

OSINT

Open-Source INTeelligence

INTRODUCCIÓN A LA INTELIGENCIA EN FUENTES ABIERTAS

«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

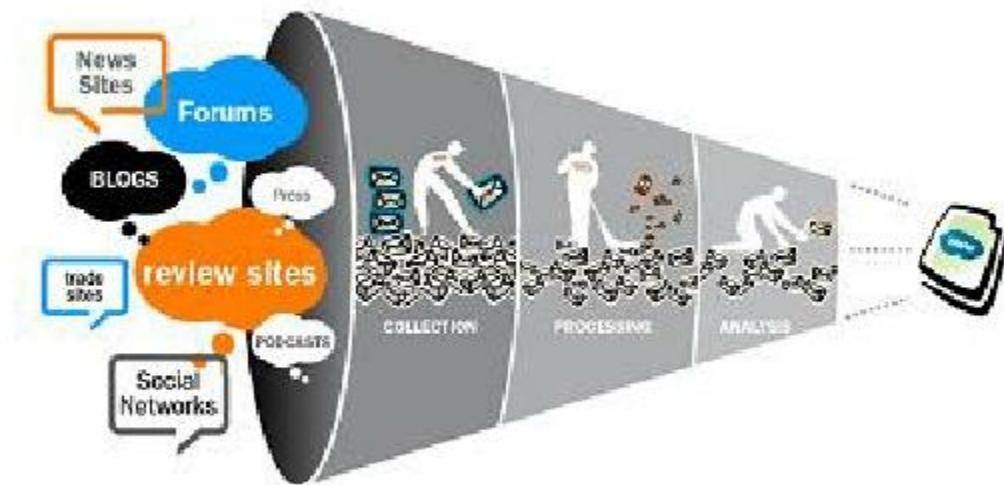
Colección de fuentes de inteligencia



- 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 PUBLICA)

¿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, auditorias de seguridad, ciberdefensa



FASES

FASE PREVIA

FASE DE IDENTIFICACIÓN

verificar y describir el ataque, incidente de segurado actividad ilegal

FASE DE RECOPILACIÓN 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:

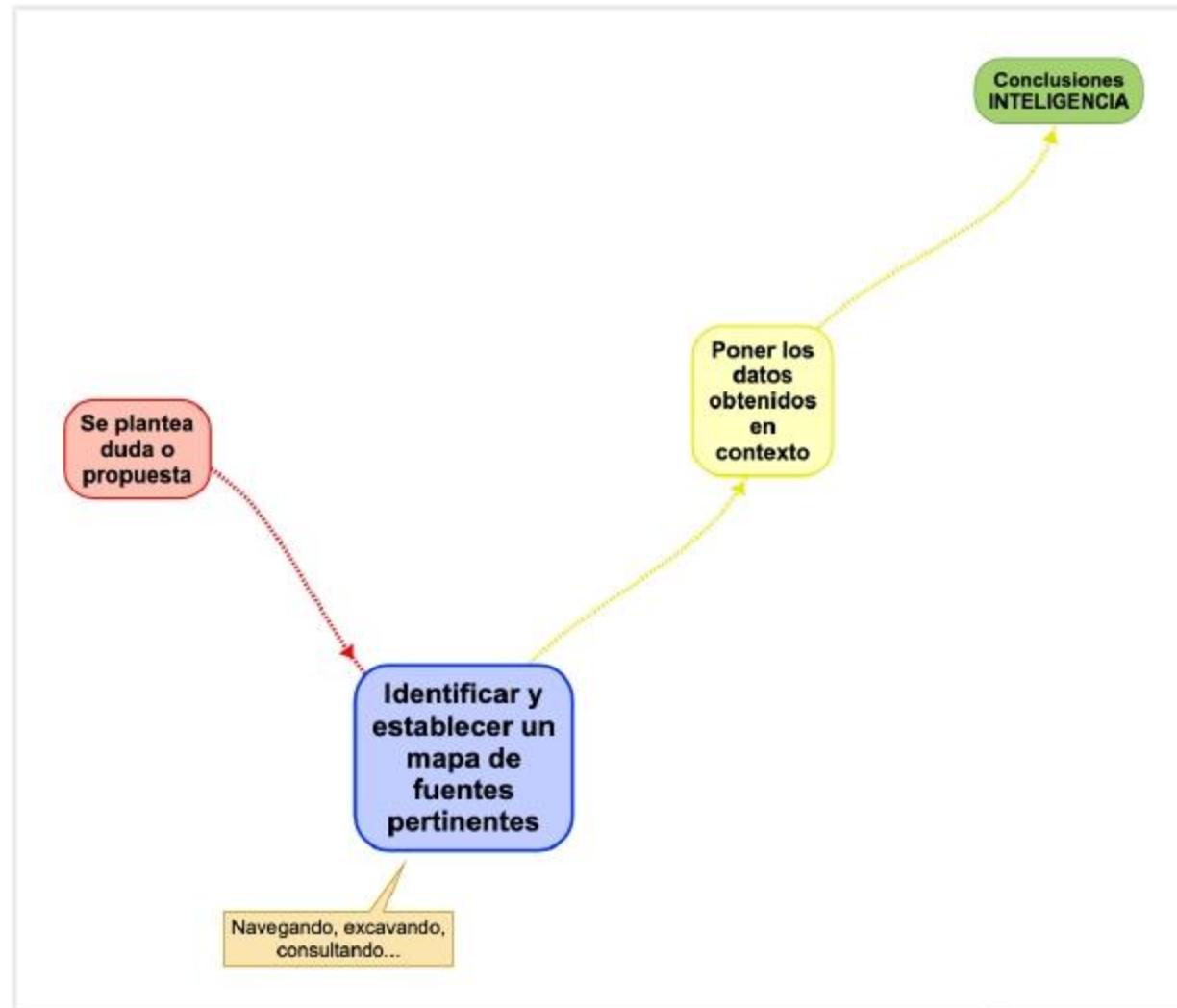
En esta fase se procede a analizar la evidencia con objeto de encontrar hechos y conclusiones relevantes para la resolución del incidente de ciberseguridad

