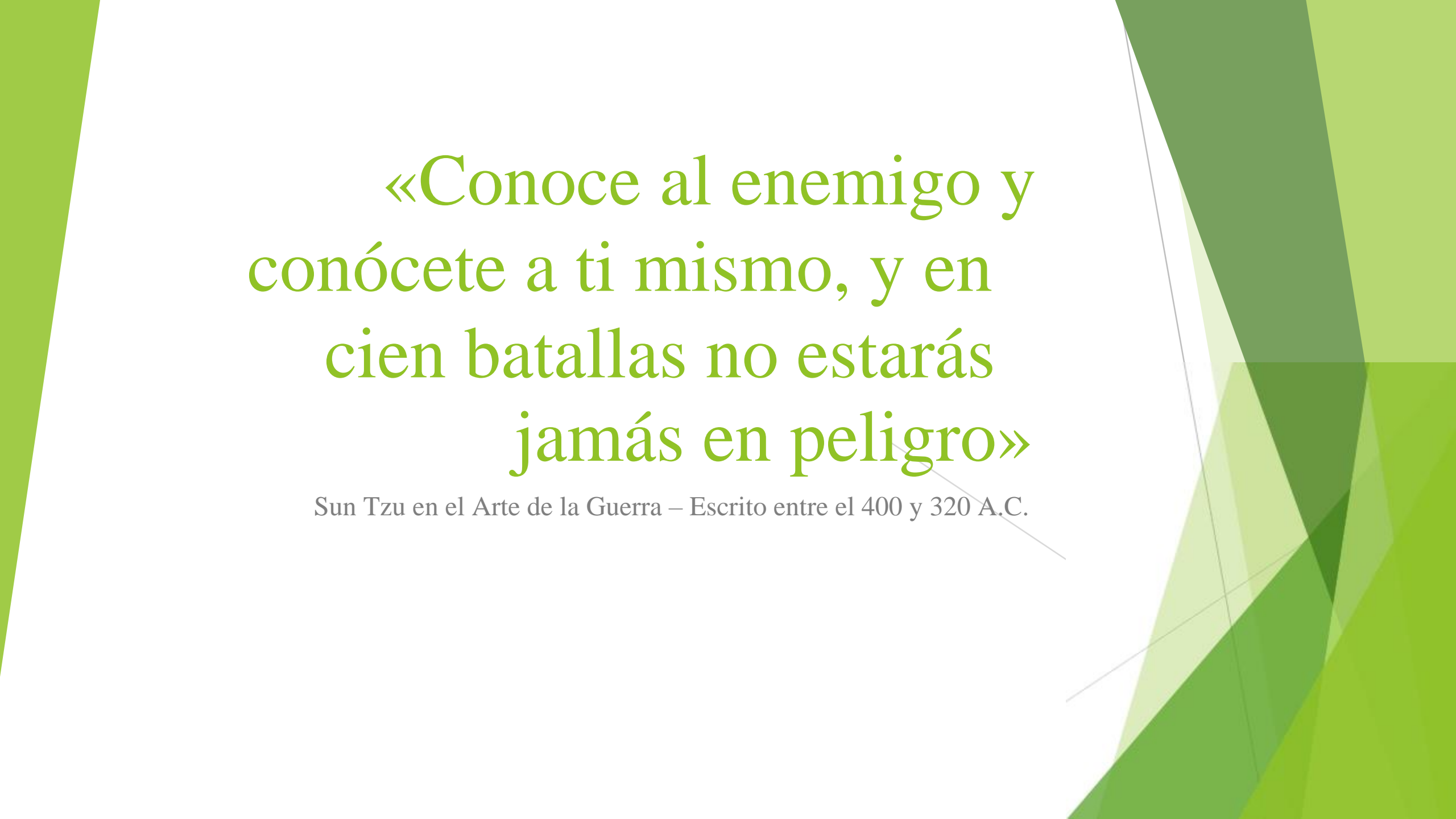


# OSINT

Open-Source INTelligence

## INTRODUCCIÓN A LA INTELIGENCIA EN FUENTES ABIERTAS

The background features abstract, overlapping geometric shapes in various shades of green, ranging from light lime to dark forest green. These shapes are primarily located on the left and right sides of the frame, creating a modern, layered effect. The central area is white, providing a clean space for the text.

«Conoce al enemigo y  
conócete a ti mismo, y en  
cien batallas no estarás  
jamás en peligro»

Sun Tzu en el Arte de la Guerra – Escrito entre el 400 y 320 A.C.



# Inteligencia

«"proceso sistemático de recolección, evaluación y análisis de información, cuya finalidad es producir conocimiento útil para la toma de decisiones."»

Detectigal.com

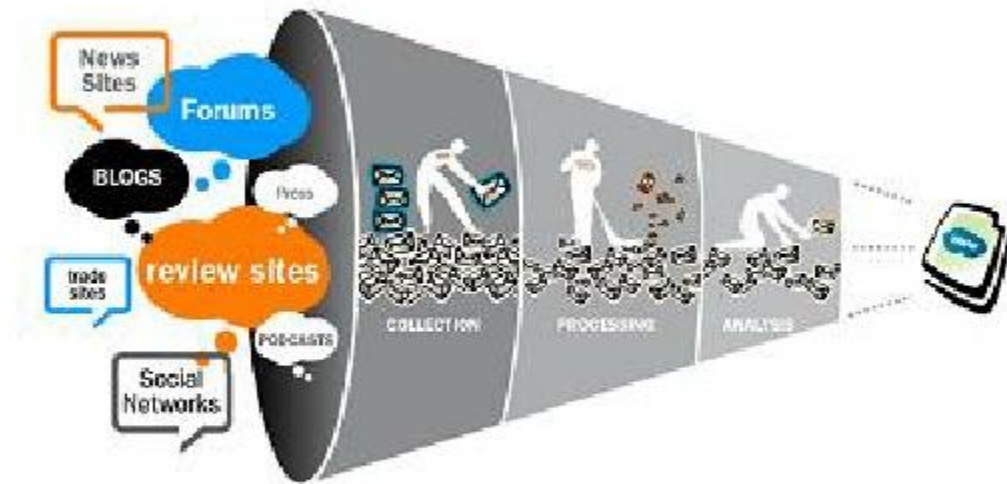
# Colección de fuentes de inteligencia



- IMINT – Inteligencia procedente de imágenes (SATELITE)
- HUMINT – Inteligencia procedente de fuentes humanas (ESPIAS)
- MASINT – Inteligencia procedente de reconocimiento y firma (ARMAS MILITARES)
- SIGINT – Inteligencia procedente de señales (RED ECHELON)
- OSINT – Inteligencia procedente de fuentes abiertas (INFORMACIÓN PÚBLICA)

# ¿QUÉ ES OSINT?

Open Source Intelligence (Inteligencia en Fuentes Abiertas)



- metodología multifactorial de recolección, análisis y toma de decisiones sobre datos de fuentes disponibles de forma pública para ser utilizados en un contexto de inteligencia.

WIKIPEDIA

# ¿De donde podemos obtener la información?

- ❑ Medios de comunicación (artículos)
- ❑ Publicaciones profesionales y académicas (artículos, libros...)
- ❑ Internet (Social media, webs, foros...)
- ❑ Datos gubernamentales (Juicios, B.D.Leyes, Boletines oficiales, ...)
- ❑ Datos comerciales (Evaluaciones financieras...)
- ❑ Literatura gris (Informes técnicos, patentes, ...)
- ❑ Informes sobre terrorismo (Videos, registros de audio,...)
- ❑ Etc.

Fuente: [www.defensa.com](http://www.defensa.com)





# Principales registros públicos

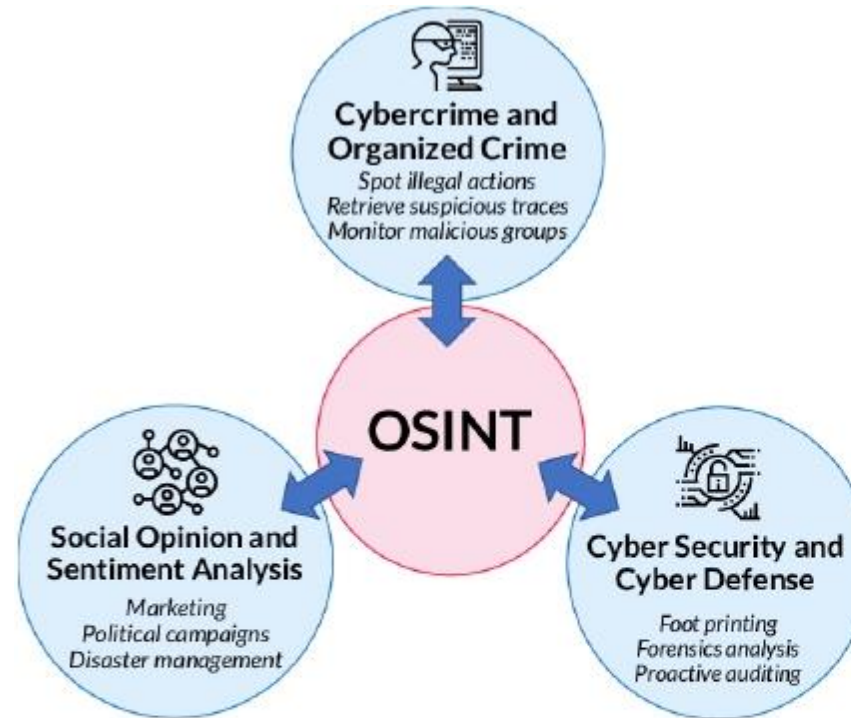
- ❑ Registros de propiedades
- ❑ Registros criminales
- ❑ Registros gubernamentales
- ❑ Registros financieros
- ❑ Registros de votantes
- ❑ Registros de patentes
- ❑ Registros de nacimientos
- ❑ Registros políticos
- ❑ Etc...



