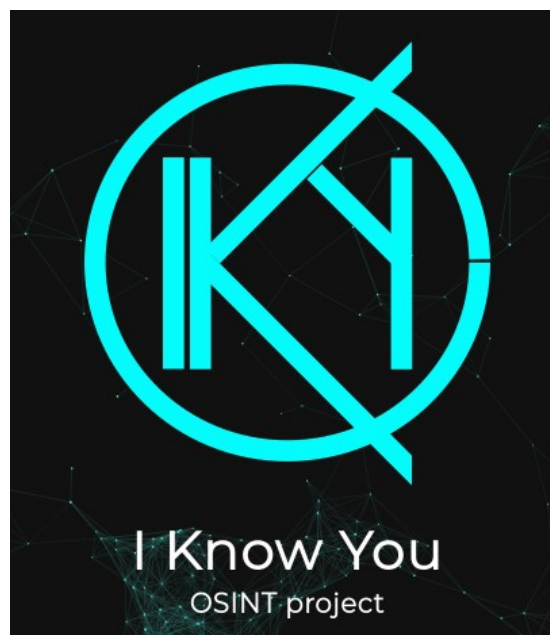
Frameworks para OSINT

► Maltego.

- **Entidades.** Objetos sobre los que se aplicarán determinadas acciones llamadas transformadas. Dos categorías:
 - **Infraestructuras.** Almacena los atributos de la compañía relacionadas a estas.
 - **Personas.** Datos referentes a los trabajadores.
- **Transformadas.** Se pueden ir encadenando sobre los diferentes resultados creando una red de entidades.
- Ejecución de pseudoscript personalizados de manera remota en servidores externos llamados máquinas (***machines***).
 - **Company Stalker.** Obtiene los emails del dominio y averigua cuales se encuentran en redes sociales.
 - **Footprinting L1, L2, L3.** Realiza un footprinting de diversa profundidad sobre un dominio. A mayor profundidad más “ruido”.
 - **Person – Email Address.** Averigua los emails de una persona y los sitios web donde aparecen.
 - **Twitter Monitor.** Busca hashtags y entidades mencionadas en torno a una determinada frase.

Frameworks para OSINT

- **Iky** (*I Know You*). Es una herramienta open source creada por KenBro para recopilar información a partir de un email, mostrando los resultados a través de una interfaz visual.
- Necesita configuración de API Keys para recolectar información en diversas fuentes.
 - Generación de informes y exportación en formato JSON.
 - Visualización de eventos importantes en una línea de tiempo.



Otras herramientas para OSINT

► BinGoo!

- Herramienta en línea de comandos de Linux que automatiza el uso de Dorks en Bing y Google (BinGoo).



- ▶ **Snitch**. Herramienta en línea de comandos desarrollada en Python para recopilar información vía dorks.

[illegible]

Otras herramientas para OSINT

- **Sherlock**. Herramienta en línea de comandos para encontrar nombres de usuario en hasta 300 redes sociales.



Otras herramientas para OSINT

- ▶ **Little Brother**. Herramienta para investigar personas francófonas (francesa, suiza, luxemburguesa o belga).



```
Invite de commandes - python LittleBrother.py

LittleBrother

Time: [ 2019-02-22 | 00:31:23 ]
Author: [ Lulz3xploit ]
Version: [ 6.0 ]
Pays: [ France | FR ]
Database: [ 0 | 4.096 Ko ]

you are free ! lol no, it was a joke.

[1] Lookup
[2] Other tool
[3] Profiler
[4] Change country

[e] Exit script [h] Help Message [c] Clear Screen

LittleBrother(-)$
```

