OSINT

Open-Source INTelligence

INTRODUCCIÓN A LA INTELIGENCIA EN FUENTES ABIERTAS

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

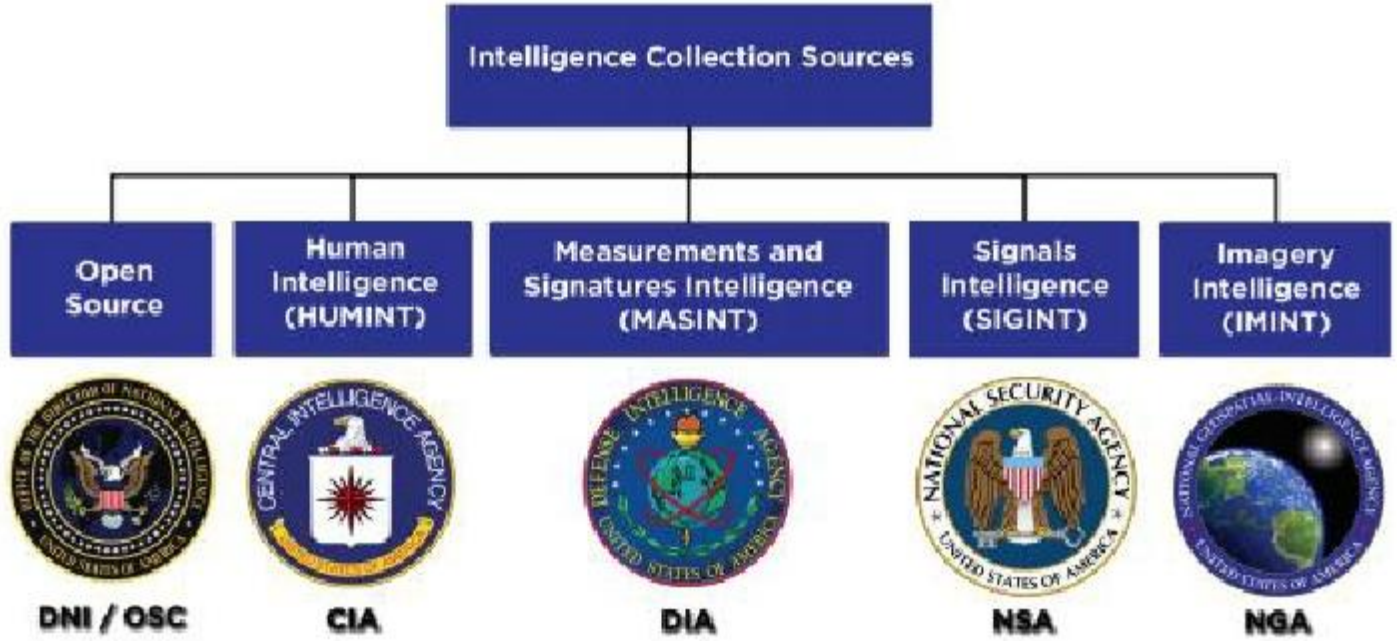
Sun Tzu en el Arte de la Guerra – Escrito entre el 400 y 320 A.C.

Inteligencia

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

Detectigal.com

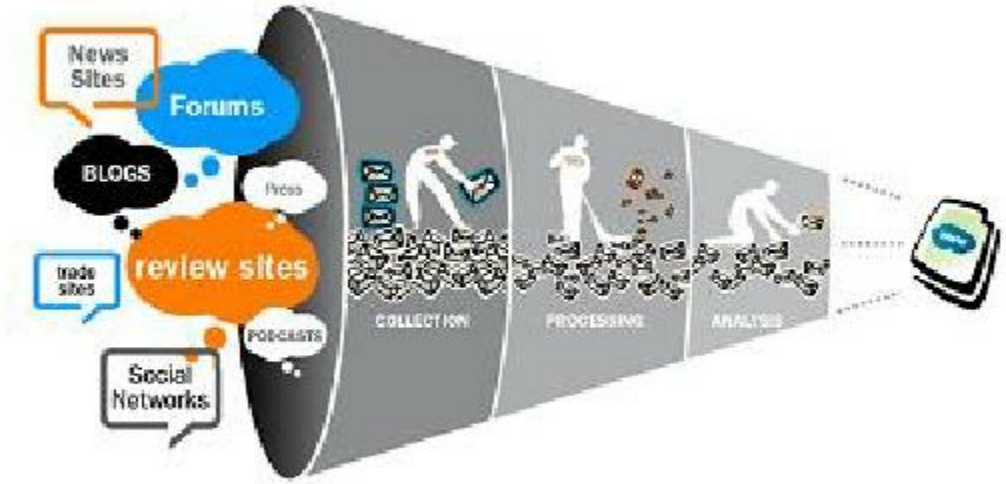
Colección de fuentes de inteligencia



- 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

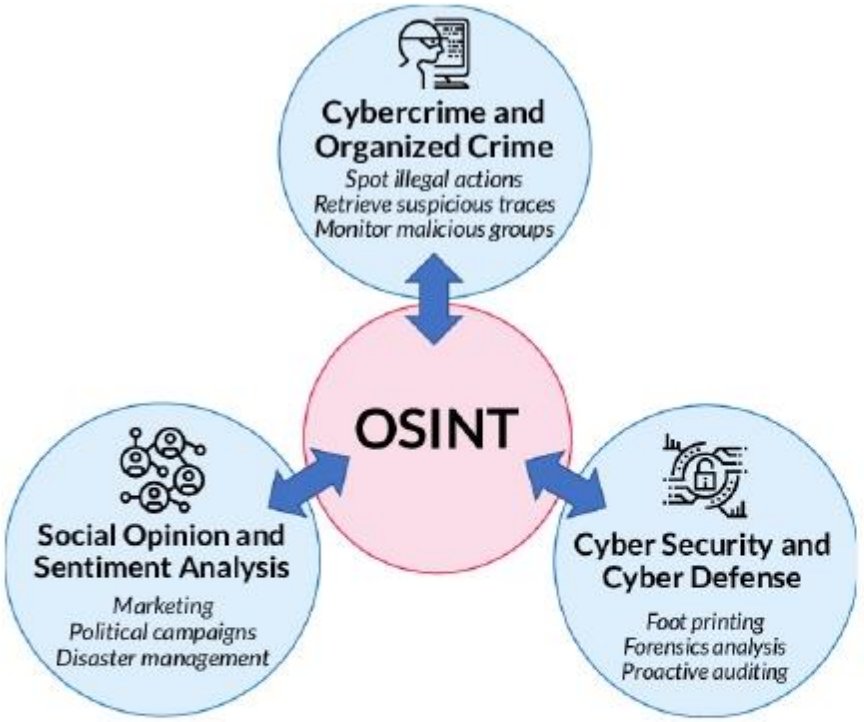
Principales registros públicos

- 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:

