

Security and Trust in Distributed Systems

Master Degree in New Technologies in Computer Science

2022/23

Open Source Intelligence (OSINT)

**Antonio Ruiz Martínez, Pantaleone Nespoli,
Félix Gómez Mármol**

Outline

Part I

- What's OSINT?
- OSINT Techniques
- OSINT Tools
- OSINT Workflows

Part II

- Maltego
 - Getting started
 - Developing a new transform

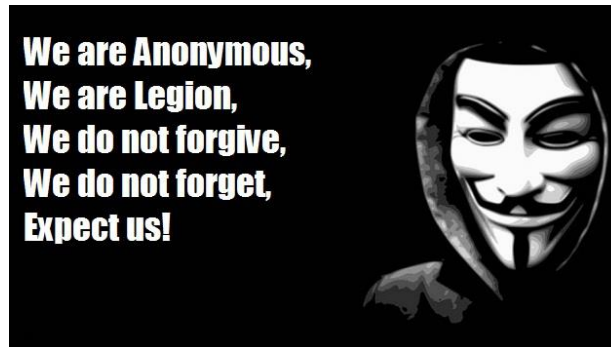
What's OSINT?

Cyber Threat Intelligence

- Its **key mission** is to research and analyze **trends** and **technical developments** in three areas



Cybercrime



Hacktivism

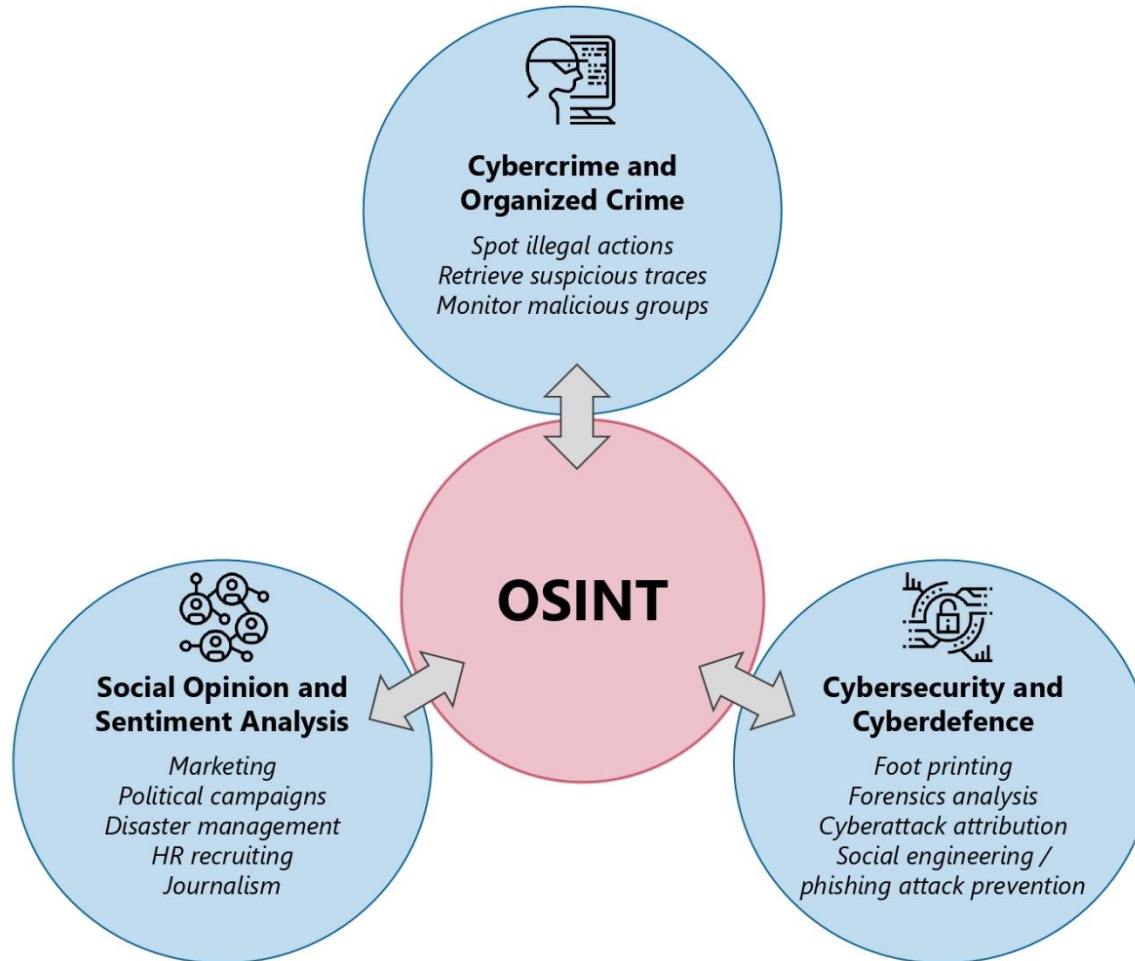


Cyberespionage

Cyber Threat Intelligence

- Collection of intelligence using different means
- **Open Source Intelligence (OSINT)**
 - Data collected from publicly available sources
- Social media intelligence
 - Intelligence gathered from social media sites, using both intrusive or non-intrusive means, from open and closed social networks
 - Sentiment analysis
- Human intelligence
 - Information collected and provided by human sources
 - Interrogations and conversations with persons having access to information
 - Social engineering
- Technical intelligence
 - Collection, evaluation, analysis, and interpretation of scientific and technical information
 - SIEM (Security Information and Event Management)

OSINT Use Cases



OSINT Sources



- **Media**

- Newspapers, magazines, radio, television, etc.



- **Internet**

- Online publications, blogs, discussion groups, social media websites (i.e. – Facebook, Twitter, Instagram, etc.)



- **Public Government Data**

- Public government reports, budgets, hearings, telephone directories, press conferences, websites, and speeches



- **Professional and Academic Publications**

- Information acquired from journals, conferences, symposia, academic papers, dissertations and theses



- **Commercial Data**

- Commercial, financial and industrial assessments and databases



- **Grey literature**

- Technical reports, preprints, patents, working papers, business documents, unpublished works, newsletters, etc.

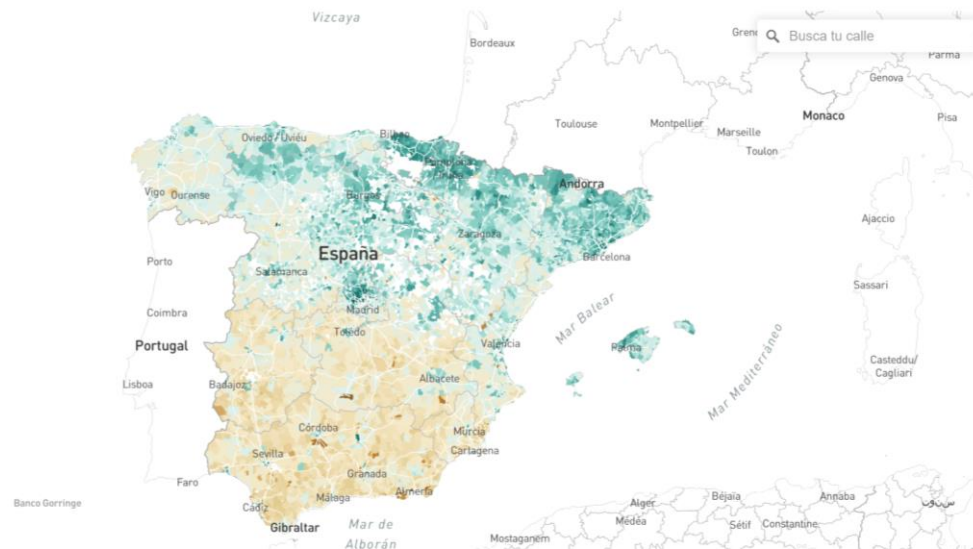
OSINT Sources: Media

- **Income by street name**
- https://elpais.com/economia/2019/09/11/actualidad/1568217626_928704.html

El mapa de la renta de los españoles, calle a calle

Consulta cómo de rico o pobre es tu vecindario comparado con el resto del país y de tu Comunidad Autónoma

Renta por persona (€)
<3000 10.250 >25.000

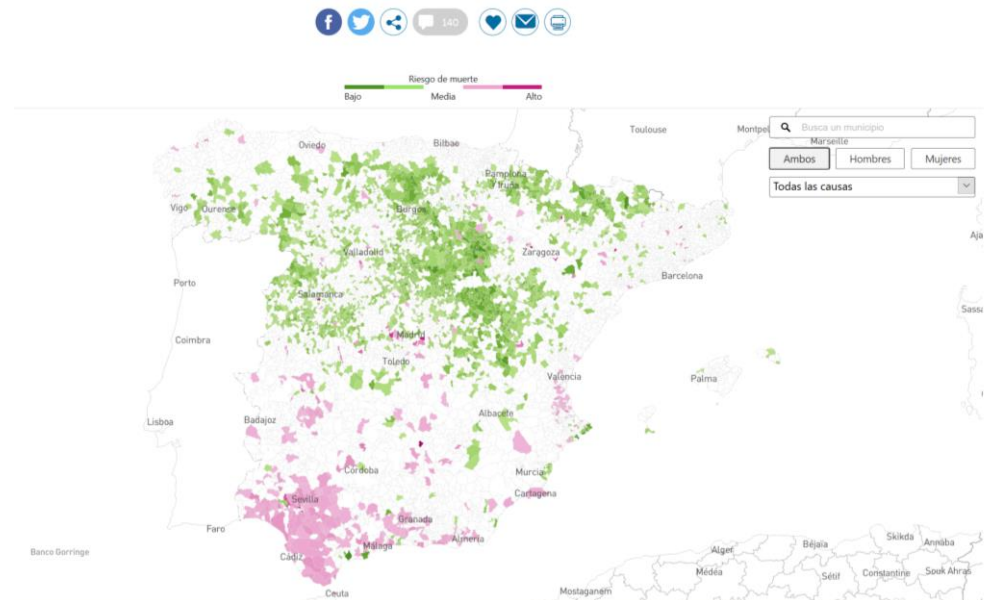


OSINT Sources: Media

- **Mortality by municipality name**
- https://elpais.com/elpais/2020/02/05/ciencia/1580906716_232241.html

El mapa de la mortalidad en España, municipio a municipio

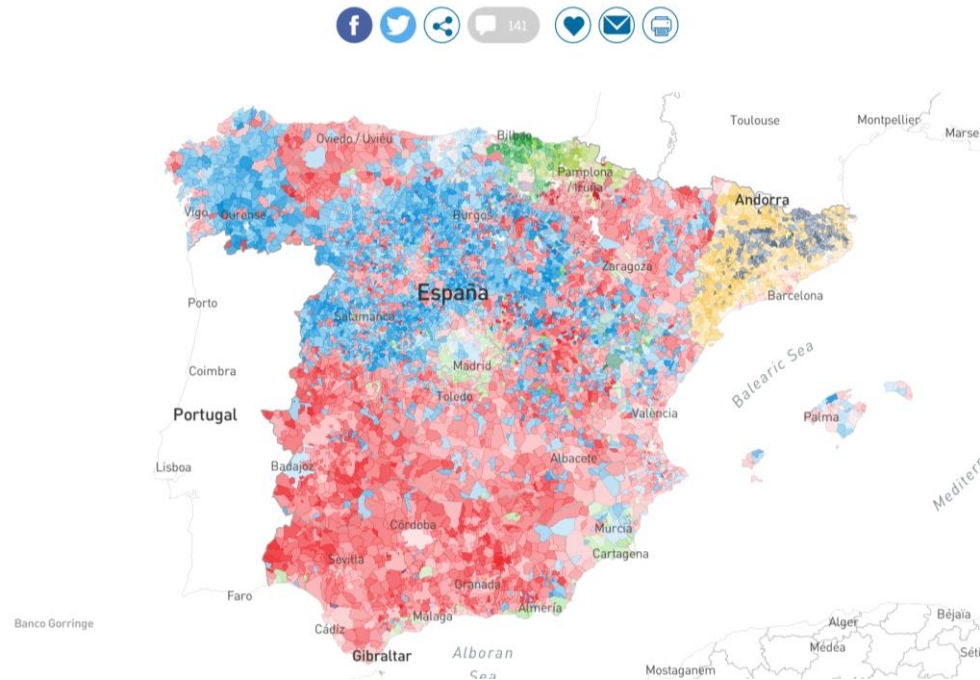
El mayor atlas nacional de los riesgos de muerte, con datos de casi 10 millones de fallecimientos, revela grandes desigualdades geográficas



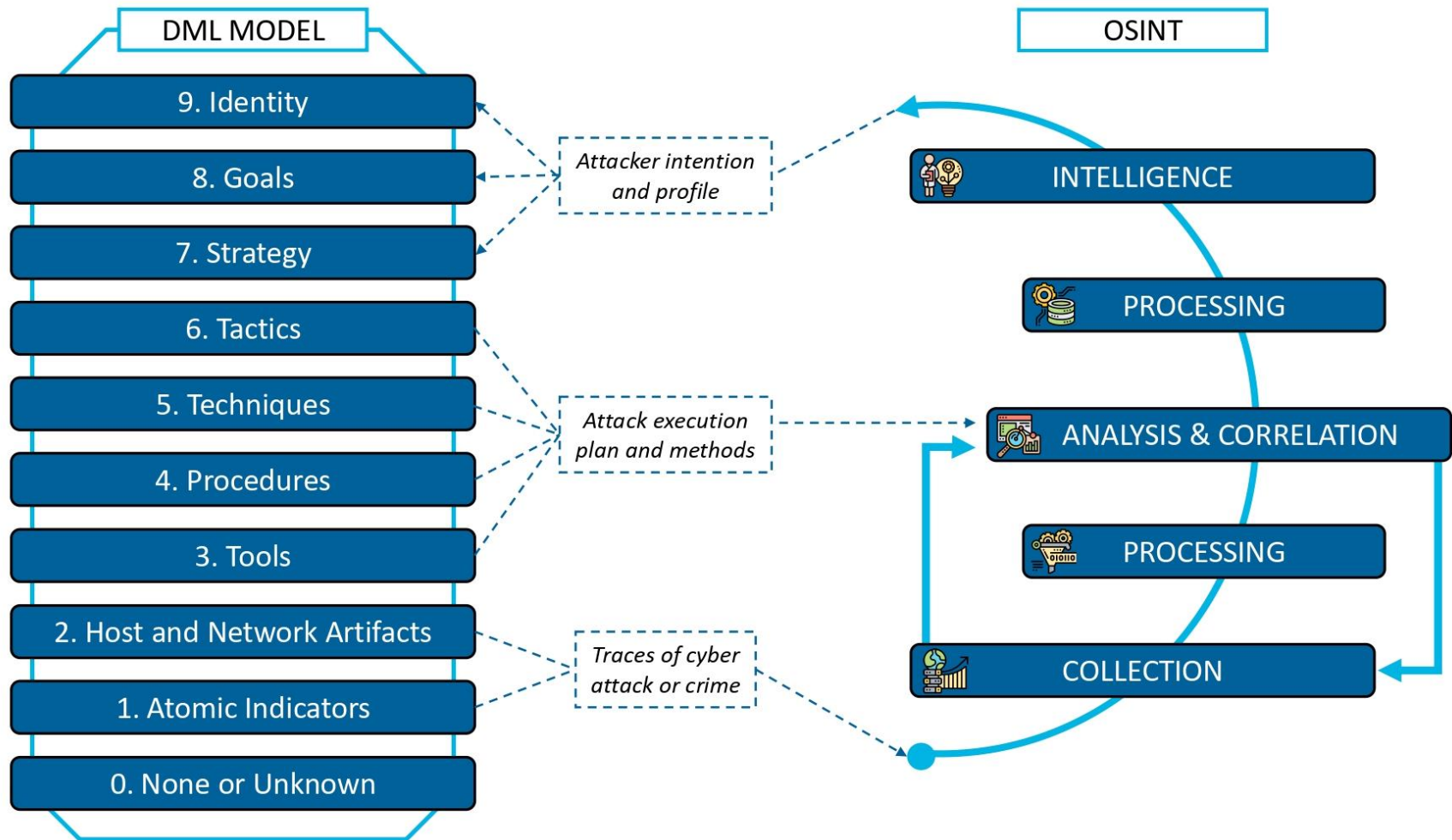
OSINT Sources: Media

- **Political inclination by municipality name**
- https://elpais.com/politica/2019/11/10/actualidad/1573410266_570919.html

