

OSINT

Open-Source INTElligence

INTRODUCCIÓN A LA INTELIGENCIA EN FUENTES ABIERTAS



OSINTUX



presentación

Manuel Torres Martínez,

Perito informático,

colegiado 20150225-A en el [Colegio Profesional de Ingenieros Técnicos en Informática de Andalucía](#),

Máster en Ciberseguridad

organizado por [Eleven Paths](#) (Telefónica), el Campus Internacional de Ciberseguridad, y la [UCAM](#)

Pedro De La Torre Rodríguez,

CEO de Indalics Peritos Informáticos,

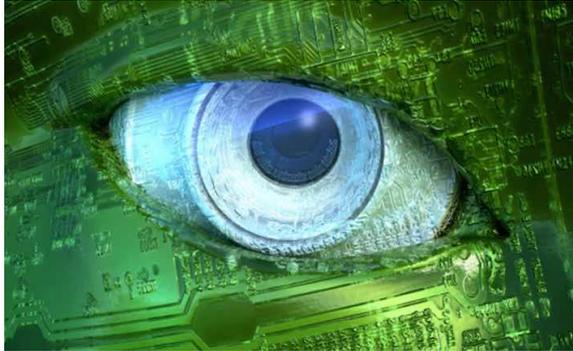
colegiado 20090318-B en el [Colegio Profesional de Ingenieros Técnicos en Informática de Andalucía](#),

Máster en Ciberseguridad

organizado por [Eleven Paths](#) (Telefónica), el Campus Internacional de Ciberseguridad, y la [UCAM](#)

«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.

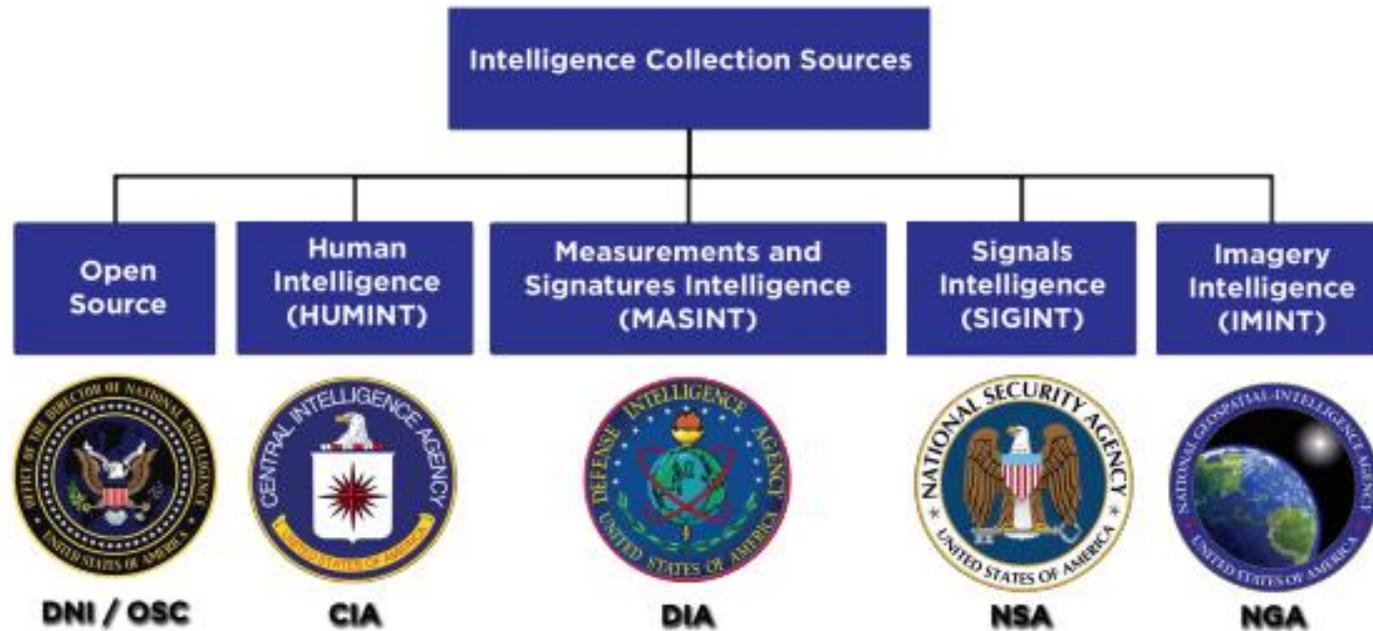


Inteligencia

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

Detectigal.com

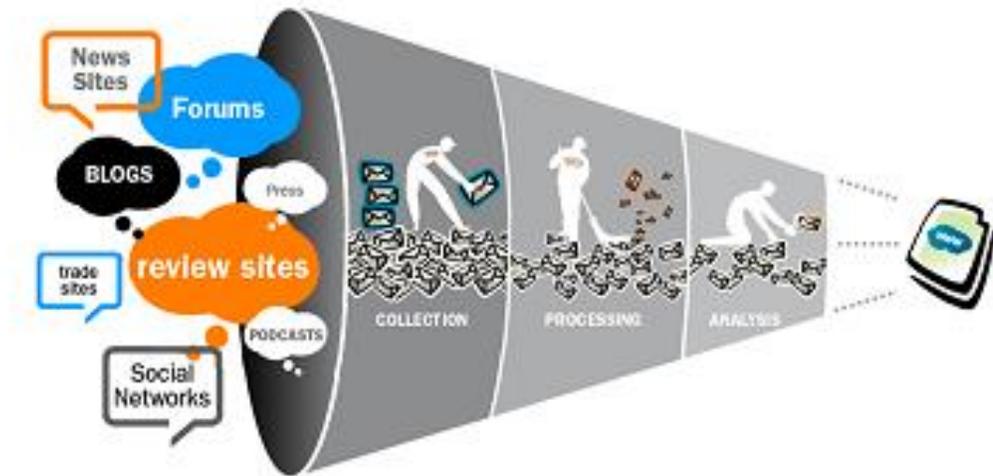
Colección de fuentes de inteligencia



- ▶ 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



Principales registros públicos

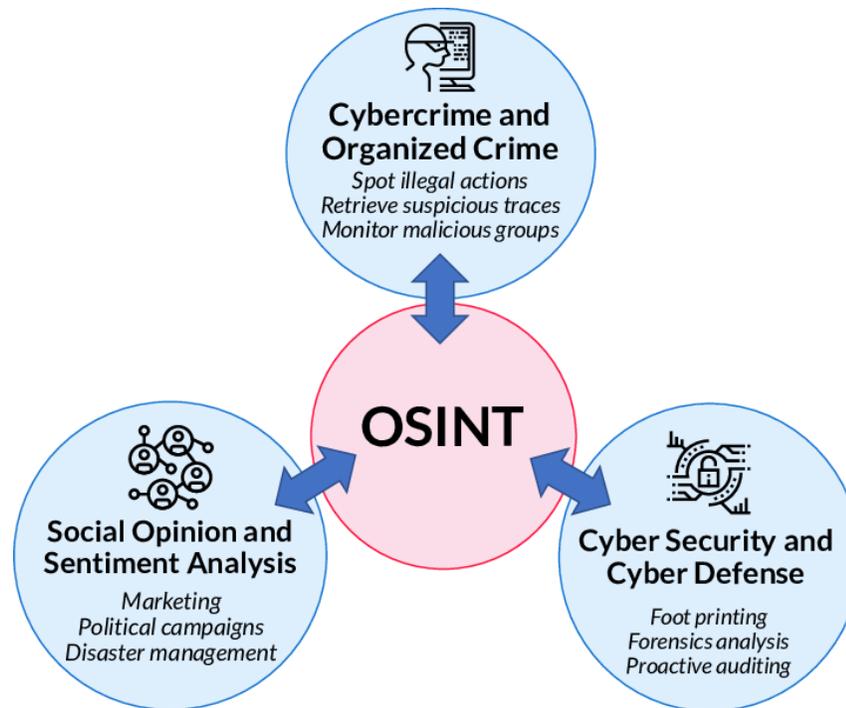
- ▶ Registros de propiedades
- ▶ Registros criminales
- ▶ Registros gubernamentales
- ▶ Registros financieros
- ▶ Registros de votantes
- ▶ Registros de patentes
- ▶ Registros de nacimientos
- ▶ Registros políticos
- ▶ Etc...