# PRINCIPALES CASOS DE USO

Podemos obtener información para resolver posibles casos de:

- ❑ **Cibercrimen** , crimen organizado, monitorización de grupos maliciosos y sospechosos
- ❑ **Marketing** , opinión social, marketing, campañas políticas
- ❑ **Ciberseguridad** , análisis forense, auditorías de seguridad, ciberdefensa





# FASES

## **FASE PREVIA**

## **FASE DE IDENTIFICACIÓN**

verificar y describir el ataque, incidente de seguridad o actividad ilegal

## **FASE DE RECOPIACIÓN U OBTENCIÓN:**

búsqueda y recopilación de datos y hechos que pueden convertirse o ser evidencias digitales aptas para ser analizadas

## **FASE DE PRESERVACIÓN DE LA EVIDENCIA DIGITAL:**

En esta fase se hace uso de los métodos, mecanismos y tecnologías adecuados para asegurarse de que la evidencia digital no sufra daños

## **FASE DE ANALISIS:**

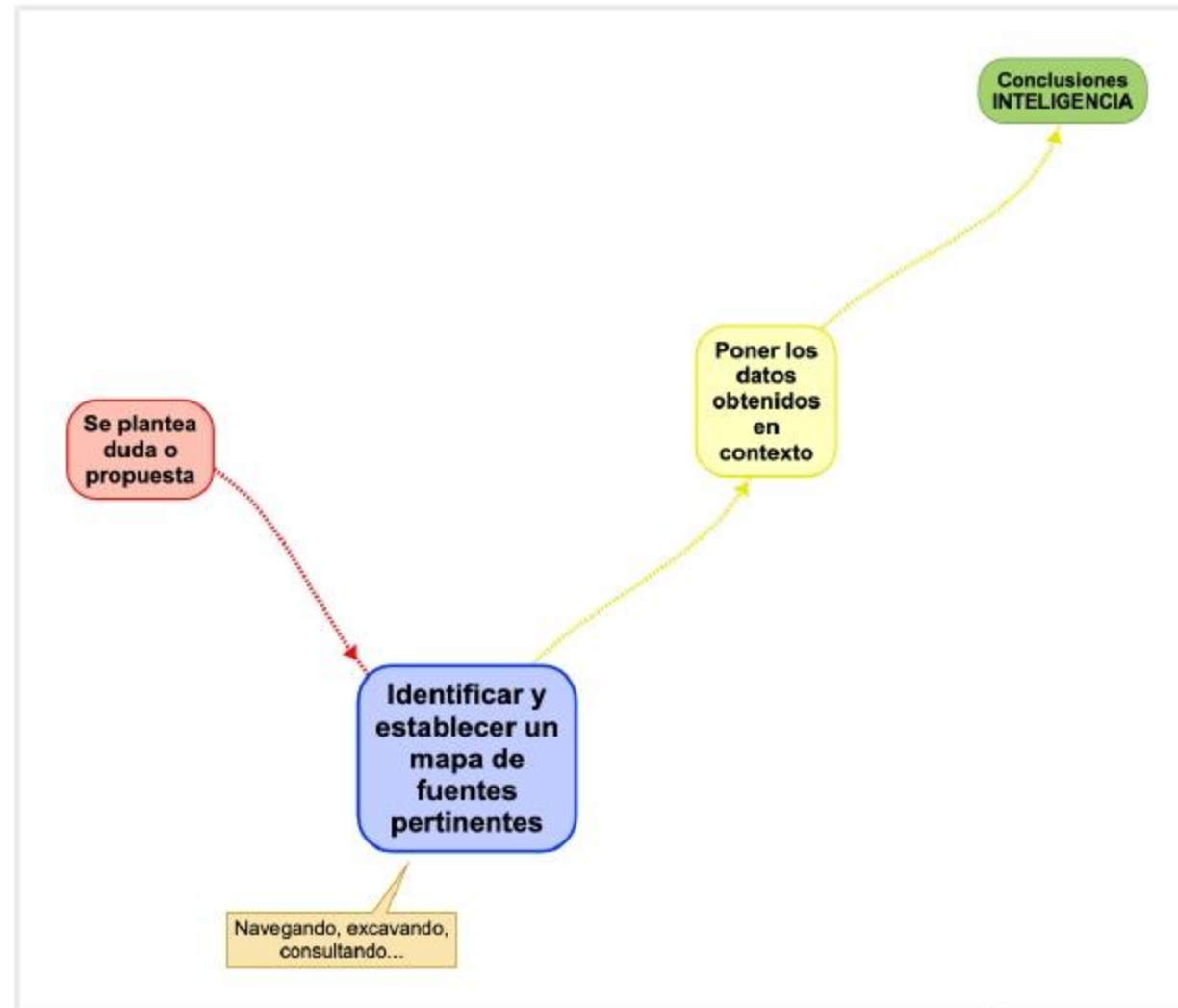
En esta fase se procede a analizar la evidencia con objeto de encontrar hechos y conclusiones relevantes para la resolución del incidente de ciberseguridad

## **FASE DE DOCUMENTACIÓN Y PRESENTACIÓN DE RESULTADOS:**

Esta última fase tiene por objeto elaborar un informe documental donde se recoja toda la información de las diferentes fases y los resultados del análisis forense

# Esquema general de una investigación

- 1. Propuesta
- 2. Establecer mapa de fuentes
- 3. Poner los datos en contexto
- 4. Justificar los datos y Conclusiones



# Ciclo de inteligencia

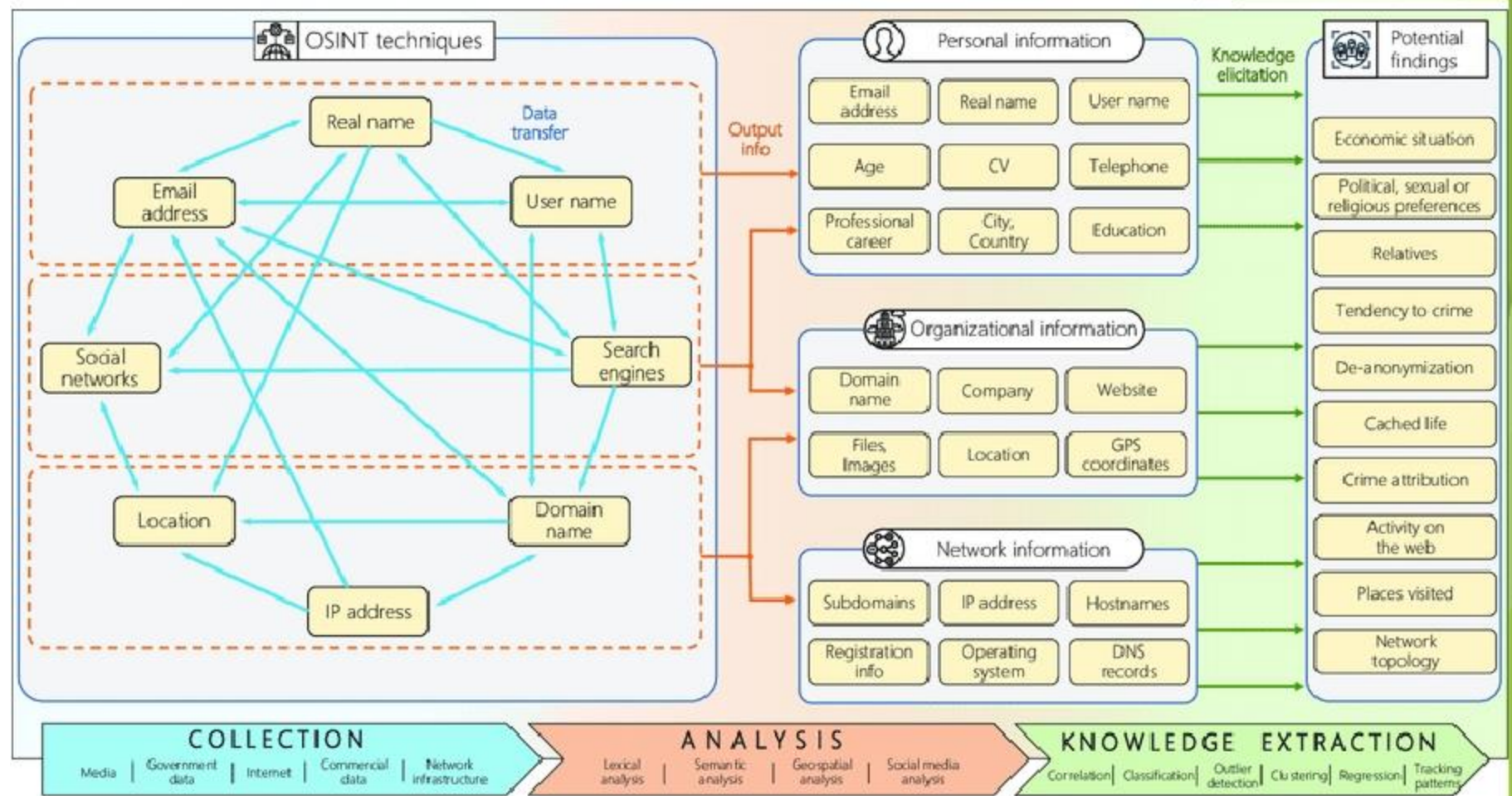
- ❑ 1. Establecer los requisitos
- ❑ 2. Concretar las Fuentes de información
- ❑ 3. Adquisición de la información
- ❑ 4. Procesamiento y formateo
- ❑ 5. Análisis y relación de los datos
- ❑ 6. Inteligencia. Presentación del informe con los datos pertinentes.



Fuente: [hackers4fun.com](http://hackers4fun.com)

# Fases de investigación en OSINT

- 1. Colección
- 2. Análisis
- 3. Extracción

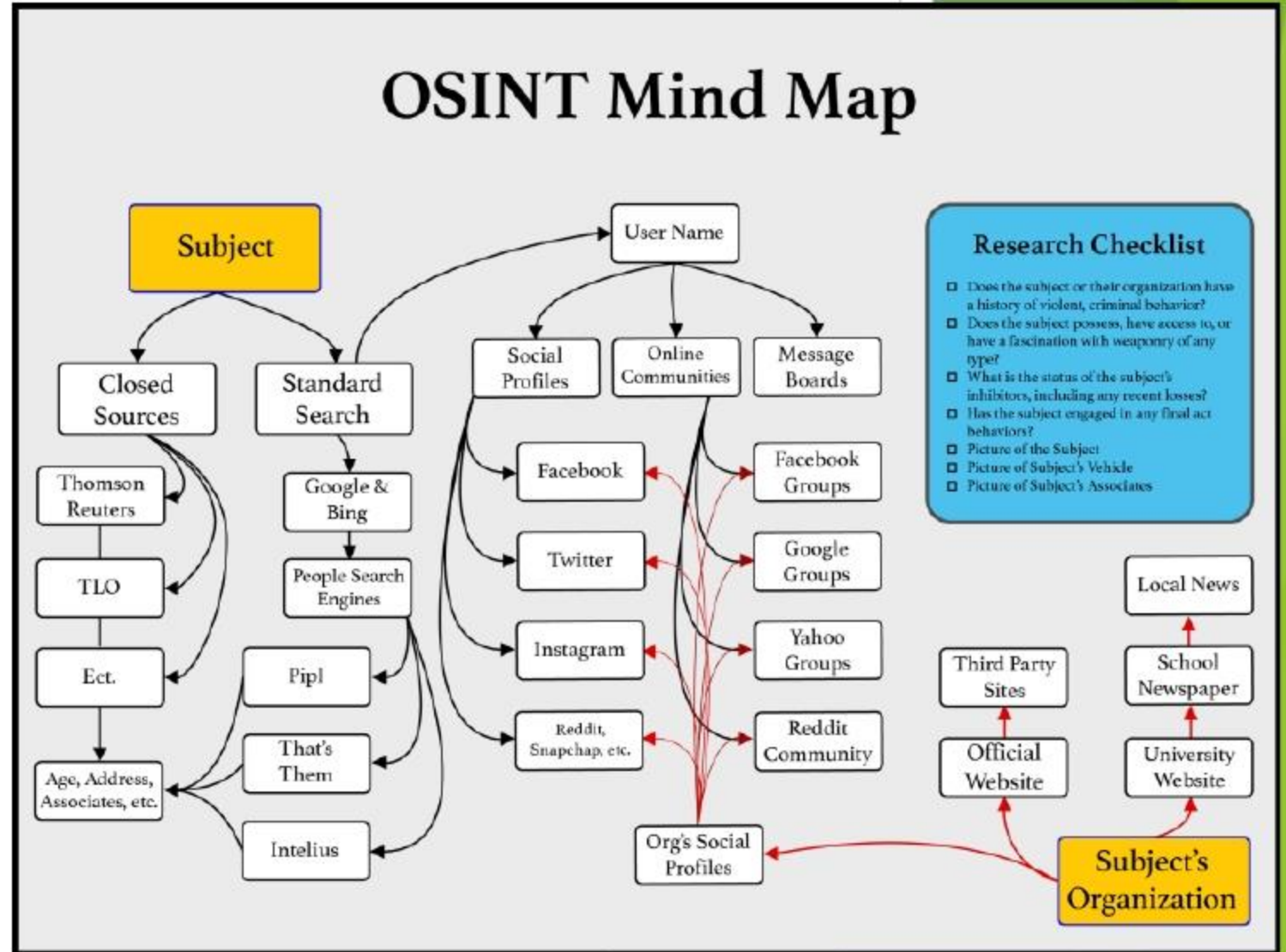


# Mapa mental (Ejemplo de investigación)

## ❑ Checklist de la investigación sobre sujeto o su organización criminal potencial

- ❑ ¿Tiene historial o comportamiento criminal?
- ❑ ¿Siente fascinación por algún tipo de armamento?
- ❑ ¿Inhibidores posibles, pérdidas recientes?
- ❑ ¿Ha participado en algún evento o acto final criminal?
- ❑ Imagen del sujeto
- ❑ Imagen de vehiculos del sujeto
- ❑ Imagen de posibles asociados