El mapa de resultados de las elecciones generales del 10-N de 2019, municipio a municipio



OSINT & Detection Maturity Level (DML)



OSINT Techniques



OSINT Techniques

- Search Engines
- Social Networks
- Email Address
- Username
- Real Name
- Location
- IP Address
- Domain

OSINT Techniques: Search Engines

Google

YAHOO!

bing



SHODAN



DuckDuckGo

Baidu 百度

searX

Yandex

OSINT Techniques: Search Engines



☐ “”

- Force an exact-match search
- E.g. “Félix Gómez Mármol”

☐ OR

- Search for X *or* Y
- The | operator is equivalent
- E.g. murcia|heidelberg

☐ AND

- Search for X *and* Y
- E.g. murcia AND heidelberg

☐ -

- Exclude a term or phrase
- E.g. murcia -heidelberg

☐ *

- Acts as wildcard
- E.g. Félix * Mármol

☐ ()

- Group terms or search operators
- E.g. Félix AND (Gómez|Mármol)

☐ ..

- Search for a range of numbers
- E.g. 2010..2019

OSINT Techniques: Search Engines



❑ filetype:

- Restrict results to those of a certain file type (e.g., pdf, ppt, docx, txt, etc.)
- ext is equivalent
- E.g. `filetype:pdf`

❑ site:

- Limit results to those from a specific website
- E.g. `site:um.es`

❑ intitle:

- Find pages with a certain word (or words) in the title
- E.g. `intitle:heidelberg`

❑ inurl:

- Find pages with a certain word (or words) in the URL
- E.g. `inurl:heidelberg`

❑ intext:

- Find pages with a certain word (or words) somewhere in the content
- E.g. `intext:heidelberg`



OSINT Techniques: Search Engines

Google

- Search for index directories within the domain um.es
 - `intitle:"index of /" site:um.es`
- Search for Excel sheets within the domain um.es with the term "salario"
 - `salario site:um.es filetype:xlsx`
- Search for ftp sites within the domain um.es
 - `site:um.es inurl:ftp -inurl:(https|http)`
- Search for usernames and passwords
 - `filetype:pwd inurl:(service | authors | administrators | users) "# -FrontPage-"`
 - `intitle:"index of" "Index of /" password.txt`
 - `filetype:sql "# dumping data for table" "`PASSWORD` varchar"`

OSINT Techniques: Search Engines

Google Full list of search commands

- **“Term”**
- **Term1 OR Term2**
- **Term1 AND Term2**
- **Term1 * Term2**
- **-Term**
- **+Term**
- **~Term**
- **#Term**
- **\$price**
- **cache:URL**
- **filetype:EXT**
- **site:URL**
- **related:URL**
- **intitle:Term**
- **allintitle:Term**
- **inurl:Term**
- **allinurl:Term**
- **intext:Term**
- **allintext:Term**
- **AROUND(number)**
- **weather:Location**
- **stocks:\$TAG**
- **map:Location**
- **movie:Term**
- **Amount in Unit**
- **source:SRC**
- **_ Term**
- **000..000**
- **inanchor:Term**
- **allinanchor:Term**
- **blogurl:URL**
- **location:Location**
- **inpostauthor:Term**
- **allinpostauthor:Term**
- **inposttitle:Term**
- **link:URL**
- **info:URL (also id:URL)**
- **daterange:0000-0000**
- **phonebook:Term**



OSINT Techniques: Social Networks



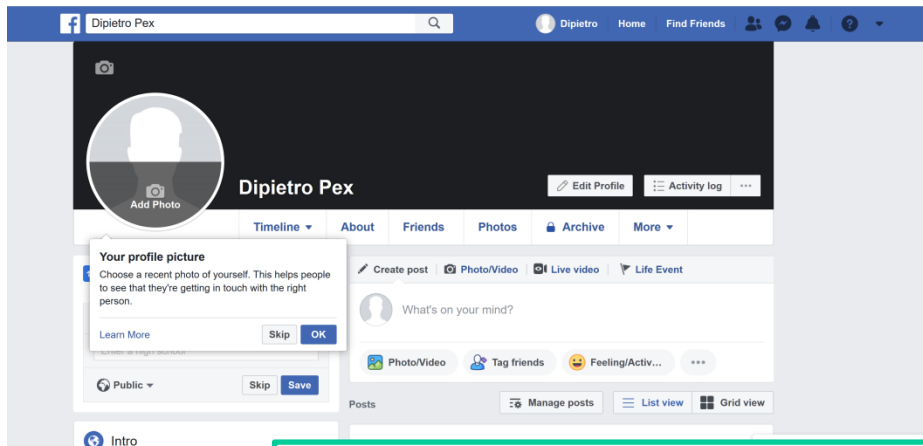
OSINT Techniques: Social Networks

Social Network	Type	Scope	Main potential for OSINT
<i>4chan</i>	Online community	Worldwide	Users interested in illicit activities
<i>Badoo</i>	Dating	Worldwide	Intimate and personal details
<i>Cloob</i>	Social connections	Iran	Personal profile, posting and community membership
<i>Draugiem</i>	Social connections	Latvia	Personal profile, publications in blogs, group membership
<i>Facebook</i>	Social connections	Worldwide	Personal profile, preferences and places visited
<i>Facenama</i>	Social connections	Iran	Personal profile, publications, photos and videos
<i>Flickr</i>	Photo-sharing	Worldwide	Activities, hobbies, places and personal relationships
<i>Instagram</i>	Social connections	Worldwide	Habits, locations and personal relationships
<i>LinkedIn</i>	Business	Worldwide	Professional profile, education, skills and languages
<i>Mixi</i>	Social connections	Japan	Personal profile, interests and opinions
<i>Odnoklassniki</i>	Social connections	Mainly Russia	Personal profile of adults, past and present friendships
<i>Qzone</i>	Social connections	Mainly China	Personal profile, preferences, habits
<i>Reddit</i>	Online community	Worldwide	Users trends, behaviors, and publications
<i>Renren</i>	Social connections	Mainly China	Personal profile of students, friendships and discussions
<i>Taringa!</i>	Social connections	Mainly Latin America	Personal profile, publications and community membership
<i>Tinder</i>	Dating	Worldwide	Intimate and personal details
<i>Tumblr</i>	Photo-sharing	Worldwide	Activities, hobbies, places and personal relationships
<i>Twitter</i>	Social connections	Worldwide	Personal profile, opinions and publications
<i>Vkontakte (VK)</i>	Social connections	Mainly Russia	Personal profile, preferences and publications
<i>Weibo</i>	Social connections	Mainly China	Personal profile, opinions and publications
<i>YouTube</i>	Video-sharing	Worldwide	Video content, opinions and comments of subscribers

OSINT Techniques: Social Networks

facebook

- Step 1 → Get your Facebook ID
 - Hover your cursor over your profile picture



https://www.facebook.com/profile/picture/menu_dialog/?profile_id=100032518218756

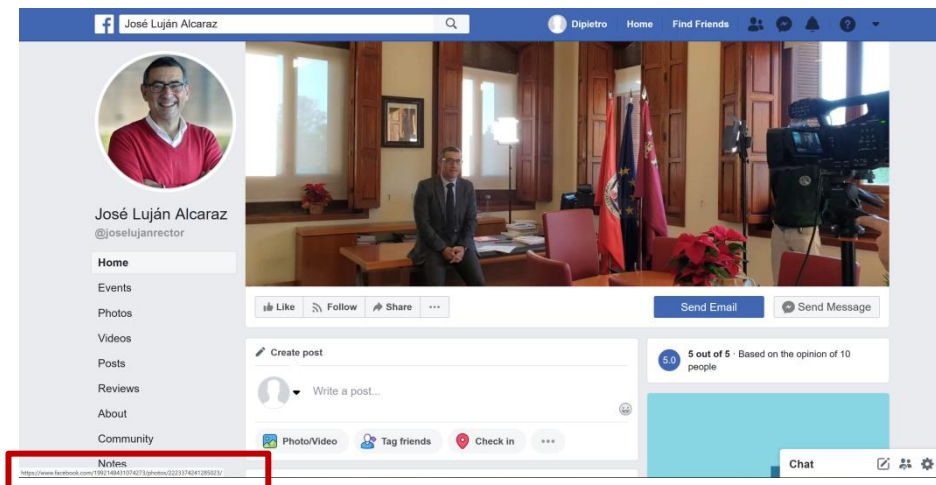
As per 2020, this field might be indicated by the `referrer_profile_id` param

https://www.facebook.com/photo.php?fbid=...&set=...&type=3&source=11&referrer_profile_id=...

OSINT Techniques: Social Networks

facebook

- Step 2.a → Get the Facebook ID of someone else
 - Hover your cursor over his/her profile picture ;-)



<https://www.facebook.com/1992148431074273/photos/2223374241285023/>

OSINT Techniques: Social Networks

facebook

- Step 2.b → Get the Facebook ID of someone else
 - Visit <https://whopostedwhat.com/>

2. Get ID

<input type="text" value="https://www.facebook.com/mattia.zago"/>	<input type="text" value="1678479836"/>	<input type="button" value="Find"/>
---	---	-------------------------------------

Example: Paste in the URL from a profile, page or place, like "https://www.facebook.com/zuck".

- Alternative websites
 - <https://findmyfbid.com/>
 - <https://lookup-id.com/>

OSINT Techniques: Social Networks

facebook

Visit: <https://graph.tips/beta/>

- E.g., photos by José Luján Alcaraz

```
https://www.facebook.com/search/posts/?q=*&epa=FILTERS&filters=eyJycF9hdXRob3IiOiJ7XCJucyYw11XCI6XCJhdXRob3JcIixcImFyZ3NcIjpcIjE5OTIxNDg0MzEwNzQyNzNcIn0ifQ%3D
```

```
eyJycF9hdXRob3IiOiJ7XCJucyYw11XCI6XCJhdXRob3JcIixcImFyZ3NcIjpcIjE5OTIxNDg0MzEwNzQyNzNcIn0ifQ
```

BASE 64

```
{"rp_author":  
  {"name":"author",  
   "args":"1992148431074273"}  
}
```

OSINT Techniques: Email Address

- Is the email address valid?
 - <https://hunter.io>

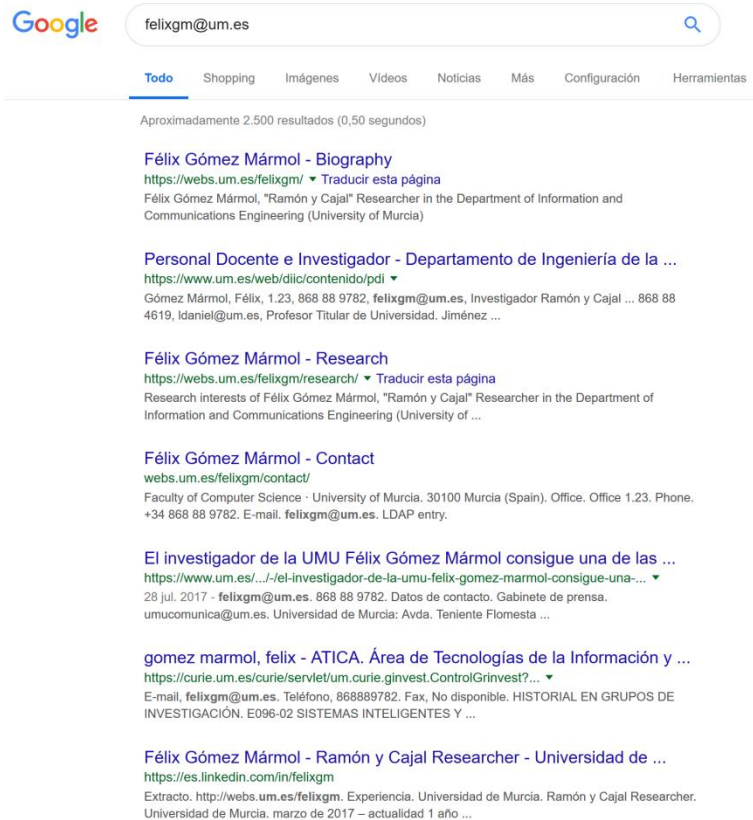
The screenshot shows the Hunter.io website's Email Verifier interface. At the top, there's a navigation bar with the Hunter logo, 'Products', 'Pricing', 'Sign in', and a 'Sign up' button. The main heading is 'Email Verifier' with a subtext: 'Verify the deliverability of any email address with the most complete email checker.' Below this is a search bar containing 'felixgm@um.es' and a 'Verify' button. The results show a green checkmark and the text 'Valid email address. This email address can be used safely.' A table below provides details: Format is 'VALID', Type is 'PROFESSIONAL', Server status is 'SUCCESS', and Email status is 'SUCCESS'. At the bottom, it lists four sources found for the email on the web, with some marked as 'REMOVED'.

- Has the email address been hacked?
 - <https://haveibeenpwned.com>

The screenshot shows the Have I Been Pwned website. The navigation bar includes 'Home', 'Notify me', 'Domain search', 'Who's been pwned', 'Passwords', 'API', 'About', and 'Donate'. The main heading is '';--have i been pwned?' with a subtext: 'Check if you have an account that has been compromised in a data breach'. Below this is a search bar containing 'felixgm@um.es' and a 'pwned?' button. A blue banner below the search bar says 'Generate secure, unique passwords for every account' with a link to 'Learn more at 1Password.com'. Below this is a section with statistics: 338 pwned websites, 5,701,036,040 pwned accounts, 86,927 pastes, and 94,839,579 paste accounts. The bottom section is divided into 'Largest breaches' and 'Recently added breaches'. The largest breaches list includes: 711,477,622 Onliner Spambot accounts, 593,427,119 Exploit.In accounts, 457,962,538 Anti Public Combo List accounts, and 393,430,309 River City Media Spam List accounts. The recently added breaches list includes: 4,848,734 Dangdang accounts, 213,415 BannerBit accounts, 7,633,234 BlankMediaGames accounts, 242,715 GoldSilver accounts, and 205,242 Mappery accounts.