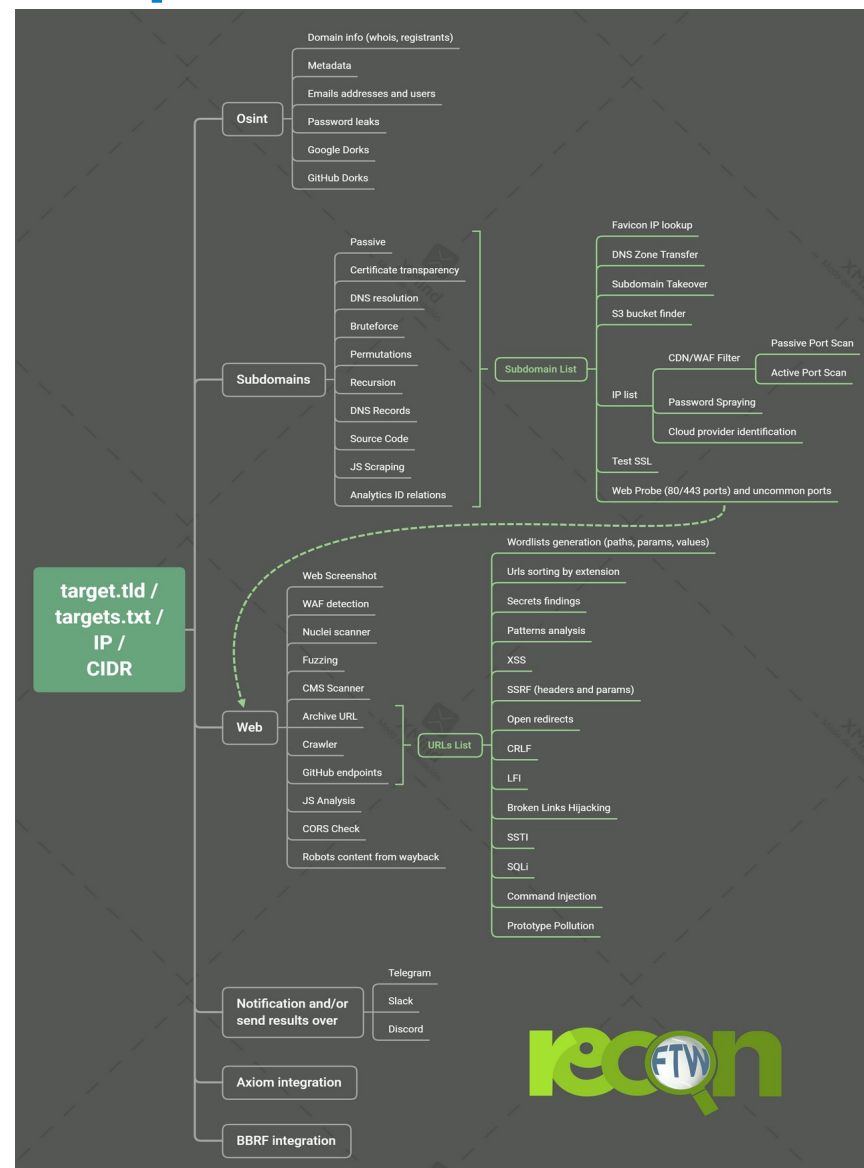
Otras herramientas para OSINT

- **ORB.** Herramienta en línea de comandos para realizar footprinting masivo con opciones de reconocimiento activo.



Otras herramientas para OSINT

- **ReconFTW**. Realiza footprinting automatizado empleando multitud de técnicas (también técnicas activas).



Otras herramientas para OSINT

- **MetaFinder**. Extracción de metadatos de documentos localizados en ficheros buscados a través de Google.