❑ Fuente: [protectioncircle.org](http://protectioncircle.org)

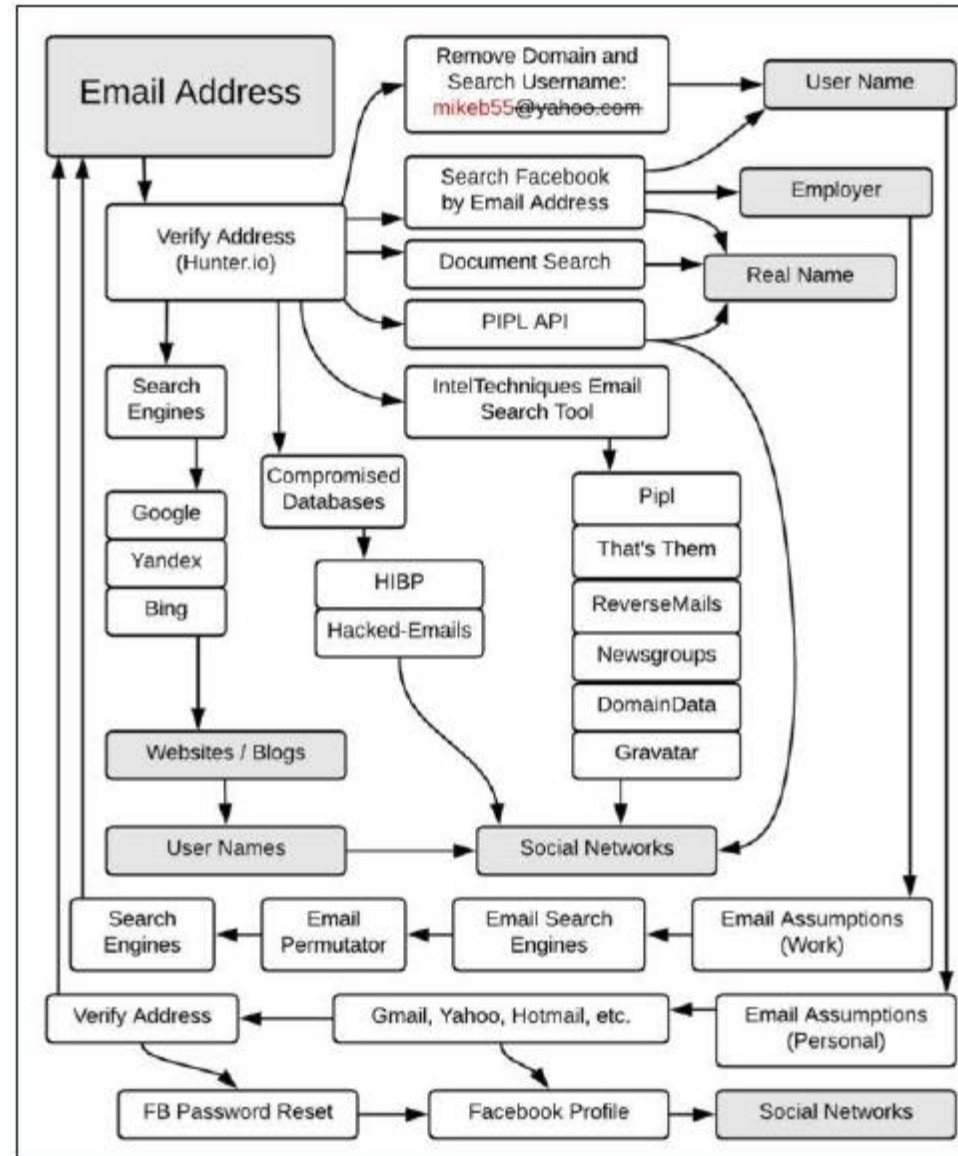




# Investigación de perfiles digitales

- Email
- Nombre real
- Nombre de dominio
- Localización
- Teléfono
- Etc...

Fuente: inteltechniques.com



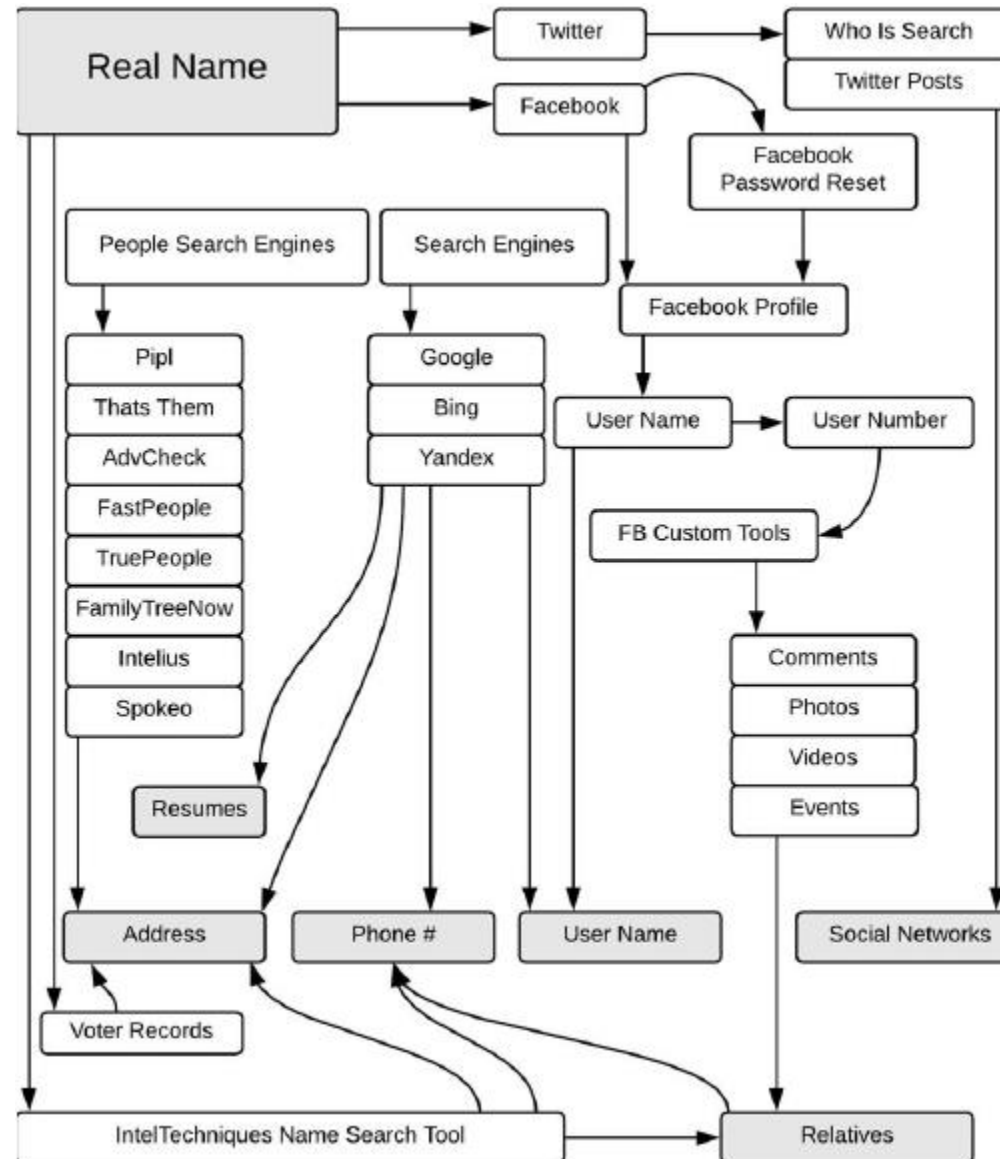


# Investigación de perfiles digitales

- Email
- Nombre real
- Nombre de dominio
- Localización
- Telefono
- Etc...

Fuente: inteltechniques.com

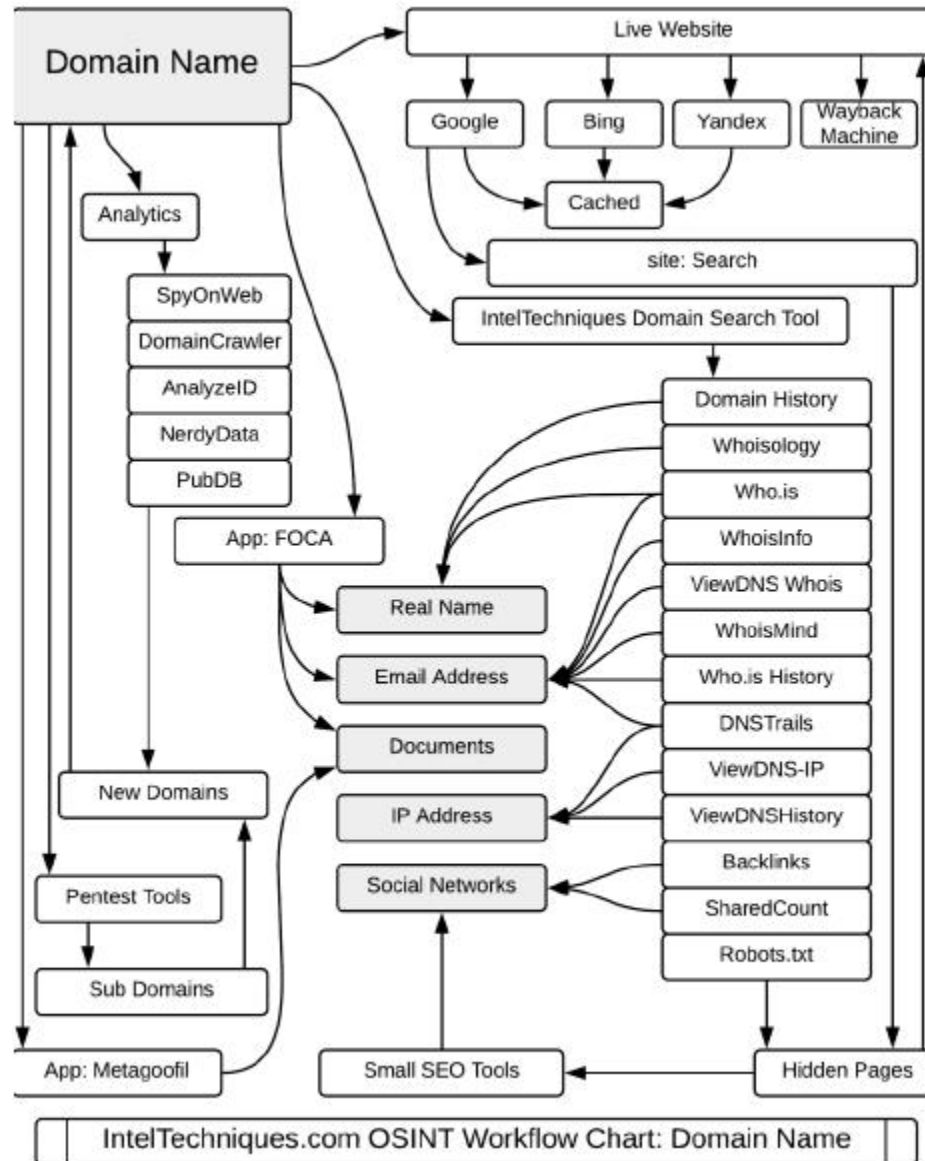
Inteltechniques - Michael Bazzell  
(consultor de seguridad y ex  
agente e investigador del Grupo  
de Trabajo de Delitos Cibernéticos  
del FBI)



# Investigación de perfiles digitales

- Email
- Nombre real
- Nombre de dominio
- Localización
- Teléfono
- Etc...