PRINCIPALES CASOS DE USO

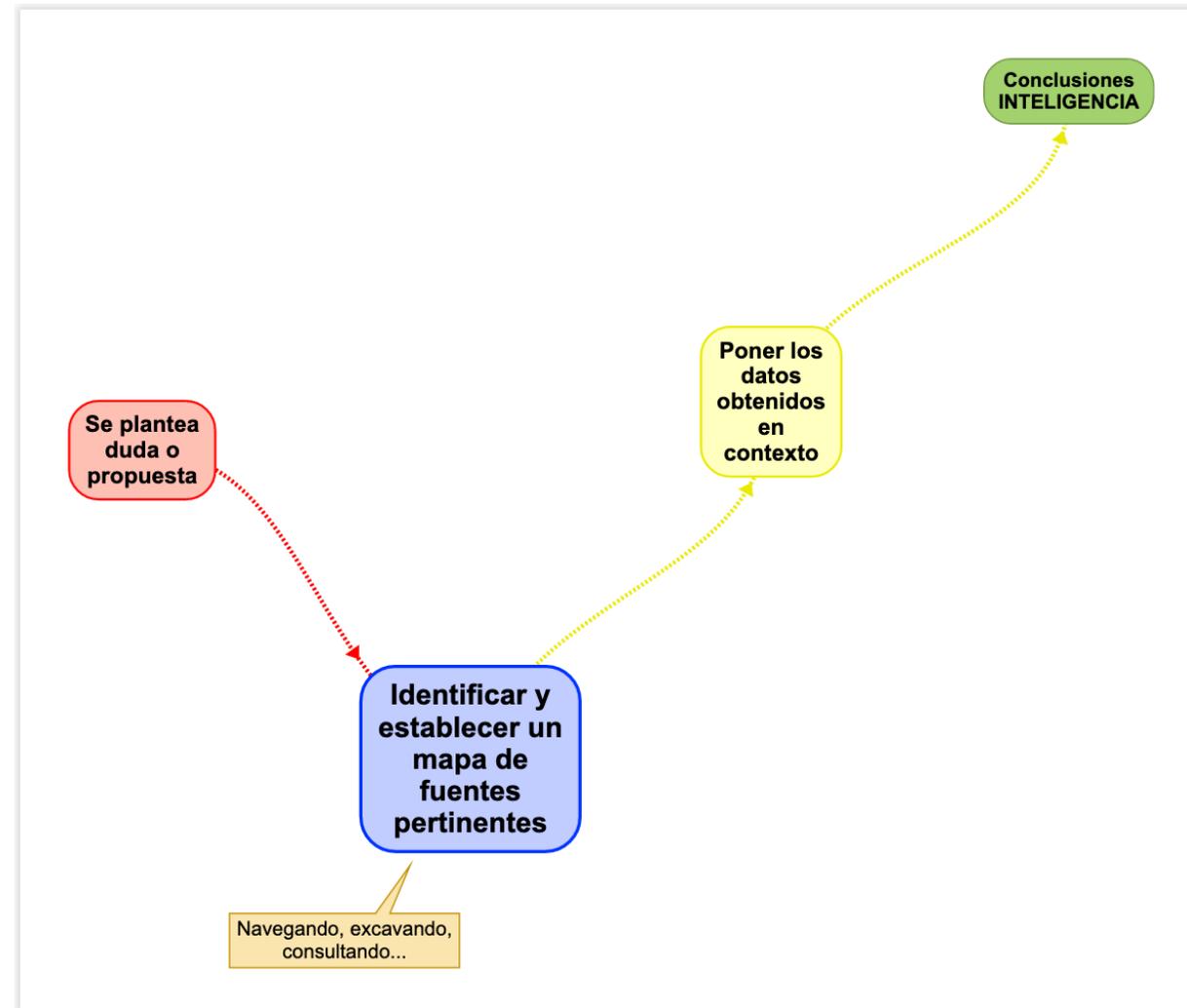
Podemos obtener información para resolver posibles casos de:

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



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

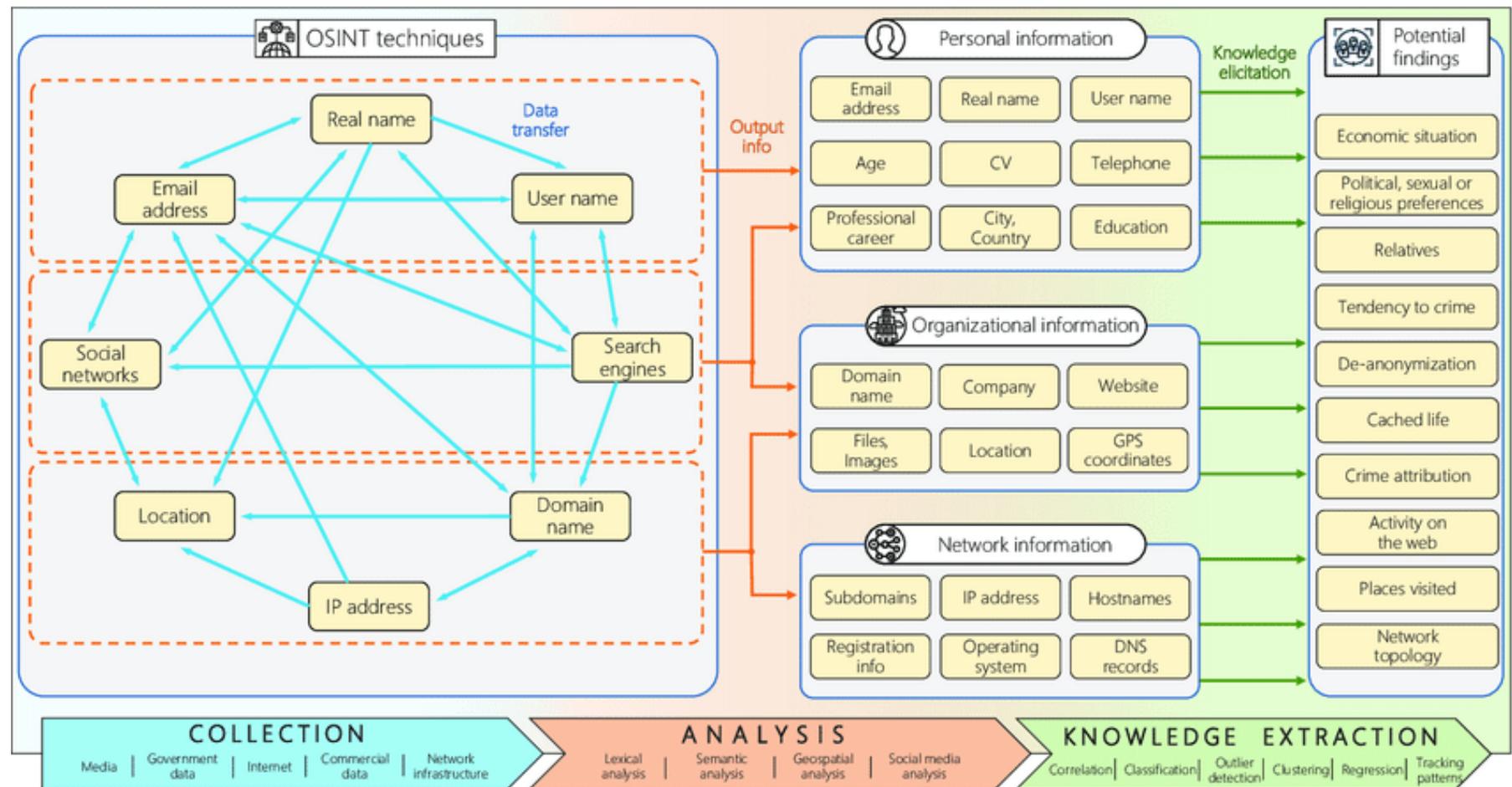
- ▶ 1. Establecer los requisitos
- ▶ 2. Concretar las Fuentes de información
- ▶ 3. Adquisición de la información
- ▶ 4. Procesamiento y formateo
- ▶ 5. Análisis y relación de los datos
- ▶ 6. Inteligencia. Presentación del informe con los datos pertinentes.