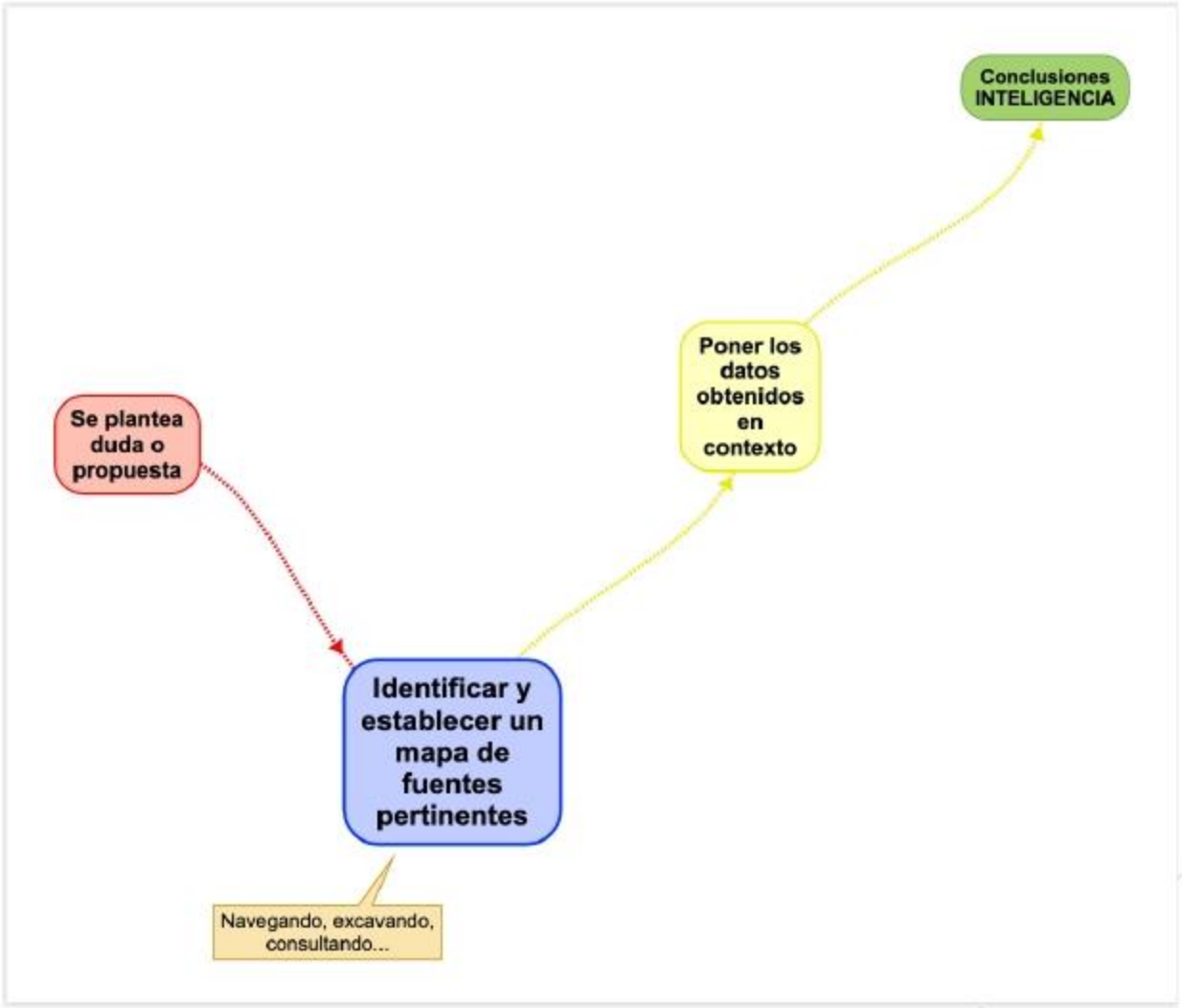
En esta fase se procede a analizar la evidencia con objeto de encontrar hechos y conclusiones relevantes para la resolución del incidente de ciberseguridad

