UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CORSO DI PERFEZIONAMENTO IN «SECURITY MANAGER»

CORSO DI FORMAZIONE IN «PROFESSIONISTA DELLA SECURITY»

12 FEBBRAIO 2022

GIOVANNI D'ALASCIO

Raccolta, analisi e sistematizzazione di dati per la tutela e la competitività dell'Organizzazione.

Le tecnologie a supporto dell'Homeland security

Dall'informazione all'Intelligence

Key terms

Informazione

- Conoscenza in forma grezza

Intelligence

- Informazioni che possono essere comprese
- Informazioni con valore aggiunto
- Informazioni che sono state valutate nel contesto della loro fonte e affidabilità

Analisi (di informazioni o intelligence)

- La risoluzione o la separazione di una cosa nelle sue parti componenti
- Accertamento delle parti
- Risalire alla fonte delle cose per scoprirne i principi generali
- Dichiarazione dei risultati del processo

Analizzare le informazioni

Processo in fasi

- Qual è esattamente il problema: quale decisione dobbiamo prendere e perché è importante?
- Quali informazioni abbiamo già o potremmo ragionevolmente ottenere che potrebbero essere rilevanti al problema in mano. Dov'è/come possiamo ottenerlo?
- Quale significato possiamo estrarre dalle informazioni: cosa ci dice di quello che sta succedendo?
- C'è solo una possibile spiegazione o ci sono altre alternative o opzioni. Sono alcune più probabili di altre?
- In che modo queste influiscono sulla decisione che dobbiamo prendere, alcune opzioni sono potenzialmente migliori di altre: alcune comportano un rischio maggiore di successo e/o fallimento?
- Siamo pronti ad agire con un ragionevole livello di fiducia o dovremmo disporre prima di maggiori informazioni? In tal caso, di cos'altro abbiamo bisogno e dove/come possiamo ottenerlo?

Analizzare le informazioni

Portando questo processo sotto il nostro controllo cosciente, possiamo monitorarlo, svilupparlo e migliorarlo e sottoporlo a controlli di qualità che possono essere piuttosto complessi.

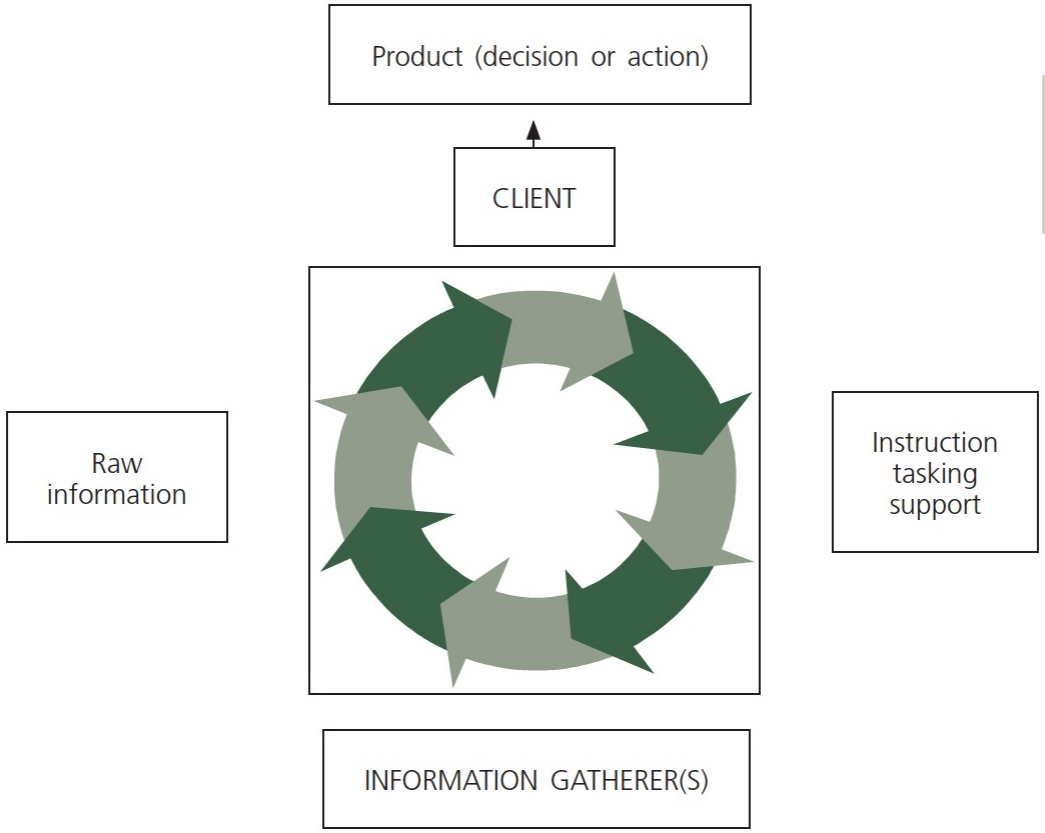
Lo sviluppo della consapevolezza è l'abilità fondamentale.