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

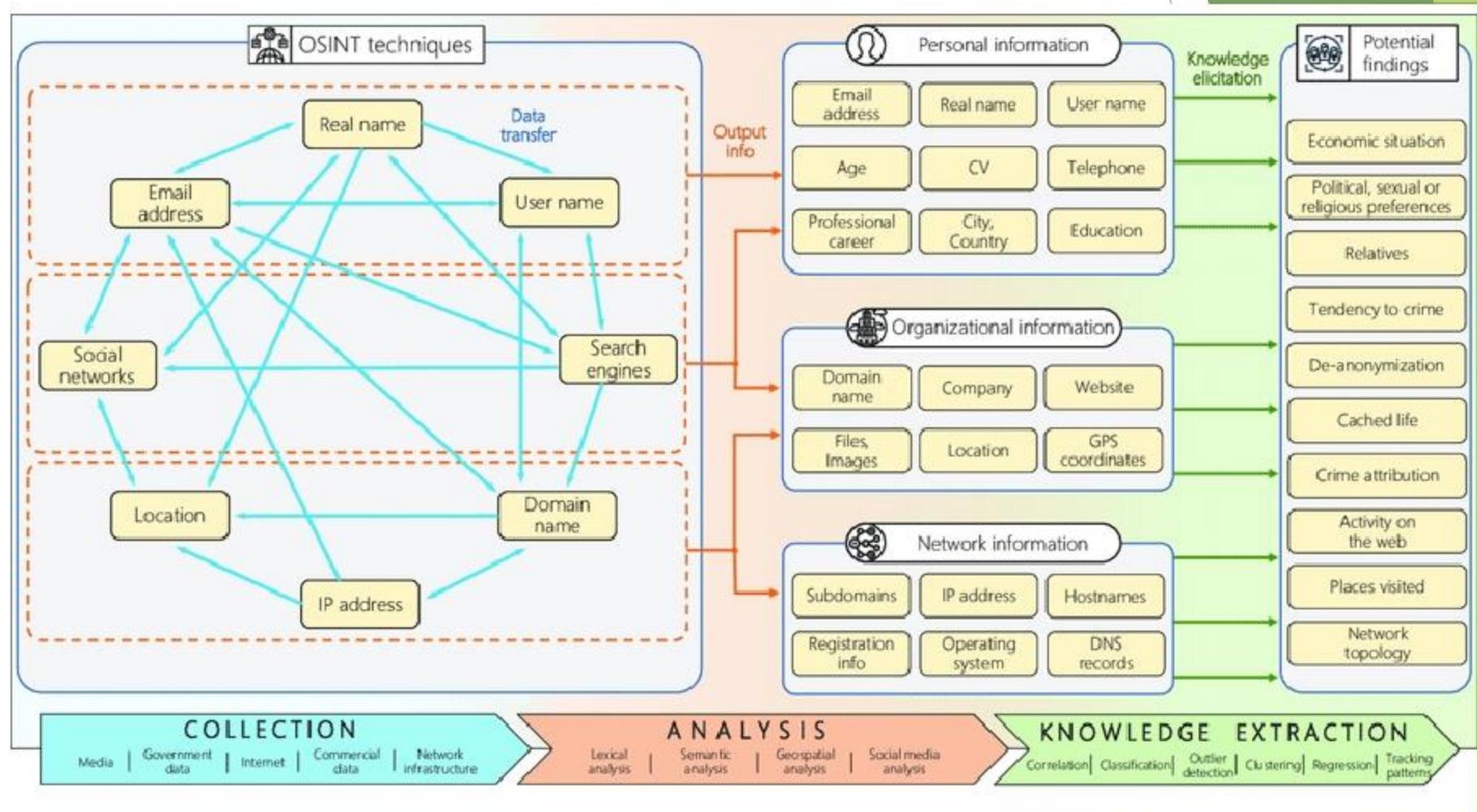
- 1. Establecer los requisitos
- 2. Concretar las Fuentes de información
- 3. Adquisición de la información
- 4. Procesamiento y formateo
- 5. Análisis y relación de los datos
- 6. Inteligencia. Presentación del informe con los datos pertinentes.



Fuente: hackers4fun.com

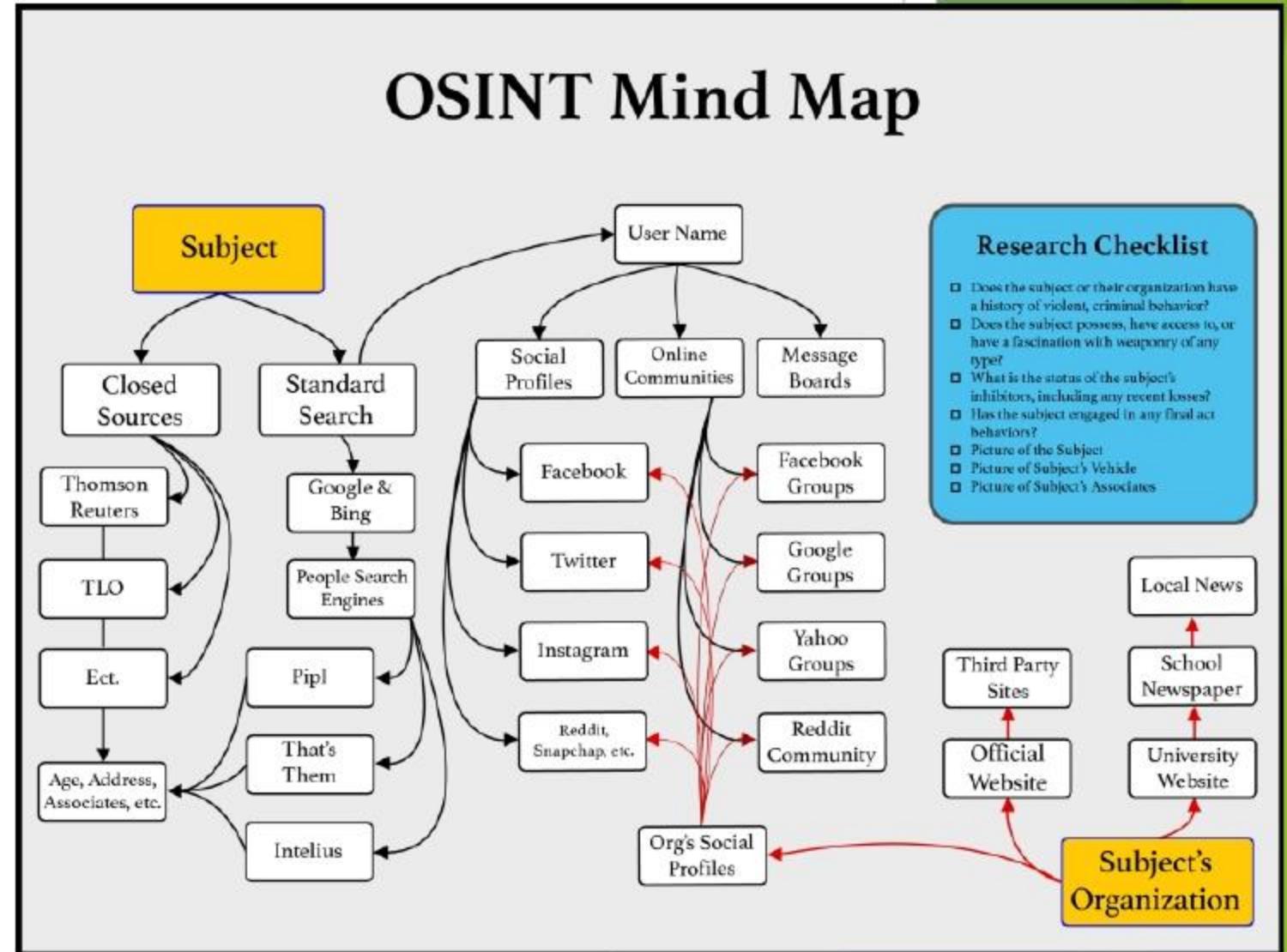
Fases de investigación en OSINT

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



Mapa mental (Ejemplo de investigación)