Fuente: hackers4fun.com

Fases de investigación en OSINT

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

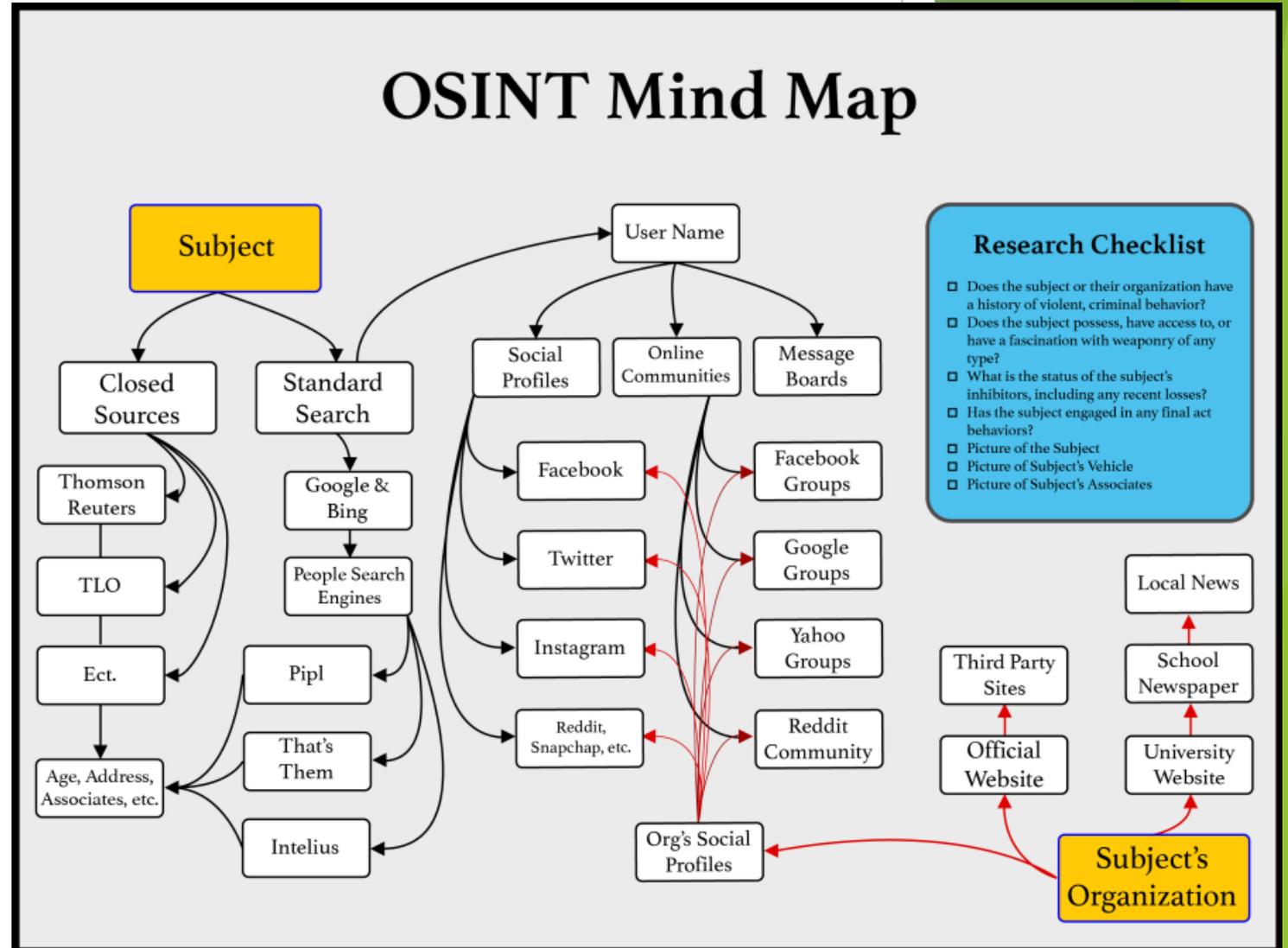


Mapa mental (Ejemplo de investigación)

► 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

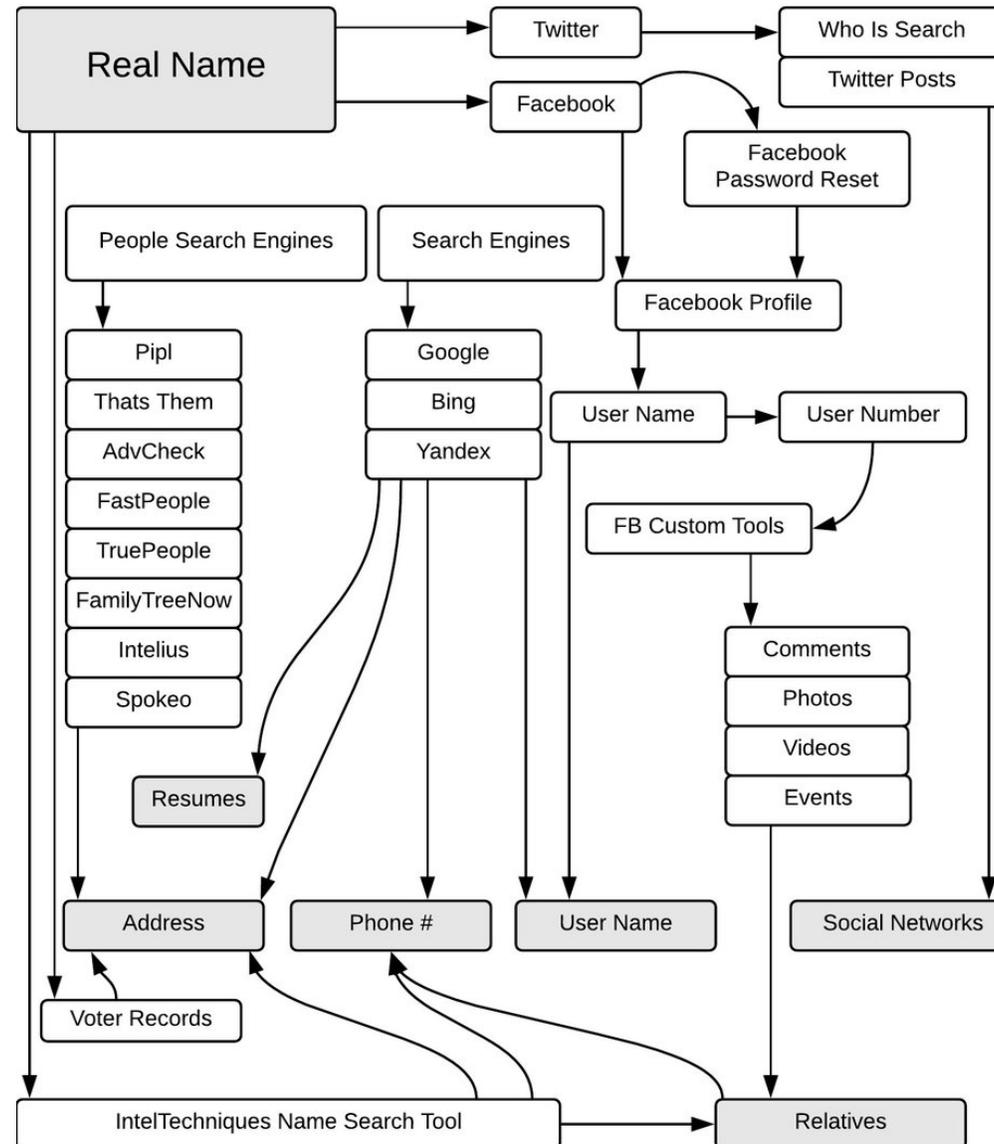


Investigación de perfiles digitales

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

Fuente: inteltechniques.com

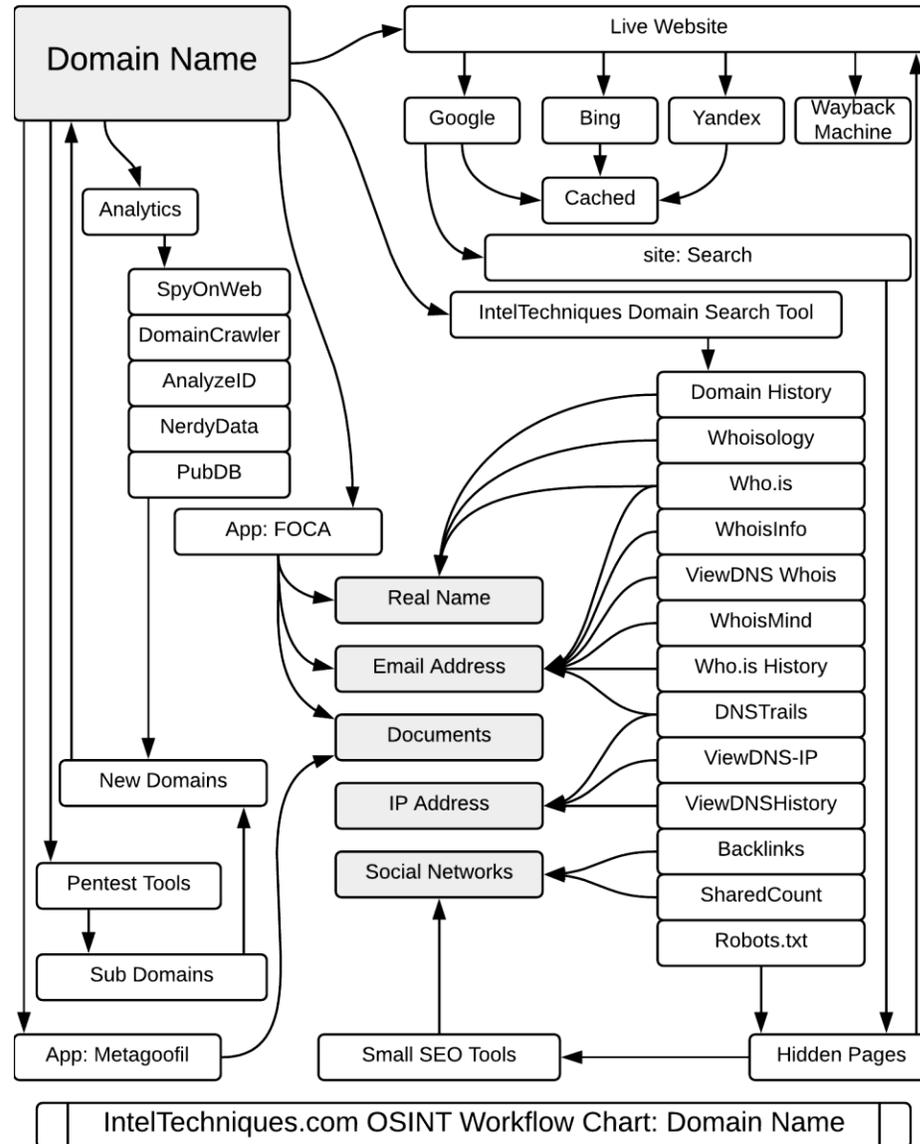
Inteltechniques - Michael Bazzell
(consultor de seguridad y ex agente e investigador del Grupo de Trabajo de Delitos Cibernéticos del FBI)