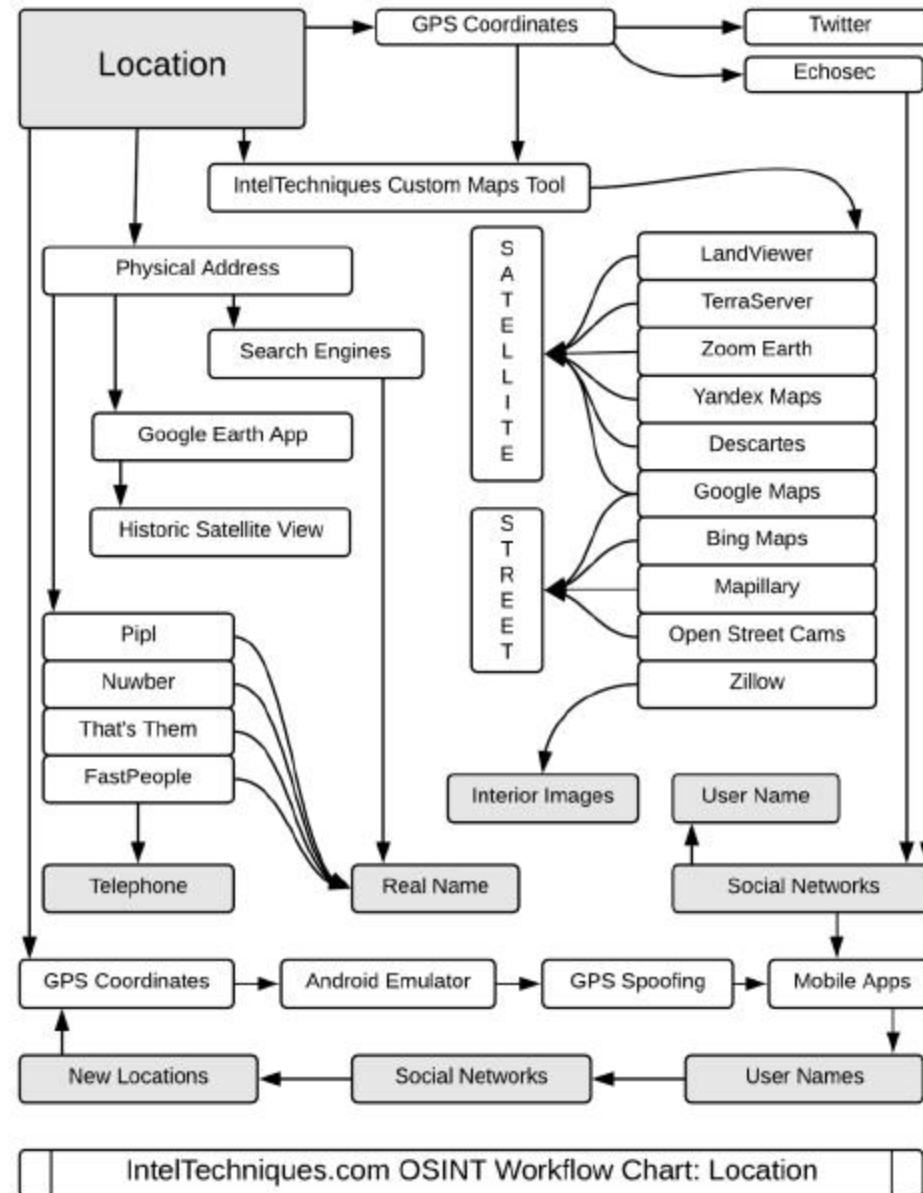
Fuente: inteltechniques.com



# Investigación de perfiles digitales

- Email
- Nombre real
- Nombre de dominio
- Localización
- Teléfono
- Etc...

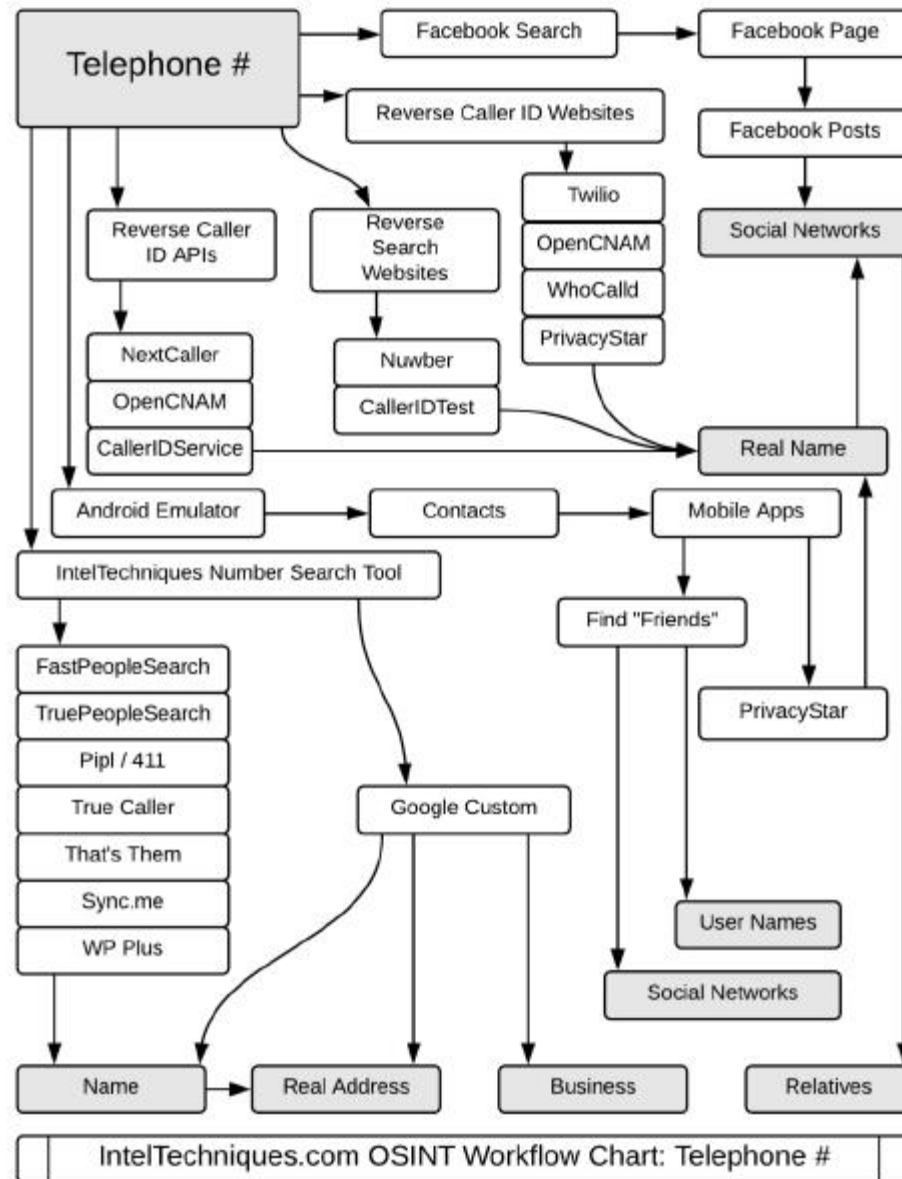
Fuente: inteltechniques.com



# Investigación de perfiles digitales

- Email
- Nombre real
- Nombre de dominio
- Localización
- Teléfono
- Etc...

Fuente: inteltechniques.com

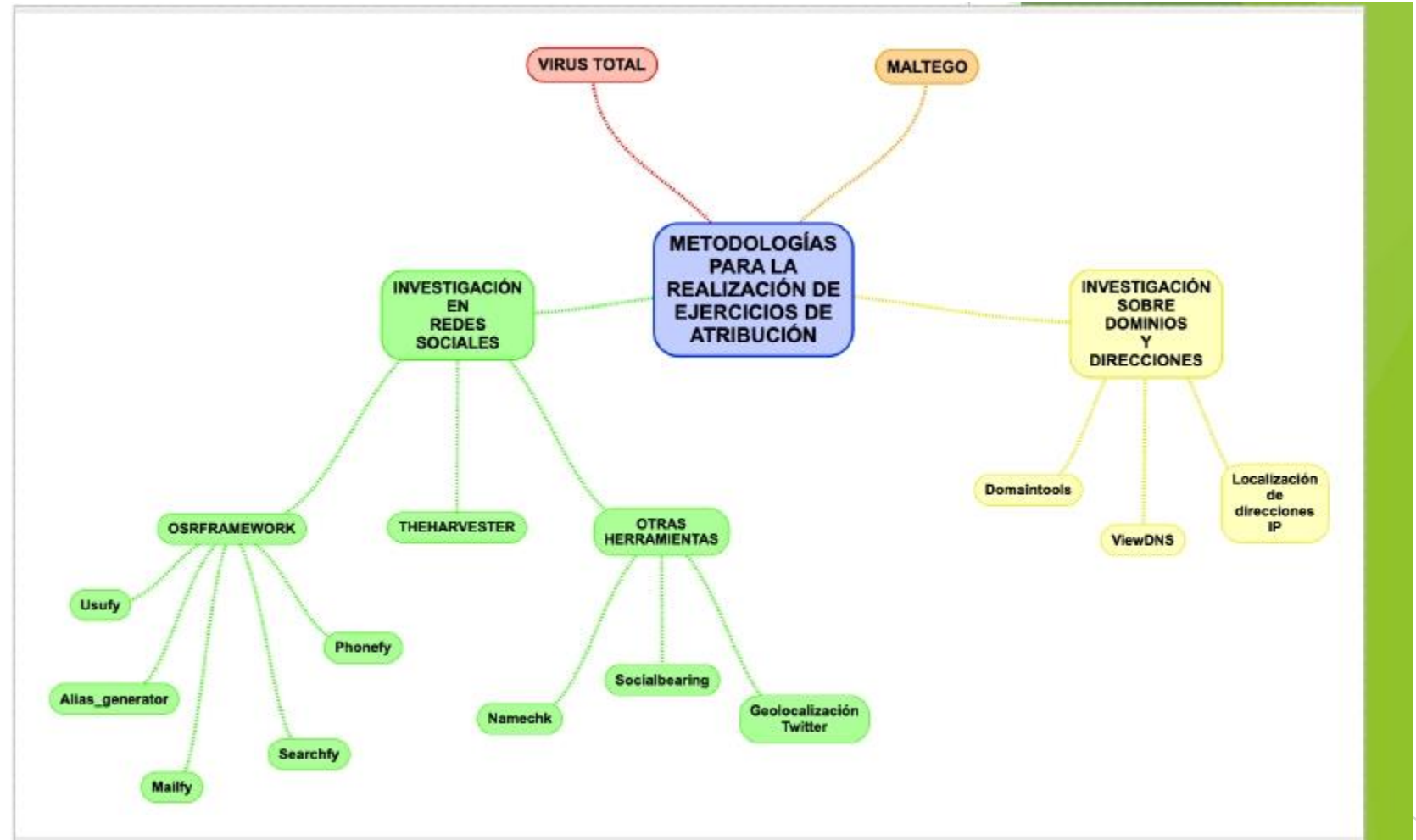


# Esquema inicial para la investigación en redes sociales y dominios

## Investigación en redes sociales

- - OSRframework
  - TheHarvester
  - Otras tools online
- Investigación sobre dominios y direcciones
  - Domaintools
  - ViewDNS
  - Localización de IPs
- Etc...