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



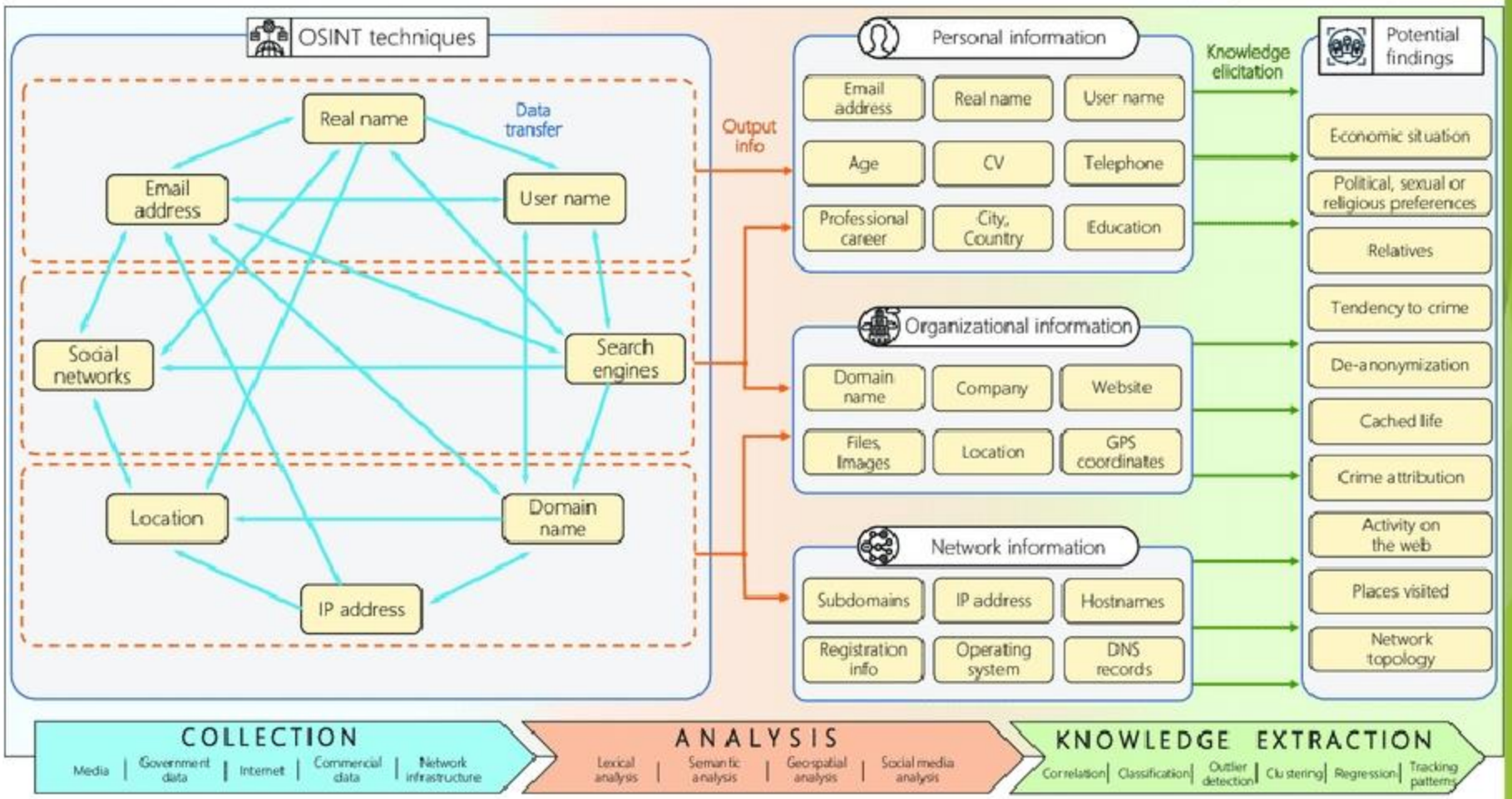
Ciclo de inteligencia

- 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

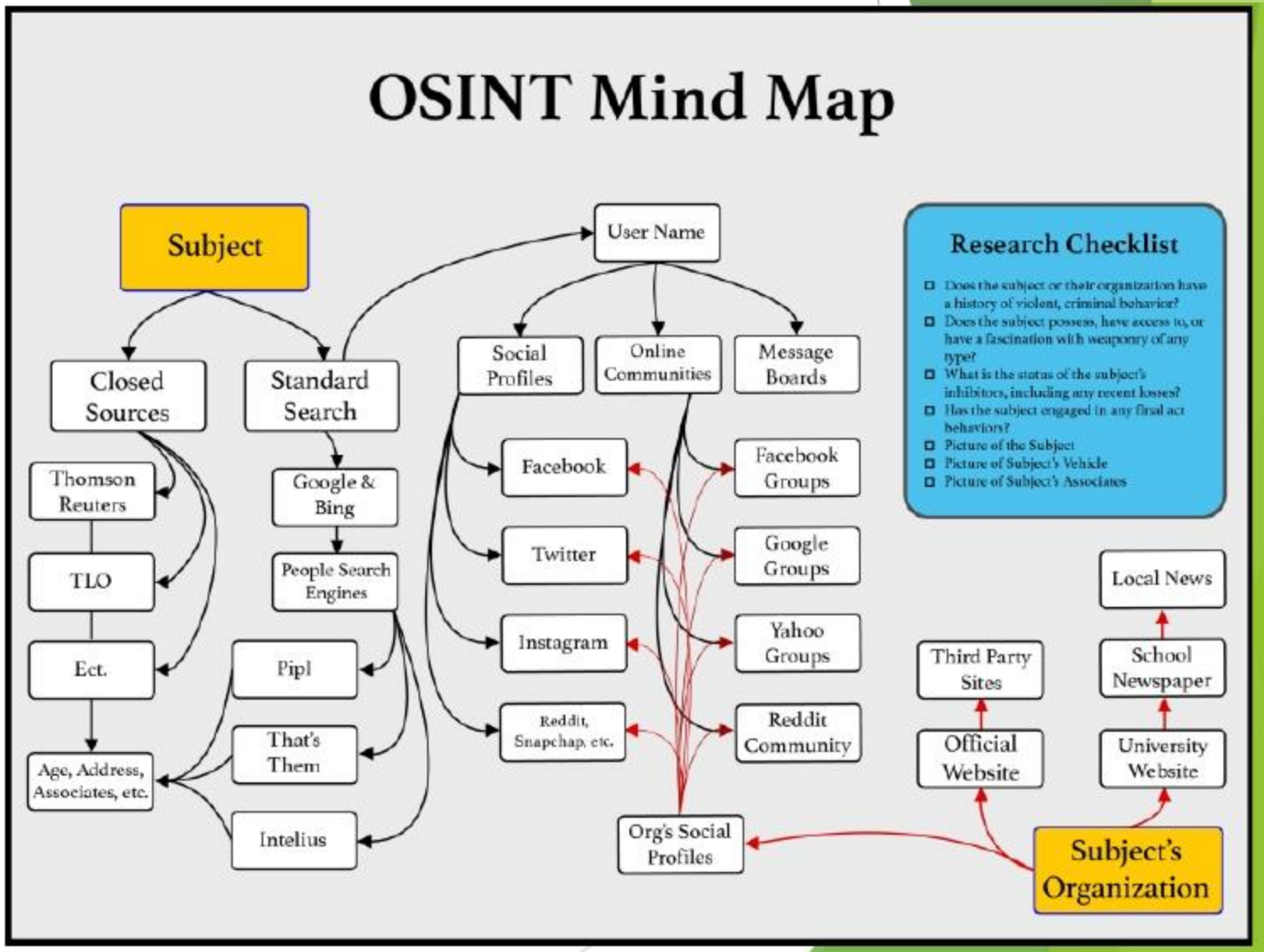


Mapa mental (Ejemplo de investigación)

- **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

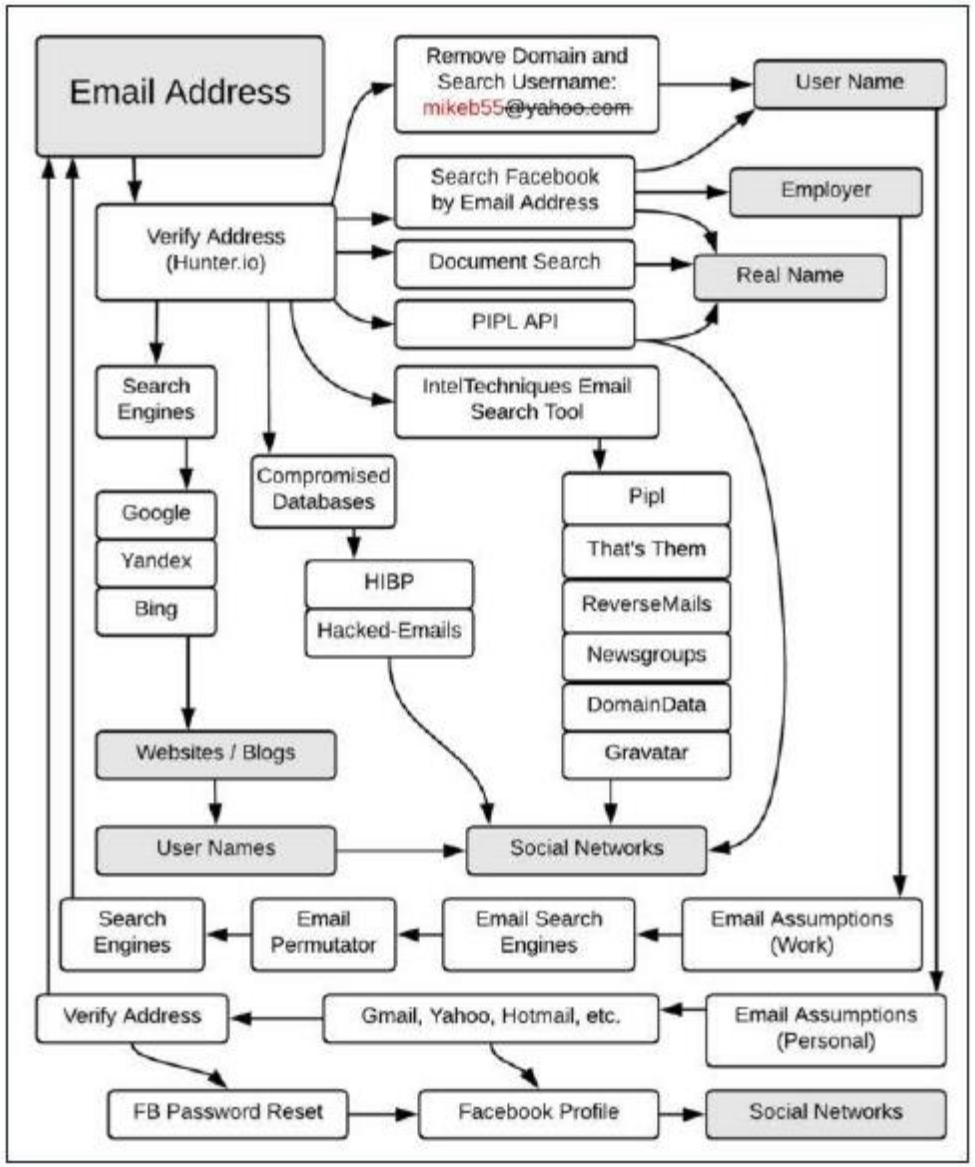
- Fuente: protectioncircle.org



Investigación de perfiles digitales

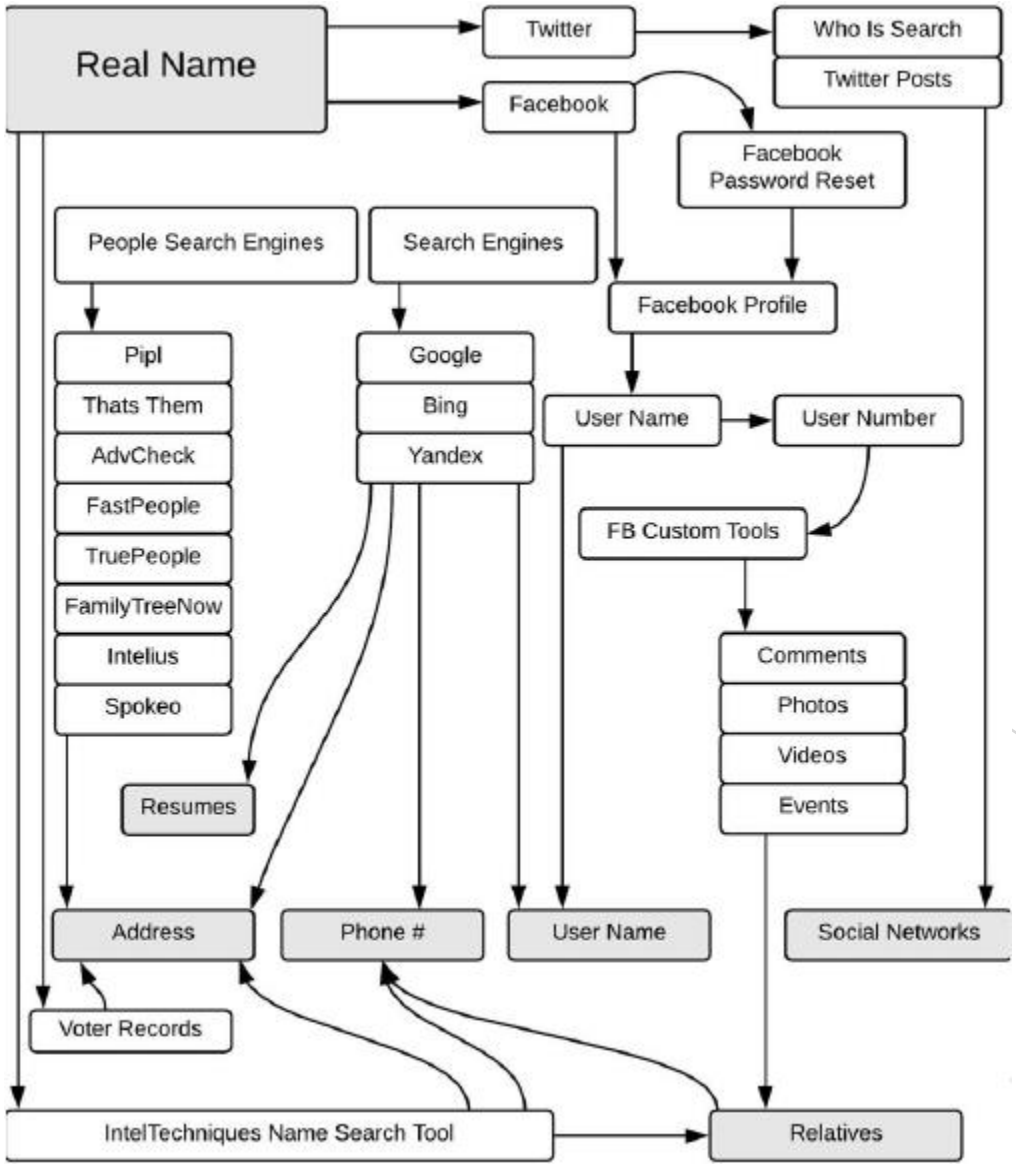
- Email
- Nombre real
- Nombre de dominio
- Localización
- Teléfono
- Etc...