Investigación de perfiles digitales

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

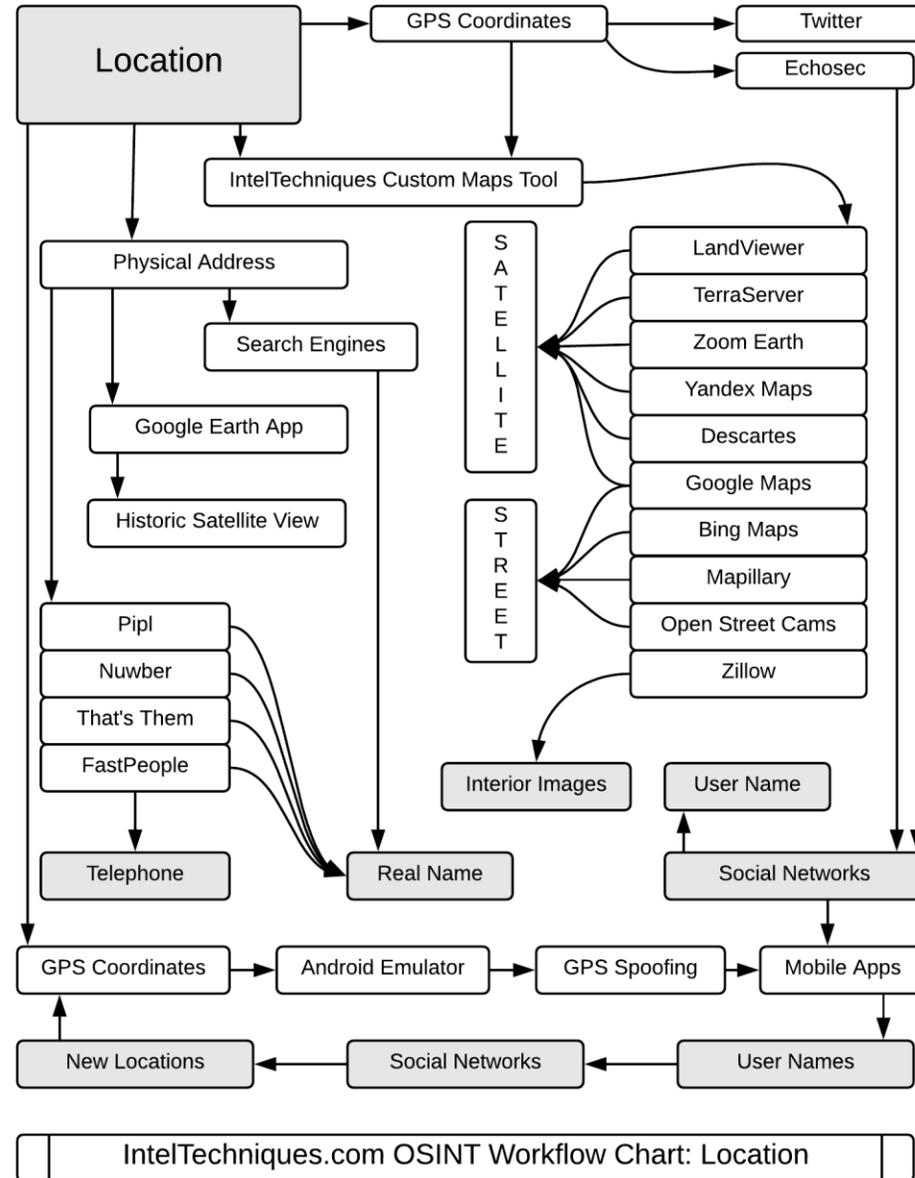
Fuente: inteltechniques.com



Investigación de perfiles digitales

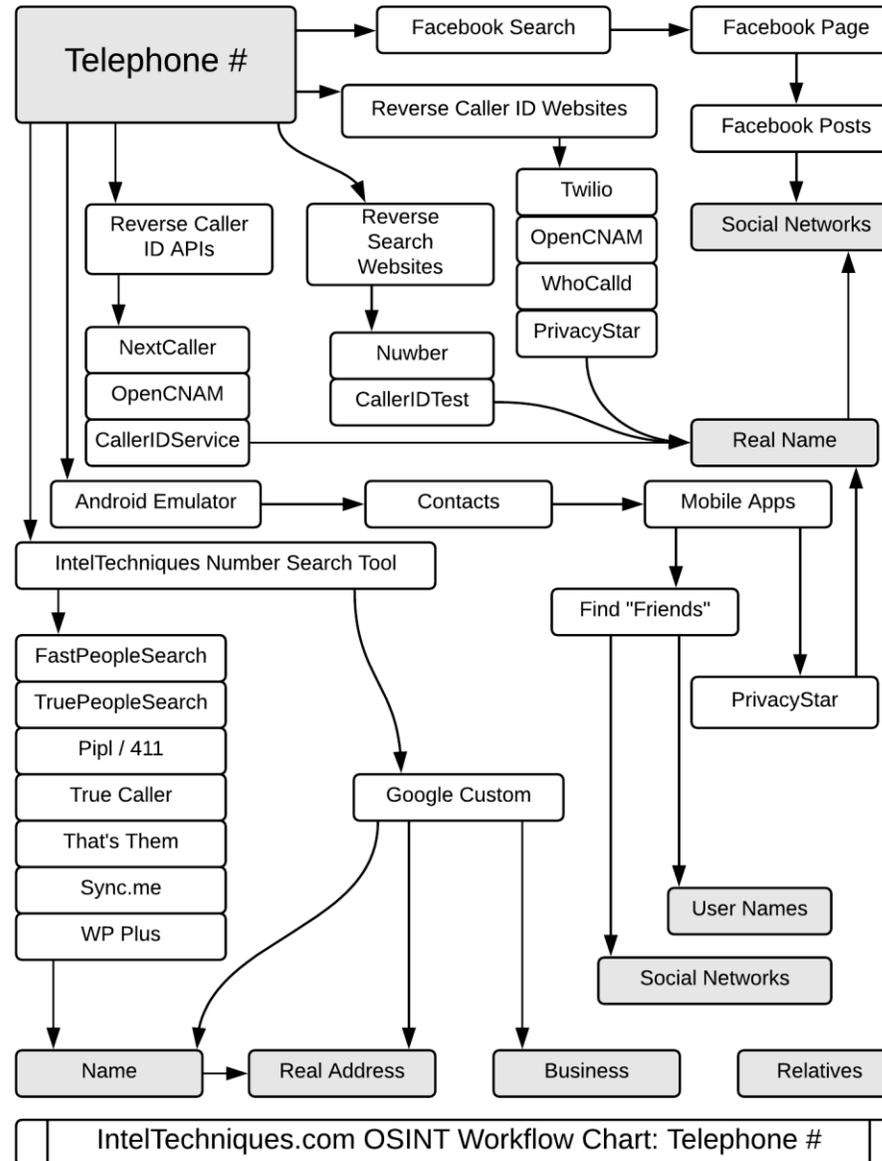
- ▶ Email
- ▶ Nombre real
- ▶ Nombre de dominio
- ▶ Localización
- ▶ Teléfono
- ▶ Etc...