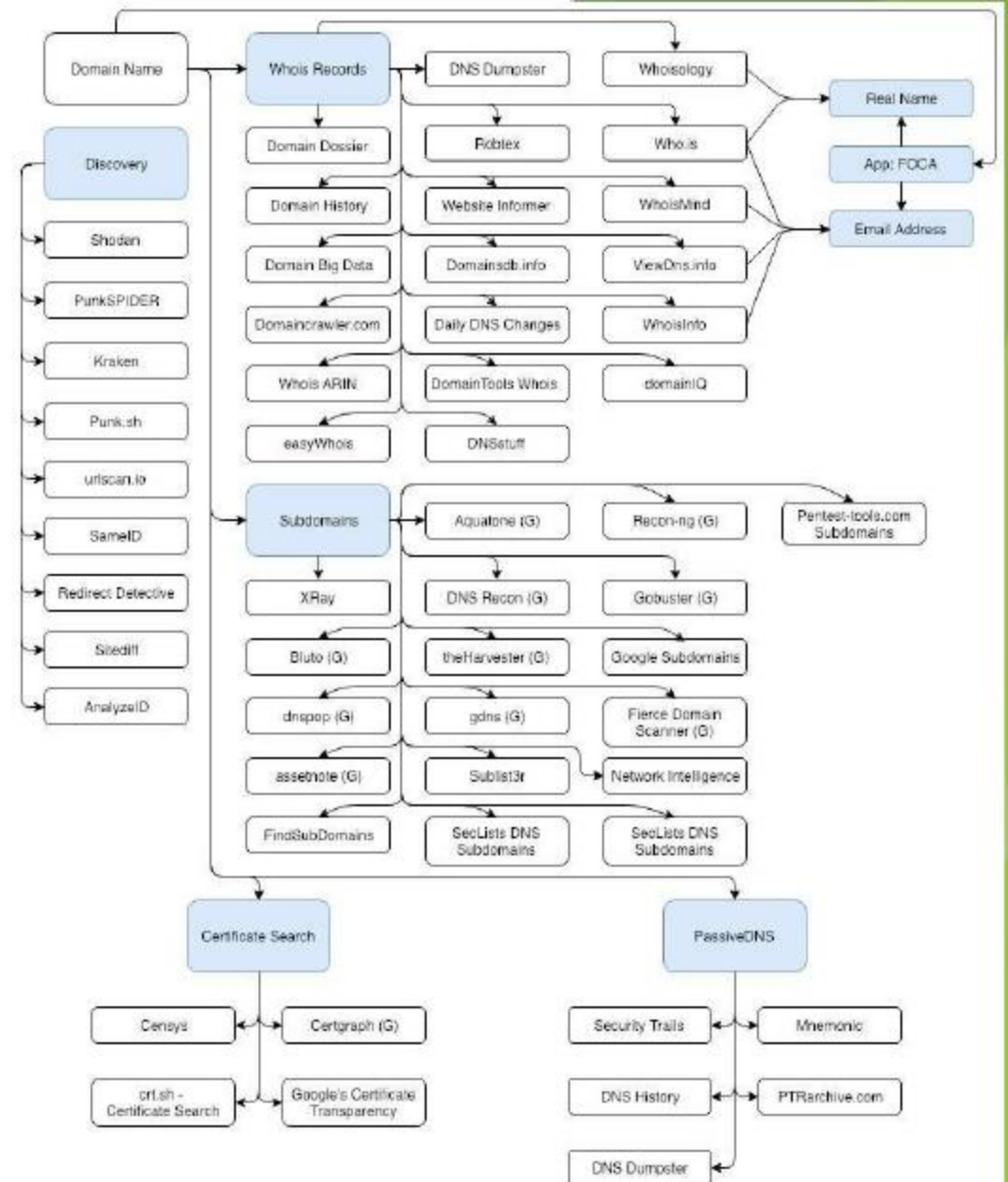
Fuente: [campusciberseguridad.com](http://campusciberseguridad.com)





# Flujo de investigación enfocado a pentesting

- Discovery
- Nombre de dominio
  - Registros whois
  - Subdominios
  - Certificados
  - Registros DNS
- Etc...



Fuente: [osint.thegelios.com](https://osint.thegelios.com)



# Analizando organizaciones (ciberseguridad)

- Nombre de dominio
- Archivos
- Exploits
- Etc...



# TOP herramientas OSINT para ciberseguridad

- ❑ OSINT Framework
- ❑ Google Dorks
- ❑ Maltego
- ❑ The Harvester
- ❑ Exiftool
- ❑ Etc...



# Colección de herramientas OSINT Framework desde MALTEGO

- Email
- Infraestructuras de redes
- Imágenes y documentos
- Registros de empresas
- Motores de búsqueda
- Histórico de sitios web
- Análisis de archivos y urls maliciosos
- Exploits
- Inteligencia de amenazas
- Etc...



# GOOGLE DORKS - Búsqueda avanzada (1)



## Tipos de búsqueda

- ☐ De concordancia exacta
- ☐ Mediante comodines o términos desconocidos
- ☐ Combinación de búsquedas
- ☐ Resultados de un dominio concreto
- ☐ Término concreto en el título de una página
- ☐ Cadena de texto en una dirección URL
- ☐ Cadena de texto en una página web
- ☐ Buscar en el cache de Google
- ☐ Información sobre un sitio web
- ☐ Obtener páginas con un determinado link
- ☐ Etc...

Fuente: [campusciberseguridad.com](http://campusciberseguridad.com)

Google es probablemente el buscador generalista más potente, pero la cantidad de resultados se puede volver inmanejable si no acotamos bien las búsquedas. Los principales operadores de búsqueda que un analista debe manejar son los siguientes:

- Para buscar una concordancia exacta:  
"ElevenPaths, la unidad de ciberseguridad de Telefónica"
- Para buscar mediante comodines o términos desconocidos:  
"ElevenPaths, la \* de Telefónica"
- Para combinar búsquedas:  
"ElevenPaths" OR "Chema Alonso"
- Para determinadas palabras incluidas en la misma página:  
"ElevenPaths" AND "Chema Alonso"
- Para que se muestren solamente los resultados de un dominio concreto:  
site:elevenpaths.com
- Para buscar un término o palabra clave en el título de la página, es decir, entre los tags <title> y </title> del código HTML:  
intitle:"ElevenPaths"
- Para buscar una cadena de texto únicamente dentro de la dirección URL:  
inurl:"profiles.php"
- Para buscar una cadena específicamente en la parte del texto de una página web:  
intext:"Kevin Mitnick"
- Para buscar sobre la versión en caché de Google sin necesidad de conectarse a dicha web:  
cache:elevenpaths.com
- Para obtener información sobre un sitio web:  
info:elevenpaths.com
- Para obtener páginas que tienen un determinado link:  
link:[www.elevenpaths.com](http://www.elevenpaths.com)



# GOOGLE DORKS - Búsqueda avanzada (1)

OPERADOR	UTILIDAD	Ejemplo
<code>" "</code>	Búsqueda con coincidencia exacta	«Derechodelared»
<code>site:</code>	Busca en el sitio web especificado en concreto	site:derechodelared.com
<code>filetype:</code>	Busca resultados que tienen la extensión de archivo especificada (pdf,txt,xls,...)	filetype:pdf
<code>ext:</code>	Misma utilidad que filetype	ext:pdf
<code>inurl:</code>	Busca la palabra especificada en una URL	inurl:dorking
<code>intext:</code>	Resultados con páginas en cuyo contenido aparece la palabra especificada	intext:dorking
<code>intitle:</code>	Resultados con páginas en cuyo título aparece la palabra especificada	intitle:dorking
<code>allinurl:</code>	Busca todas las palabras especificadas en una URL	allinurl:Google Dorks
<code>allintext:</code>	Resultados con páginas en cuyo contenido aparecen todas las palabras especificadas	allintext:Google Dorks
<code>allintitle:</code>	Resultados con páginas en cuyo título aparecen todas las palabras especificadas	allintitle:Google Dorks
<code>-</code>	Simbolo de exclusion, se excluirá de los resultados lo que vaya a continuación de el	dorking -Google
<code>*</code>	Se usa como comodín, el asterisco representa que puede ser sustituido por cualquier palabra	site:*.ejemplo.com
<code>cache:</code>	Mostrará la versión en caché de la web en cuestión	cache:derechodelared.com
<code>OR</code>	Operador lógico, también se puede representar por	ext:pdf OR ext:txt
<code>AND</code>	Operador lógico, normalmente se deja el espacio en blanco	Google AND Bing

# GOOGLE DORKS - Búsqueda avanzada (2)

## Otros tipos de búsqueda

- Por extensión de archivo
- Para negar un determinado operador
- Para buscar fuentes parecidas

## Colección de búsquedas compartida entre usuarios



- Para buscar por extensión de archivo:  
`ext:pdf`
- Para negar un determinado operador:  
`-ext:pdf`
- Para buscar fuentes parecidas:  
`related:elevenpaths.com`

Adicionalmente, existe un proyecto que nació ya hace algunos años llamado **Google Hacking DataBase** donde la gente comparte búsquedas avanzadas para conseguir determinada información. Se puede acceder a los contenidos desde la propia página de Exploit-DB (<https://www.exploit-db.com/google-hacking-database/>)



# Herramientas

## Mail

ProtonMail

## SMS

afreesms.com

## Tarjetas de Crédito

[Herramientas-online.com/generador-tarjeta-credito-cvv.php](https://herramientas-online.com/generador-tarjeta-credito-cvv.php)  
[Generadordetarjetas.org](https://generadordetarjetas.org)

## Fotos:

App.generative.photos



# Herramientas

## Auditoria

Tails (es un sistema operativo portátil que te protege de la vigilancia y la censura)

## Analisis vulnerabilidades:

Robtex

Viewdns.info

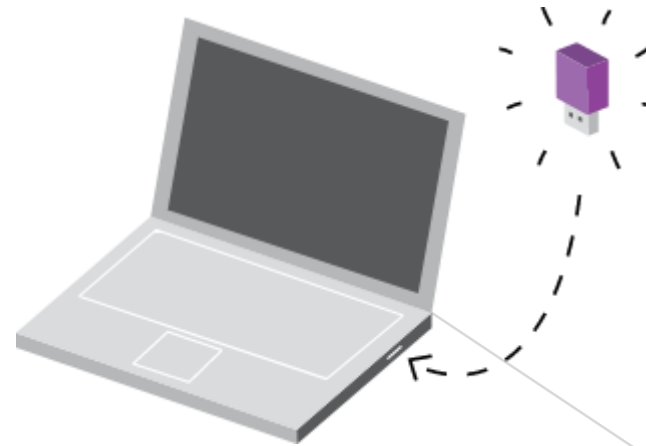
## VPN

Vpsserver.com

VPSbitcoin

## Web

<https://pentest-tools.com/>



# Herramientas

## **Maltego:**

Transformaciones

.