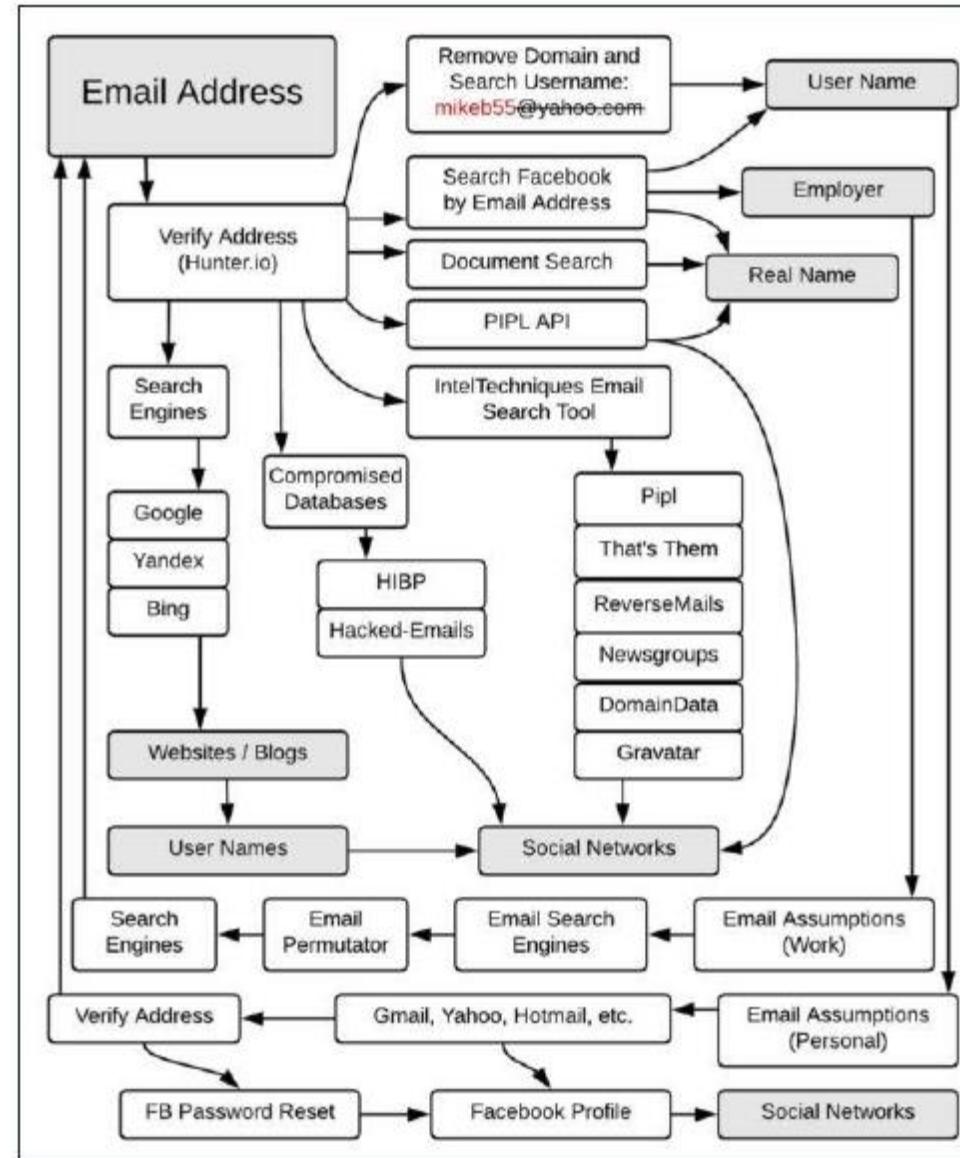
- Checklist de la investigación sobre sujeto o su organización criminal potencial
 - ¿Tiene historial o comportamiento criminal?
 - ¿Siente fascinación por algún tipo de armamento?
 - ¿Inhibidores posibles, perdidas recientes?
 - ¿Ha participado en algún evento o acto final criminal?
 - Imagen del sujeto
 - Imagen de vehiculos del sujeto
 - Imagen de posibles asociados
- Fuente: protectioncircle.org