I vantaggi pratici dello sviluppo nell'individuo delle capacità analitiche sono molti, riassunti come segue

ANALYSIS GOES BEYOND THE FACTS

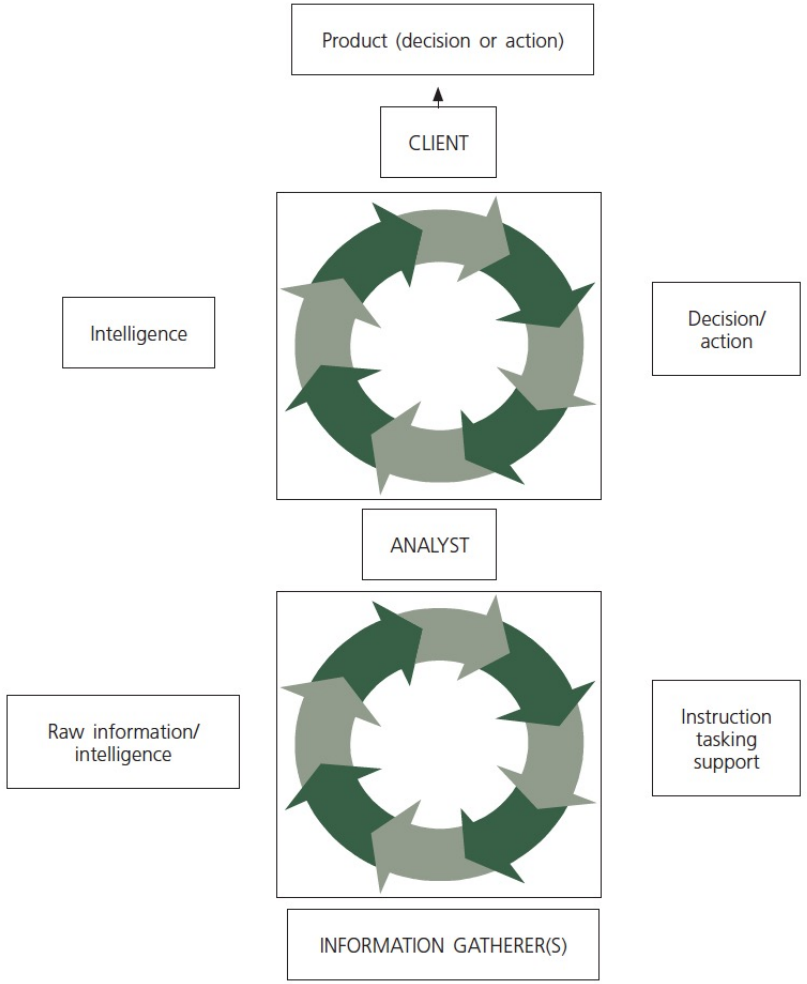
- It can tell you how good (or poor) your information/intelligence is
- It can tell you things you didn't know before
- It can tell you what you need to know to understand a situation
- It can tell you where to look further
- It can help you to communicate your understanding to others

Basic tasking model



PARTIAL UNDERSTANDING MUST INCORPORATE A DEGREE OF MISUNDERSTANDING.
MISUNDERSTANDING LEADS TO POOR CONCLUSIONS.