## **Buscadores:**

Google, Bing, Shodan, Yandex Baidu, Google Hacking.

## **. Database:**

<http://netbootcamp.org/osinttools> Metadatos, Metagoofil, Foca, Visores de Exif

.

## **.Vulnerabilidades:**

CVE, CCE <https://nvd.nist.gov> <https://www.exploit-db.com/webapps>

## **. Reputación:**

Alexa, WOT.

## **Nombre usuario**

<https://whatsmyname.app/>



# Herramientas

## . SEO:

<https://moz.com/researchtools/ose>

<http://explorer.cognitiveseo.com>

<https://es.majestic.com>

Domain tolos

## .Correos:

The harvester.

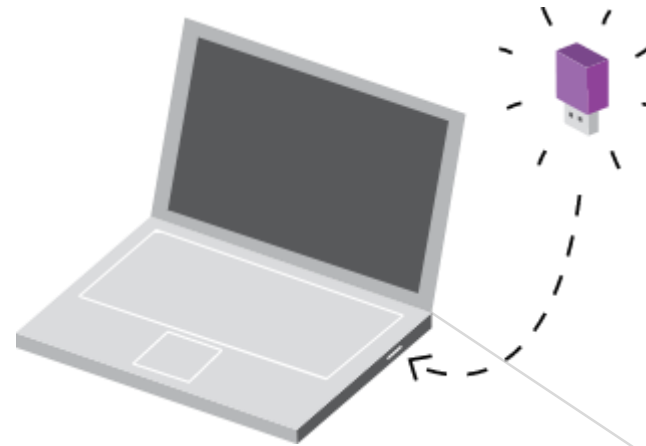
## . Información Geográfica y a pie de calle:

Google Maps, Bing Maps.

## . Información Personal:

<http://www.pipl.com> y <http://www.peakyou.com>

## .Listines telefónicos



# Herramientas

Busqueda por nombre en RRSS

Lullar

The screenshot displays the Lullar tool interface. At the top, there is a search bar with the text 'alvarobadia' and a magnifying glass icon. To the right of the search bar is a dropdown menu set to 'All'. Below the search bar, the status 'Found: 14 Processed: 385 / 383' is shown, along with three buttons: 'Show All', 'Show Found', and 'Show Not Found'. The main area is a grid of 16 green boxes, each representing a found account. Each box contains the platform name, the category, and the status 'Account Found'. The platforms and categories are as follows:

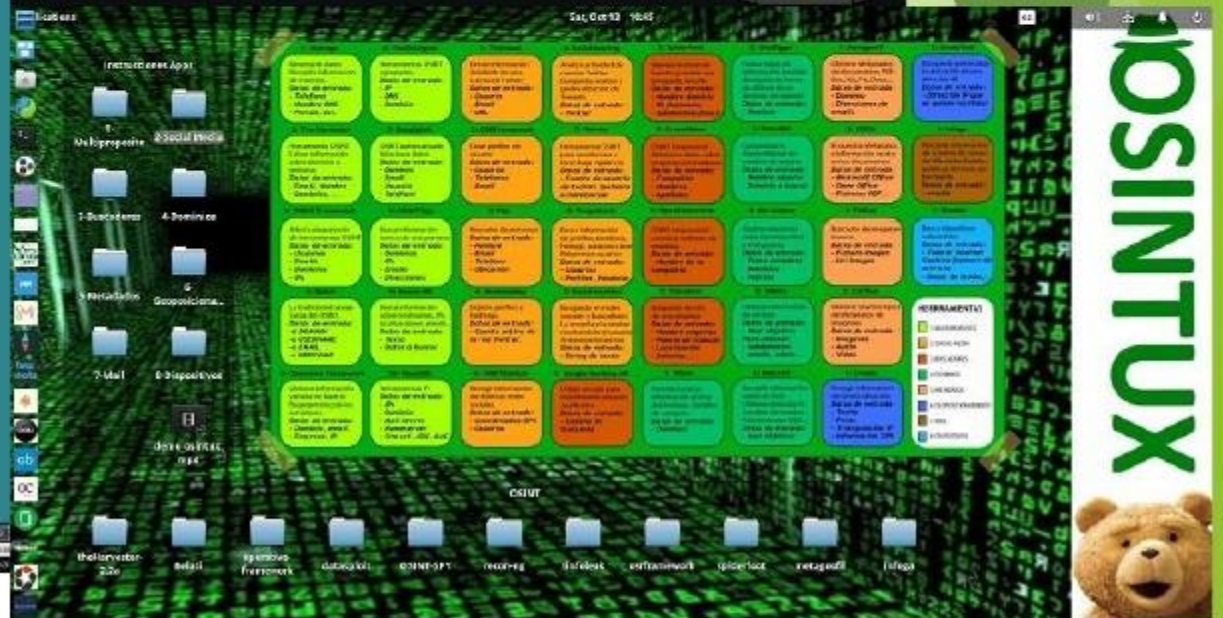
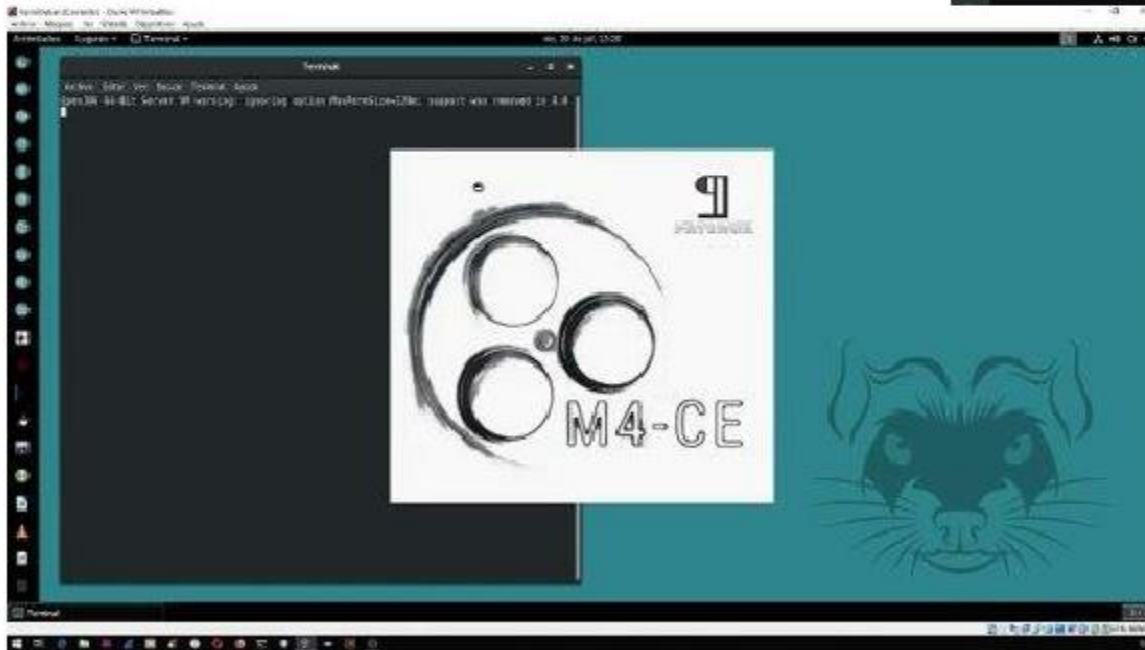
Platform	Category	Status
Snapshot	social	Account Found
MCUID (Minecraft)	gaming	Account Found
imgur	images	Account Found
waibad	social	Account Found
scratch	coding	Account Found
GitLab	coding	Account Found
Gravatar	images	Account Found
idoshare	social	Account Found
DeviantArt	images	Account Found
TikTok	social	Account Found
GitHub	coding	Account Found
smule	music	Account Found
Roblox	gaming	Account Found
Fortnite Tracker	gaming	Account Found

On the right side, there is a 'Found Accounts' section with buttons for 'Copy', 'Export', 'CSV', and 'PDF'. Below these buttons is a search bar. A table lists the found accounts with columns for 'SITE', 'CATEGORY', and 'LINK'.

SITE	CATEGORY	LINK
DeviantArt	images	<a href="https://www.deviantart.com/alvarobadia">https://www.deviantart.com/alvarobadia</a>
Fortnite Tracker	gaming	<a href="https://fortnitracker.com/profile/alvarobadia">https://fortnitracker.com/profile/alvarobadia</a>
GitHub	coding	<a href="https://github.com/alvarobadia">https://github.com/alvarobadia</a>
GitLab	coding	<a href="https://gitlab.com/alvarobadia">https://gitlab.com/alvarobadia</a>
Gravatar	images	<a href="http://en.gravatar.com/profile/alvarobadia">http://en.gravatar.com/profile/alvarobadia</a>
imgur	images	<a href="https://api.imgur.com/account/v1/ac">https://api.imgur.com/account/v1/ac</a>
MCUID (Minecraft)	gaming	<a href="https://playerto.co/api/player/minec">https://playerto.co/api/player/minec</a>
Roblox	gaming	<a href="https://auth.roblox.com/v1/username">https://auth.roblox.com/v1/username</a>
scratch	coding	<a href="https://scratch.mit.edu/users/alvarobadia">https://scratch.mit.edu/users/alvarobadia</a>
idoshare	social	<a href="https://www.idoshare.com/profile/alvarobadia">https://www.idoshare.com/profile/alvarobadia</a>

# Distros Linux OSINT

- ❑ Buscador — inteltechniques.com
- ❑ Huron - github.com/HuronOsint
- ❑ Osintux
- ❑ Etc...





# Distro Osintux

## Listado de herramientas instaladas

- Beati v0.2.4.1
- Creepy v1.4
- Crunchbase
- DataSploit for OSINT
- Dmitry (Deepmagic information gathering tool)
- Exiftool v11.03
- Google Hacking Database
- Infoga - Email Information Gathering vM4110k
- GeolIP
- Glassdoor
- Knowem
- Maltego v4.1.6.11045
- MentionMap
- Metagoofil v2.2
- MrLooquer
- Netcraft
- Shodan
- Opencorporates
- Operative Framework
- OSINTSpy v0.0.1
- OSRFramework v2018
- OSINTFramework
- Pipl
- Recon-ng v4.9.3
- SocialBeering
- Socialmention
- SpiderFoot v2.12
- The Harvester v2.2a
- TinEye
- Tinfoleak v2.1
- Twopcharts
- ViewDNS
- YouGetSignal
- Whois

## Sobre la distribución Linux Osintux

Un poco de información sobre Osintux



OSINTUX es una distribución Linux en castellano, con base en Ubuntu LTS y distribuida bajo licencia "[GNU General Public License v3](#)" destinada a labores de inteligencia en fuentes abiertas (OSINT). El proyecto nació como consecuencia del trabajo fin de Máster del [Máster de Ciberseguridad](#), organizado por [Eleven Paths](#) (Telefonica), el Campus Internacional de Ciberseguridad, y la UCAM.