Investigación de perfiles digitales

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

Fuente: inteltechniques.com

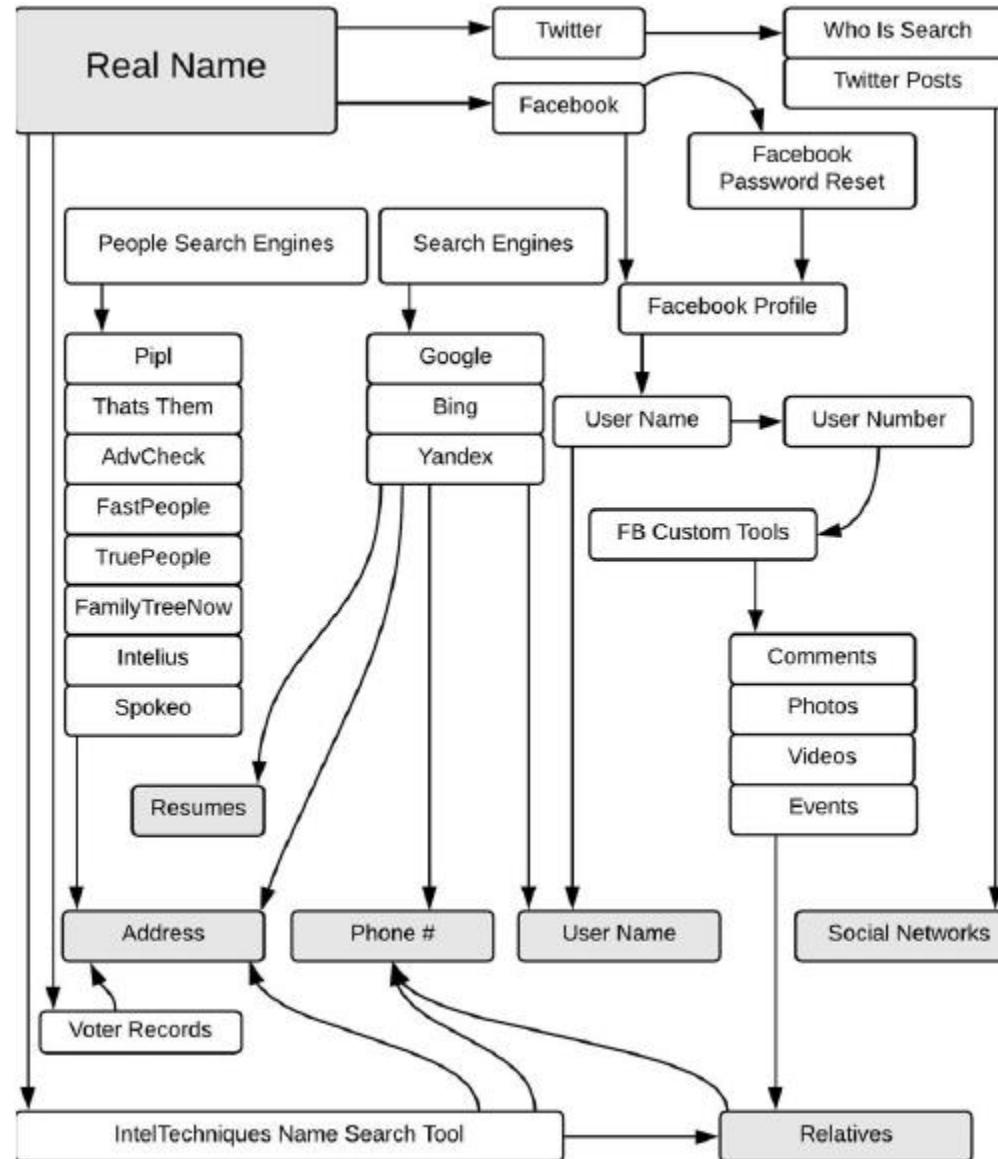


Investigación de perfiles digitales

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

Fuente: inteltechniques.com

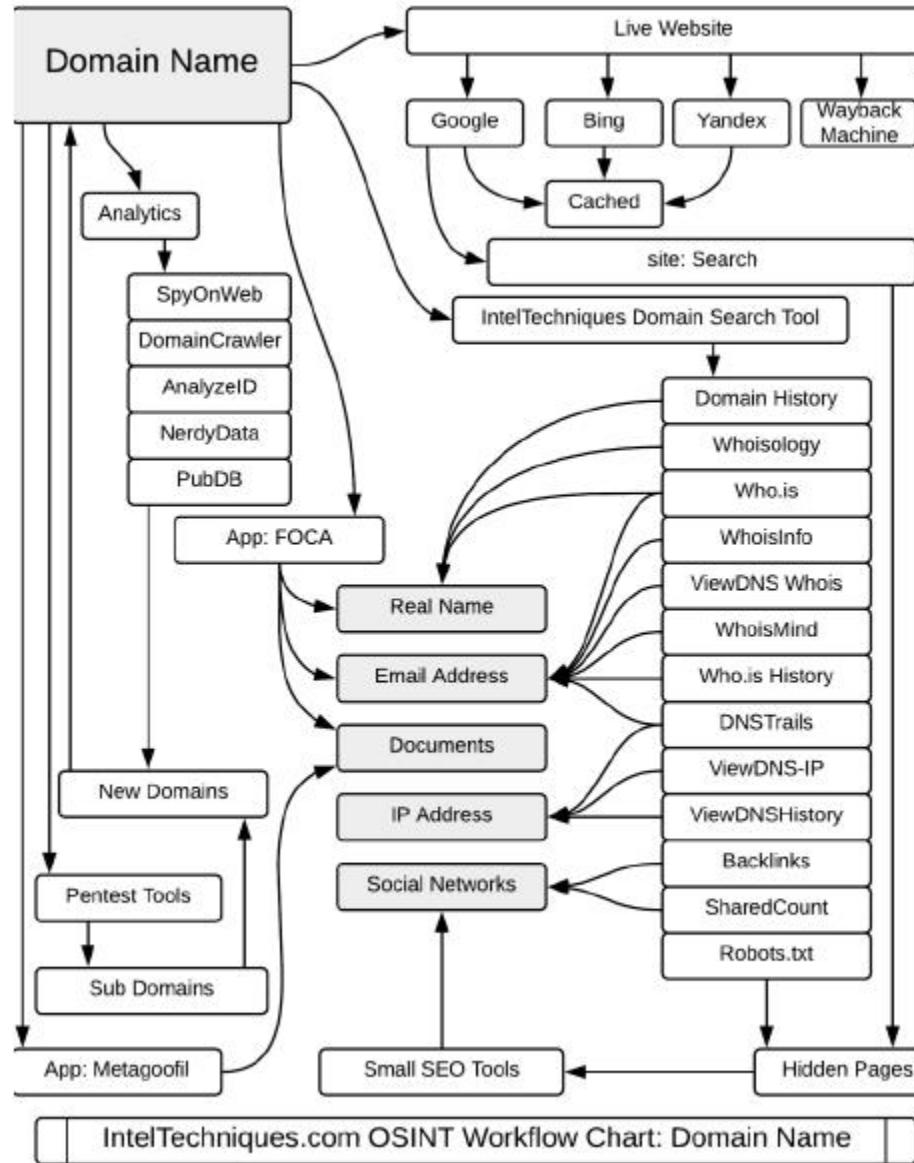
Inteltechniques - Michael Bazzell
(consultor de seguridad y ex agente e investigador del Grupo de Trabajo de Delitos Cibernéticos del FBI)