OSINT Techniques: Email Address

- Check search engines



Google felixgm@um.es

Todo Shopping Imágenes Vídeos Noticias Más Configuración Herramientas

Aproximadamente 2.500 resultados (0,50 segundos)

Félix Gómez Mármol - Biography
<https://webs.um.es/felixgm/> Traducir esta página
Félix Gómez Mármol, "Ramón y Cajal" Researcher in the Department of Information and Communications Engineering (University of Murcia)

Personal Docente e Investigador - Departamento de Ingeniería de la ...
<https://www.um.es/web/diic/contenido/pdi>
Gómez Mármol, Félix, 1.23, 868 88 9782, felixgm@um.es, Investigador Ramón y Cajal ... 868 88 4619, Idaniel@um.es, Profesor Titular de Universidad. Jiménez ...

Félix Gómez Mármol - Research
<https://webs.um.es/felixgm/research/> Traducir esta página
Research interests of Félix Gómez Mármol, "Ramón y Cajal" Researcher in the Department of Information and Communications Engineering (University of ...

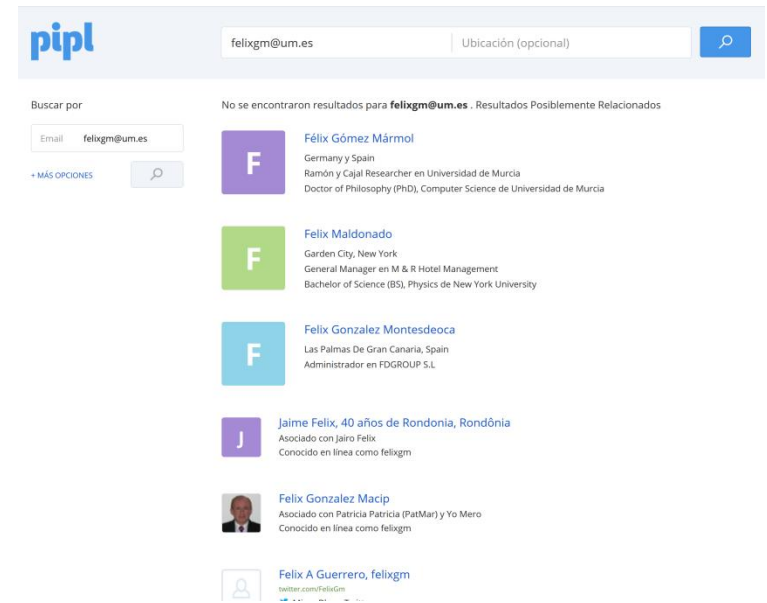
Félix Gómez Mármol - Contact
webs.um.es/felixgm/contact/
Faculty of Computer Science · University of Murcia. 30100 Murcia (Spain). Office. Office 1.23. Phone. +34 868 88 9782. E-mail. felixgm@um.es. LDAP entry.

El investigador de la UMU Félix Gómez Mármol consigue una de las ...
<https://www.um.es/.../el-investigador-de-la-umu-felix-gomez-marmol-consigue-una-...>
28 jul. 2017 · felixgm@um.es. 868 88 9782. Datos de contacto. Gabinete de prensa. umucomunica@um.es. Universidad de Murcia: Avda. Teniente Flomesta ...

gomez marmol, felix - ATICA. Área de Tecnologías de la Información y ...
<https://curie.um.es/curie/servlet/um.curie.ginvest.ControlGrinvest?...>
E-mail, felixgm@um.es. Teléfono, 868889782. Fax, No disponible. HISTORIAL EN GRUPOS DE INVESTIGACIÓN. E096-02 SISTEMAS INTELIGENTES Y ...

Félix Gómez Mármol - Ramón y Cajal Researcher - Universidad de ...
<https://es.linkedin.com/in/felixgm>
Extracto. <http://webs.um.es/felixgm>. Experiencia. Universidad de Murcia. Ramón y Cajal Researcher. Universidad de Murcia. marzo de 2017 – actualidad 1 año ...

- Check Pipl
– <https://pipl.com>



pipl felixgm@um.es Ubicación (opcional)

Buscar por Email felixgm@um.es

+ MÁS OPCIONES

No se encontraron resultados para felixgm@um.es. Resultados Posiblemente Relacionados

- F Félix Gómez Mármol**
Germany and Spain
Ramón y Cajal Researcher in Universidad de Murcia
Doctor of Philosophy (PhD), Computer Science de Universidad de Murcia
- F Felix Maldonado**
Garden City, New York
General Manager en M & R Hotel Management
Bachelor of Science (BS), Physics de New York University
- F Felix Gonzalez Montesdeoca**
Las Palmas De Gran Canaria, Spain
Administrador en FDGROUP S.L
- J Jaime Felix. 40 años de Rondonia, Rondônia**
Asociado con Jairo Felix
Conocido en línea como felixgm
- Felix Gonzalez Macip**
Asociado con Patricia Patricia (PatMar) y Yo Mero
Conocido en línea como felixgm
- Felix A Guerrero, felixgm**
twitter.com/FelixGm

OSINT Techniques: Username

- Check availability in social networks

knowem? SIGN IN SIGN UP

RESERVE YOUR NAME ON HUNDREDS OF SITES

Check Username Create Profile Community Networks About

Remember me? Need Help? Have Questions? (800) 691-KNOW (5669)

Check Your Brand, Product or Username

Search over 575 popular social media networks to instantly secure your brand across the social web.

felixgm SEARCH Most Popular Social Networks Domains Trademarks

Enter your personal username or business brand name in the "enter name here" box above and click Search. Then click "Check This Category" to further specify the search for your brand name's availability in each section. Please note Social Media usernames and accounts cannot contain spaces, symbols, or anything other than letters and numbers.

Tired of checking and registering all these names yourself? Want to claim your Brand on all of these sites before someone else does? Then you want our [Social Profile Creation Service!](#) Just give us your personal brand, product or business information, and a highly trained Social Media Specialist assigned to you will begin creating up to 300 Social Media Profiles for you, today!

Since we launched in 2009 the KnowEm team has helped to reserve over 650,000 profiles and reported back to our clients over 50,000 issues of brand squatting and/or misrepresentation of a brand, username or trademarked term. Don't be one of those companies that get stuck with a different handle on every Social Network - Make your Social Branding consistent, and [reserve your name](#) today!

Blogging

AMERICAN	Available	42NEWS	Available	Blogger	Available	blogtalkradio	Available
DISQUS	Available	Hatena	Available	medium	Available	issuu	Available
moblog	Available	LIVEJOURNAL	Available	myname?	Available	overblog	Available
moonfruit	Available	Pen.io	Available	pen.io	Available	PORTFOLIOJOB	Available
Open-Free Website	Available	Page4	Available	tumblr	Available	weebly	Available
SMBLOGS	Available	SOUP	Available	zimbio	Available	ZUMVU	Available
WordPress	Available	write.as	Available				

Bookmarking

bitly	Available	diigo	Available	LibraryThing	Available
folkd.com	Available	Instapaper	Available	myname?	Available
MIX	Available	Pinterest	Available	myname?	Available
myname?	Available	My Site Vote	Available	myname?	Available
we ♥ it	Available	THAT TIME	Available	wanelo	Available

- Check availability in domains

knowem? SIGN IN SIGN UP

RESERVE YOUR NAME ON HUNDREDS OF SITES

Check Username Create Profile Community Networks About

Remember me? Need Help? Have Questions? (800) 691-KNOW (5669)

Check Your Brand, Product or Username

Search over 575 popular social media networks to instantly secure your brand across the social web.

felixgm SEARCH Most Popular Social Networks Domains Trademarks

Check Domain Availability

Find out if your username, brand, product or trademark is still available as a top level domain name on the internet.

Common Popular Domains:

felixgm.com Available	felixgm.net Available
felixgm.org Available	felixgm.info Available
felixgm.biz Available	felixgm.tel Available
felixgm.mobi Available	felixgm.name Available
felixgm.co Available	felixgm.ag Available
felixgm.tv Available	felixgm.me Available
felixgm.travel Available	

Domains from North America:

felixgm.ca Available	felixgm.mx Available
felixgm.com.mx Available	felixgm.cc.com For Sale?
felixgm.us Available	felixgm.us.com Available

Domains from South America:

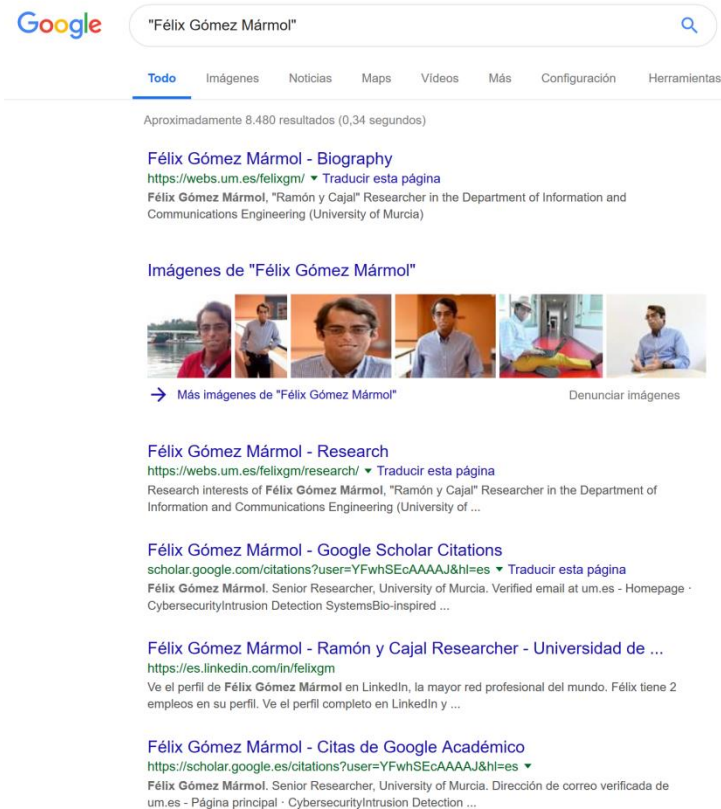
felixgm.ar.com For Sale?	felixgm.br.com Available
felixgm.cl Available	felixgm.gs Available
felixgm.pe Available	felixgm.uy.com For Sale?

Domains from Central America and Caribbean:


felixgm.com.ag Available	felixgm.net.ag Available
felixgm.org.ag Available	felixgm.bz Available
felixgm.cr Available	felixgm.gd Available
felixgm.hk Available	felixgm.ht Available
felixgm.lc Available	felixgm.ms Available
felixgm.tc Available	felixgm.vc Available
felixgm.net.vc Available	felixgm.vg Available

OSINT Techniques: Real Name

- Check search engines



A screenshot of a Google search for "Félix Gómez Mármol". The search bar shows the name and a magnifying glass icon. Below the search bar, there are tabs for "Todo", "Imágenes", "Noticias", "Maps", "Vídeos", "Más", "Configuración", and "Herramientas". The search results show approximately 8,480 results in 0.34 seconds. The first result is a biography from webs.um.es, followed by a research page, Google Scholar citations, a LinkedIn profile, and Google Academic citations.


Google "Félix Gómez Mármol" 

Todo Imágenes Noticias Maps Vídeos Más Configuración Herramientas

Aproximadamente 8.480 resultados (0,34 segundos)

Félix Gómez Mármol - Biography
<https://webs.um.es/felixgm/> Traducir esta página
Félix Gómez Mármol, "Ramón y Cajal" Researcher in the Department of Information and Communications Engineering (University of Murcia)

Imágenes de "Félix Gómez Mármol"



→ Más imágenes de "Félix Gómez Mármol" Denunciar imágenes

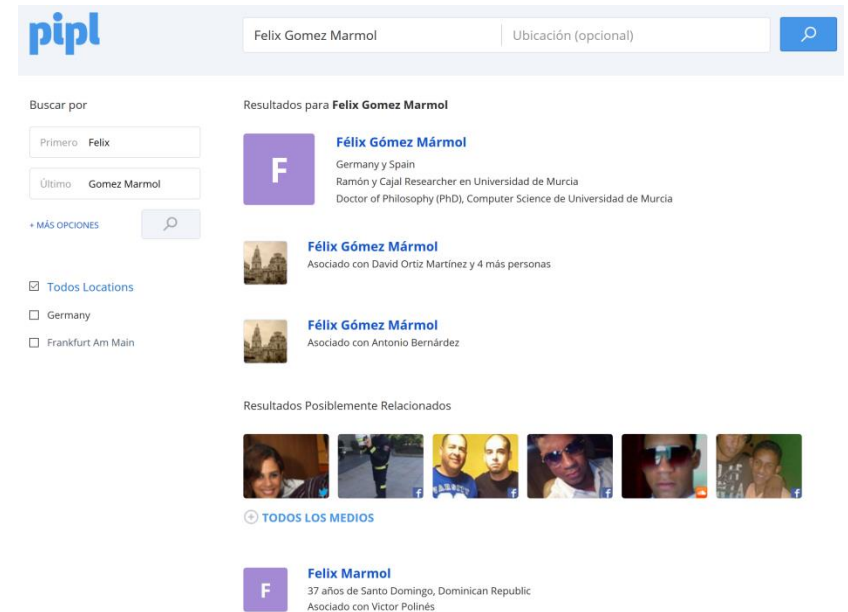
Félix Gómez Mármol - Research
<https://webs.um.es/felixgm/research/> Traducir esta página
Research interests of Félix Gómez Mármol, "Ramón y Cajal" Researcher in the Department of Information and Communications Engineering (University of ...)

Félix Gómez Mármol - Google Scholar Citations
scholar.google.com/citations?user=YFwhSEcAAAAJ&hl=es Traducir esta página
Félix Gómez Mármol. Senior Researcher, University of Murcia. Verified email at um.es - Homepage · CybersecurityIntrusion Detection SystemsBio-inspired ...


Félix Gómez Mármol - Ramón y Cajal Researcher - Universidad de ...
<https://es.linkedin.com/in/felixgm>
Ve el perfil de Félix Gómez Mármol en LinkedIn, la mayor red profesional del mundo. Félix tiene 2 empleos en su perfil. Ve el perfil completo en LinkedIn y ...

Félix Gómez Mármol - Citas de Google Académico
<https://scholar.google.es/citations?user=YFwhSEcAAAAJ&hl=es>
Félix Gómez Mármol. Senior Researcher, University of Murcia. Dirección de correo verificada de um.es - Página principal · CybersecurityIntrusion Detection ...