Fuente: inteltechniques.com



Investigación de perfiles digitales

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

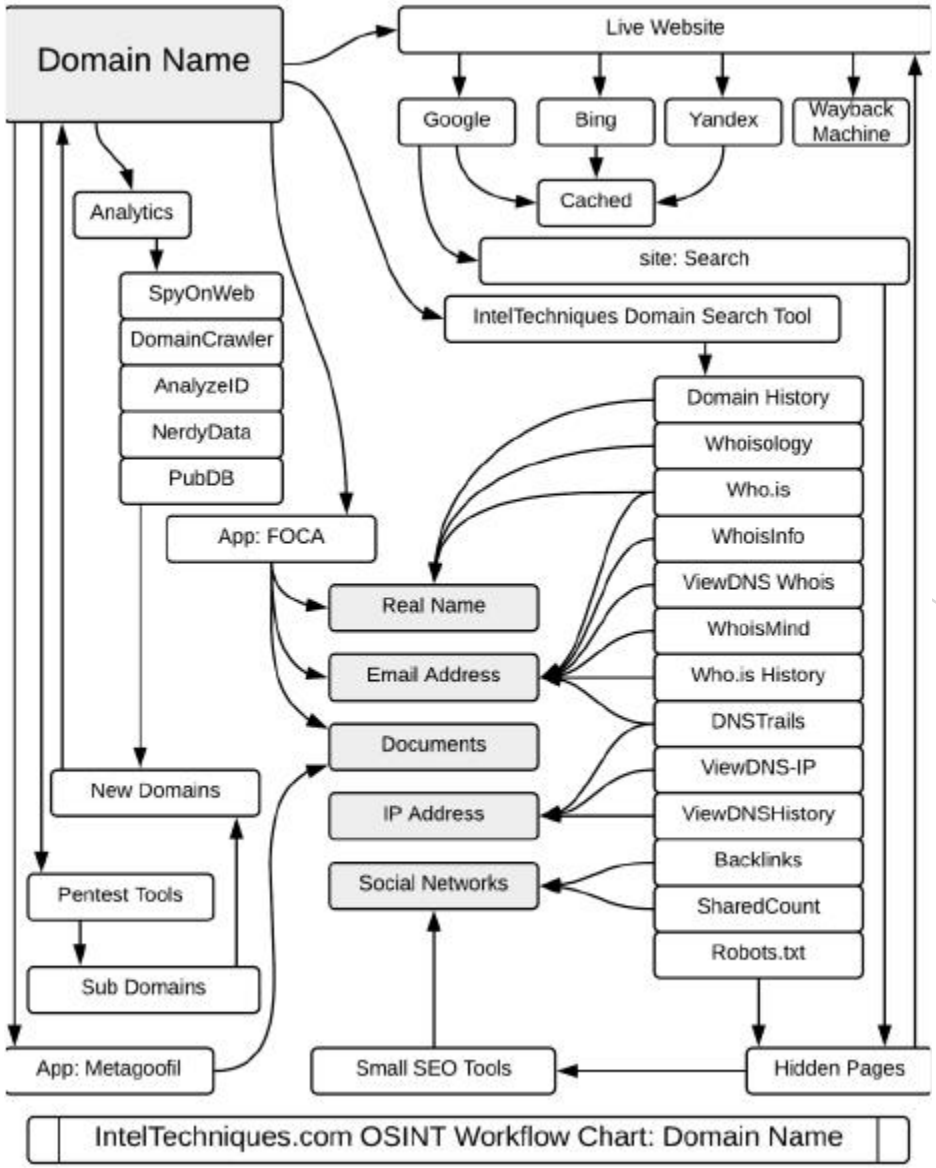


Fuente: inteltechniques.com

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...