Fuente: inteltechniques.com



Investigación de perfiles digitales

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

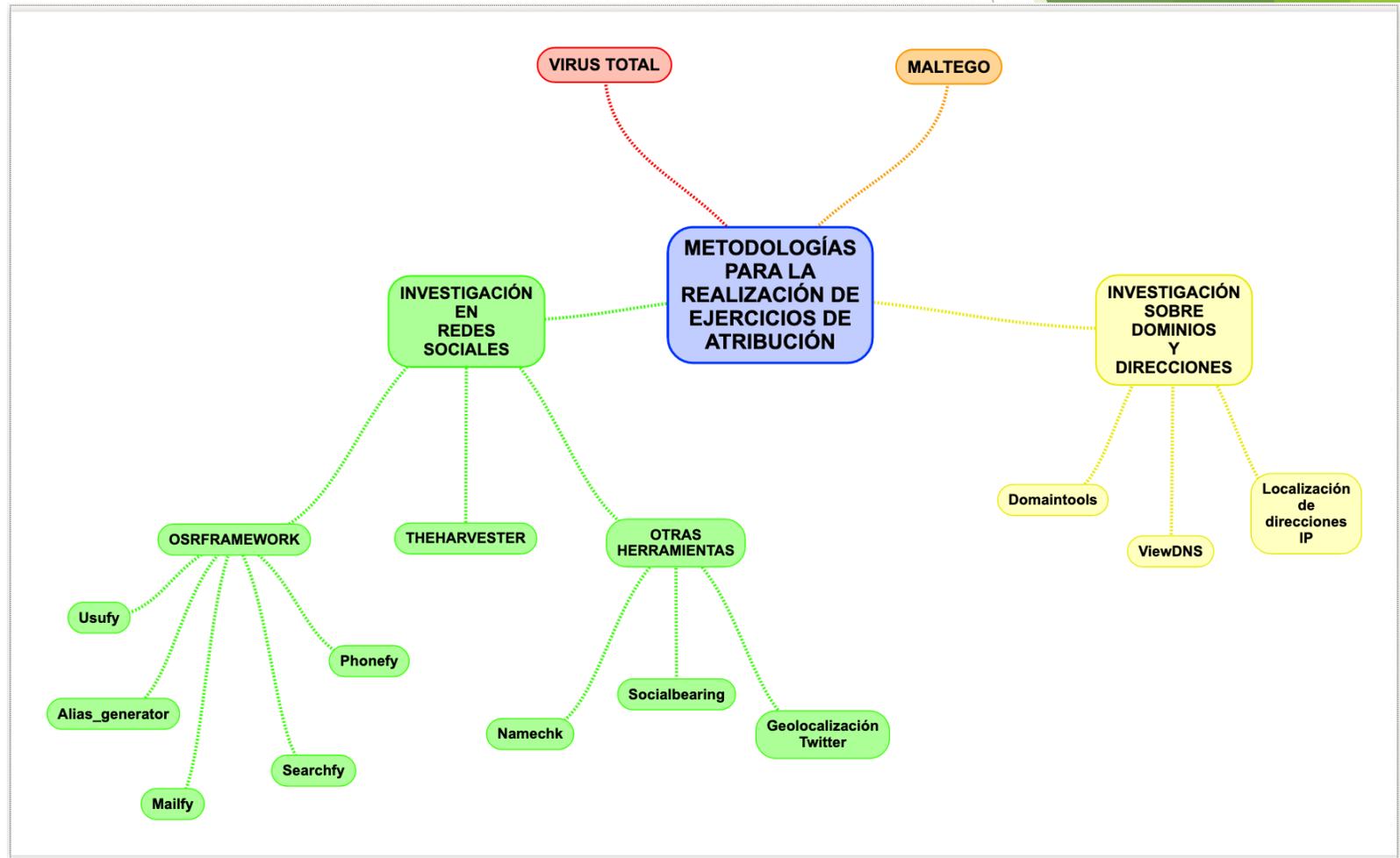


Fuente: inteltechniques.com

Esquema inicial para la investigación en redes sociales y dominios

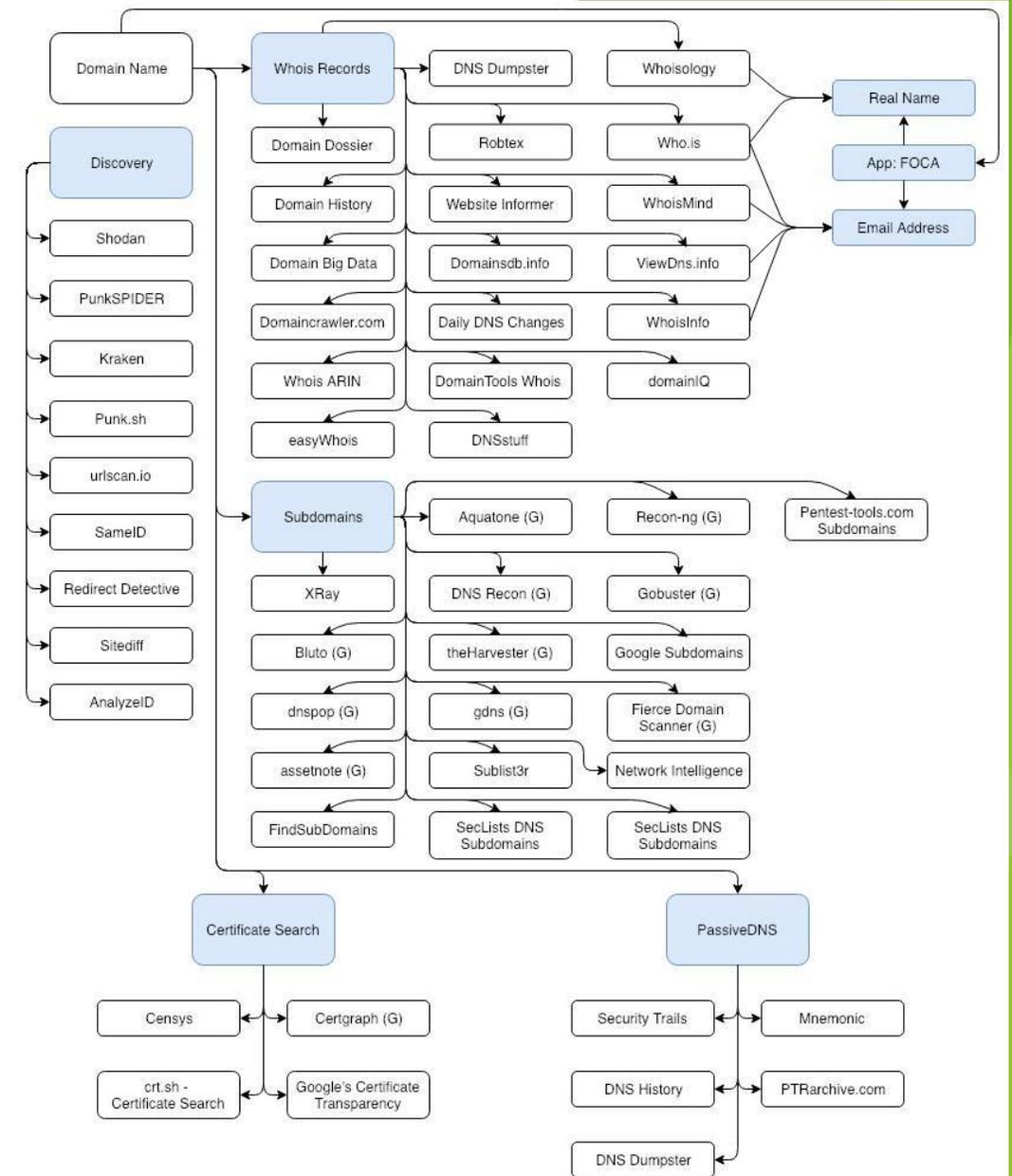
- ▶ Investigación en redes sociales
 - ▶ OSRframework
 - ▶ TheHarvester
 - ▶ Otras tools online
- ▶ Investigación sobre dominios y direcciones
 - ▶ Domaintools
 - ▶ ViewDNS
 - ▶ Localización de IPs
- ▶ Etc...

Fuente: campusciberseguridad.com



Flujo de investigación enfocado a pentesting

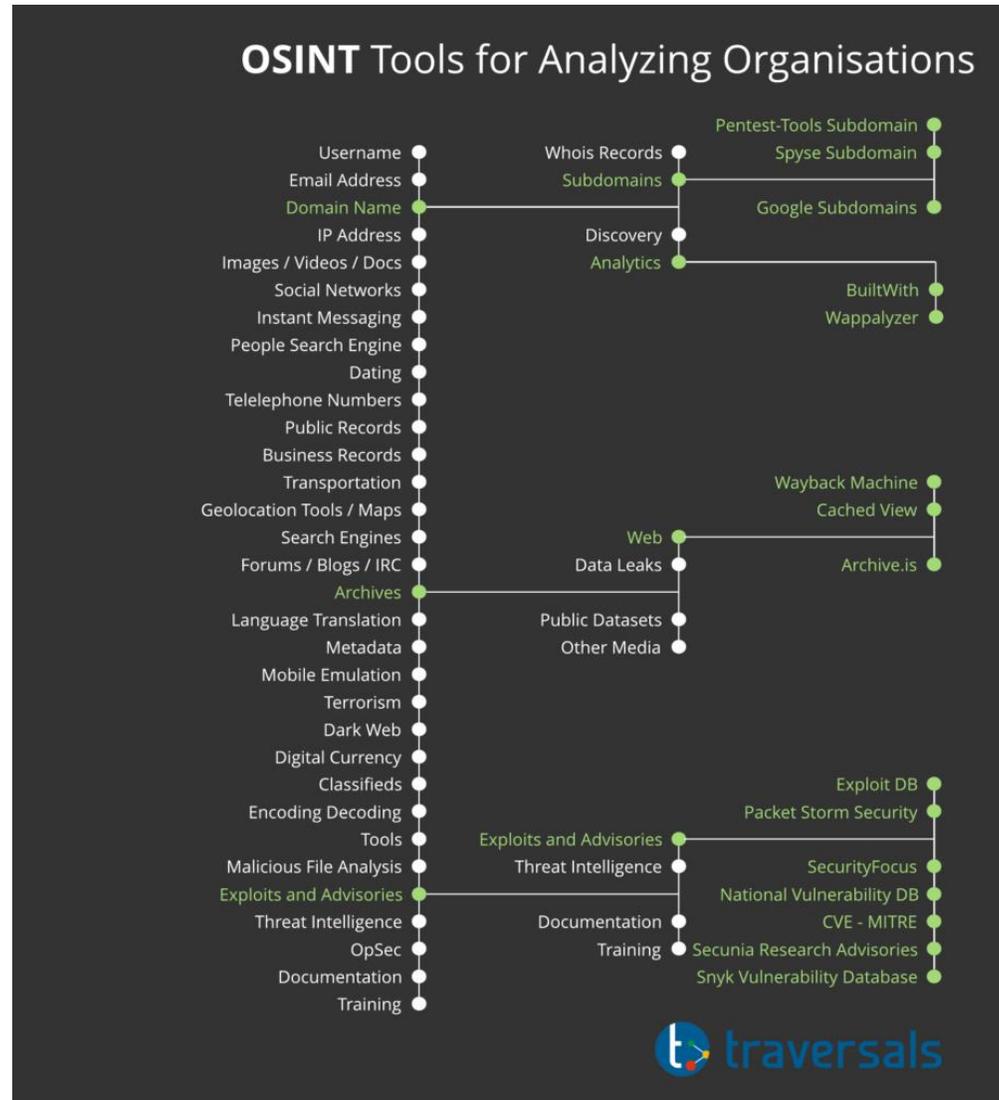
- Discovery
- Nombre de dominio
 - Registros whois
 - Subdominios
 - Certificados
 - Registros DNS
- Etc...