- Check Pipl
– <https://pipl.com>




A screenshot of the Pipl search engine. The search bar contains "Felix Gomez Marmol" and "Ubicación (opcional)". The results show a list of profiles for "Félix Gómez Mármol", including a main profile with a bio and location, and several other profiles with photos and associated names. There is also a section for "Resultados Posiblemente Relacionados" with a row of small profile pictures.

pipl Felix Gomez Marmol Ubicación (opcional) 

Buscar por

Primero Felix

Último Gomez Marmol

+ MÁS OPCIONES 

Todos Locations

Germany

Frankfurt Am Main


Resultados para **Felix Gomez Marmol**


F **Félix Gómez Mármol**
Germany y Spain
Ramón y Cajal Researcher en Universidad de Murcia
Doctor of Philosophy (PhD), Computer Science de Universidad de Murcia

F **Félix Gómez Mármol**
Asociado con David Ortiz Martínez y 4 más personas

F **Félix Gómez Mármol**
Asociado con Antonio Bernárdez

Resultados Posiblemente Relacionados



 TODOS LOS MEDIOS

F **Felix Marmol**
37 años de Santo Domingo, Dominican Republic
Asociado con Victor Polines

OSINT Techniques: Location

- Get GPS coordinates from location name
 - <https://www.gps-coordinates.net>

Home Directions Converter Satellite Street View API Geolocation Maps Custom

GPS coordinates converter

This tool is all about **GPS coordinates conversion**. As soon as you modify one end of the data (either the decimal or sexagesimal degrees coordinates), the other end is simultaneously updated, as well as the position on the map.

The GPS coordinates are presented in the infowindow in an easy to copy and paste format.

You can also start to convert latitude and longitude by clicking on the map, which will pre-fill the fields with the GPS coordinates of the location you clicked on. In any case, the address will not be geocoded automatically. If you want to convert the GPS coordinates into an address, you have to click on the button "Get Address" below the decimal coordinates.

Address:

DD (decimal degrees)*

Latitude:

Longitude:

DMS (degrees, minutes, seconds)*

Latitude: N S 38 ° 1 ' 25.666 "

Longitude: E W 1 ° 10 ' 26.565 "

* World Geodetic System 84 (WGS 84)

- E.g., GPS coordinates for the Faculty of Computer Science at UMU are
 - 38.023796; -1.17404590000001

- Find out location from GPS coordinates



Google Maps



OSINT Techniques: IP Address

- Get location from IP Address
 - <https://www.iplocation.net>

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2019-1-1)

IP Address	Country	Region	City
155.54.1.1	Spain 🇪🇸	Murcia, Region de	Murcia
ISP	Organization	Latitude	Longitude
Universidad de Murcia	Not Available	37.9870	-1.1300

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

IP Address	Country	Region	City
155.54.1.1	Spain 🇪🇸	Murcia	Murcia
ISP	Organization	Latitude	Longitude
Entidad Publica Empresarial Red.es	Universidad de Murcia (um.es)	37.9870	-1.1300

Geolocation data from [EurekAPI](#) (Product: API, real-time)

IP Address	Country	Region	City
155.54.1.1	Spain 🇪🇸	Murcia	Murcia
ISP	Organization	Latitude	Longitude
Universidad de Murcia	Universidad de Murcia	37.987	-1.13

Geolocation data from [DB-IP](#) (Product: Full, 2019-1-1)

IP Address	Country	Region	City
155.54.1.1	Spain 🇪🇸	Murcia	Espinarido
ISP	Organization	Latitude	Longitude
Universidad de Murcia	Not Available	38.0098	-1.15422

- <https://viewdns.info>
 - Whois, Reverse IP Lookup, Traceroute, etc,

The screenshot shows the ViewDNS.info website interface with a grid of tools. The tools include:

- Reverse IP Lookup:** Find all sites hosted on a given server.
- Reverse Whois Lookup:** Find domain names owned by an individual or company.
- IP History:** Show historical IP addresses for a domain.
- DNS Report:** Provides a complete report on your DNS settings.
- Reverse MX Lookup [NEW]:** Find all sites that use a given mail server.
- Reverse NS Lookup:** Find all sites that use a given nameserver.
- IP Location Finder:** Find the geographic location of an IP Address.
- Chinese Firewall Test:** Check whether a site is accessible from China.
- DNS Propagation Checker:** Check whether recent DNS changes have propagated.
- Is My Site Down:** Check whether a site is actually down or not.
- Iran Firewall Test:** Check whether a site is accessible in Iran.
- Domain / IP Whois:** Lookup information on a Domain or IP address.
- Get HTTP Headers:** View the HTTP headers returned by a domain.
- DNS Record Lookup:** View all DNS records for a specified domain.
- Port Scanner:** Check if common ports are open on a server.
- Traceroute:** Trace the servers between ViewDNS and a remote host.
- Spam Database Lookup:** Determine if your mail server is on any spam lists.
- Reverse DNS Lookup:** View the reverse DNS entry for an IP address.
- ASN Lookup:** Lookup information on an ASN.
- Ping:** Test the latency of a remote system from ViewDNS.
- DNSSEC Test:** Test if any domain name is configured for DNSSEC.
- URL / String Decode:** Convert a URL with %a-f values to a readable format.
- Abuse Contact Lookup:** Find the abuse contact address for a domain name.
- MAC Address Lookup:** Determine the manufacturer of a network device.
- Free Email Lookup:** Determine if a domain provides free email addresses.

SINT Techniques: IP Address

Whois 155.54.1.1

Viewdns.info

Tools API Research Data

ViewDNS.info > Tools > Domain / IP Whois

Displays owner/contact information for a domain name or IP address. Can also be used to determine if a domain name is registered or not.

Need to lookup a large number of domains? Enquire about our [bulk whois](#) service by emailing us with your requirements.

Domain / IP Address:

WHOIS Information for 155.54.1.1

! This is the RIPE Database query service.

! The objects are in RPEL format.

! The RIPE Database is subject to Terms and Conditions.

! See <http://www.ripe.net/db/support/db-terms-conditions.pdf>

! Information related to "155.54.0.0 - 155.54.255.255"

! Abuse contact for "155.54.0.0 - 155.54.255.255" is "iris@ortel.es"

inetnum: 155.54.0.0 - 155.54.255.255

netname: UM

descr: Universidad de Murcia

country: ES

admin-c: MAGL1-RIPE

admin-c: JAMP1-RIPE

tech-c: MAGL1-RIPE

tech-c: JAMP1-RIPE

abuse-c: RIAC2-RIPE

status: LEGACY

remarks: For information on "status:" attribute read <https://www.ripe.net/data-tools/db/faq/faq-status-values-legacy-resources>

remarks: mail spam reports: abuse@um.es

remarks: security incidents: cert@um.es

notify: glax@um.es

notify: jamape@um.es

notify: iris-nic@rediris.es

mnt-by: UNIMURNET-MNT

mnt-by: REDIRIS-NMC

created: 1970-01-01T00:00:00Z

last-modified: 2017-10-11T13:16:22Z

source: RIPE

person: Jose Angel Martinez Perez

address: Jefe Seccion Redes

address: Edificio ATICA

address: Campus Espinardo

address: 30100

address: Murcia, SPAIN

phone: +34 868 884 913

e-mail: jamape@um.es

nic-hdl: JAMP1-RIPE

notify: jamape@um.es

notify: iris-nic@rediris.es

mnt-by: UNIMURNET-MNT

mnt-by: REDIRIS-NMC

created: 2005-01-12T10:06:35Z

last-modified: 2017-10-30T21:46:33Z

source: RIPE

person: Miguel Angel Garcia Lax

address: Jefe Infraestructuras TIC

address: Universidad de Murcia

address: Edificio ATICA

address: Campus Universitario de Espinardo

address: E-30100 Murcia

address: SPAIN

phone: +34 868 884 849

fax-no: +34 868 898 337

e-mail: glax@um.es

nic-hdl: MAGL1-RIPE

notify: glax@um.es

notify: iris-nic@rediris.es

mnt-by: UNIMURNET-MNT

mnt-by: REDIRIS-NMC

created: 2002-11-26T10:39:43Z

last-modified: 2017-10-30T21:45:51Z

source: RIPE

! Information related to "155.54.0.0/16#766"

route: 155.54.0.0/16

descr: UM

origin: AS766

mnt-by: REDIRIS-NMC

created: 1970-01-01T00:00:00Z

last-modified: 2012-09-12T08:09:52Z

source: RIPE

! This query was served by the RIPE Database Query Service version 1.92.6 (BLAARROOP)

```
inetnum: 155.54.0.0 - 155.54.255.255
```

```
netname: UM
```

```
descr: Universidad de Murcia
```

```
descr: Murcia
```

```
country: ES
```

```
admin-c: MAGL1-RIPE
```

```
admin-c: JAMP1-RIPE
```

```
tech-c: MAGL1-RIPE
```

```
tech-c: JAMP1-RIPE
```

```
abuse-c: RIAC2-RIPE
```

```
status: LEGACY
```

```
remarks: For information on "status:" attribute read https://www.ripe.net/data-tools/db/faq/faq-status-values-legacy-resources
```

```
remarks: mail spam reports: abuse@um.es
```

```
remarks: security incidents: cert@um.es
```

```
notify: glax@um.es
```

```
notify: jamape@um.es
```

```
notify: iris-nic@rediris.es
```

```
mnt-by: UNIMURNET-MNT
```

```
mnt-by: REDIRIS-NMC
```

```
created: 1970-01-01T00:00:00Z
```

```
last-modified: 2017-12-11T13:16:22Z
```

```
source: RIPE
```

```
person: Jose Angel Martinez Perez
```

```
address: Jefe Seccion Redes
```

```
address: Edificio ATICA
```

```
address: Campus Espinardo
```

```
address: 30100
```

```
address: Murcia, SPAIN
```

```
phone: +34 868 884 913
```

```
e-mail: jamape@um.es
```

```
nic-hdl: JAMP1-RIPE
```

```
notify: jamape@um.es
```

```
notify: iris-nic@rediris.es
```

```
mnt-by: UNIMURNET-MNT
```

```
mnt-by: REDIRIS-NMC
```

```
created: 2005-01-12T10:06:35Z
```

```
last-modified: 2017-10-30T21:46:33Z
```

```
source: RIPE
```

```
person: Miguel Angel Garcia Lax
```

```
address: Jefe Infraestructuras TIC
```

```
address: Universidad de Murcia
```

```
address: Edificio ATICA
```

```
address: Campus Universitario de Espinardo
```

```
address: E-30100 Murcia
```

```
address: SPAIN
```

```
phone: +34 868 884 849
```

```
fax-no: +34 868 898 337
```

```
e-mail: glax@um.es
```

```
nic-hdl: MAGL1-RIPE
```

```
notify: glax@um.es
```

```
notify: iris-nic@rediris.es
```

```
mnt-by: UNIMURNET-MNT
```

```
mnt-by: REDIRIS-NMC
```

```
created: 2002-11-26T10:39:43Z
```

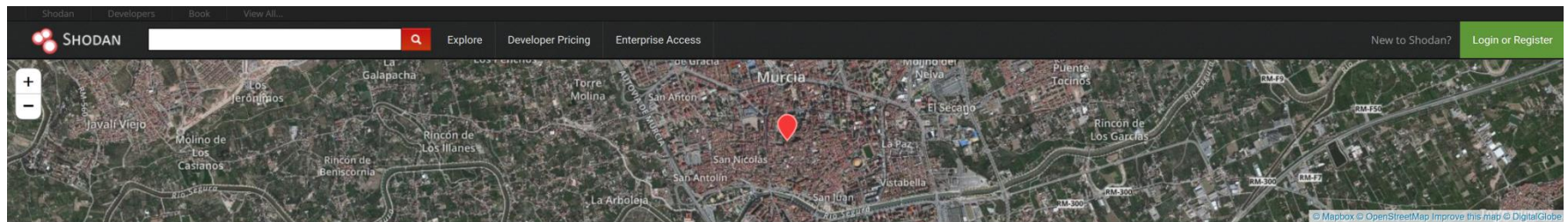
```
last-modified: 2017-10-30T21:45:51Z
```

```
source: RIPE
```



OSINT Techniques: IP Address

- Shodan search engine
 - <https://www.shodan.io>



🌐 155.54.212.103 wwwclu.um.es

City	Murcia
Country	Spain
Organization	Universidad de Murcia
ISP	Universidad de Murcia
Last Update	2019-01-10T23:46:10.285823
Hostnames	wwwclu.um.es
ASN	AS766

⚡ Web Technologies

- 📦 Bootstrap
- 🏷️ Google Tag Manager
- 🔗 JQuery
- 🏠 Modernizr

🏠 Ports



📋 Services

```
21
tcp
ftp
220 FTP Server ready
230 Anonymous access granted, restrictions apply
214-The following access commands are recognized (* =>'s unimplemented):
214-CMD XCMD CDUP XCUP SMNT* QUIT PORT PASV
214-EPRM EPSV ALLO* RNFR RNTD DELE MDTM RMD
214-XRMD MKD XMKD PWD XPWD SIZE SVST HELP
214-NOOP FEAT OPTS AUTH CCC* CONF* ENC* MIC*
214-PBSZ PROT TYPE STRU MODE RETR STOR STOU
214-APPE REST ABOR USER PASS ACCT* REIN* LST
214-NLST STAT SITE MLSD MLST
214 Direct comments to root@araneus51.um.es
211-Features:
MDTM
MFMT
UTFS
MFF modify;UNIX.group;UNIX.mode;
MLST modify*;perm*;size*;type*;unique*;UNIX.group*;UNIX.mode*;UNIX.owner*;
LANG en-US*
REST STREAM
SIZE
211 End
```