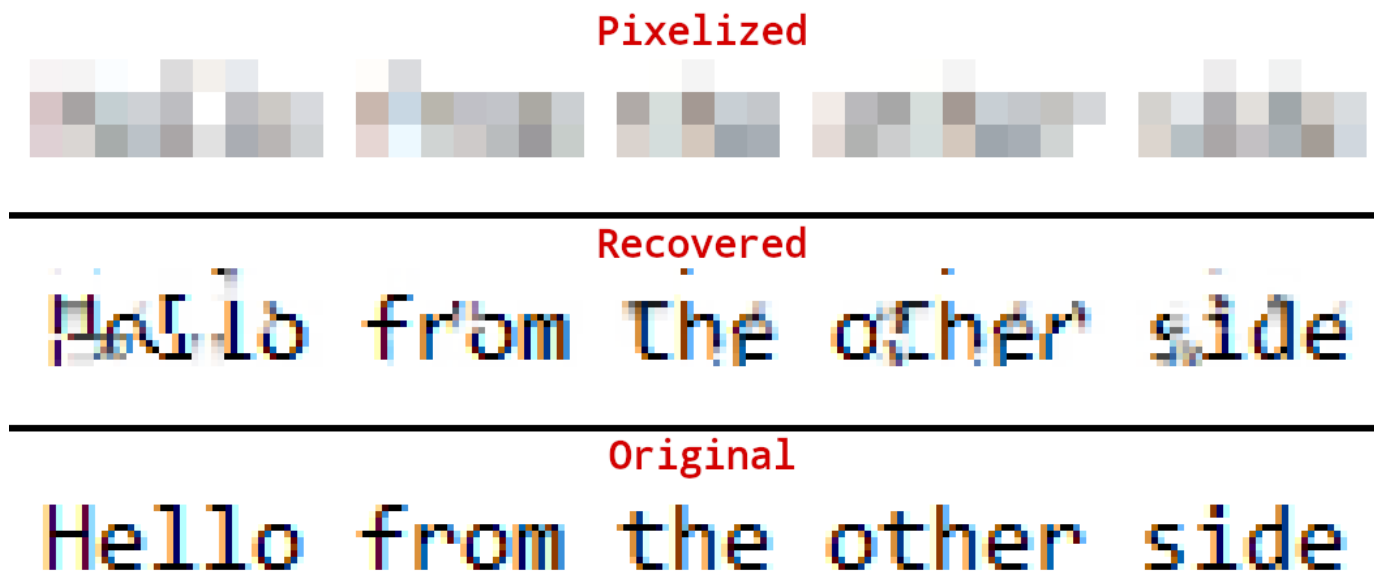
```
metafinder -d domain.com -l 20 -o folder [-t 10] [-v]
```

Parameters:

- d: Specifies the target domain.
- l: Specify the maximum number of results to be searched.
- o: Specify the path to save the report.
- t: Optional. Used to configure the threads (4 by default).
- v: Optional. It is used to display the results on the screen as well.

Otras herramientas para OSINT

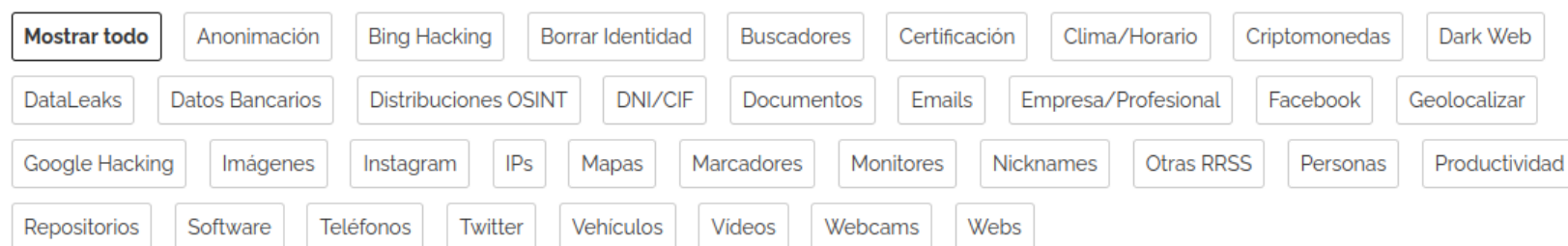
- **Depix**. Recupera contraseñas de imágenes pixeladas, creadas con un filtro de caja lineal.
 - También es posible hacerlo con rostros (a veces con una búsqueda inversa en Google es suficiente).



<https://www.microsiervos.com/archivo/seguridad/recuperar-textos-contrasenas-rostros-imagenes-pixeladas-mosaicos.html>

Otras herramientas para OSINT

- **Buscador y recopilación de herramientas para OSINT de Ciberpatrulla.**
 - En esta web podemos encontrar multitud de herramientas clasificadas en categorías.
 - <https://ciberpatrulla.com/links/>



Anonimación

➤ Generador de conversaciones de WhatsApp	46
➤ Whonix - Sistema operativo navegación anónima	42
➤ Yopmail - Cuentas de Email temporales	33

Bing Hacking

➤ Sitios alojados en la misma IP	17
➤ Buscar por tipo de archivo en una web	6
➤ Ficheros con una extensión concreta	6

FIN