Fuente: 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...

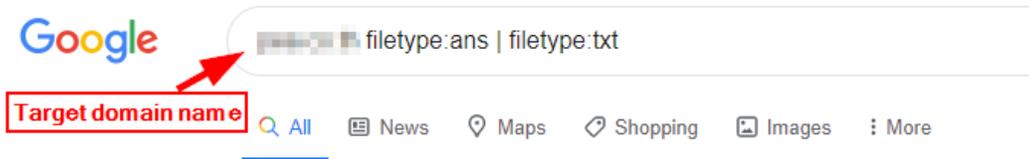


Colección de herramientas OSINT Framework desde MALTEGO

- ▶ 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...

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

GOOGLE DORKS - Búsqueda avanzada (2)

Otros tipos de búsqueda

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

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

Colección de búsquedas compartida entre usuarios

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/>)

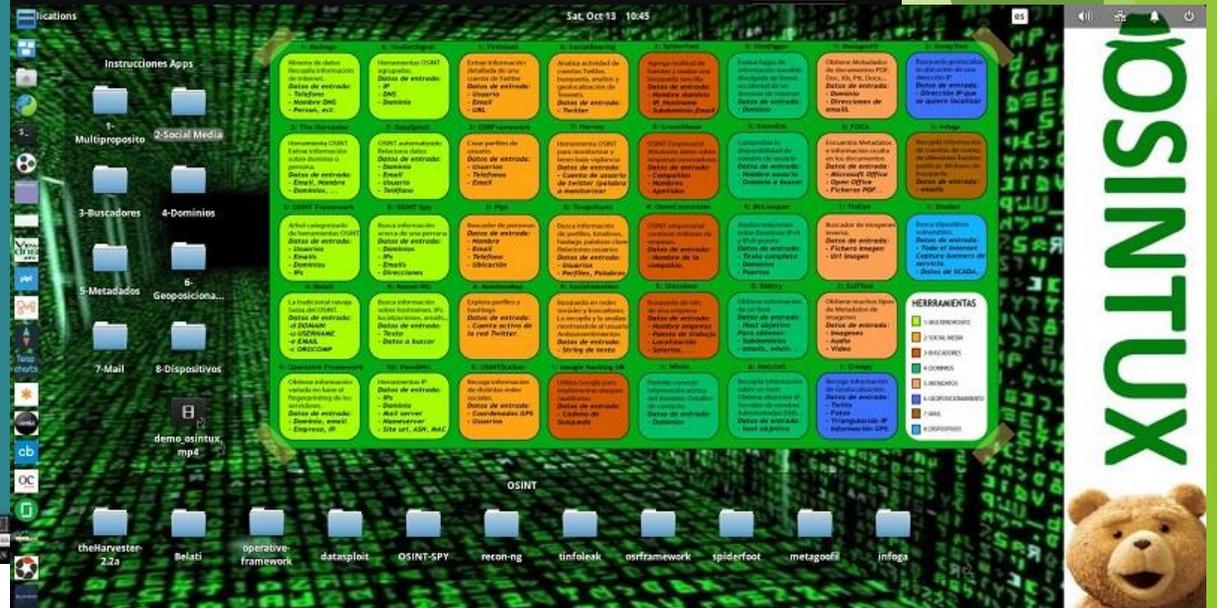
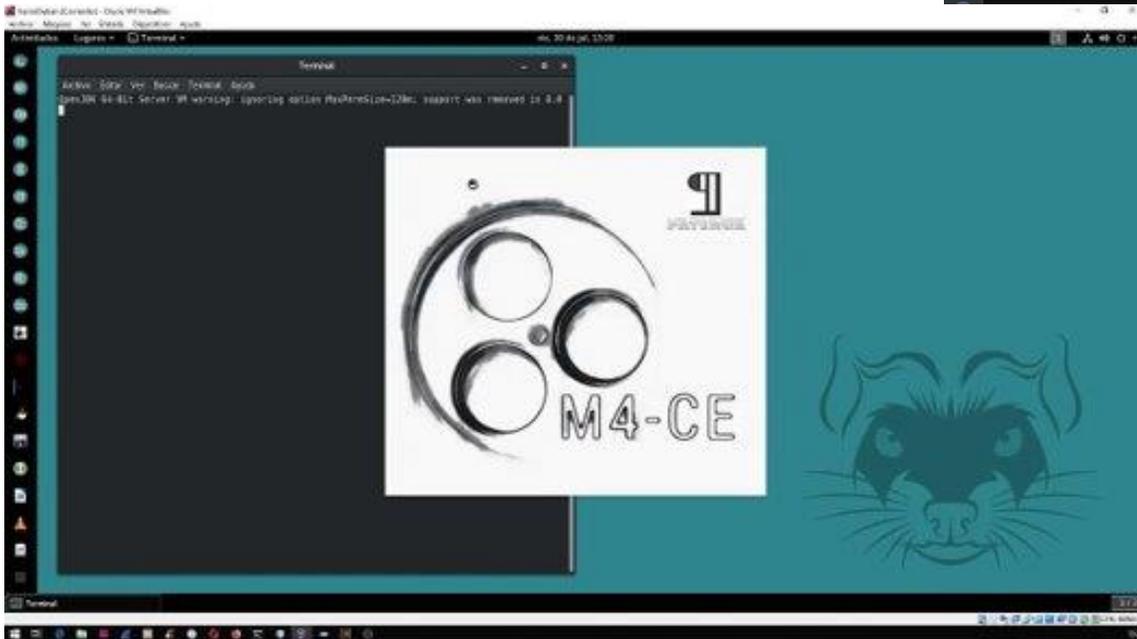


The screenshot shows the Google Hacking Database interface. At the top, it features the logo 'GOOGLE HACKING-DATABASE' with the tagline 'Welcome to the google hacking database'. Below this is a search bar with a dropdown menu set to 'All' and a 'Search' button. The main content area is titled 'Latest Google Hacking Entries' and contains a table with columns for Date, Title, and Category.

Date	Title	Category
2014-05-19	inurl:dfshealth.jsp	Various Online Devices
2014-05-08	intext:"Hikvision" inurl:"login.asp...	Various Online Devices
2014-05-06	inurl:"/public.php?service=files"	Various Online Devices
2014-05-05	"OpenSSL" AND "1.0.1 Server at"...	Vulnerable Servers
2014-04-30	inurl:"/cacti/graph_view.php" OR inurl:6...	Network or vulnerability data

Distros Linux OSINT

- ▶ Buscador - inteltechniques.com
- ▶ Huron - github.com/HuronOsint
- ▶ Osintux
- ▶ Etc...



Distro Osintux

Listado de herramientas instaladas

- [Belati v.0.2.4.1](#)
- [Creepy v1.4](#)
- [Crunchbase](#)
- [Datasploit for OSINT](#)
- [Dmitry \(Deepmagic information gathering tool\)](#)
- [Exiftool v11.03](#)
- [Google Hacking Database](#)
- [Infoga – Email Information Gathering vM4110k](#)
- [GeolP](#)
- [Glassdoor](#)
- [Knowem](#)
- [Maltego v4.1.6.11045](#)
- [MentionMap](#)
- [Metagoofil v2.2](#)
- [MrLooquer](#)
- [Netcraft](#)
- [Shodan](#)
- [Opencorporates](#)
- [Operative Framework](#)
- [OSINT-Spy v0.0.1](#)
- [OSRFramework v2018](#)
- [OSINTFramework](#)
- [PIPL](#)
- [Recon-NG v4.9.3](#)
- [SocialBearing](#)
- [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 [I Máster de Ciberseguridad](#), organizado por [Eleven Paths](#) (Téléfonica), 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 continúa 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...