Los dos precursores del proyecto son:



[Pedro De La Torre Rodríguez](#), perito informático y emprendedor, colegiado 20090318-B en el [Colegio Profesional de Ingenieros Técnicos en Informática de Andalucía](#), especializado en proyectos tecnológicos, ciberseguridad y gestión de la innovación.



[Manuel Torres Martínez](#), consultor TIC y auditor de seguridad informática, colegiado 20150225-A en el [Colegio Profesional de Ingenieros Técnicos en Informática de Andalucía](#). En continua búsqueda e investigación de los factores que intervienen en la mejora de la implantación de procesos seguros en la empresa.

# Categorías de herramientas Osintux

- ❑ Multi propósito
- ❑ Social media
- ❑ Buscadores
- ❑ Dominios
- ❑ Metadatos
- ❑ Geoposicionamiento
- ❑ Mail
- ❑ Dispositivos
- ❑ Etc...

<b>1: Maltego</b> Minería de datos Recopila información de Internet. <b>Datos de entrada:</b> - Telefono - Nombre DNS - Person, ect.	<b>6: YouGetSignal</b> Herramientas OSINT agrupadas. <b>Datos de entrada:</b> - IP - DNS - Dominio	<b>1: Tinfoleak</b> Extrae información detallada de una cuenta de Twitter <b>Datos de entrada:</b> - Usuario - Email - URL	<b>6: SocialBearing</b> Analiza actividad de cuentas Twitter, búsqueda, análisis y geolocalización de Tweets. <b>Datos de entrada:</b> - Twitter	<b>2: Spiderfoot</b> Agrega multitud de fuentes y realiza una búsqueda sencilla <b>Datos de entrada:</b> - Nombre dominio - IP, Hostname - Subdominio, Email	<b>2: SiteDigger</b> Evalúa fugas de información sensible divulgada de forma accidental de un dominio de Internet <b>Datos de entrada:</b> - Dominio	<b>1: Metagoofil</b> Obtiene Metadatos de documentos PDF, Doc, Xls, Ppt, Docx... <b>Datos de entrada:</b> - Dominio - Direcciones de email	<b>2: Geoiptool</b> Búsqueda geolocaliza la ubicación de una dirección IP. <b>Datos de entrada:</b> - Dirección IP que se quiere localizar
<b>2: The Harvester</b> Herramienta OSINT Extrae información sobre dominio o persona. <b>Datos de entrada:</b> - Email, Nombre - Dominios, ...	<b>7: DataSploit</b> OSINT automatizado Relaciona datos <b>Datos de entrada:</b> - Dominio - Email - Usuario - Teléfono	<b>2: OSRFramework</b> Crear perfiles de usuario. <b>Datos de entrada:</b> - Usuarios - Telefonos - Email	<b>7: Harvey</b> Herramienta OSINT para monitorizar y tener bajo vigilancia <b>Datos de entrada:</b> - Cuenta de usuario de twitter /palabra a monitorizar	<b>3: Crunchbase</b> OSINT Empresarial Almacena datos sobre empresas innovadoras <b>Datos de entrada:</b> - Compañías - Open Office - Apellidos	<b>3: KnowEm</b> Comprobar la disponibilidad de nombre de usuario <b>Datos de entrada:</b> - Nombre usuario - Dominio a buscar	<b>2: FOCA</b> Encuentra Metadatos e información oculta en los documentos <b>Datos de entrada:</b> - Microsoft Office - Open Office - Ficheros PDF...	<b>1: Infoq</b> Recopila información de cuentas de correo de diferentes fuentes públicas. Motores de búsqueda. <b>Datos de entrada:</b> - emails
<b>3: OSINT Framework</b> Arbol categorizado de herramientas OSINT <b>Datos de entrada:</b> - Usuarios - Emails - Dominios - IPs	<b>8: OSINT Spy</b> Busca información acerca de una persona <b>Datos de entrada:</b> - Dominios - IPs - Emails - Direcciones	<b>3: Pipi</b> Buscador de personas <b>Datos de entrada:</b> - Nombre - Email - Telefono - Ubicación	<b>8: Twopcharts</b> Busca información de perfiles, timelines, hashtags, palabras clave Relaciones usuarios <b>Datos de entrada:</b> - Usuarios - Perfiles, Palabras	<b>4: OpenCorporates</b> OSINT empresarial contiene millones de empresas <b>Datos de entrada:</b> - Nombre de la compañía.	<b>4: MrLooquer</b> Analiza relaciones entre Dominios IPv4 y IPv6-puerto <b>Datos de entrada:</b> - Texto completo - Dominios - Puertos	<b>1: TinEye</b> Buscador de imágenes inverso. <b>Datos de entrada:</b> - Fichero Imagen - Uri imagen	<b>1: Shodan</b> Busca dispositivos vulnerables. <b>Datos de entrada:</b> - Todo el internet - Captura banners de servicio. - Datos de SCADA...
<b>4: Belati</b> La tradicional navaja Suiza del OSINT. <b>Datos de entrada:</b> -d DOMAIN -u USERNAME -e EMAIL -c ORGCOMP	<b>9: Recon-NG</b> Busca información sobre hostnames, IPs, localizaciones, emails... <b>Datos de entrada:</b> - Texto - Datos a buscar	<b>4: MentionMap</b> Explora perfiles y hashtags. <b>Datos de entrada:</b> - Cuenta activa de la red Twitter.	<b>9: Socialmention</b> Búsqueda en redes sociales y buscadores. La recopila y la analiza mostrándole al usuario Análisis sentimientos <b>Datos de entrada:</b> - String de texto	<b>5: Glassdoor</b> Búsqueda de info de una empresa <b>Datos de entrada:</b> - Nombre empresa - Puesto de trabajo - Localización - Salarios, ...	<b>5: DMitry</b> Obtiene información de un host <b>Datos de entrada:</b> - Host objetivo Para obtener: - Subdominios - emails, whois...	<b>2: ExifTool</b> Obtiene muchos tipos de Metadatos de imágenes <b>Datos de entrada:</b> - Imágenes - Audio - Video	<b>HERRRAMIENTAS</b> 1: MULTIPROPOSITO 2: SOCIAL MEDIA 3: BUSCADORES 4: DOMINIOS 5: METADATOS 6: GEOPOSICIONAMIENTO 7: MAIL 8: DISPOSITIVOS
<b>9: Operative Framework</b> Obtiene información variada en base al fingerprinting de los servidores. <b>Datos de entrada:</b> - Dominio, email. - Empresa, IP.	<b>10: ViewDNS</b> Herramientas IP <b>Datos de entrada:</b> - IPs - Dominio - Mail server - Nameserver - Site url, ASN, MAC	<b>5: OSINTstalker</b> Recoge información de distintas redes sociales. <b>Datos de entrada:</b> - Coordenadas GPS - Usuarios	<b>1: Google Hacking DB</b> Utiliza Google para implementar ataques /auditorías <b>Datos de entrada:</b> - Cadena de búsqueda	<b>1: Whois</b> Permite conocer información acerca del dominio. Detalles de contacto. <b>Datos de entrada:</b> - Dominios	<b>6: Netcraft</b> Recopila información sobre un host. Obtiene dirección IP, Servidor de nombre, Administrador DNS. <b>Datos de entrada:</b> - host objetivo	<b>1: Creepy</b> Recoge información de Geolocalización. <b>Datos de entrada:</b> - Twits - Fotos - Triangulación IP - Información GPS	

OSINTUX

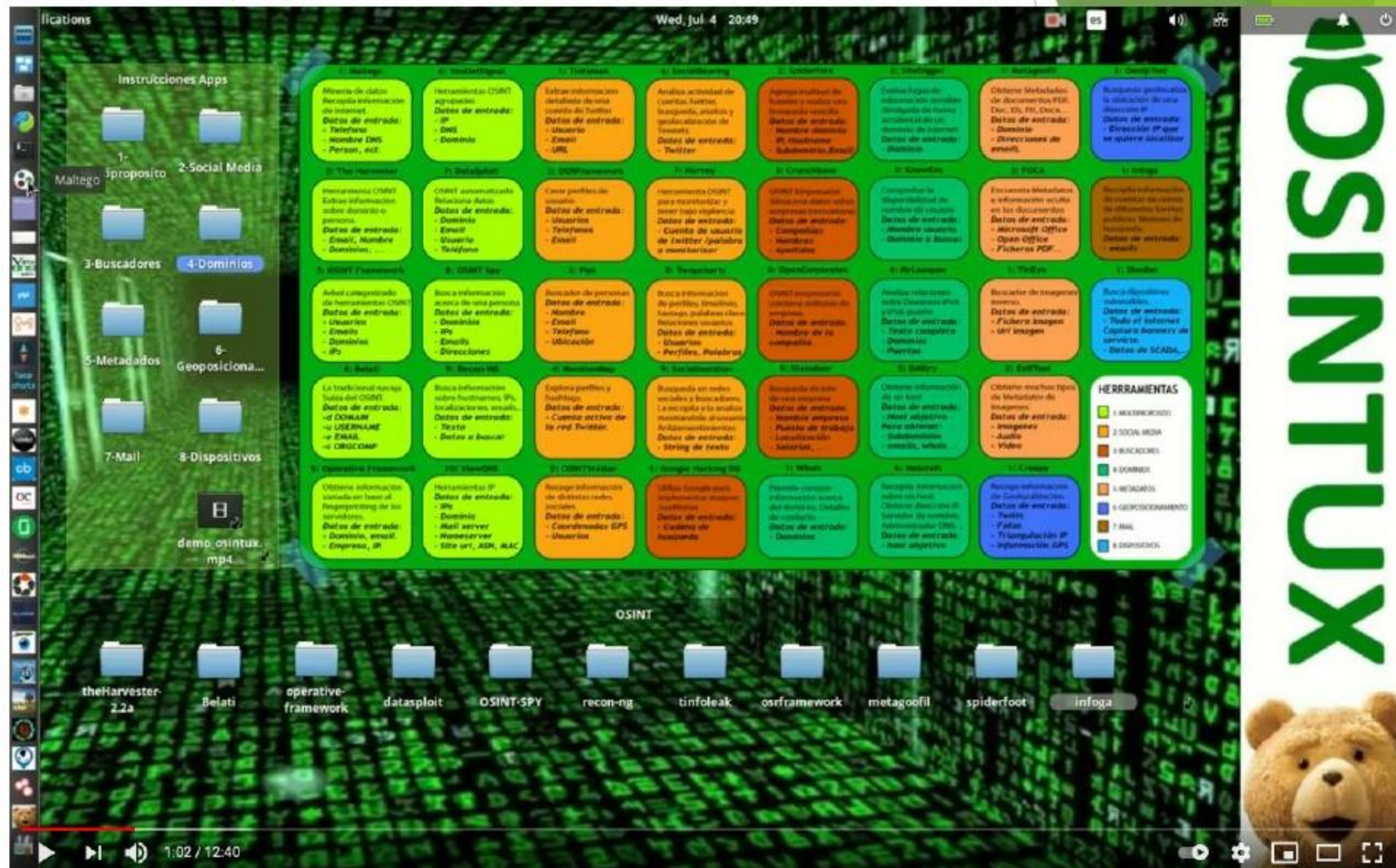




# Distro Osintux

## Listado de herramientas instaladas (v1.0)

- [Belati v0.2.4.1](#)
- [Creepy v1.4](#)
- [Crunchbase](#)
- [Datasploit for OSINT](#)
- [Dmitry \(Deepmagic information gathering tool\)](#)
- [Exiftool v11.03](#)
- [Google Hacking Database](#)
- [Infoga - Email information Gathering vM4110k](#)
- [GeolIP](#)
- [Glassdoor](#)
- [Knowem](#)
- [Maltego v4.1.6.11045](#)
- [MentionMap](#)
- [Metagoofil v2.2](#)
- [Mri\\_oocker](#)
- [Netcraft](#)
- [Shodan](#)
- [Opencorporates](#)
- [Operative Framework](#)
- [OSINT-Spy v0.0.1](#)
- [OSRFramework v2016](#)
- [OSINTFramework](#)
- [PIPL](#)
- [Recon-NG v4.9.3](#)
- [SocialBearing](#)
- [Socialmention](#)
- [SpiderFoot v2.12](#)
- [The Harvester v2.2a](#)
- [Tineye](#)
- [Tinfoleak v2.1](#)
- [Twopcharts](#)
- [ViewDNS](#)
- [YouGetSignal](#)
- [Whois](#)





# Ejemplo de investigación de imágenes fake

## A la caza de fake news

El día 30 de octubre el conseller de la Generalitat Josep Rull se presentó en su despacho de la Generalitat de Cataluña y se tomó una famosa imagen trabajando. ¿Qué aspectos de la imagen te llaman más la atención? ¿Qué elementos han sido más probablemente manipulados?