Investigación de perfiles digitales

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

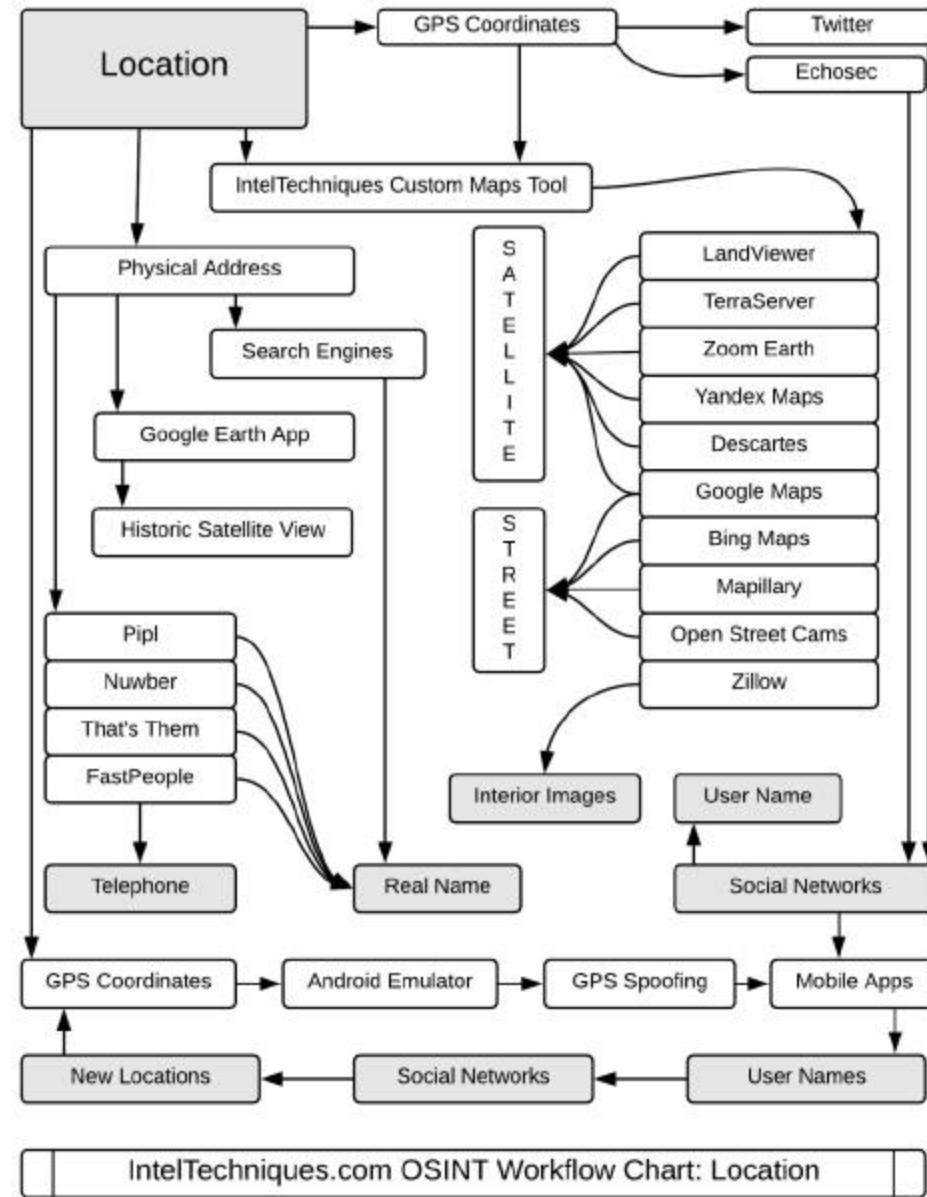
Fuente: inteltechniques.com



Investigación de perfiles digitales

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

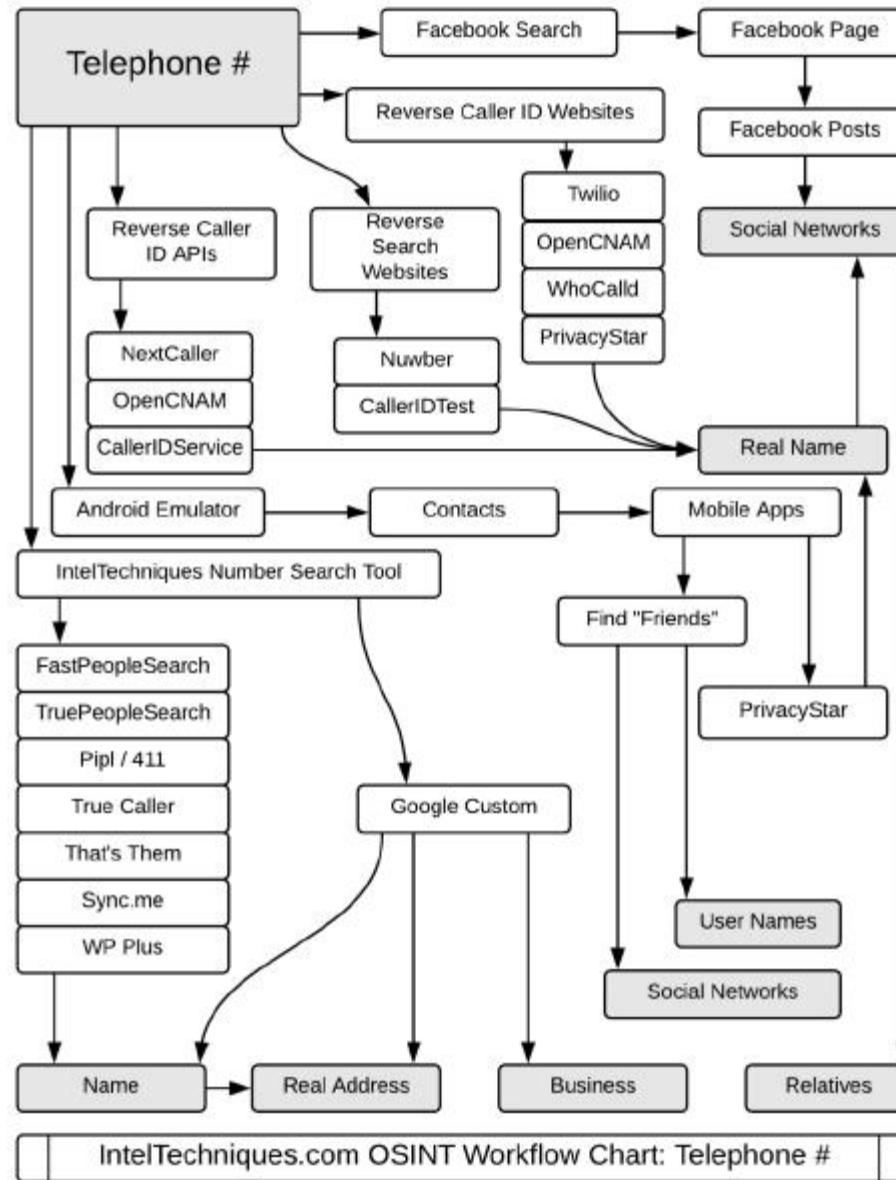
Fuente: inteltechniques.com



Investigación de perfiles digitales

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

Fuente: inteltechniques.com

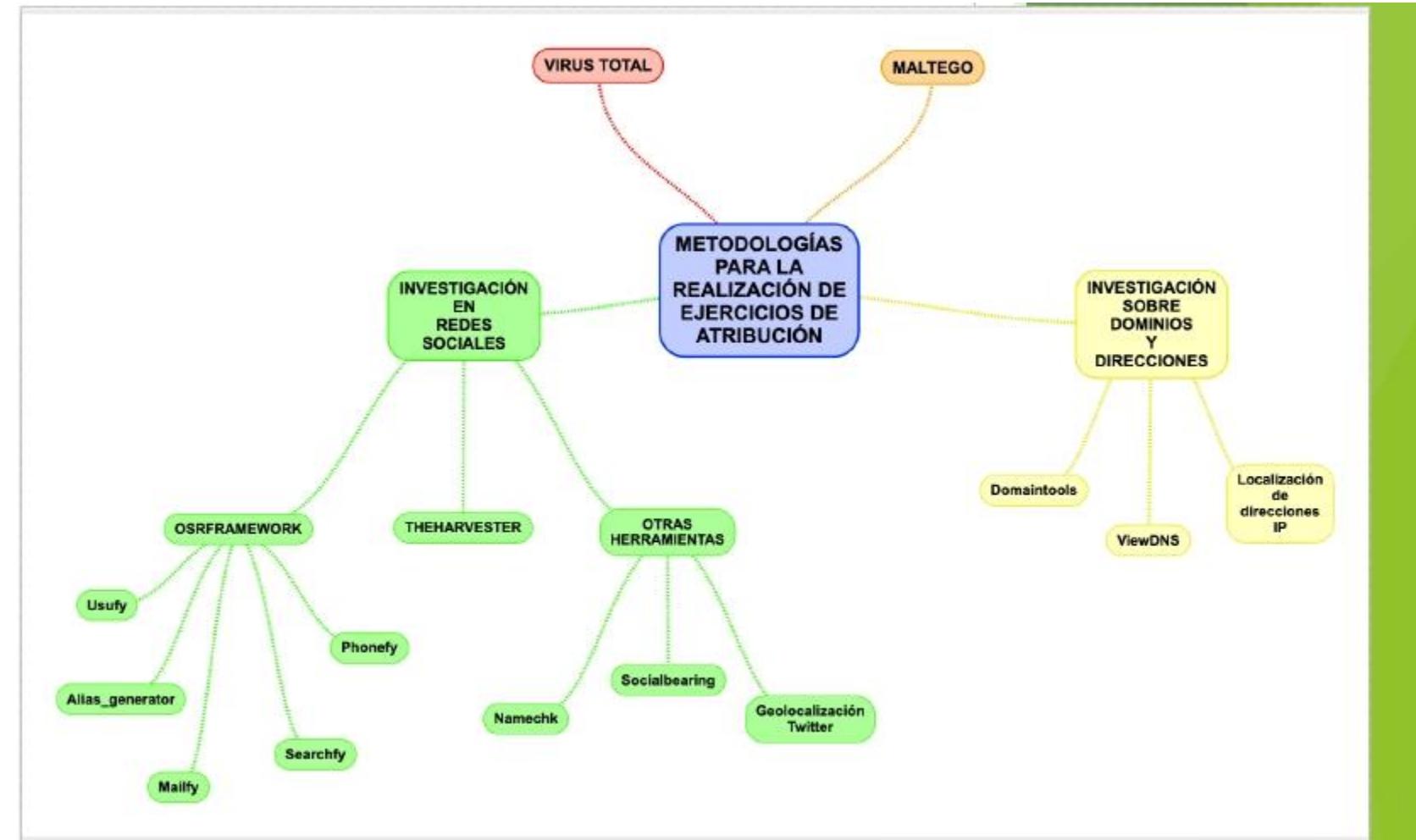


Esquema inicial para la investigación en redes sociales y dominios