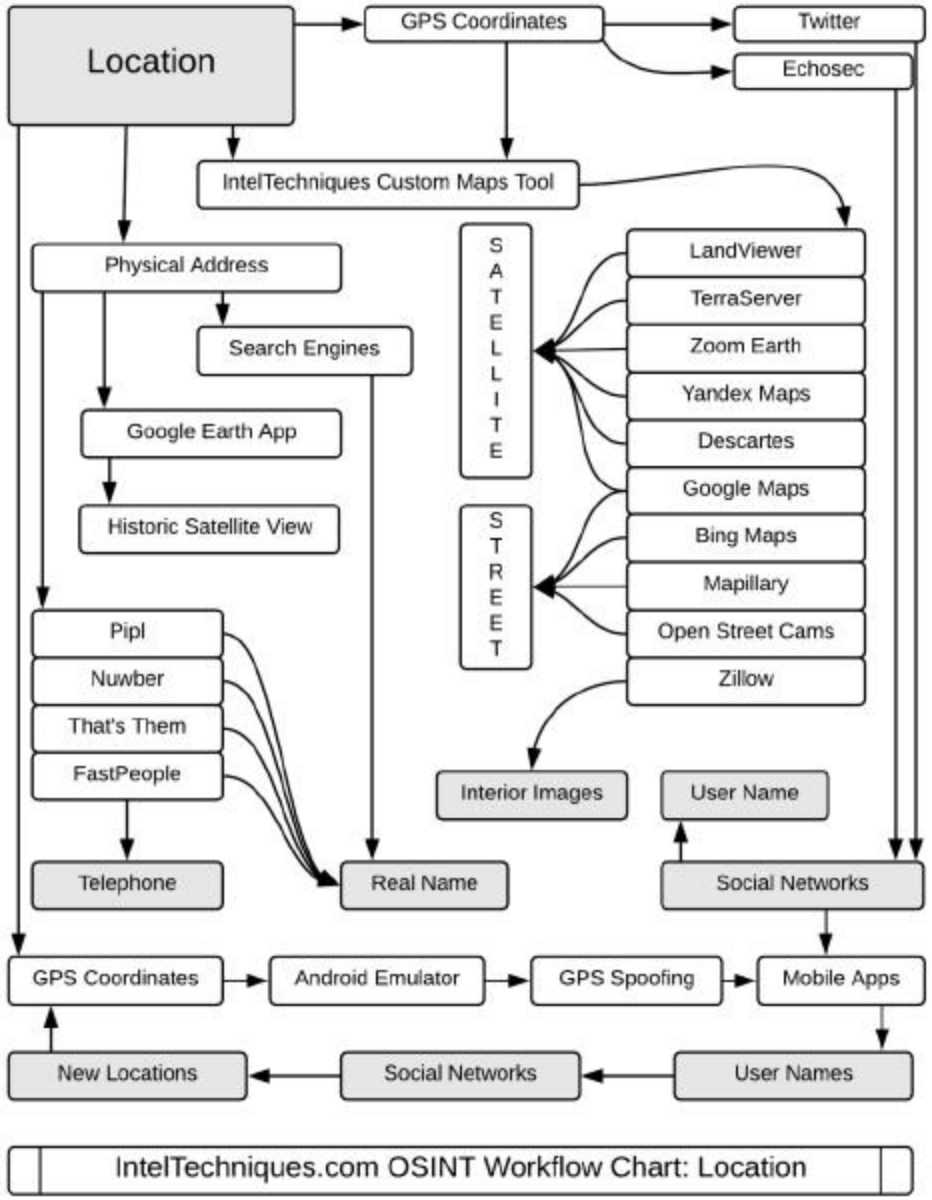


Fuente: inteltechniques.com

Investigación de perfiles digitales

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

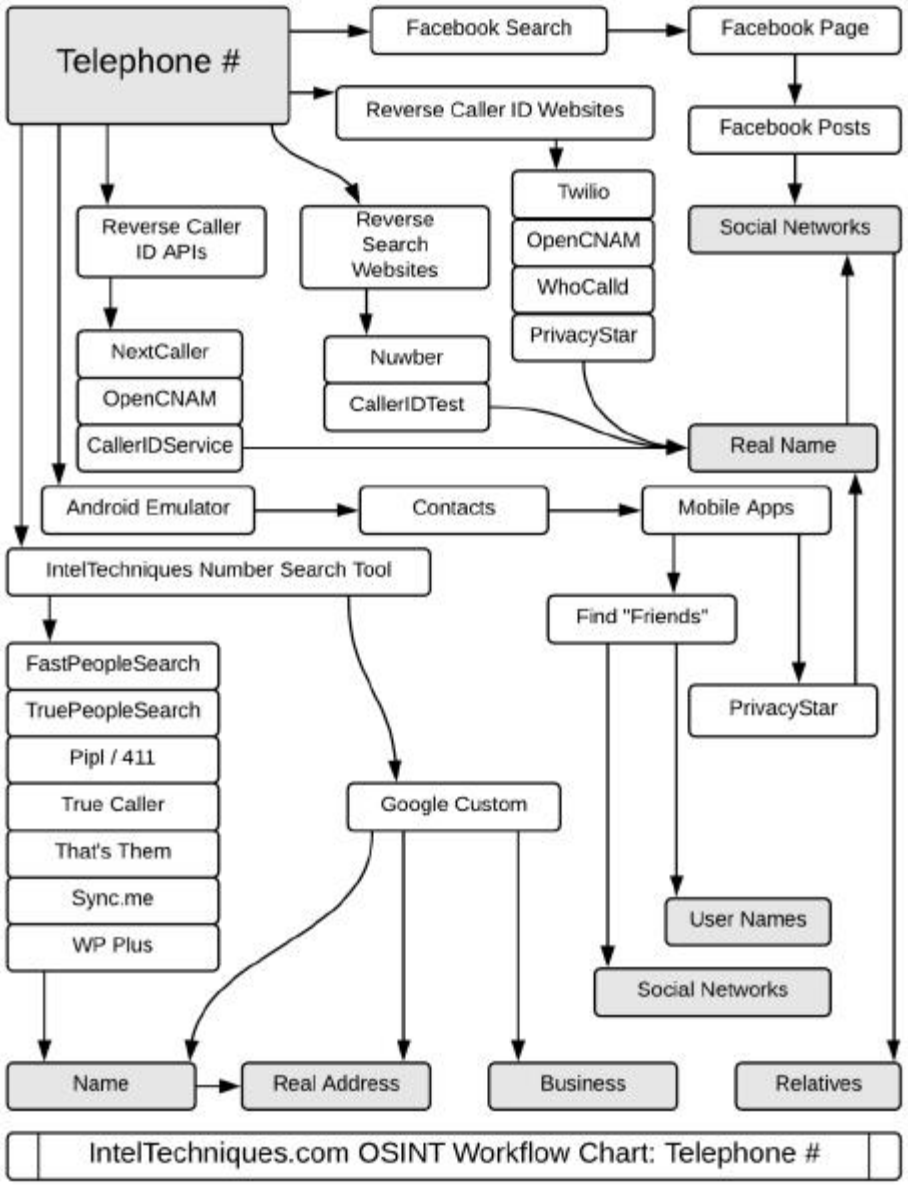
Fuente: inteltechniques.com



Investigación de perfiles digitales

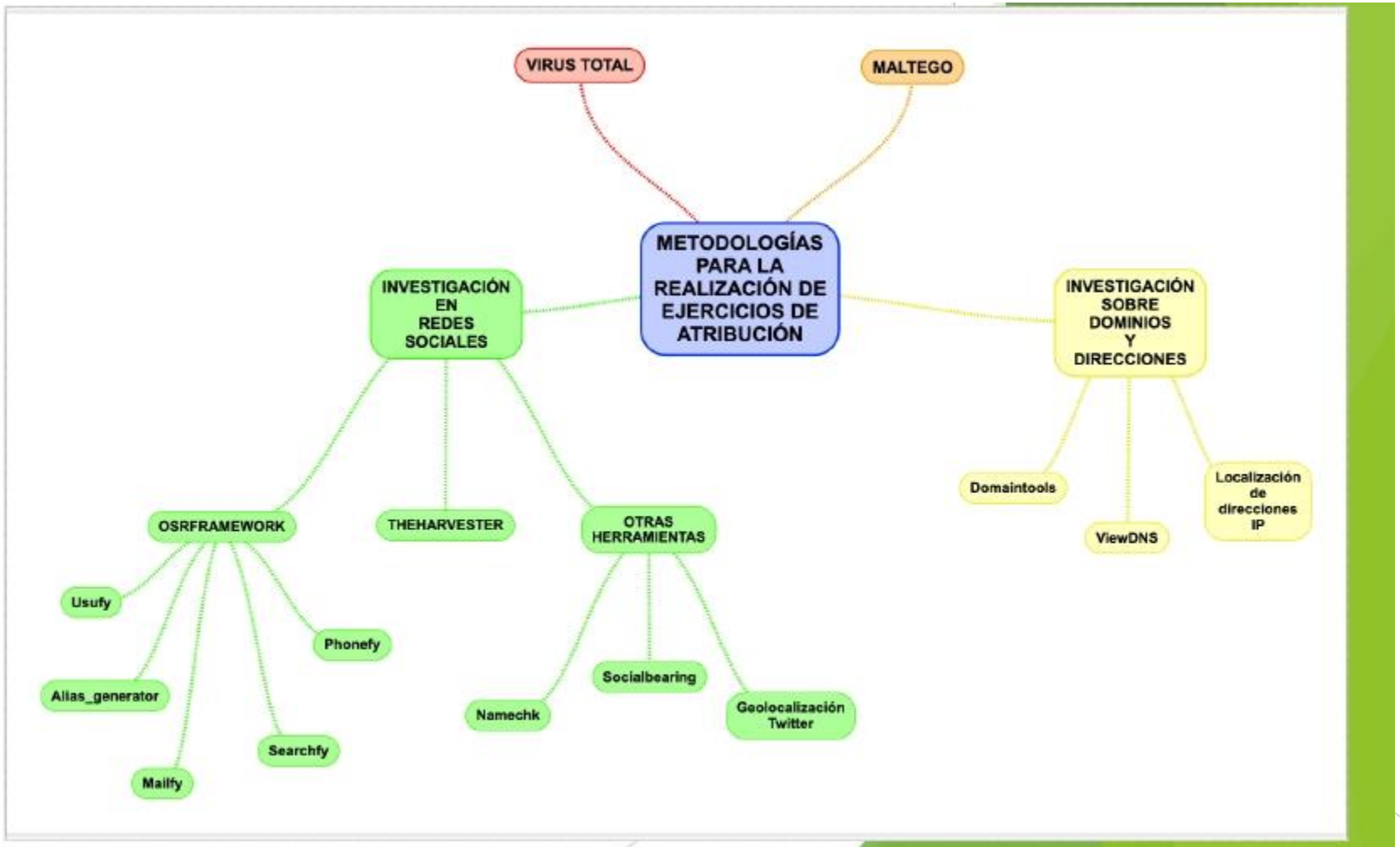
- Email
- Nombre real
- Nombre de dominio
- Localización
- Teléfono
- Etc...

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...