1: Maltego Minería de datos Recopila información de Internet. Datos de entrada: - Telefono - Nombre DNS - Person, ect.	6: YouGetSignal Herramientas OSINT agrupadas. Datos de entrada: - IP - DNS - Dominio	1: Tinfoleak Extrae información detallada de una cuenta de Twitter Datos de entrada: - Usuario - Email - URL	6: SocialBearing Analiza actividad de cuentas Twitter, búsqueda, análisis y geolocalización de Tweets. Datos de entrada: - Twitter	2: Spiderfoot Agrega multitud de fuentes y realiza una búsqueda sencilla Datos de entrada: - Nombre dominio - IP, Hostname - Subdominio, Email	2: SiteDigger Evalua fugas de información sensible divulgada de forma accidental de un dominio de internet Datos de entrada: - Dominio	1: Metagoofil Obtiene Metadatos de documentos PDF, Doc, Xls, Ppt, Docx, ... Datos de entrada: - Dominio - Direcciones de email	2: GeolpTool Búsqueda geolocaliza la ubicación de una dirección IP Datos de entrada: - Dirección IP que se quiere localizar
2: The Harvester Herramienta OSINT Extrae información sobre dominio o persona. Datos de entrada: - Email, Nombre - Dominios, ...	7: DataSploit OSINT automatizado Relaciona datos Datos de entrada: - Dominio - Email - Usuario - Teléfono	2: OSRFramework Crear perfiles de usuario. Datos de entrada: - Usuarios - Telefonos - Email	7: Harvey Herramienta OSINT para monitorizar y tener bajo vigilancia Datos de entrada: - Cuenta de usuario de twitter /palabra a monitorizar	3: Crunchbase OSINT Empresarial Almacena datos sobre empresas innovadoras Datos de entrada: - Compañías - Nombres - Apellidos	3: KnowEm Comprobar la disponibilidad de nombre de usuario Datos de entrada: - Nombre usuario - Dominio a buscar	2: FOCA Encuentra Metadatos e información oculta en los documentos Datos de entrada: - Microsoft Office - Open Office - Ficheros PDF...	1: Infoga Recopila información de cuentas de correo de diferentes fuentes publicas. Motores de búsqueda. Datos de entrada: - emails
3: OSINT Framework Arbol categorizado de herramientas OSINT Datos de entrada: - Usuarios - Emails - Dominios - IPs	8: OSINT Spy Busca información acerca de una persona Datos de entrada: - Dominios - IPs - Emails - Direcciones	3: Pipl Buscador de personas Datos de entrada: - Nombre - Email - Telefono - Ubicación	8: Twopcharts Busca información de perfiles, timelines, hastags, palabras clave Relaciones usuarios Datos de entrada: - Usuarios - Perfiles, Palabras	4: OpenCorporates OSINT empresarial contiene millones de empresas. Datos de entrada: - Nombre de la compañía.	4: MrLooquer Analiza relaciones entre Dominios IPv4 y IPv6-puerto Datos de entrada: - Texto completo - Dominios - Puertos	1: TinEye Buscador de imagenes inverso. Datos de entrada: - Fichero Imagen - Url imagen	1: Shodan Busca dispositivos vulnerables. Datos de entrada: - Todo el internet - Captura banners de servicio. - Datos de SCADA...
4: Belati La tradicional navaja Suiza del OSINT. Datos de entrada: -d DOMAIN -u USERNAME -e EMAIL -c ORGCOMP	9: Recon-NG Busca información sobre hostnames, IPs, localizaciones, emails, ... Datos de entrada: - Texto - Datos a buscar	4: MentionMap Explora perfiles y hashtags. Datos de entrada: - Cuenta activa de la red Twitter.	9: Socialmention Búsqueda en redes sociales y buscadores. La recopilación y la analiza mostrandole al usuario Anlizensentimientos Datos de entrada: - String de texto	5: Glassdoor Búsqueda de info de una empresa Datos de entrada: - Nombre empresa - Puesto de trabajo - Localización - Salarios, ...	5: DMitry Obtiene información de un host Datos de entrada: - Host objetivo Para obtener: - Subdominios - emails, whois...	2: ExifTool Obtiene muchos tipos de Metadatos de imagenes Datos de entrada: - Imagenes - Audio - Video	HERRAMIENTAS 1: MULTIPROPOSITO 2: SOCIAL MEDIA 3: BUSCADORES 4: DOMINIOS 5: METADATOS 6: GEOPOSICIONAMIENTO 7: MAIL 8: DISPOSITIVOS
5: Operative Framework Obtiene información variada en base al fingerprinting de los servidores. Datos de entrada: - Dominio, email. - Empresa, IP.	10: ViewDNS Herramientas IP Datos de entrada: - IPs - Dominio - Mail server - Nameserver - Site url, ASN, MAC	5: OSINTStalker Recoge información de distintas redes sociales. Datos de entrada: - Coordenadas GPS - Usuarios	1: Google Hacking DB Utiliza Google para información acerca /auditorias Datos de entrada: - Cadena de búsqueda	1: Whois Permite conocer información acerca del dominio. Detalles de contacto. Datos de entrada: - Dominios	6: Netcraft Recopila información sobre un host. Obtiene dirección IP, Servidor de nombre, Administrador DNS, ... Datos de entrada: - host objetivo	1: Creepy Recoge información de Geolocalización. Datos de entrada: - Twiits - 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](#)
- [MrLooquer](#)
- [Netcraft](#)
- [Shodan](#)
- [Opencorporates](#)
- [Operative Framework](#)
- [OSINT-Spy v0.0.1](#)
- [OSRFramework v2018](#)
- [OSINTFramework](#)
- [PIPL](#)
- [Recon-NG v4.9.3](#)
- [SocialBearing](#)
- [Socialmention](#)
- [SpiderFoot v2.12](#)
- [The Harvester v2.2a](#)
- [Tineye](#)
- [Tinfoleak v2.1](#)
- [Twopcharts](#)
- [ViewDNS](#)
- [YouGetSignal](#)
- [Whois](#)

The screenshot displays the OSINTux desktop environment with a grid of installed tools. Each tool card includes a number, a name, a brief description, and a list of input data types. A legend on the right side of the grid categorizes the tools by type: 1-MULTIPROPOSITO (green), 2-SOCIAL MEDIA (orange), 3-BUSCADORES (yellow), 4-DOMINIOS (light green), 5-METADATOS (light blue), 6-GEOPOSICIONAMIENTO (blue), 7-MAIL (dark blue), and 8-DISPOSITIVOS (purple). A 'HERRAMIENTAS' legend is also present. At the bottom, a folder view shows icons for theHarvester-2.2a, Belati, operative-framework, datasploit, OSINT-SPY, recon-ng, tinfoleak, osrframework, metagoofil, spiderfoot, and infoga. A video player at the bottom shows a video titled 'demo.osintux.mp4' with a progress bar at 1:02 / 12:40. A teddy bear icon is visible in the bottom right corner.

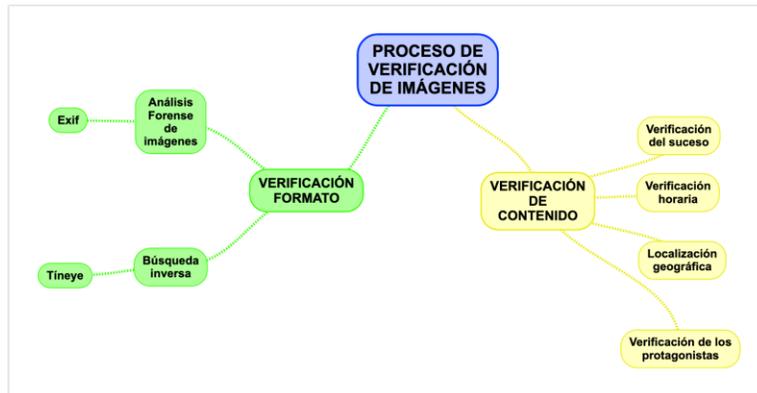
Number	Tool Name	Description	Input Data
1	Maltego	Minería de datos. Recopila información de Internet.	- Teléfono - Nombre DNS - Person, ect.
2	The Harvester	Herramienta OSINT agrupada.	- IP - DNS - Dominio
3	OSINT Framework	Arbol categorizado de herramientas OSINT.	- Usuarios - Emails - Dominios - IPs
4	Belati	La tradicional tarjeta Salta del OSINT.	- DOMAIN - USERNAME - EMAIL - ORGCOMP
5	Operative Framework	Obtiene información variada en base al fingerprinting de los servidores.	- Dominio, email, - Empresa, IP
6	Geoposiciona...	Busca información acerca de una persona.	- Dominio - Email - Usuario - Teléfono
7	DataSploit	OSINT automatizado.	- Dominio - Email - Usuario - Teléfono
8	OSINT Spy	Busca información acerca de una persona.	- Dominios - IPs - Emails - Direcciones
9	Recon-NG	Busca información sobre hostnames, IPs, localizaciones, emails.	- Texto - Datos a buscar
10	ViewDNS	Herramientas IP.	- IPs - Dominio - Mail server - Nameserver - Site url, ASN, MAC
11	Maltego	Extrae información detallada de una cuenta de Twitter.	- Usuario - Dirección de Twitter - Email - URL
12	SocialBearing	Análisis de actividad de cuentas Twitter.	- Twitter
13	Tinfoleak	Extrae información de cuentas de Twitter.	- Usuario - Nombre de dominio - IP - Subdominio, Email
14	SocialBearing	Análisis de actividad de cuentas Twitter.	- Twitter
15	SpiderFoot	Agrega resultados de fuentes y realiza una búsqueda sencilla.	- Nombre de dominio - IP - Subdominio, Email
16	Sitewhacker	Evalúa fugas de información sensible.	- Dominio
17	Metagoofil	Obtiene Metadatos de documentos PDF, Doc, Xls, Ppt, Docx...	- Dominio - Direcciones de email.
18	GeotIPTool	Busqueda geolocaliza la ubicación de una dirección IP.	- Dirección IP que se quiere localizar
19	The Harvester	Extrae información sobre dominio o persona.	- Email, Nombre - Dominios, ...
20	DataSploit	OSINT automatizado.	- Dominio - Email - Usuario - Teléfono
21	OSRFramework	Crear perfiles de usuarios.	- Usuarios - Telefonos - Email
22	SocialBearing	Herramienta OSINT para monitorizar y tener baja vigilancia.	- Cuenta de usuario de twitter (palabra a monitorizar)
23	Crunchbase	OSINT Empresarial.	- Compañías - Miembros - Apellidos
24	KnowEm	Compartir la disponibilidad de nombre de usuario.	- Nombre usuario - Dominio a buscar
25	FOCA	Encuentra Metadatos e información oculta en los documentos.	- Microsoft Office - Open Office - Ficheros PDF...
26	Infoga	Recopila información de cuentas de correo de diferentes fuentes públicas.	- Datos de entrada - Datos de búsqueda
27	OSINT Framework	Arbol categorizado de herramientas OSINT.	- Usuarios - Emails - Dominios - IPs
28	OSINT Spy	Busca información acerca de una persona.	- Dominios - IPs - Emails - Direcciones
29	Whois	Buscador de personas.	- Nombre - Email - Telefono - Ubicación
30	Twopcharts	Busca información de perfiles, timelines, hashtags, palabras clave.	- Usuarios - Perfiles, Palabras
31	OpenCorporates	OSINT empresarial.	- Nombre de la compañía
32	MrLooquer	Análisis de relaciones entre Dominios IPv4 y IPv6.	- Dominio completo - Dominios - Puertos
33	Tineye	Buscador de imágenes inverso.	- Fichero imagen - Url imagen
34	Shodan	Busca dispositivos vulnerables.	- Todo el Internet - Captura banners de servicios - Datos de SCADA...
35	Operative Framework	Obtiene información variada en base al fingerprinting de los servidores.	- Dominio, email, - Empresa, IP
36	ViewDNS	Herramientas IP.	- IPs - Dominio - Mail server - Nameserver - Site url, ASN, MAC
37	OSINTSpy	Recoge información de distintas redes sociales.	- Coordenadas GPS - Usuarios
38	Google Hacking DB	Utiliza Google para implementar ataques.	- Cadena de búsqueda
39	Whois	Permite consultar información acerca del dominio.	- Dominio
40	Netcraft	Recopila información sobre un host.	- Host objetivo
41	Creepy	Recopila información de cookies de sitios web.	- Dirección IP - Servidor de nombres - Administrador DNS - Datos de entrada - Host objetivo