Investigación en redes sociales

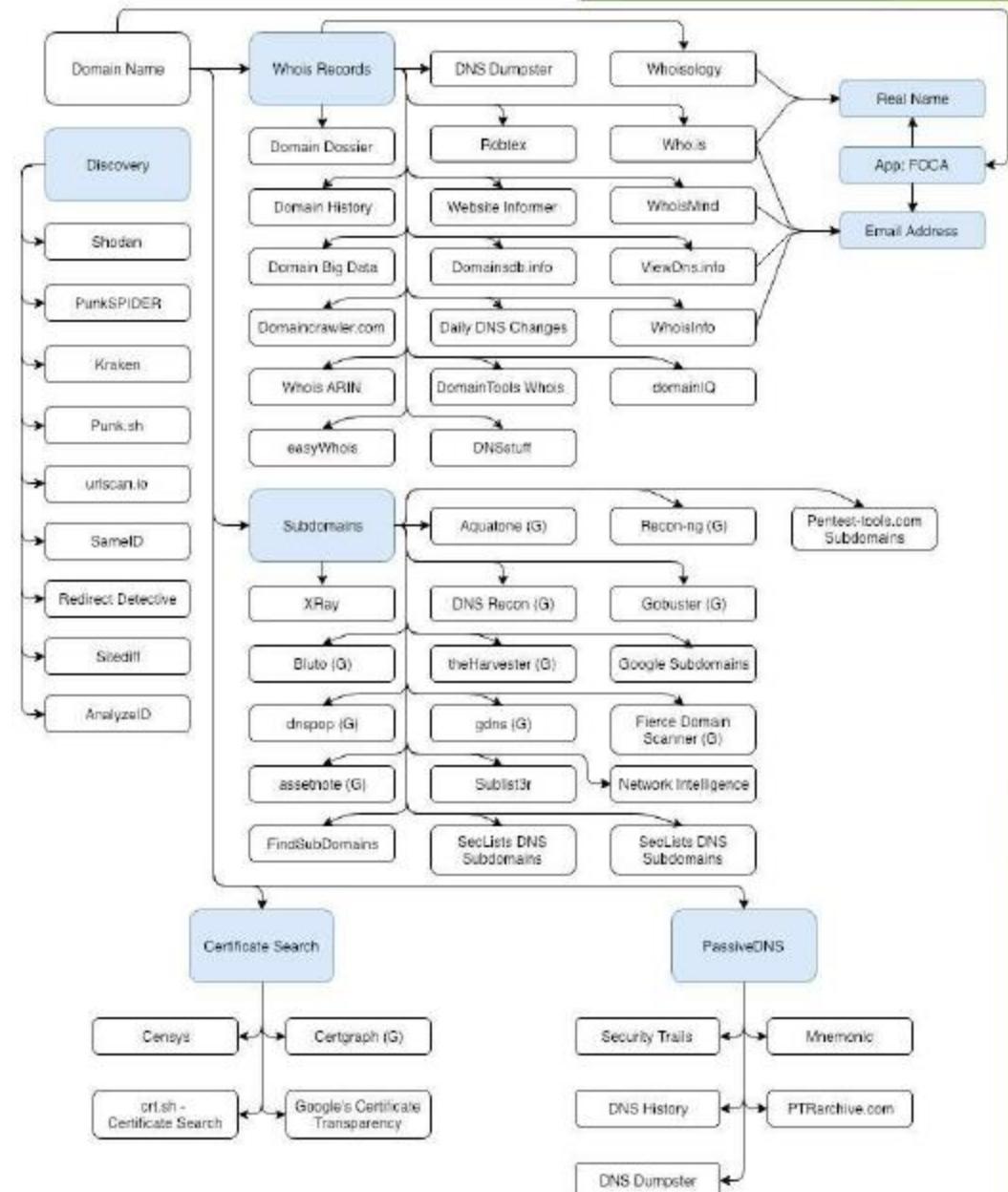
- OSRframework
 - TheHarvester
 - Otras tools online
- Investigación sobre dominios y direcciones
 - Domaintools
 - ViewDNS
 - Localización de IPs
- Etc...

Fuente: campusciberseguridad.com



Flujo de investigación enfocado a pentesting

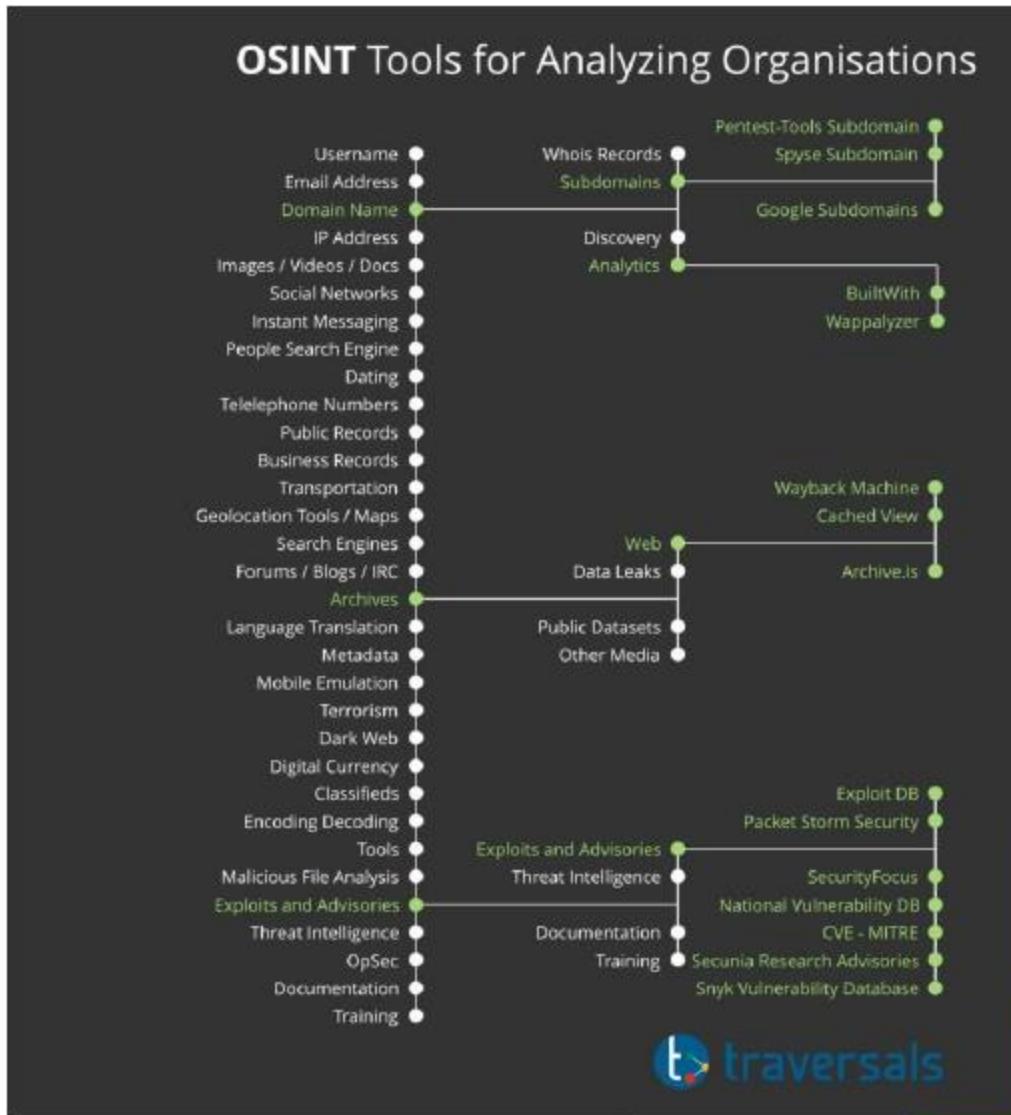
- Discovery
- Nombre de dominio
 - Registros whois
 - Subdominios
 - Certificados
 - Registros DNS
- Etc...



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...