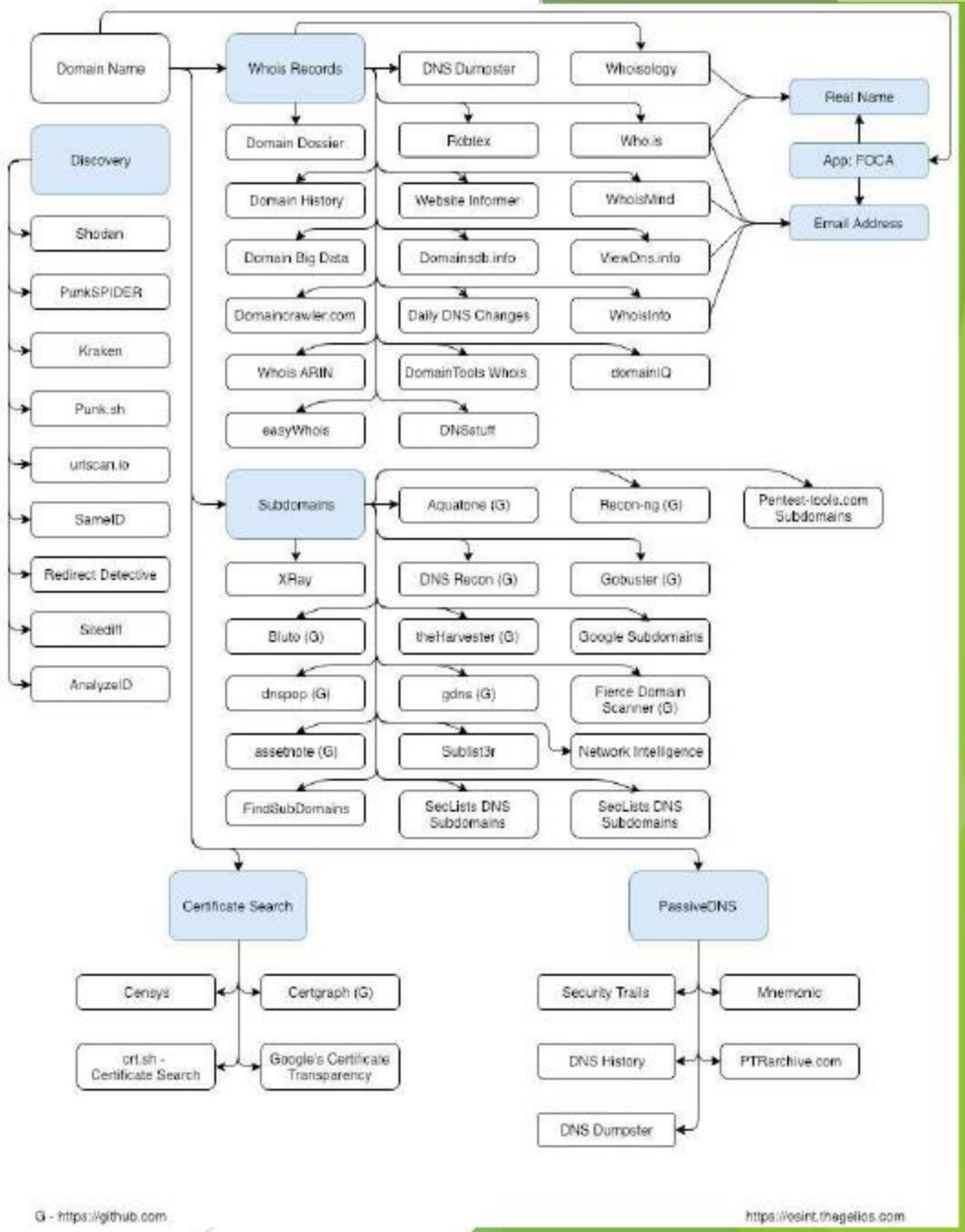


Fuente: campusciberseguridad.com

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
- Termino concreto en el título de una pagina
- 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,xlsl,...)	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
-	Simbolo de exclusion, se excluirá de los resultados lo que vaya a continuación de el	dorking -Google
*	Se usa como comodín, el asterísco 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

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
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:

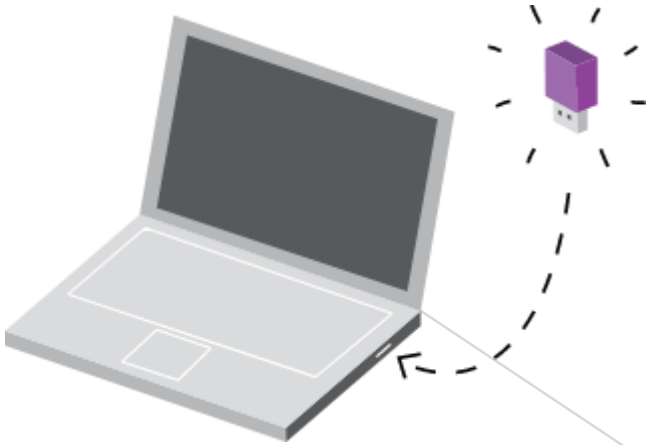
Robtex
Viewdns.info

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

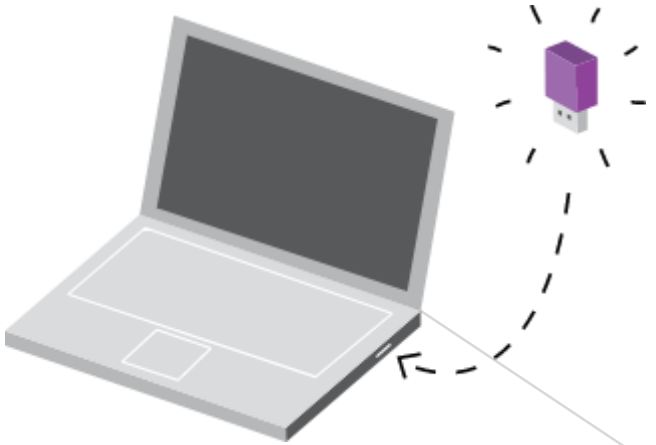
. SEO:
https://moz.com/researchtools/ose
http://explorer.cognitiveseo.com
https://es.majestic.com
Domain tolos