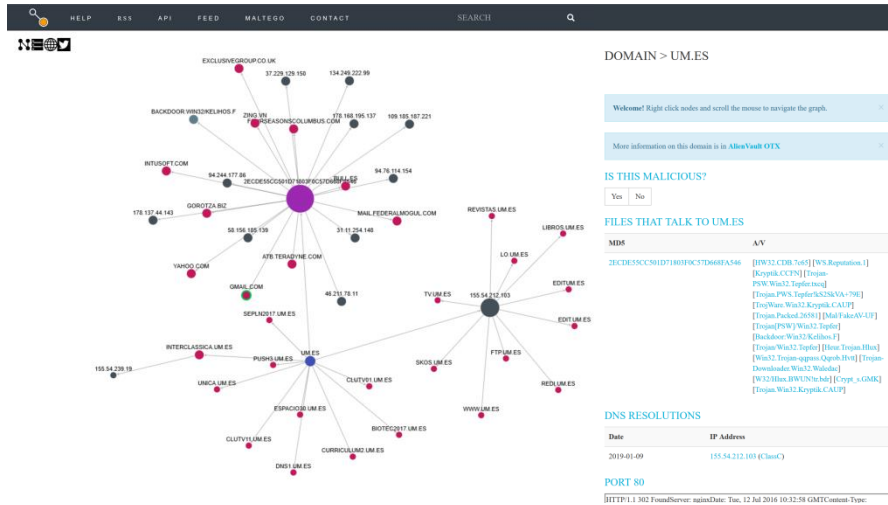


OSINT Techniques: IP Address

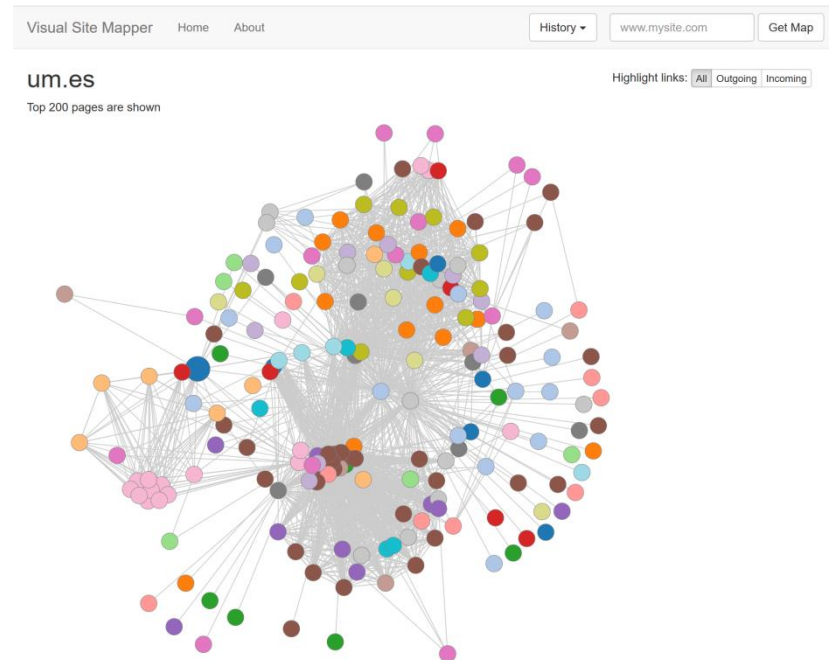
- Shodan search keywords examples
 - webserver, webcam, ssh, telnet, default password, apache, cisco, linksys,...
- Shodan search filters
 - city:
 - Find devices in a particular city
 - country:
 - Find devices in a particular country
 - geo:
 - You can pass it coordinates
 - hostname:
 - Find values that match the hostname
 - net:
 - Filter results by a specific IP range or subnet
 - os:
 - Search based on operating system
 - port:
 - find particular ports that are open
 - before/after:
 - find results within a timeframe

OSINT Techniques: Domain

- Visualize domain connections
 - <https://www.threatcrowd.org>



- <http://www.visualsitemapper.com>



OSINT Techniques: Domain

- Check DNS and mailservers
- <http://www.domaincrawler.com>

The screenshot shows the DomainCrawler website interface. At the top, there's a navigation bar with 'Domain Information', 'SEO Hosting', 'About Us', and 'Widgets'. A search bar contains 'http://um.es'. Below the search bar, there's a 'Dashboard' section with tabs for 'Social', 'Whois', 'Subdomains', 'DNS Report', and 'Widgets'. The main content area is titled 'Domain Information for um.es'. It lists various categories of information:

- IP-address(es):** 155.54.212.103 (shared with 0 domains)
- Nameserver(s):**
 - chico.rediris.es (130.206.1.3 (24))
 - dns1.um.es (155.54.1.1 (2))
 - dns2.um.es (155.54.1.2 (2))
 - sun.rediris.es (130.206.1.2 (39))
- Mailservers(s):**
 - mx01.puc.rediris.es (130.206.18.10 (11), 130.206.18.11 (11), 130.206.18.129 (11), 130.206.18.130 (11), 130.206.18.131 (11), 130.206.18.7 (11))
 - mx02.puc.rediris.es (130.206.18.132 (11), 130.206.18.134 (11), 130.206.18.3 (11), 130.206.18.4 (11), 130.206.18.8 (11))

There are also two small embedded images: one showing a news article snippet and another showing a 'Google PR for um.es' line graph from 2011-12-22 to 2014-09-01.

- <https://who.is/dns>

The screenshot shows the who.is website interface. At the top, there's a search bar with 'um.es'. Below the search bar, there's a message: 'um.es is already registered. Interested in buying it? Make an Offer'. There's a table of domain extensions with their status and prices:

Extension	Status	Price
.es	Taken	
.com	Taken	
.net	Taken	
.org	Taken	
.rocks	Available	\$250.00
.news	Available	\$1250.00
.ninja	Available	\$250.00
.social	Available	\$250.00

Below this, there's a section for 'um.es' with tabs for 'Whois', 'DNS Records', and 'Diagnostics'. The 'DNS Records' tab is active, showing a table of DNS records:

Hostname	Type	TTL	Priority	Content
um.es	SOA	21599		dns1.um.es hostmaster@um.es 2010120958 7200 720 2419200 7200
um.es	NS	4864		sun.rediris.es
um.es	NS	4864		dns1.um.es
um.es	NS	4864		chico.rediris.es
um.es	NS	4864		dns2.um.es
um.es	A	21599		155.54.212.103
um.es	AAAA	15741		2001:720:1710:212::1:d
um.es	MX	20120	10	mx02.puc.rediris.es
um.es	MX	20120	10	mx01.puc.rediris.es
www.um.es	A	3723		155.54.212.103
www.um.es	AAAA	599		2001:720:1710:212::1:d
www.um.es	CNAME	3492		wwwclu.um.es

OSINT Techniques: Domain

- Check DNS and mailservers
 - <https://mxtoolbox.com/NetworkTools.aspx>

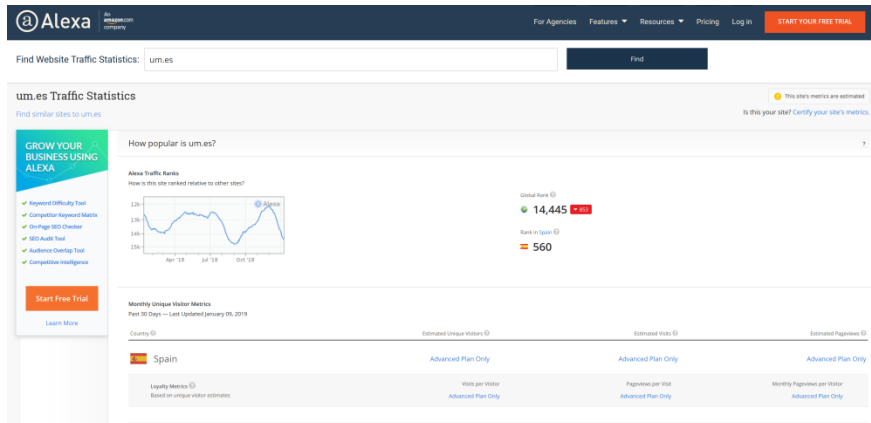
Network Tools

All Tools | Email | Network | Website | DNS | **NEW!** | My Favorite Tools | Delivery Center

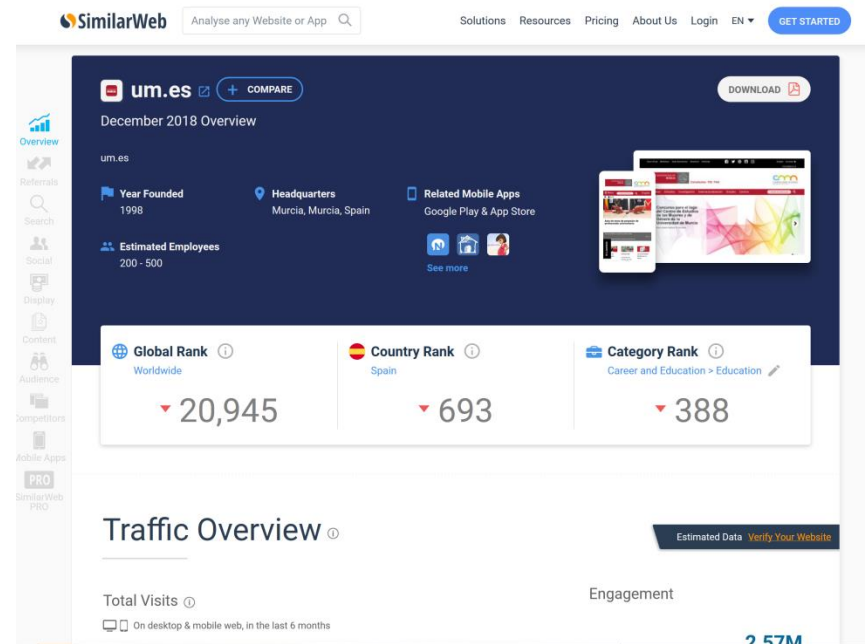
The screenshot displays a grid of 48 tool cards, each with an icon, a title, a brief description, and a search input field with a play button and a heart icon. The tools are organized into 8 rows and 6 columns. The first row includes tools like 'mx' (DNS Lookup for MX records), 'blacklist' (Check IP or host), 'a' (DNS Lookup for IP address), 'smtp' (Test mail server SMTP (25)), 'ptr' (DNS reverse lookup), 'whois' (Domain lookup), and 'dns' (Check your DNS Servers). The second row includes 'spf' (Sender Policy Framework), 'dkim' (Domain Keys Identified Mail), 'dmarc' (DMARC Lookup), 'aaaa' (DNS Lookup for IPv6), 'srv' (DNS Lookup Service Record), 'dnskey' (DNSKEY Lookup), and 'cert' (CERT Lookup). The third row includes 'loc' (DNS Lookup for Location), 'ipseckey' (IPSECKEY Lookup), 'domain' (Domain Health Report), 'asn' (ASN Lookup), 'rrsig' (DNSSEC Signature), 'nsec' (NSEC Lookup), and 'ds' (DS Lookup). The fourth row includes 'nsec3param' (NSEC3PARAM), 'bimi' (BIMI Lookup), 'whatisyip' (IP and location), 'cname' (DNS Lookup Canonical), 'txt' (DNS Lookup Text Record), 'soa' (DNS Start of Authority), and 'tcp' (Port status (ip:port)). The fifth row includes 'http' (Website query (http://)), 'https' (Website query (https://)), 'ping' (ICMP - Echo Request), 'trace' (ICMP - Traceroute), 'arin' (IP Address Blocks), 'header analyzer' (Diagnose Delivered Email), and 'mailflow' (End-to-End Email Monitoring). The sixth row includes 'subnet calculator' (Monitor an Entire Subnet), 'email extraction' (Extract Emails from any Text), 'bulk lookup' (Run Bulk Lookups), 'email deliverability' (View your full Deliverability Report), 'dns propagation' (Dns Propagation Check), 'password generator' (Password Generator), and 'dmarc delivery report' (DMARC Delivery Report). The seventh row includes 'dmarc report analyzer' (DMARC Email XML Parser), 'dmarc generator' (DMARC Generator), 'spf generator' (SPF Generator), 'investigator' (Investigator), and 'spam analyzer' (Spam Analyzer). The 'NEW!' badge is present on several tools, including 'rrsig', 'nsec', 'nsec3param', 'bimi', and 'spam analyzer'.

OSINT Techniques: Domain

- Check traffic statistics
 - <https://www.alexa.com>



- <https://www.similarweb.com>



OSINT Techniques: Domain

- Check subdomains
 - <https://findsubdomains.com>

The screenshot shows the FindSubdomains website interface. At the top, there is a navigation bar with the FindSubdomains logo, a search icon, and links for 'Login' and 'Registration'. The main content area is titled 'subdomains of um.es' and includes buttons for 'View graph' and 'Hide info'. Below this, there are three summary boxes: 'Countries - 1' showing Spain with 947 subdomains; 'IP - 665' with a 'Show all' button and a list of IP addresses and their counts; and 'AS Blocks - 2' showing two AS blocks with their respective counts. Below these boxes, there is a section for 'Subdomains - 50 of 1 283' with a 'Domain names list' dropdown. A search filter is set to 'Filter by Domain, IP, OSH...' and a search button is present. The main table displays the following data:

Domain	IP	OSH [?]	Region	AS [?]	Organization
eventos.um.es	87.253.228.167	105	Spain	AS48846	Informatica El Corte Ingles SA
entrada.um.es	155.54.212.118	1	Spain	AS766	Entidad Publica Empresarial Red.es
salidasprofesionales.um.es	155.54.216.27	1	Spain	AS766	Entidad Publica Empresarial Red.es
atica.um.es		-			
pcigrp.atica.um.es	155.54.216.54	14	Spain	AS766	Entidad Publica Empresarial Red.es
histclinic.um.es	155.54.216.54	14	Spain	AS766	Entidad Publica Empresarial Red.es
histclinicw.um.es		-			
azarbewl.um.es		-			
azarbe.um.es		-			



OSINT Techniques: Domain

- Check for archives
 - <http://web.archive.org>

INTERNET ARCHIVE Explore more than 345 billion web pages saved over time

Wayback Machine um.es

Find the Wayback Machine useful? [DONATE](#)

Saved 1,663 times between October 12, 1997 and January 9, 2019.