Fuente: 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

GOOGLE DORKS - Búsqueda avanzada (1)

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

- 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

The screenshot shows the homepage of the Google Hacking Database. At the top, it features the "GOOGLE HACKING-DATABASE" logo and the tagline "Welcome to the google hacking database". Below this, a message reads: "We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe!" A search bar at the top has the placeholder "Search Google Dorks". Below the search bar, there are two input fields: "Category: All" and "Free text search: [empty field]". Underneath these, a section titled "Latest Google Hacking Entries" displays a table of recent findings. The table has columns for Date, Title, and Category. The data is as follows:

Date	Title	Category
2014-05-19	inurl:itsthealth.jsp	Various Online Devices
2014-05-08	intext:"NitroSilver" inurl:login.asp...	Various Online Devices
2014-05-06	inurl:"/public/photservice-ws.asmx"	Various Online Devices
2014-05-05	"OpenSSL" AND "1.0.1 server at..."	Vulnerable servers
2014-04-10	inurl:"/jboss/graph_view.php" OR inurl:...	Network or vulnerability data

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

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

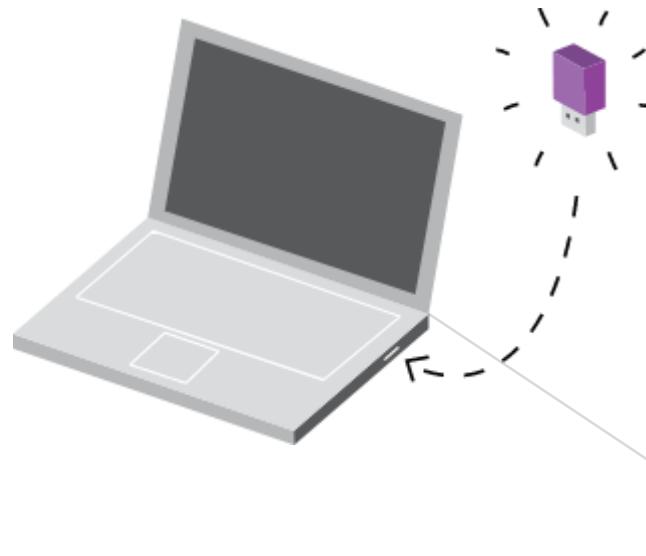
VPN

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:

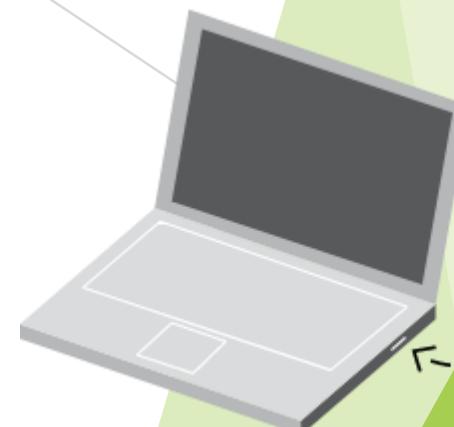
CVE, CCE <https://nvd.nist.gov> <https://www.exploit-db.com/webapps>

. 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.

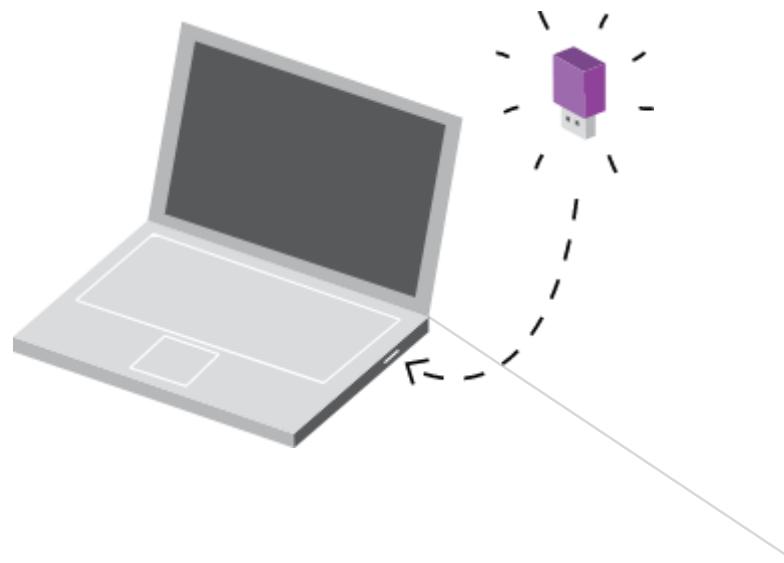
. Información Geográfica y a pie de calle:

Google Maps, Bing Maps.

. Información Personal:

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

.Listines telefónicos



Herramientas

Busqueda por nombre en RRSS

Lullar

The screenshot shows a search results page for the name 'alvarobadia'. At the top, there is a search bar with the query 'alvarobadia' and a magnifying glass icon. Below the search bar, the text 'Found: 14 Processed: 385 / 383' is displayed, along with buttons for 'Show All', 'Show Found', and 'Show Not Found'. The results are presented in a grid format:

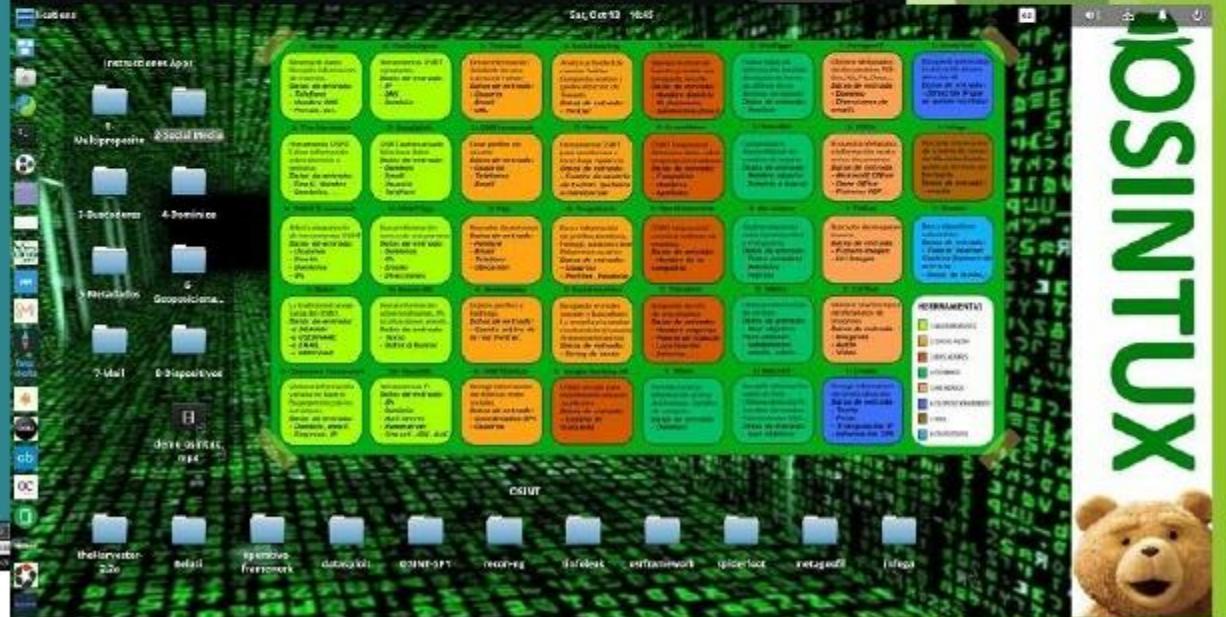
Platform	Category	Description
Snapchat	social	Account Found
MCUUID (Minecraft)	gaming	Account Found
Imgur	images	Account Found
Wattpad	social	Account Found
Scratch	coding	Account Found
GitHub	coding	Account Found
Gravatar	images	Account Found
SlideShare	social	Account Found
DeviantArt	images	Account Found
TikTok	social	Account Found
GitHub	coding	Account Found
Smule	music	Account Found
Roblox	gaming	
Fortnite Tracker	gaming	