.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

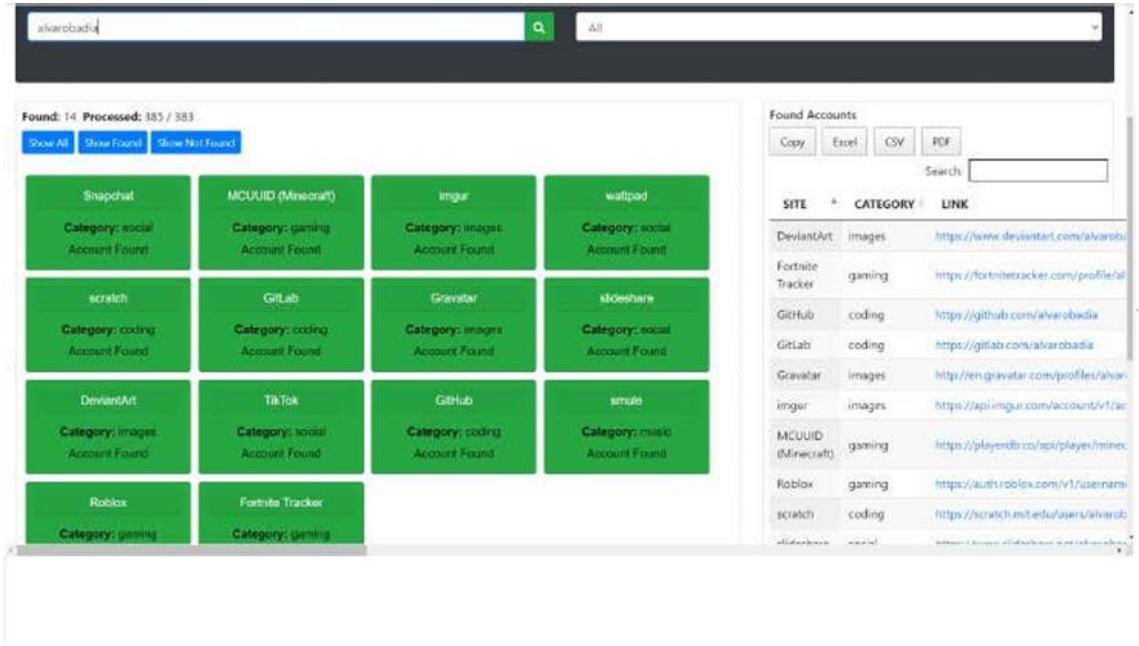
.Listines telefónicos



Herramientas

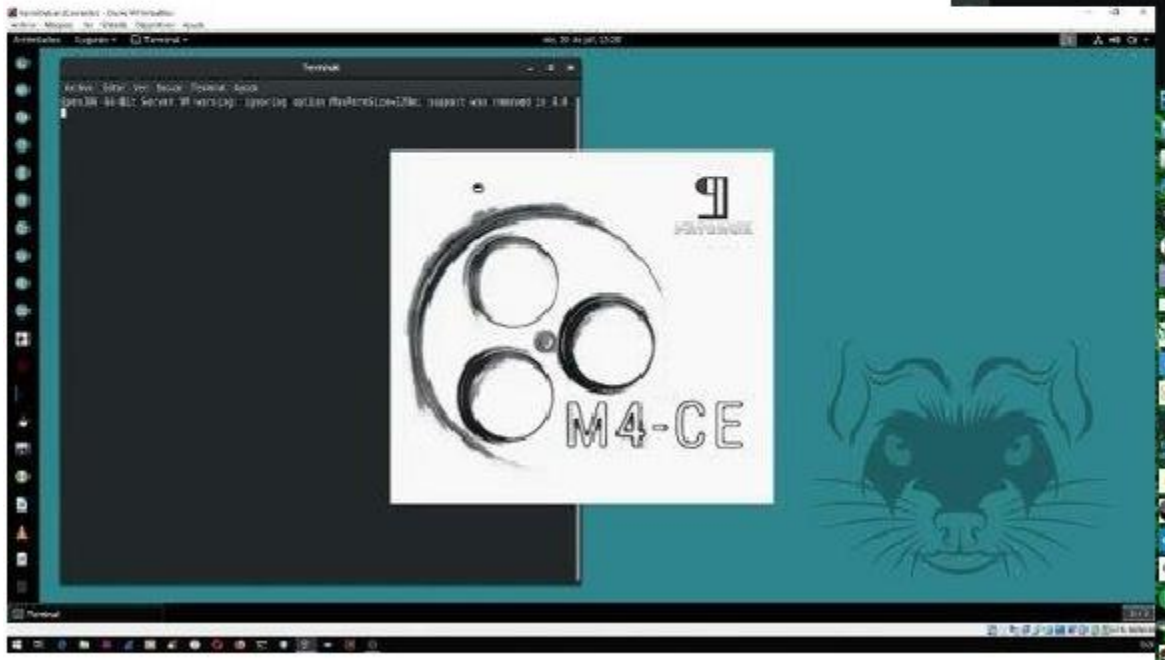
Busqueda por nombre en RRSS

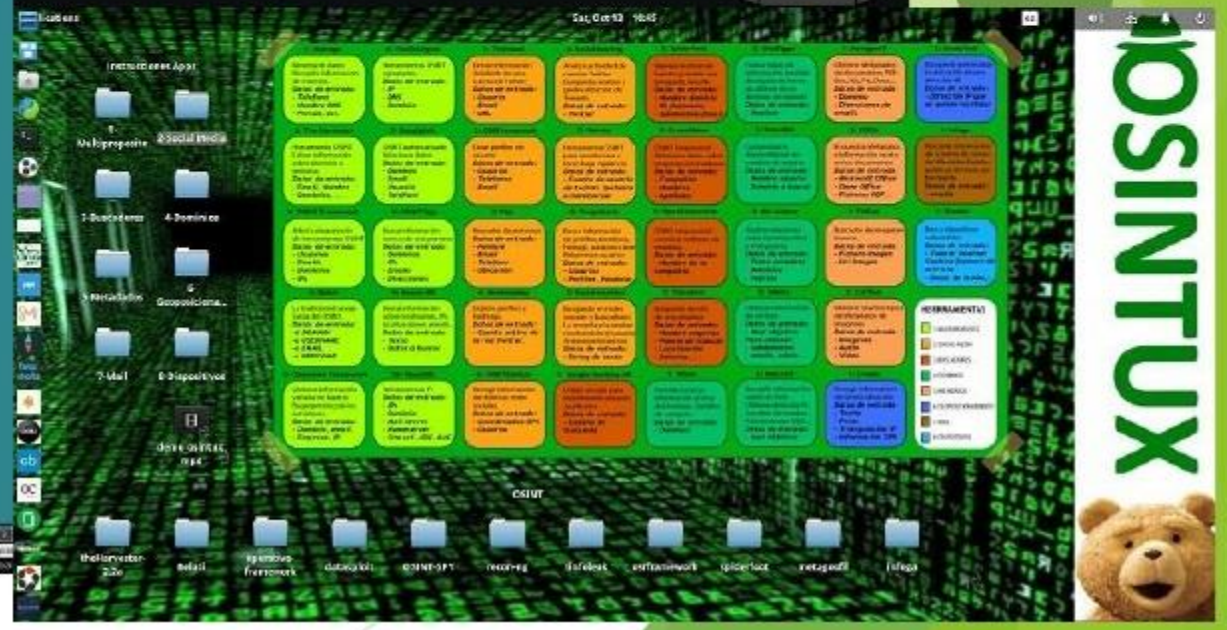
Lullar



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
- Dataspiolt for OSINT
- Dmitry (Deepmagic information gathering tool)
- Exiftool v11.03
- Google Hacking Database
- Infoga – Email Information Gathering v.M4110k
- GeoIP
- Glassdoor
- Knowem
- Maltego v4.1.6.11045
- MentionMap
- Metagoofil v2.2
- Mr.Looquer
- 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 (Télefonica), el Campus Internacional de Ciberseguridad, y la UCAM.

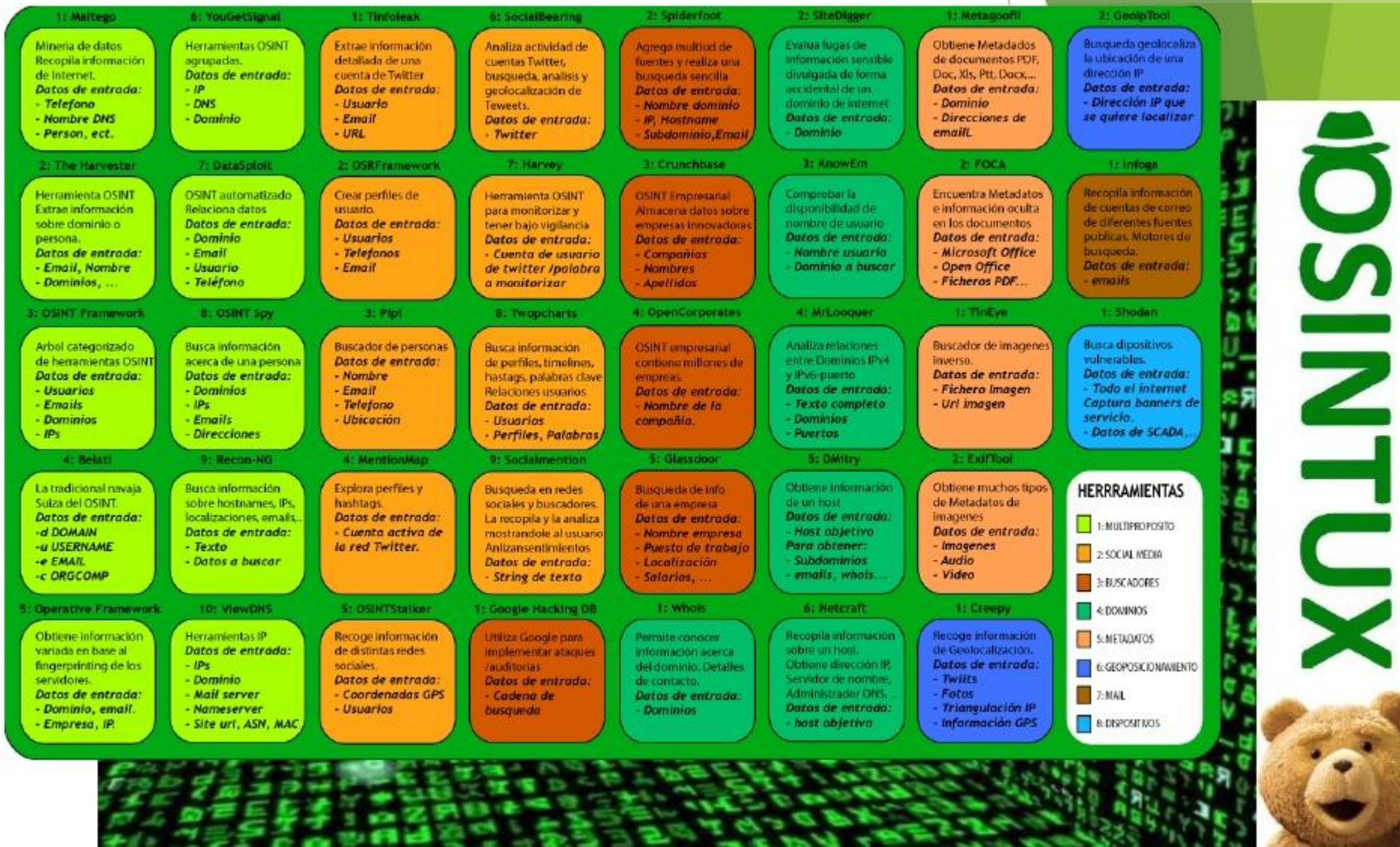
Los dos precusores del proyecto son:

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 continúa búsqueda e investigación de los factores que intervenen en la mejora de la implantación de procesos seguros en la empresa.