[Summary of um.es](#) · [Site Map of um.es](#)

1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018

















JAN	FEB	MAR	APR
1 2 3 4 5	1 2	1 2	1 2 3 4 5 6
6 7 8 9 10 11 12	3 4 5 6 7 8 9	3 4 5 6 7 8 9	7 8 9 10 11 12 13
13 14 15 16 17 18 19	10 11 12 13 14 15 16	10 11 12 13 14 15 16	14 15 16 17 18 19 20
20 21 22 23 24 25 26	17 18 19 20 21 22 23	17 18 19 20 21 22 23	21 22 23 24 25 26 27
27 28 29 30 31	24 25 26 27 28	24 25 26 27 28 29 30	28 29 30
		31	
MAY	JUN	JUL	AUG
1 2 3 4	1	1 2 3 4 5 6	1 2 3
5 6 7 8 9 10 11	2 3 4 5 6 7 8	7 8 9 10 11 12 13	4 5 6 7 8 9 10
12 13 14 15 16 17 18	9 10 11 12 13 14 15	14 15 16 17 18 19 20	11 12 13 14 15 16 17
19 20 21 22 23 24 25	16 17 18 19 20 21 22	21 22 23 24 25 26 27	18 19 20 21 22 23 24
26 27 28 29 30 31	23 24 25 26 27 28 29	28 29 30 31	25 26 27 28 29 30 31

30



OSINT Tools

OSINT Tools

Tool	License	Input Data	Platform
 Maltego	MIT	Domain, username, url, email image, DNS, IP, location...	
 Metagoofil	GNU 2.0	URL and type of file (extension)...	
 The Foca	GPL 3.0	Type of file, domain, search engine...	
 Shodan	MIT	IP, country, protocol, keywords, url, dns...	
 The Harvester	GPL 2.0	Domain, search engine,,,	
 Recon-NG	GNU 2.0	Domain, special modules for gathering...	
 Spiderfoot	GPL 2.0	Domain, username, files, url, email...	
 Intel Techniques	N/A	(almost) All the above	

OSINT Tools

OSINT tool	Input				Output	Extensibility	Interface	Platform	Other feature
	Identity data	Network data	File data	Selectable data source					
<i>FOCA</i>	X	Domain	File name, Folder	Google, Bing, DuckDuckGo	Identity info, Network info, File info	X	Stand-alone program	Windows	Server discovery module
<i>Maltego</i>	Personal information, company, community	Domain	File URL	X	Identity info, Network info, File info	Custom transforms	Stand-alone program	Linux, Windows, MAC	Location, Auto input/output refeed, Results in oriented graph
<i>Metagoofil</i>	X	Domain	File type	X	Network info, File info	X	Command line	Linux, Windows	Option to narrow results
<i>Recon-NG</i>	Personal information	Domain	X	Several	Identity info, Network info, File info	X	Command line	Linux	Location, Modules for discovery and exploitation
<i>Shodan</i>	Country, City, Keyword	Operating system, IP Address, Port, Host name	X	X	Network info	X	Web interface	Online	Location, Webcam captures
<i>Spiderfoot</i>	Email, Real name, Phone Number	Domain, IP Address, Subnet, Host name	X	Several	Network info	Custom modules	Web interface	Linux, Windows, MAC	Different types of scan, Results in oriented graph
<i>The Harvester</i>	Company	Domain, DNS server	X	Several	Identity info, Network info	X	Command line	Linux, Windows, MAC	Results in reports, Option to narrow files and results
<i>IntelTechniques</i>	Personal information, company, community	Domain, IP Address	File name, File type, File URL	Several	Identity info, Network info	X	Web interface	Online	Location, Public records, OSINT virtual machine

OSINT Tools: IntelTechniques



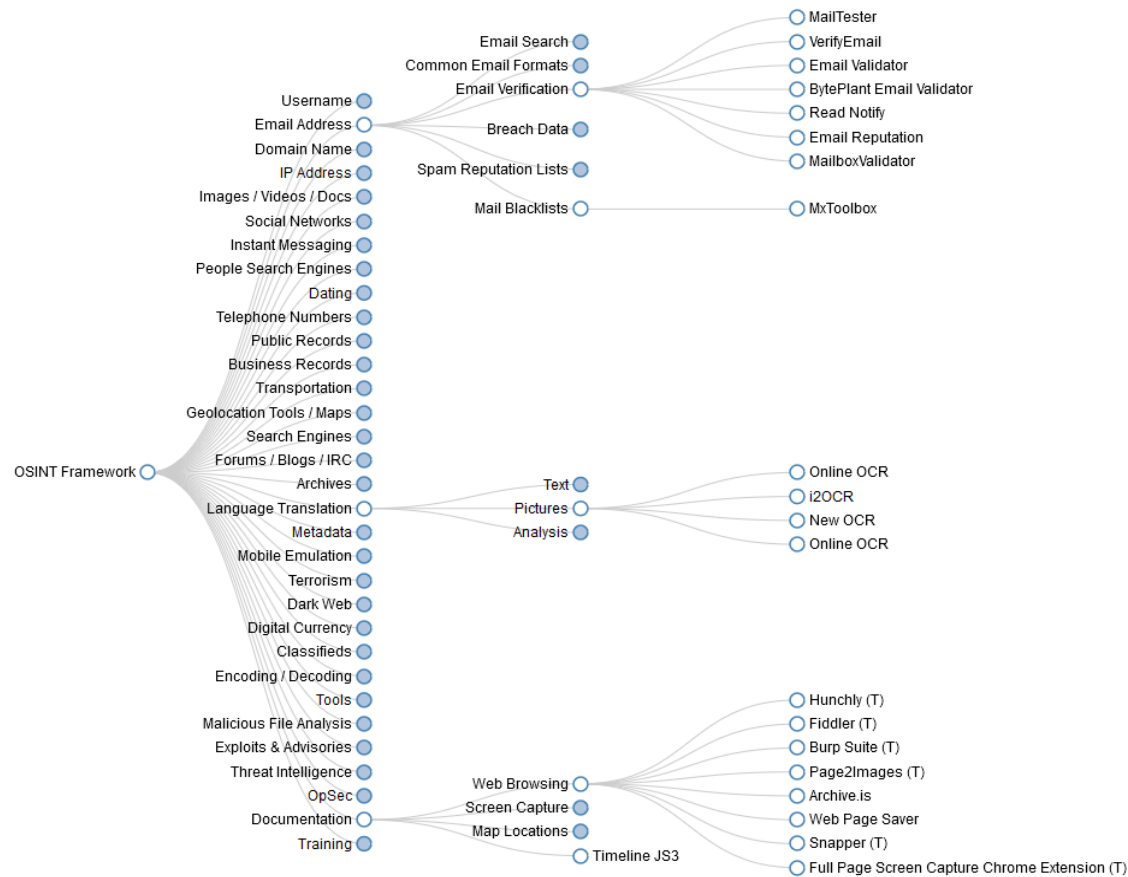
- <https://inteltechniques.com>

The screenshot shows the IntelTechniques website homepage. The header features the site name 'INTELTECHNIQUES By Michael Bazzell' and a navigation menu with items like 'Online Training', 'Live Events', 'Services', 'Tools', 'Links', 'Books', and 'Contact'. Below the header, there are two main sections: 'IntelTechniques Services' and 'IntelTechniques Resources'. The 'Services' section includes icons for 'Online Training', 'Live Events', 'Services', and 'Books'. The 'Resources' section includes icons for 'Search Tools', 'Book Links', 'Web Forum', 'Blog', and 'Podcast'. On the right side, there is a 'Online Training' section with a description of the courses and two pricing options: 'Buy Now: \$499 - 90 Days' and 'Buy Now: \$999 - 1 Year'. A large red diagonal banner with the text 'NOT WORKING ANYMORE' is overlaid across the entire screenshot.



OSINT Tools: OSINT Framework

- <https://osintframework.com/>



OSINT Tools: Aware Online



- <https://www.aware-online.com>

People search tool

In many OSINT investigations you will be looking for information about a **person**. For example, you search for background information, assets, or accounts on someone's social media. The way you search for information will have a lot of impact on the results you see. The the following custom OSINT tool can help you to effectively search for people on the internet.

Username	(Fill in some of the fields below)		
Important	Surname	Check	(Google gives alternatives)
Important	Surname	Check	(Google exact search I)
Important	Surname	Check	(Google exact search II)
Important	Surname	Check	(Google exact search III)
Important	Surname	Check	(Google resource Name)



OSINT Tools: Maltego



- <https://www.maltego.com/products>



PATERVA
A new train of thought

ABOUT PRODUCTS QUOTES & PRICING DOWNLOADS COMMUNITY DOCS CONTACT



Maltego CE

Maltego CE is used by security professionals worldwide and ships with Kali Linux out-the-box.

What is Maltego?

Maltego is an interactive data mining tool that renders directed graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the Internet.

Maltego uses the idea of transforms to automate the process of querying different data sources. This information is then displayed on a node based graph suited for performing link analysis.



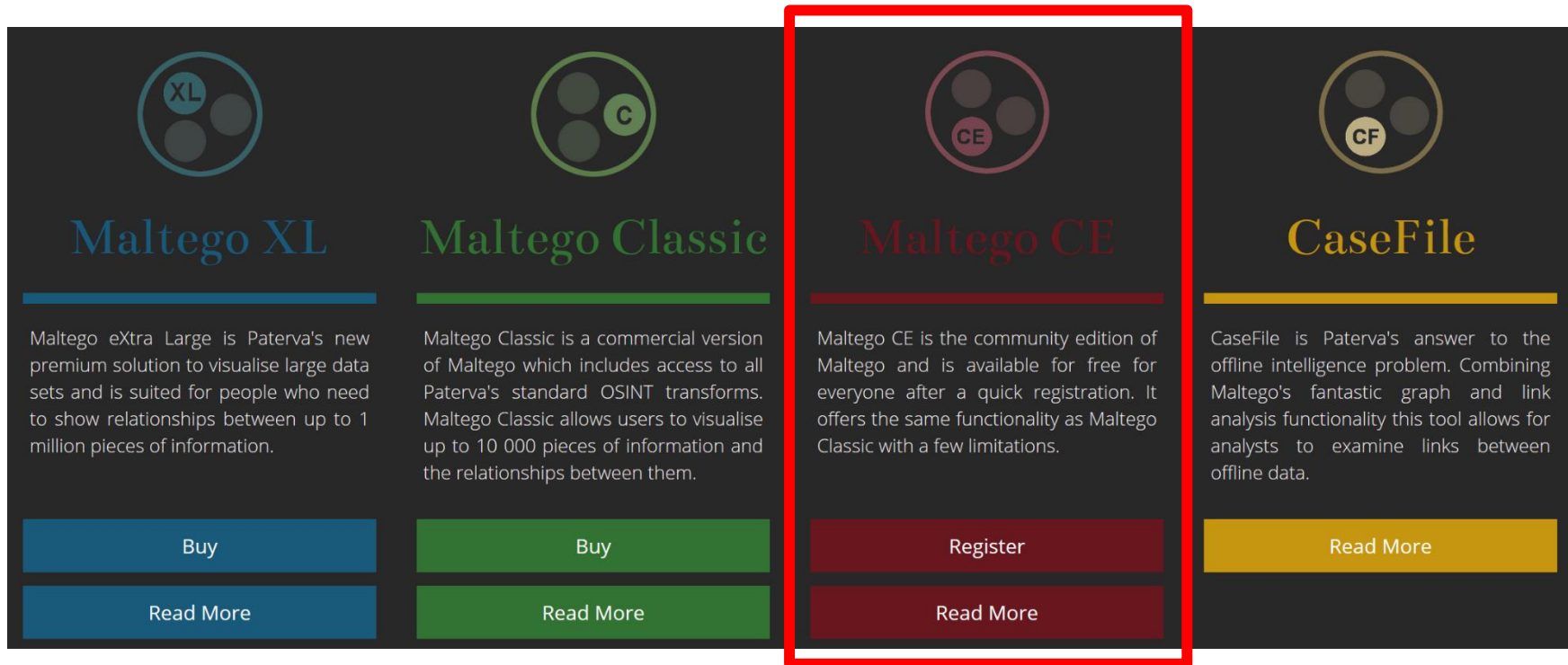
What is Maltego CE?



OSINT Tools: Maltego



- Maltego clients

A screenshot of the Maltego pricing page, showing four product cards: Maltego XL, Maltego Classic, Maltego CE, and CaseFile. The Maltego CE card is highlighted with a red border. Each card includes a logo, a title, a description, and a call-to-action button.

Product	Icon	Description	Call-to-Action
Maltego XL	XL	Maltego eXtra Large is Paterva's new premium solution to visualise large data sets and is suited for people who need to show relationships between up to 1 million pieces of information.	Buy, Read More
Maltego Classic	C	Maltego Classic is a commercial version of Maltego which includes access to all Paterva's standard OSINT transforms. Maltego Classic allows users to visualise up to 10 000 pieces of information and the relationships between them.	Buy, Read More
Maltego CE	CE	Maltego CE is the community edition of Maltego and is available for free for everyone after a quick registration. It offers the same functionality as Maltego Classic with a few limitations.	Register, Read More
CaseFile	CF	CaseFile is Paterva's answer to the offline intelligence problem. Combining Maltego's fantastic graph and link analysis functionality this tool allows for analysts to examine links between offline data.	Read More

OSINT Tools: Maltego

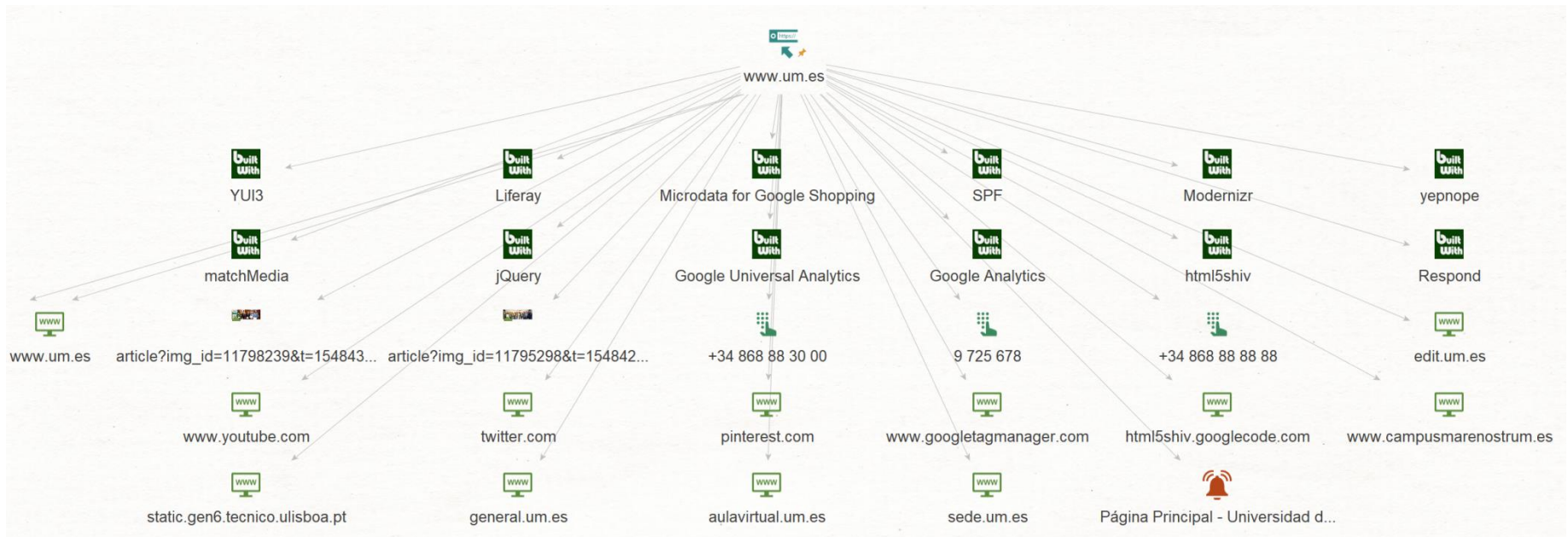


- Maltego concepts
 - An **Entity** is represented as a node on a graph and can be anything such as a DNS Name, Person, Phone number, etc.
 - The Maltego client comes with about 20 entities targeted for use in online investigations, but you can also make your own custom ones
 - A **Transform** is a piece of code that takes one entity to another
 - It does this by querying a data source and returning the results as new entities on your graph
 - The data sources are places like DNS servers, search engines, social networks, WHOIS information, etc.
 - **Machines** chain multiple transforms together to automate common/tedious tasks