To the right of the grid, a detailed list of found accounts is shown:

SITE	CATEGORY	LINK
DeviantArt	images	https://www.deviantart.com/alvarobadia
Fortnite Tracker	gaming	https://fortnitetracker.com/profile/alvarobadia
Github	coding	https://github.com/alvarobadia
Gravatar	images	http://en.gravatar.com/profile/alvarobadia
Imgur	images	https://api.imgur.com/account/v1/account
MCUUID (Minecraft)	gaming	https://playeido.co/api/player/mcuuid
Roblox	gaming	https://auth.roblox.com/v1/username
Scratch	coding	https://scratch.mit.edu/users/alvarobadia

Distros Linux OSINT

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



Distro Osintux

Listado de herramientas instaladas

- [Beauti v0.2.4.1](#)
- [Creepy v1.4](#)
- [Crunchbase](#)
- [Dataexploit for OSINT](#)
- [Dmitry \(Deepmagic information gathering tool\)](#)
- [Exifool v11.03](#)
- [Google Hacking Database](#)
- [Infoga – Email Information Gathering vMA110k](#)
- [GeoIP](#)
- [Glossedoor](#)
- [Knownm](#)
- [Metagoofil v4.1.6.11045](#)
- [MentionMap](#)
- [Metagoofil v2.2](#)
- [MrLocque](#)
- [Netcraft](#)
- [Shodan](#)
- [Opencorporates](#)
- [Operative Framework](#)
- [OSINTSpy v0.0.1](#)
- [OSRFramework v2018](#)
- [OSINTFramework](#)
- [PITA](#)
- [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 [Máster de Ciberseguridad](#), organizado por [Eleven Paths](#) (Telefónica), el Campus Internacional de Ciberseguridad, y la [UCAM](#).

Los dos precusores 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...

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

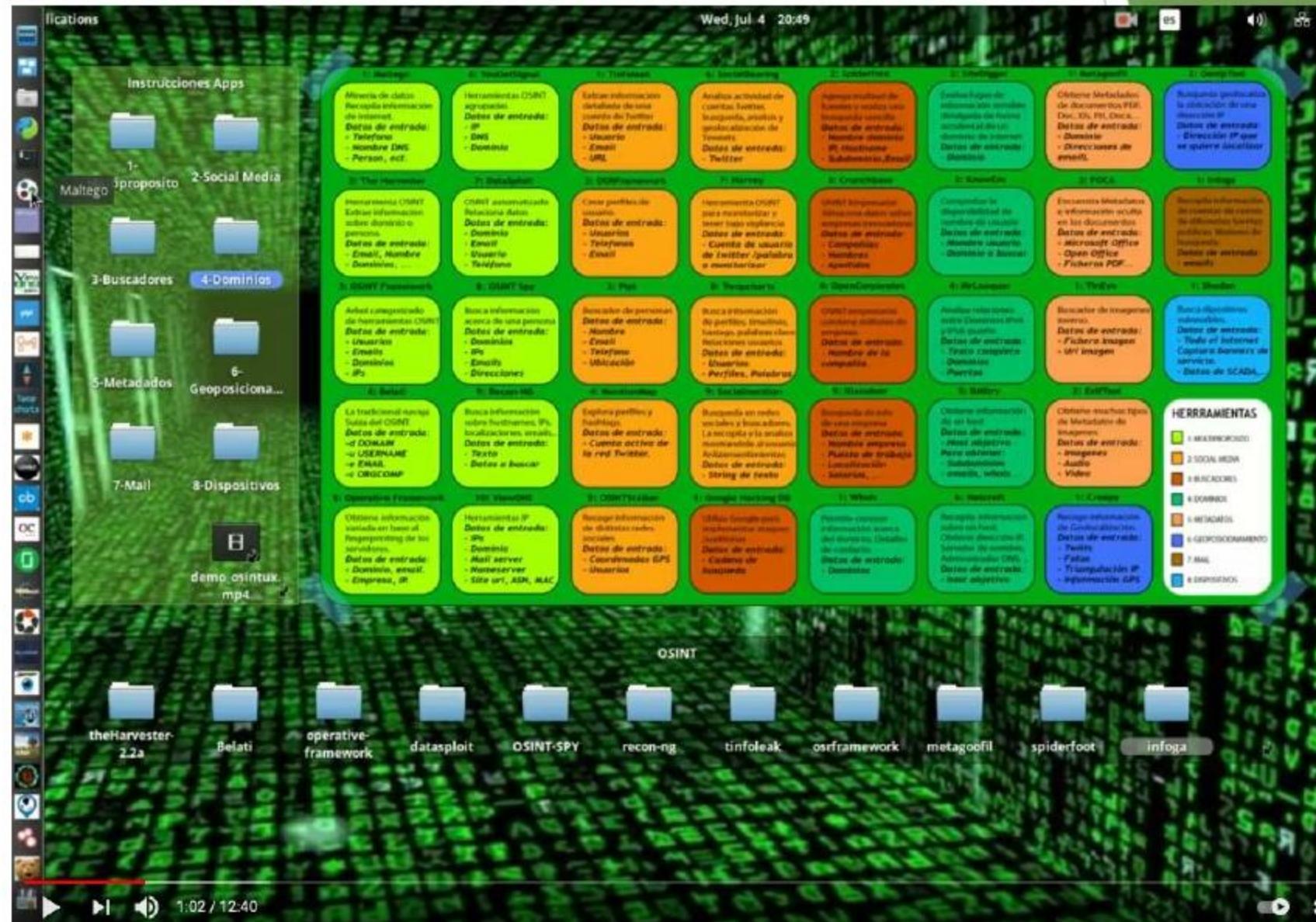
XUNLISUX



Distro Osintux

Listado de herramientas instaladas (v1.0)

- Belati v 0.2.4.1
- Creepy v1.4
- Crunchbase
- Dataspoilt for OSINT
- Dmitry (Deepmagic information gathering tool)
- Exitool v11.03
- Google Hacking Database
- Infoga – Email Information Gathering vM4110k
- GeoIP
- Glassdoor
- Knowem
- Maltego v4.1.6.11045
- MentionMap
- Metagoofil v2.2
- MrLoquer
- Netcraft
- Shodan
- Opencorporates
- Operative Framework
- OSINT-Spy v0.0.1
- OSRFramework v2018
- OSINTFramework
- PIFI
- 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.



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

A detailed screenshot of a Google Images search result for 'josep rull twitter'. The search bar shows 'josep rull twitter'. The results page includes a thumbnail of a man in a suit at a desk, a text snippet about his Twitter account, and a section for 'Imágenes visualmente similares' (Visually similar images) showing other photos of the same man. Below this, there's a link to 'Páginas con imágenes que coinciden con la búsqueda' (Pages with images matching the search) leading to an article from 'el Periódico' titled 'La 'profecía belga' de Rull'. The article features a large image of Josep Rull in his office, which has been manipulated to include Belgian comic book panels ('Tintín') overlaid on the background. The original image shows him at his desk with a computer monitor and papers.

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/main/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://xmh57jzrnw6insl.onion/
Evil FOCA	https://github.com/ElevenPaths/EvilFOCA	Maltego	https://paterva.com	Ubuntu	https://ubuntu.com
Exiftool	http://search.cpan.org/~exiftool/	MrLooquer	https://mrlooquer.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/ischulen/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		
HavieBeenPwned	https://haveibeenpwned.com	Reddit	https://reddit.com		
HeSidoHackeado	https://hesidohackeado.es	Regexper	https://regexper.com		
		Searx	https://searx.me		
		Shodan	https://shodan.io		