Categorías de herramientas Osintux

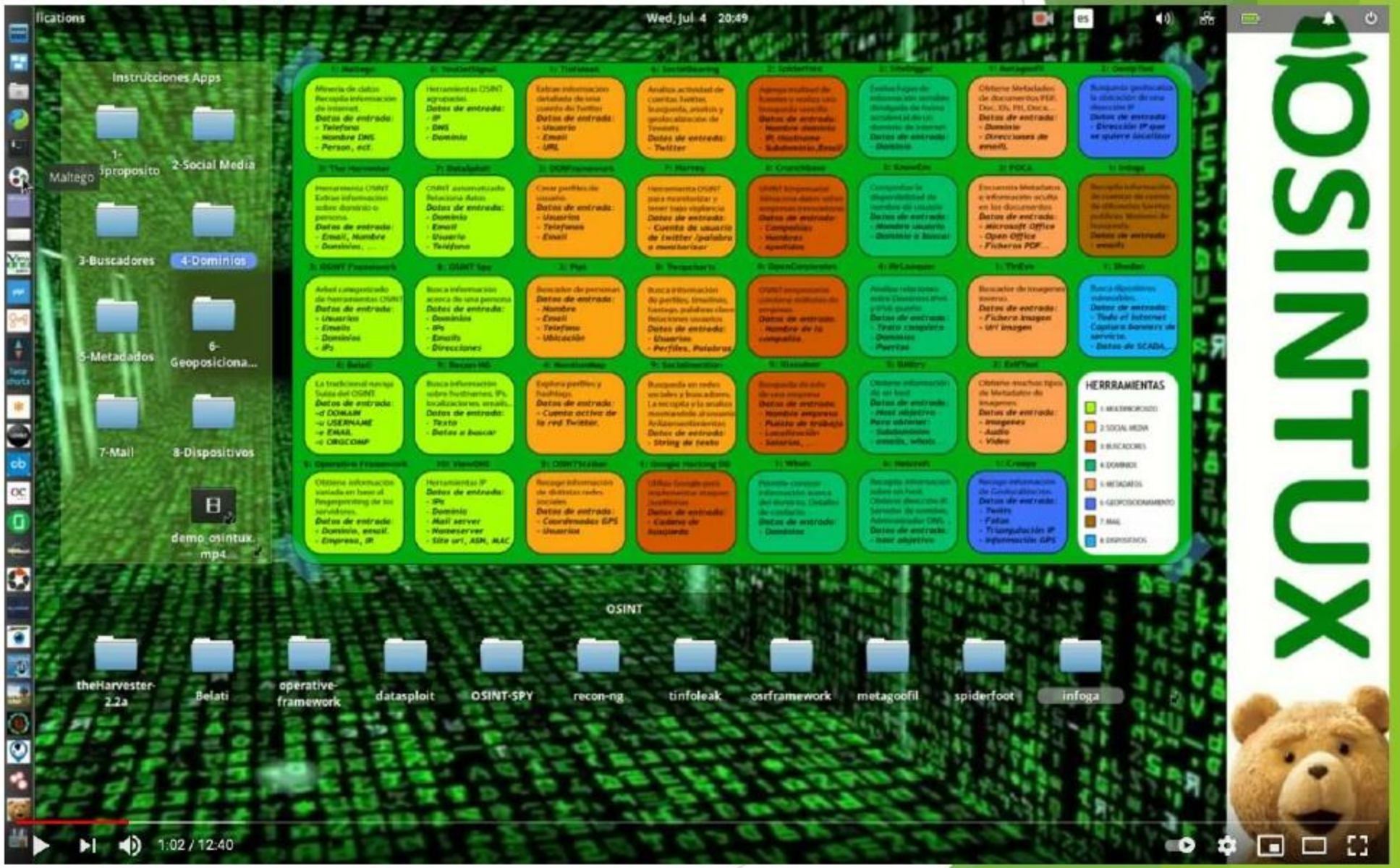
- Multi propósito
- Social media
- Buscadores
- Dominios
- Metadatos
- Geoposicionamiento
- Mail
- Dispositivos
- Etc...



Distro Osintux

Listado de herramientas instaladas (v1.0)

- 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
- GeoIP
- 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



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

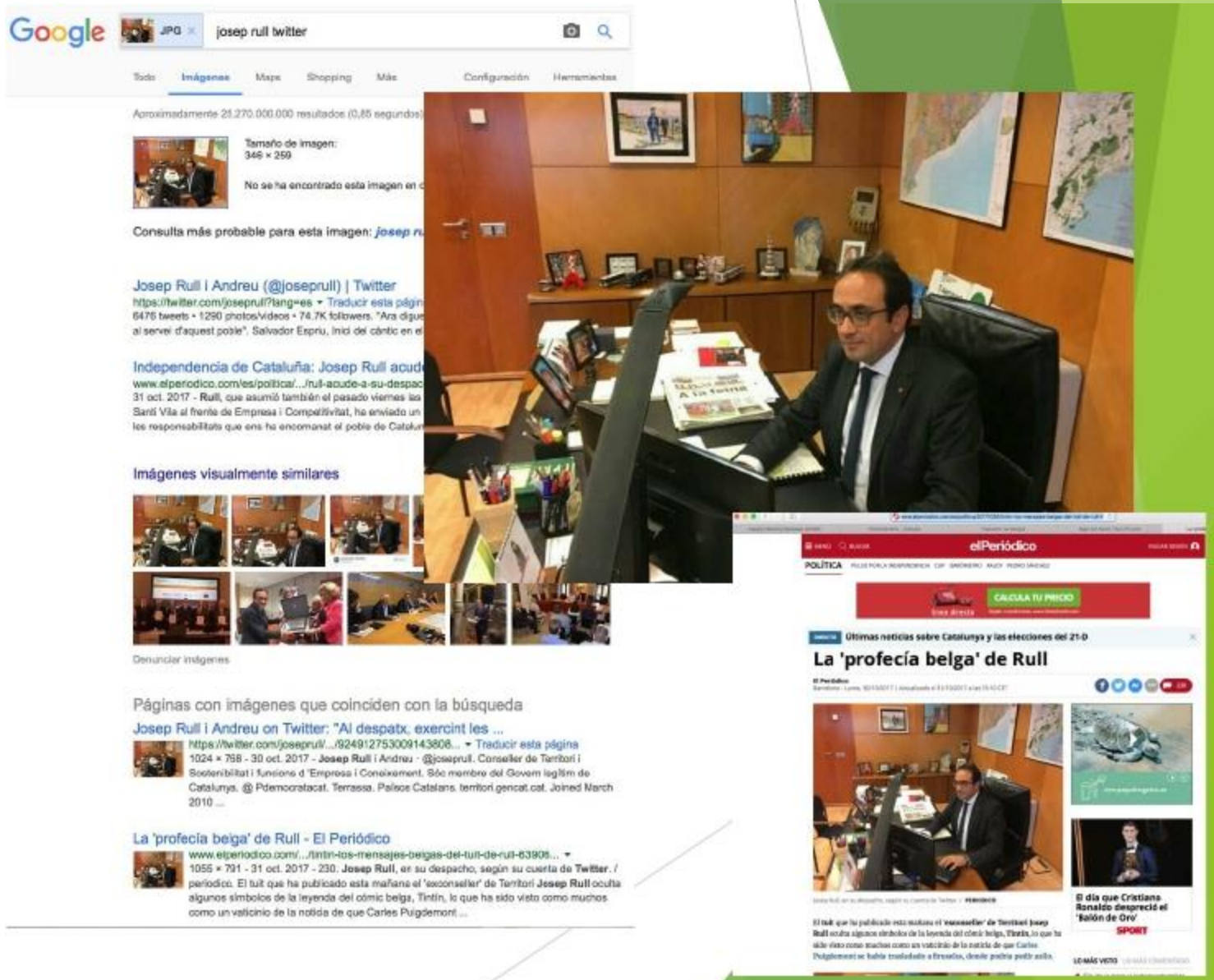
Si utilizamos la herramienta online FotoForensics podemos apreciar que los dos mapas de Bélgica muestras una luminancia distinta a la del resto de la foto.

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/tintin-los-mensajes-belgas-del-tuit-de-rull-6390 691



Repositorio de herramientas OSINT

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