OSINT Tools: Maltego



- Maltego graph



OSINT Tools: Maltego



- Maltego entities

- Devices				
Desktop Computer A personal computer in a form intended for regular use at a single location			Device A device such as a phone or camera	
Mobile Computer A portable computer suitable for use while traveling			Mobile Phone A device which can make and receive telephone calls over a radio link whilst moving around a wide geographic area	
Smartphone A mobile phone that offers more advanced computing ability and connectivity				
- Events				
Conversation (Email) A conversation via email	Conversation (Phone) A telephonic conversation		Incident An event or occurrence (for instance a murder or robbery)	Meeting (Business) A gathering of people for a commercial purpose
Meeting (Social) A gathering of people for discussion or entertainment				
- Groups				
Company A business organization	Education Institution An institution dedicated to education such as a school or university		Gang An organized group of criminals	
Online Group A socializing service on the Internet such as Facebook, an IRC channel or a mailing list	Organization A social group which distributes tasks for a collective goal		Political Movement A group of people working together to achieve a political goal	
Religious Group A group of people who share religious or spiritual beliefs				
- Infrastructure				
AS An internet Autonomous System (AS)	Banner Banner	DNS Name Domain Name System server name	Domain An internet domain	IPv4 Address An IP version 4 address
MX Record A DNS mail exchange record	NS Record A DNS name server record	Netblock A range of IP version 4 addresses	URL An internet Uniform Resource Locator (URL)	Tracking Code Represents a tracking code for a web service.
Website An internet website				
- Locations				
University University			Airport A complex of runways and buildings for the takeoff, landing, and maintenance of aircraft	
Church A place of worship			Circular Area A circular area somewhere on Earth	
City A relatively large and permanent settlement			Country A nation with its own government, occupying a particular territory	
Crime Scene A location where an illegal act took place			GPS Coordinate A location on a World Geodetic System coordinate frame for Earth	
Harbor A sheltered port where ships can load or unload passengers or goods			Home A place of living	
Location			Office	

OSINT Tools: Maltego



- Maltego transforms

Transform	Input	Output
✚ Mirror: Email addresses found	Website	Email Address
✚ Mirror: External links found	Website	Phrase
✚ Parse meta information	Document	maltego.Person,maltego.EmailAddress,maltego.Phrase,maltego.Document
✚ To AS number	Netblock	AS
✚ To Alias	Affiliation - Twitter	Alias
✚ To Aliases [mentioned in Tweet]	Tweet	Alias
✚ To Circular Area	GPS Coordinate	Circular Area
✚ To Company [Owner]	AS	Phrase
✚ To DNS Name (interesting) [Robtex]	Domain	DNS Name
✚ To DNS Name - MX (mail server)	Domain	MX Record
✚ To DNS Name - NS (name server)	Domain	NS Record
✚ To DNS Name - SOA (Start of Authority)	Domain	maltego.NSRecord, maltego.EmailAddress
✚ To DNS Name - SPF (sender policy framework)	Domain	maltego.Netblock, maltego.IPv4Address, maltego.DNSName, maltego.MXRecord, maltego.DNSName, maltego.Domain
✚ To DNS Name [Attempt zone transfer]	Domain	DNS Name
✚ To DNS Name [Enumerate hostname numerically]	DNS Name	DNS Name
✚ To DNS Name [Find common DNS names]	Domain	DNS Name
✚ To DNS Name [From DynDNS username]	Alias	DNS Name
✚ To DNS Name [Reverse DNS]	IPv4 Address	DNS Name
✚ To DNS Name [Robtex]	Domain	DNS Name
✚ To DNS Name [Using Name Schema dictionary]	Domain	DNS Name
✚ To DNS Name from passive DNS [Robtex]	IPv4 Address	DNS Name
✚ To DNS Names in netblock [Reverse DNS]	Netblock	DNS Name
✚ To Domain [DNS]	Email Address	Domain
✚ To Domain [Find other TLDs]	Domain	Domain
✚ To Domain [Sharing this MX]	IPv4 Address	Domain
✚ To Domain [Sharing this NS]	IPv4 Address	maltego.Domain,maltego.Netblock
✚ To Domains [DNS]	DNS Name	Domain
✚ To Domains [DNS]	Domain	Domain
✚ To Domains [Sharing this MX]	MX Record	Domain
✚ To Domains [Sharing this NS]	NS Record	Domain
✚ To Email Address [Verify common]	Person	Email Address
✚ To Email Address [using Search Engine]	Phone Number	Email Address
✚ To Email Addresses [Found on web page]	URL	Email Address
✚ To Email Addresses [PGP (signed)]	Email Address	Email Address
✚ To Email Addresses [PGP]	Email Address	Email Address
✚ To Email Addresses [PGP]	Person	Email Address



OSINT Tools: Maltego

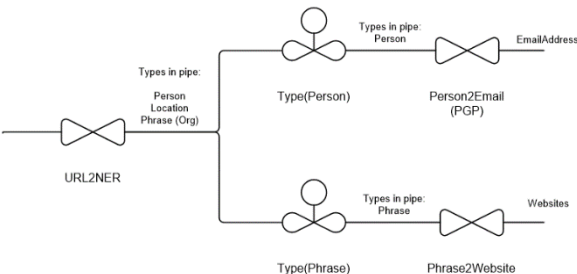


- Maltego machines

Name	Description
<input checked="" type="checkbox"/> Company Stalker	This machine will try to get all email addresses at a domain then see which resolves on social networks. It also gets documents and extracts meta data. Input is domain.
<input checked="" type="checkbox"/> Find Wikipedia Edits	This machine takes a domain and looks for possible Wikipedia edits.
<input checked="" type="checkbox"/> Footprint L1	This performs a level 1 (fast, basic) footprint of a domain.
<input checked="" type="checkbox"/> Footprint L2	This performs a level 2 (mild) footprint of a domain.
<input checked="" type="checkbox"/> Footprint L3	This performs a level 3 (intense) footprint on a domain. It takes a while and it eats resources. Use with care.
<input checked="" type="checkbox"/> Footprint XXL	This machine is built to work on really large targets that's hosting their own infrastructure. It tries to obtain the footprint by looking at SPF records hoping for netblocks as w
<input checked="" type="checkbox"/> Person - Email Address	Tries to obtain someone's email address and sees where it's used on the Internet. Input is an email address.
<input checked="" type="checkbox"/> Twitter Digger X	Works on a Twitter alias (or aliases), analyzes Tweets.
<input checked="" type="checkbox"/> Twitter Digger Y	Works on a Twitter affiliation(s). Finds Tweets and analysis it.
<input checked="" type="checkbox"/> Twitter Monitor	This machine monitors Twitter for hashtags, and named entities mentioned around a certain phrase. Input is the phrase.
<input checked="" type="checkbox"/> URL To Network And Domain Information	From URL To Network And Domain Information.

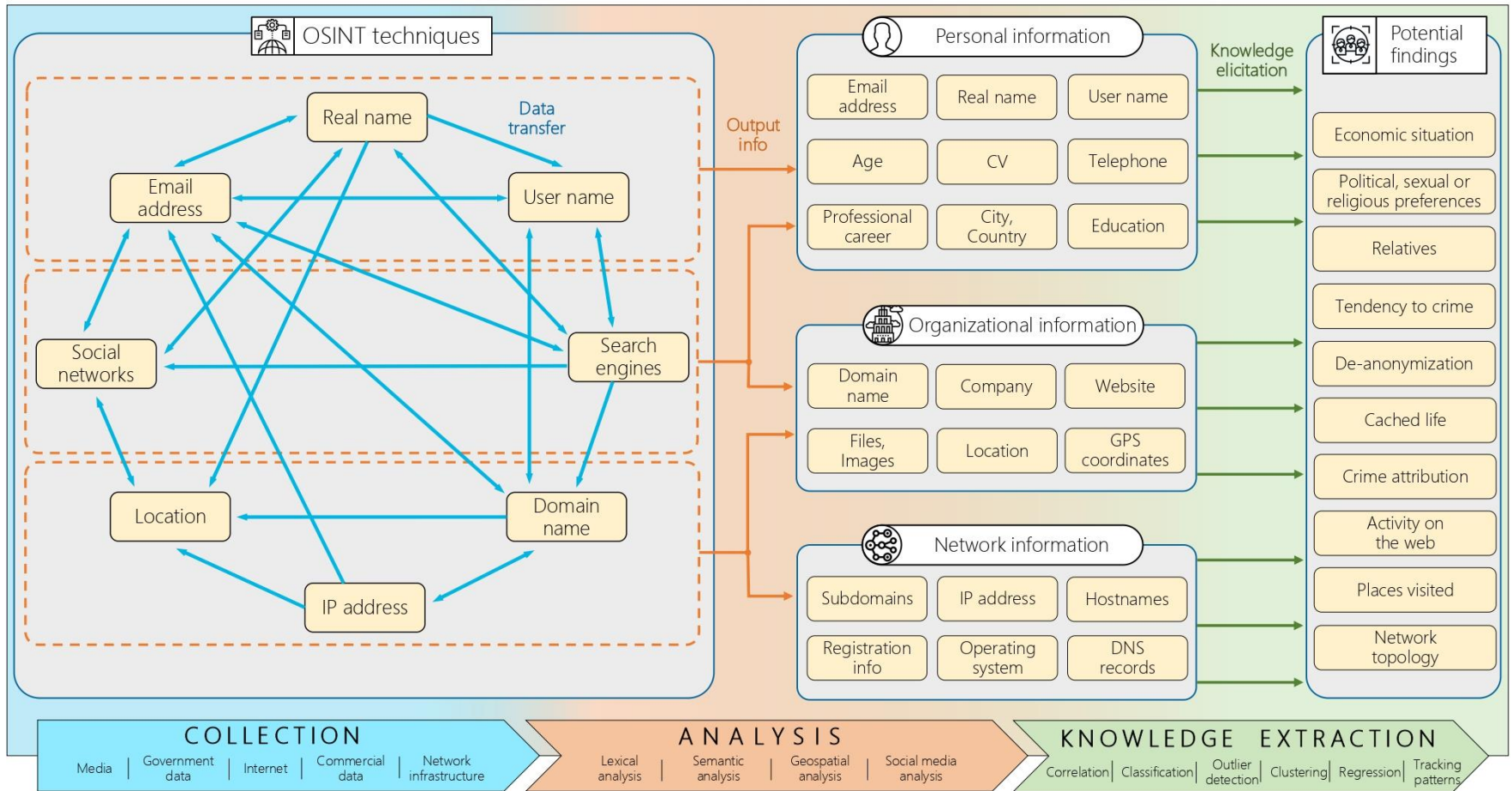
```
machine("paterva.company.stalking",
  displayName:"Company Stalker",
  author:"Paterva",
  description:"This machine will try to get all email addresses at a domain then see which resolves on social networks. It also

start {
  status("Company stalker")
  paths {
    path {
      log("Searching for email addresses...",showEntities:false)
      paths {
        run("paterva.v2.DomainToEmailAddress_AtDomain_SE",slider:200)
        run("paterva.v2.DomainToEmailAddress_PGP",slider:200)
      }
      userFilter(title:"Filter email addresses",heading:"Email addresses",description:"Filter out the silly catchall em
      log("Trying Flickr and Myspace for what it's worth")
      paths {
        run("paterva.v2.emailToFlickrAccount")
        run("paterva.v2.emailToMyspaceAccount")
      }
    }
    path {
      log("Searching for documents...",showEntities:false)
      run("paterva.v2.DomainToDocument_SE","engine":"google",slider:50)
      log("Extracting meta data from documents",showEntities:false)
      run("paterva.v2.DocumentToPersonEmail_Meta")
    }
  }
}
```