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.

The screenshot displays the FotoForensics web application interface. At the top, the browser address bar shows 'fotoforensics.com'. The main content area features a large image of a man in a white lab coat sitting at a desk with a computer. Below this image is a dark, noisy version of the same image, likely representing a forensic analysis result. On the left side, there is an 'Analysis' panel with a list of analysis options: Digest, ELA, JPEG %, Metadata, and Original. Below this list are several icons for image manipulation. At the bottom right, there is a 'Color Adjustment' panel with sliders for Rotate hue, Saturation, and Brightness, and buttons for 'Invert' and 'Reset'. The browser tabs at the top show 'FotoForensics - Analysis' and 'Traductor de Google'. The footer of the page contains a URL to the page, a view button, and social media sharing icons.

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 videos, la música y las personas que marcaron el 2017.

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

Google josep rull twitter

Todo **Imágenes** Maps Shopping Más Configuración Herramientas

Aproximadamente 25.270.000.000 resultados (0,85 segundos)

Tamaño de imagen: 346 x 259
No se ha encontrado esta imagen en...

Consulta más probable para esta imagen: [Josep Rull](#)

Josep Rull i Andreu (@joseprull) | Twitter
<https://twitter.com/joseprull?lang=es> Traducir esta página
6476 tweets • 1290 photos/videos • 74.7K followers. "Ara digue al servei d'aquest poble". Salvador Espriu, Inici del càntic en el...

Independencia de Cataluña: Josep Rull acude...
www.elperiodico.com/es/politica/.../rull-acude-a-su-despach
31 oct. 2017 - Rull, que asumió también el pasado viernes las Santi Vila al frente de Empresa i Competitivitat, ha enviado un les responsabilitats que ens ha encomanat el poble de Catalun...

Imágenes visualmente similares

Denunciar imágenes

Páginas con imágenes que coinciden con la búsqueda

Josep Rull i Andreu on Twitter: "Al despatx, exercint les ..."
<https://twitter.com/joseprull/.../924912753009143808...> Traducir esta página
1024 x 768 - 30 oct. 2017 - Josep Rull i Andreu · @joseprull. Conseller de Territori i Sostenibilitat i funcions d'Empresa i Coneixement. Sóc membre del Govern legítim de Catalunya. @ Pdemocratacat. Terrassa. Països Catalans. territori.gencat.cat. Joined March 2010 ...

La 'profecía belga' de Rull - El Periódico
www.elperiodico.com/.../tintin-los-mensajes-belgas-del-tuit-de-rull-6390691 Traducir esta página
1055 x 791 - 31 oct. 2017 - 230. Josep Rull, en su despacho, según su cuenta de Twitter, / periódico. El tuit que ha publicado esta mañana el 'exconseller' de Territori Josep Rull oculta algunos símbolos de la leyenda del cómic belga, Tintín, lo que ha sido visto como muchos como un vaticinio de la noticia de que Carles Puigdemont se había trasladado a Bruselas, donde podría pedir asilo.

el Periódico

POLÍTICA PULSO POR LA INDEPENDENCIA CLIP BARÓMETRO RAJOY PEDRO SÁNCHEZ

Últimas noticias sobre Catalunya y las elecciones del 21-D

La 'profecía belga' de Rull

El Periódico
Barcelona - Lunes, 30/10/2017 | Actualizado el 31/10/2017 a las 15:10 CET

Josep Rull, en su despacho, según su cuenta de Twitter. / PERIÓDICO

El tuit que ha publicado esta mañana el 'exconseller' de Territori Josep Rull oculta algunos símbolos de la leyenda del cómic belga, Tintín, lo que ha sido visto como muchos como un vaticinio de la noticia de que Carles Puigdemont se había trasladado a Bruselas, donde podría pedir asilo.

El día que Cristiano Ronaldo desprecia el 'Balón de Oro'

LO MÁS VISTO LO MÁS COMENTADO

Repositorio de herramientas OSINT

Recurso	Dirección URL				
Abiword	https://www.abisource.com/	I2P	https://geti2p.com	SocialBearing	https://socialbearing.com
Ahmia	https://ahmia.fi	IP-API	https://ip-api.com	Tails	https://tails.boum.org
Archive.is	https://archive.is	IP2Location	https://ip2location.com	Tesseract	https://github.com/tesseract-ocr
Baidu	https://baidu.com	Ifconfig.co	https://ifconfig.co	Telegram Purple	https://github.com/majn/telegram-purple
Bing	https://bing.com	IPFS	https://ipfs.io	TheHarvester	https://github.com/laramies/theHarvester
CaseFile	https://paterva.com	Kali Linux	https://kali.org	TinEye	https://tineye.com
Domaintools	https://domaintools.com	KeePass	https://keepass.info	Tor Project	https://torproject.org
DuckDuckGo	https://duckduckgo.com	Kibana	https://www.elastic.co/products/logstash	Tor2Web	https://www.tor2web.org/
ElasticSearch	https://www.elastic.co/products/elasticsearch	Logstash	https://www.elastic.co/products/logstash	Torch	http://xmh57jrznw6insl.onion/
Evil FOCA	https://github.com/ElevenPaths/EvilFOCA	Maltego	https://paterva.com	Ubuntu	https://ubuntu.com
Exiftool	http://search.cpan.org/~exiftool/	MrLooquer	https://mrlouquer.com	ViewDNS	https://viewdns.info
Flickr	https://flickr.com	Namechk	https://namechk.com	Virustotal	https://virustotal.com
FOCA	https://github.com/elevenpaths/FOCA	OpenStreetMap	https://openstreetmap.org	VirtualBox	https://virtualbox.org
GeoSocialFootprint	http://geosocialfootprint.com	OSRFramework	https://github.com/i3visio/osrframework	Wayback Machine (archive.org)	https://archive.org
GOCR	http://www-e.uni-magdeburg.de/jschulen/ocr/download.html	Onion.link	https://onion.link	Whonix	https://www.whonix.org/
Google	https://google.com	Onion.plus	https://onion.plus	Wordreference	https://wordreference.com
Google Custom Search Engine	https://cse.google.com	Pidgin	https://pidgin.im	Yacy	https://yacy.net
Google Hacking Database	https://www.exploit-db.com/google-hacking-database/	PIVPN	https://pivpn.io	Yandex	https://yandex.com
Google Imágenes	https://images.google.com	ProtonVPN	https://www.protonvpn.com	Yandex Imágenes	https://images.yandex.com
Google Maps	https://maps.google.com	Qubes OS	https://www.qubes-os.org/	Zoomeye	https://zoomeye.com
Grok Debugger	https://grokdebug.herokuapp.com/	Quora	https://quora.com		
HaveIBeenPwned	https://haveibeenpwned.com	Reddit	https://reddit.com		
HeSidoHackeado	https://hesidohackeado.es	Regexper	https://regexper.com		
		Searx	https://searx.me		
		Shodan	https://shodan.io		

GRACIAS
OSINTUX 

[Osintux.org](https://osintux.org)