Fuente: campusciberseguridad.com



# Ejemplo de investigación de imágenes fake

## Fotoforensics

Si utilizamos la herramienta online FotoForensics podemos apreciar que los dos mapas de Bélgica muestran una luminancia distinta a la del resto de la foto.





# Ejemplo de investigación de imágenes fake

## Google imágenes

Si utilizamos la herramienta de búsqueda inversa de imágenes de Google podemos localizar la imagen real y verificar que los mapas de Bélgica fueron puestos después en la foto.



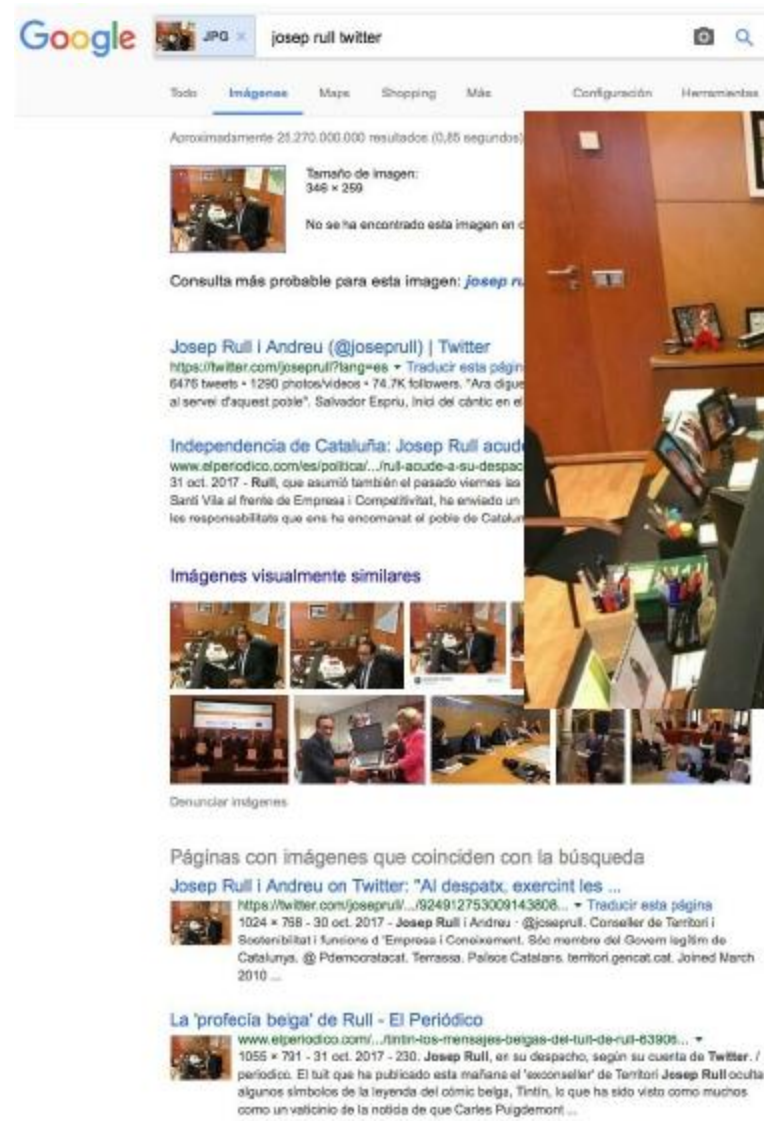
//pbs.twimg.com/media/DNZWRSSWsAAMW5.jpg:large



Buscar por imagen

#YouTubeRewind: celebremos los vídeos, la música y las personas que marcaron el 2017.

<http://www.elperiodico.com/es/politica/20171030/tin-tin-los-mensajes-belgas-del-tuit-de-rull-6390691>



# Repositorio de herramientas OSINT

Recurso	Dirección URL				
Abiword	<a href="https://www.abisource.com/">https://www.abisource.com/</a>	I2P	<a href="https://geti2p.com">https://geti2p.com</a>	SocialBearing	<a href="https://socialbearing.com">https://socialbearing.com</a>
Ahmia	<a href="https://ahmia.fi">https://ahmia.fi</a>	IP-API	<a href="https://ip-api.com">https://ip-api.com</a>	Tails	<a href="https://tails.boum.org">https://tails.boum.org</a>
Archive.is	<a href="https://archive.is">https://archive.is</a>	IP2Location	<a href="https://ip2location.com">https://ip2location.com</a>	Tesseract	<a href="https://github.com/tesseract-ocr">https://github.com/tesseract-ocr</a>
Baidu	<a href="https://baidu.com">https://baidu.com</a>	Ifconfig.co	<a href="https://ifconfig.co">https://ifconfig.co</a>	Telegram Purple	<a href="https://github.com/majin/telegram-purple">https://github.com/majin/telegram-purple</a>
Bing	<a href="https://bing.com">https://bing.com</a>	IPFS	<a href="https://ipfs.io">https://ipfs.io</a>	TheHarvester	<a href="https://github.com/laramies/theHarvester">https://github.com/laramies/theHarvester</a>
CaseFile	<a href="https://paterva.com">https://paterva.com</a>	Kali Linux	<a href="https://kali.org">https://kali.org</a>	TinEye	<a href="https://tineye.com">https://tineye.com</a>
DomainTools	<a href="https://domaintools.com">https://domaintools.com</a>	KeePass	<a href="https://keepass.info">https://keepass.info</a>	Tor Project	<a href="https://torproject.org">https://torproject.org</a>
DuckDuckGo	<a href="https://duckduckgo.com">https://duckduckgo.com</a>	Kibana	<a href="https://www.elastic.co/products/logstash">https://www.elastic.co/products/logstash</a>	Tor2Web	<a href="https://www.tor2web.org/">https://www.tor2web.org/</a>
ElasticSearch	<a href="https://www.elastic.co/products/elasticsearch">https://www.elastic.co/products/elasticsearch</a>	Logstash	<a href="https://www.elastic.co/products/logstash">https://www.elastic.co/products/logstash</a>	Torch	<a href="http://xmh57jrzrnw6insl.onion/">http://xmh57jrzrnw6insl.onion/</a>
Evil FOCA	<a href="https://github.com/ElevenPaths/EvilFOCA">https://github.com/ElevenPaths/EvilFOCA</a>	Maltego	<a href="https://paterva.com">https://paterva.com</a>	Ubuntu	<a href="https://ubuntu.com">https://ubuntu.com</a>
Exiftool	<a href="http://search.cpan.org/~exiftool/">http://search.cpan.org/~exiftool/</a>	MrLooquer	<a href="https://mrlouquer.com">https://mrlouquer.com</a>	ViewDNS	<a href="https://viewdns.info">https://viewdns.info</a>
Flickr	<a href="https://flickr.com">https://flickr.com</a>	Namechk	<a href="https://namechk.com">https://namechk.com</a>	Virustotal	<a href="https://virustotal.com">https://virustotal.com</a>
FOCA	<a href="https://github.com/elevanpaths/FOCA">https://github.com/elevanpaths/FOCA</a>	OpenStreetMap	<a href="https://openstreetmap.org">https://openstreetmap.org</a>	VirtualBox	<a href="https://virtualbox.org">https://virtualbox.org</a>
GeoSocialFootprint	<a href="http://geosocialfootprint.com">http://geosocialfootprint.com</a>	OSRFramework	<a href="https://github.com/i3visio/osrframework">https://github.com/i3visio/osrframework</a>	Wayback Machine (archive.org)	<a href="https://archive.org">https://archive.org</a>
GOOCR	<a href="http://www-e.uni-magdeburg.de/jschulen/ocr/download.html">http://www-e.uni-magdeburg.de/jschulen/ocr/download.html</a>	Onion.link	<a href="https://onion.link">https://onion.link</a>	Whonix	<a href="https://www.whonix.org/">https://www.whonix.org/</a>
Google	<a href="https://google.com">https://google.com</a>	Onion.plus	<a href="https://onion.plus">https://onion.plus</a>	Wordreference	<a href="https://wordreference.com">https://wordreference.com</a>
Google Custom Search Engine	<a href="https://cse.google.com">https://cse.google.com</a>	Pidgin	<a href="https://pidgin.im">https://pidgin.im</a>	Yacy	<a href="https://yacy.net">https://yacy.net</a>
Google Hacking Database	<a href="https://www.exploit-db.com/google-hacking-database/">https://www.exploit-db.com/google-hacking-database/</a>	PIVPN	<a href="https://pivpn.io">https://pivpn.io</a>	Yandex	<a href="https://yandex.com">https://yandex.com</a>
Google Imágenes	<a href="https://images.google.com">https://images.google.com</a>	ProtonVPN	<a href="https://www.protonvpn.com">https://www.protonvpn.com</a>	Yandex Imágenes	<a href="https://images.yandex.com">https://images.yandex.com</a>
Google Maps	<a href="https://maps.google.com">https://maps.google.com</a>	Qubes OS	<a href="https://www.qubes-os.org/">https://www.qubes-os.org/</a>	Zoomeye	<a href="https://zoomeye.com">https://zoomeye.com</a>
Grok Debugger	<a href="https://grokdebug.herokuapp.com/">https://grokdebug.herokuapp.com/</a>	Quora	<a href="https://quora.com">https://quora.com</a>		
HavelBeenPwned	<a href="https://haveibeenpwned.com">https://haveibeenpwned.com</a>	Reddit	<a href="https://reddit.com">https://reddit.com</a>		
HeSidoHackeado	<a href="https://hesidohackeado.es">https://hesidohackeado.es</a>	Regexper	<a href="https://regexper.com">https://regexper.com</a>		
		Searx	<a href="https://searx.me">https://searx.me</a>		
		Shodan	<a href="https://shodan.io">https://shodan.io</a>		