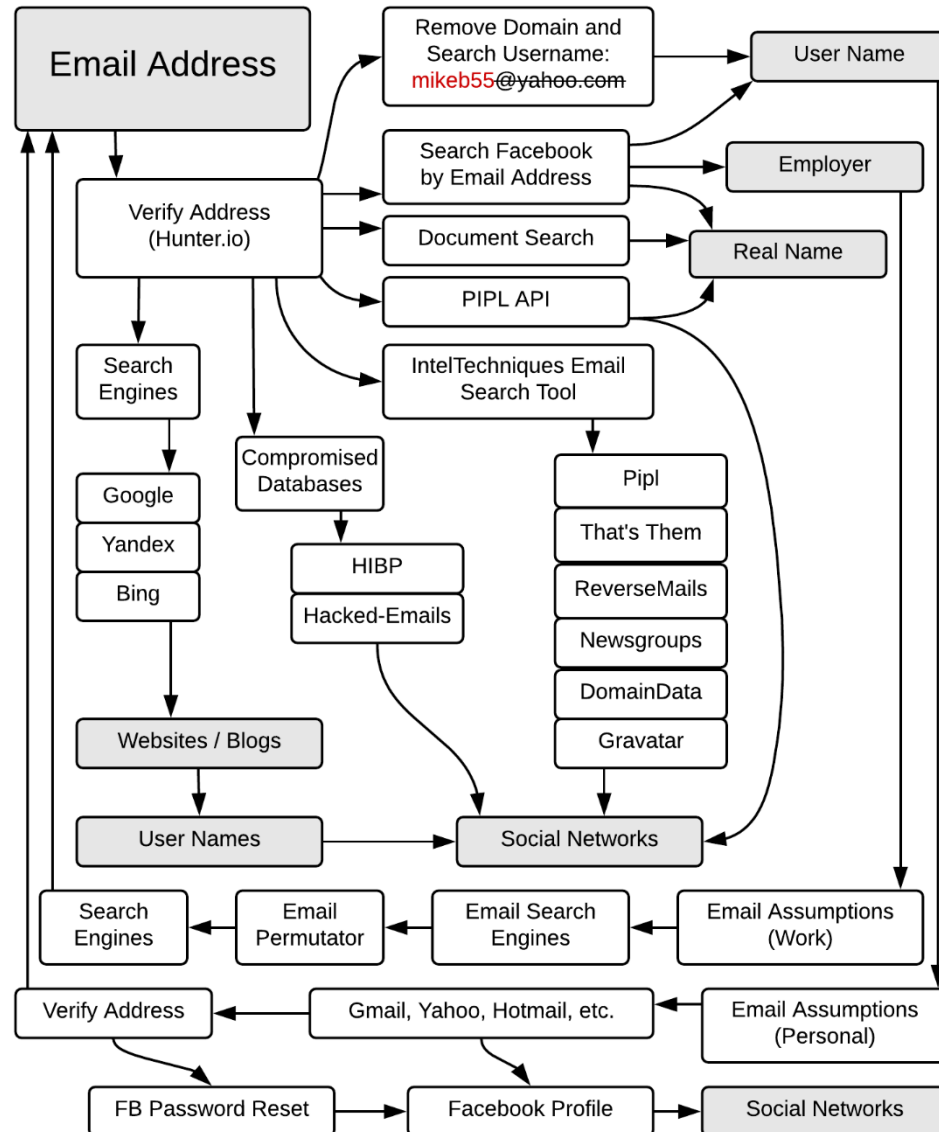
OSINT Workflows

OSINT Workflows



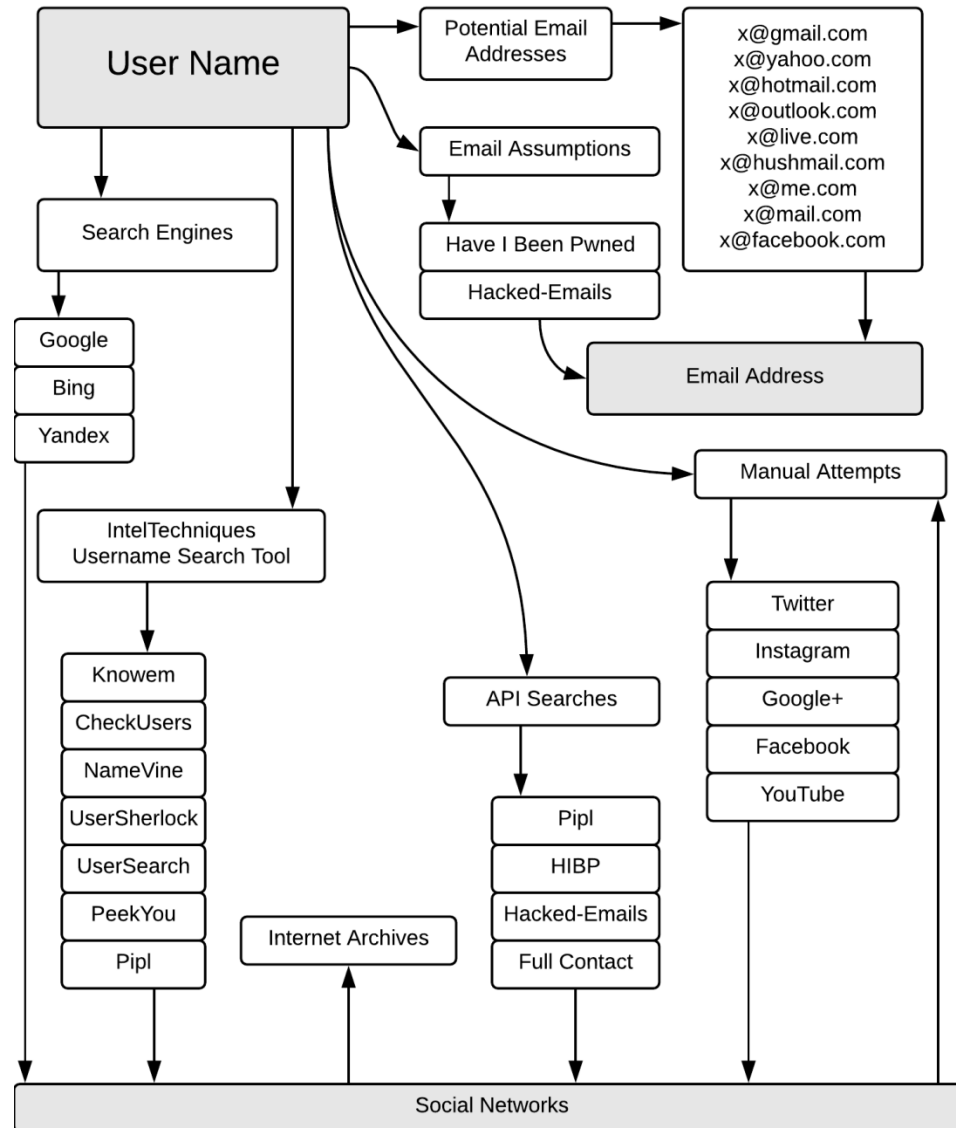
OSINT Workflows: Email Address

- Which **new information** can I obtain from an **Email Address**?
- Which **paths** can I follow to reach such new information?



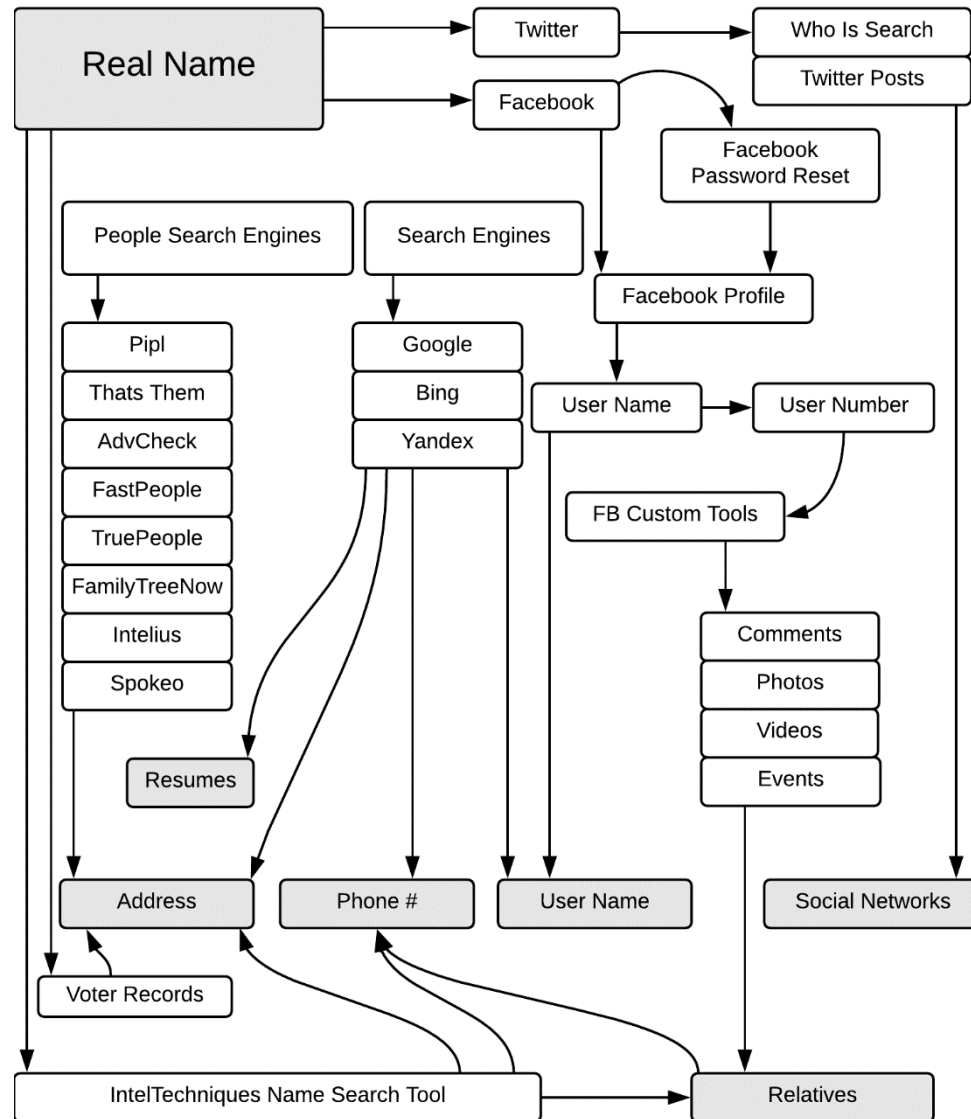
OSINT Workflows: User Name

- Which **new information** can I obtain from a **User Name**?
- Which **paths** can I follow to reach such new information?



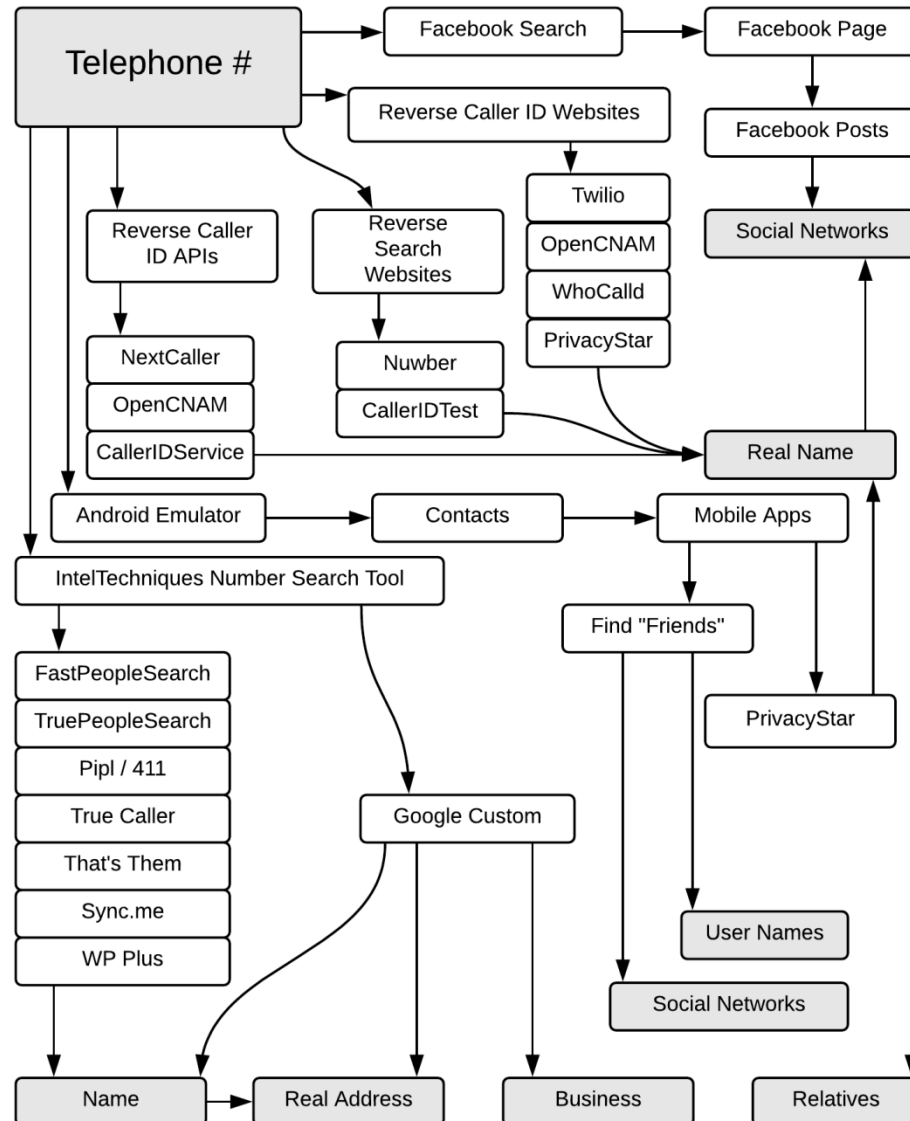
OSINT Workflows: Real Name

- Which **new information** can I obtain from a **Real Name**?
- Which **paths** can I follow to reach such new information?



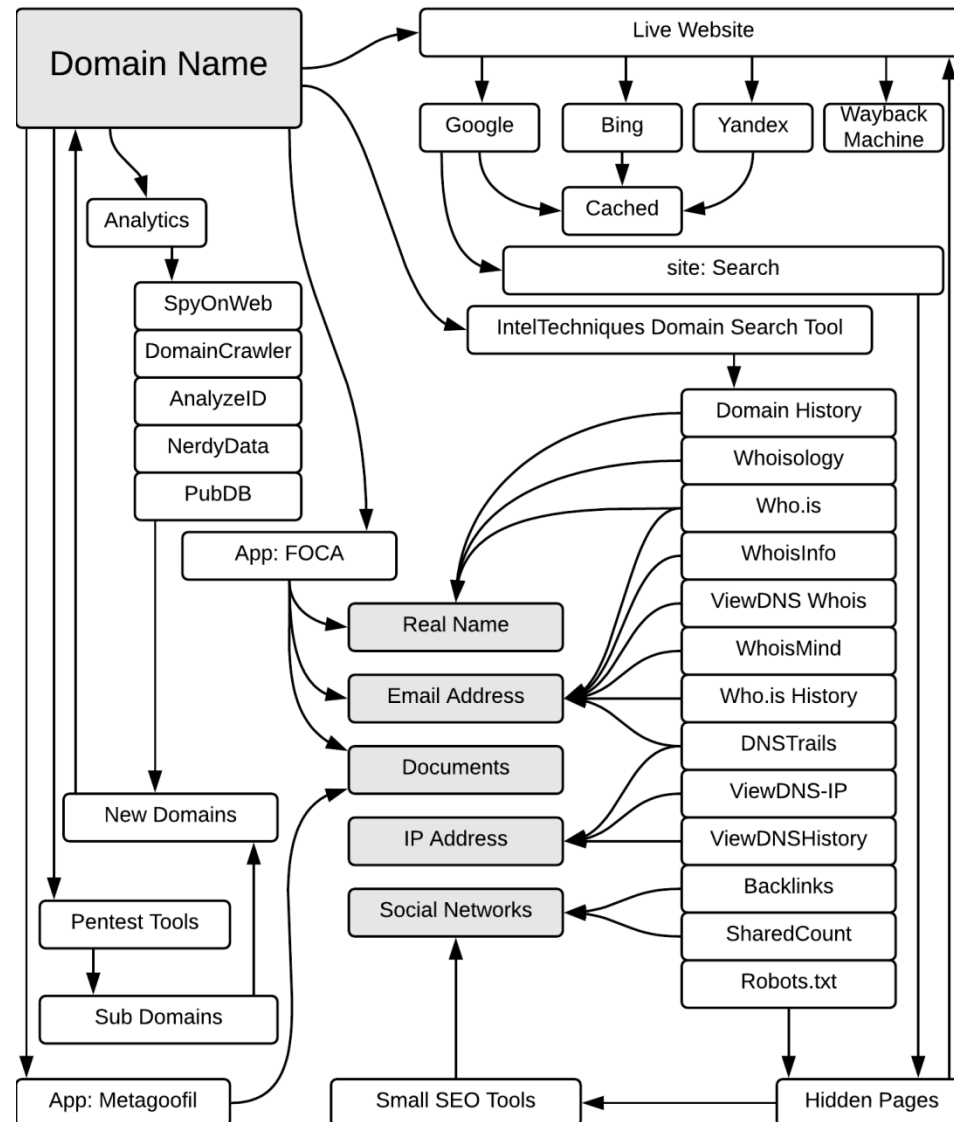
OSINT Workflows: Telephone Number

- Which **new information** can I obtain from a **Telephone Number**?
- Which **paths** can I follow to reach such new information?



OSINT Workflows: Domain Name

- Which **new information** can I obtain from a **Domain Name**?
- Which **paths** can I follow to reach such new information?



Bibliography

- [1] J. Pastor Galindo, P. Nespoli, F. Gómez Mármol, and G. Martínez Pérez, **“The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends,”** *IEEE Access*, vol. 8, no. 1, pp. 10282–10304, 2020
- [2] Bazzell, M., **“Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information”**, 6th Edition, ISBN 978-1984201577, 2018
- [3] J. Pastor-Galindo, F. Gómez Mármol, G. Martínez Pérez, **“Nothing to Hide? On the Security and Privacy Threats Beyond Open Data”**, *IEEE Internet Comput.* 25(4): 58-66 (2021)
- [4] Quick, D., Kim-Kwang, R. C., **“Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+ OSINT): A timely and cohesive mix”**, *Future Generation Computer Systems*, vol. 78, pp. 558-567, 2018
- [5] Mediná Martin, J. H., et al., **“Open source intelligence (OSINT) in a Colombian context and sentiment analysis”**, *Revista Vínculos: Ciencia, tecnología y sociedad*, vol. 15, no. 2, pp. 195-214, 2018