Developed tasking model



Necessità di una fase intermedia (analyst), dove la maggior parte delle informazioni devono essere raccolte, registrate, valutate ed esaminate, per interpretarne ed estrarne il significato intrinseco e contestuale, prima che il risultato raggiunga definitivamente al cliente.

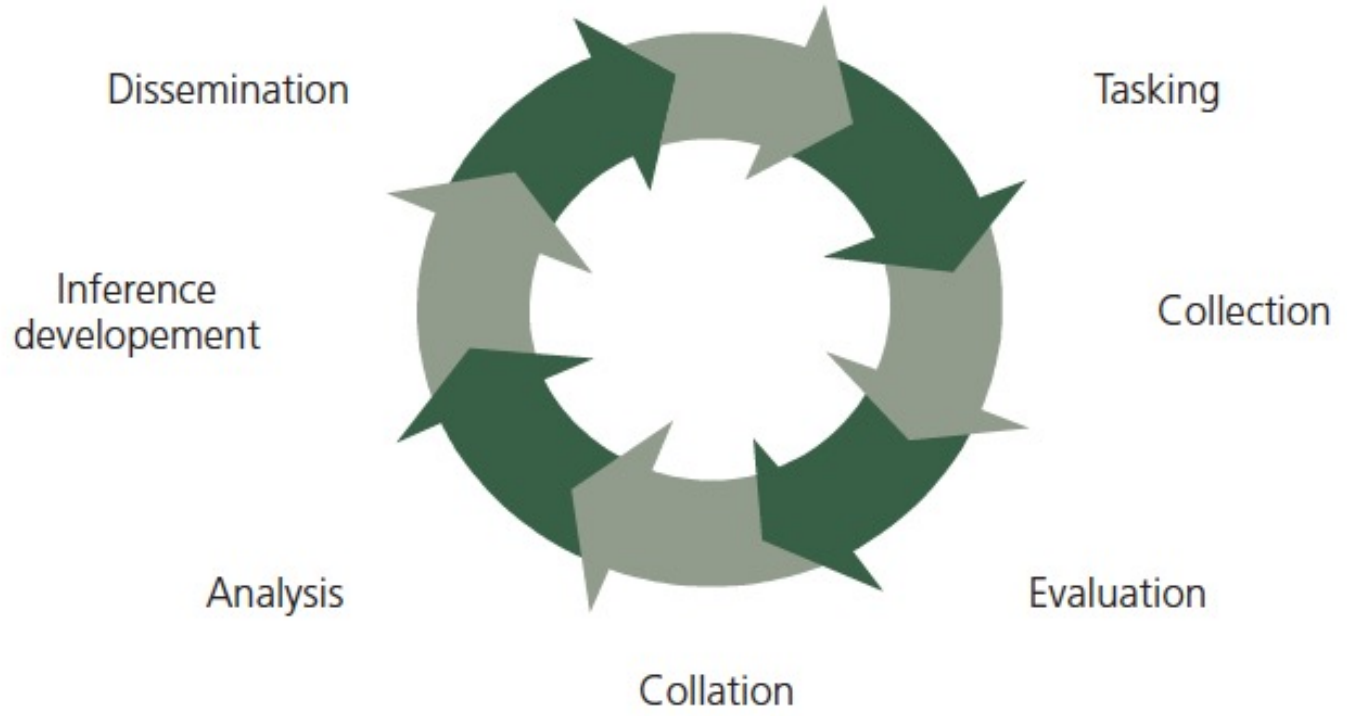
Questa è l'origine della figura dell'analista

Intelligence
knowledge designed for action

Strategic intelligence: Focuses on the long-term aims of law enforcement agencies. It typically reviews current and emerging trends changes in the crime environment, threats to public safety and order, opportunities for controlling action and the development of counter programmes and likely avenues for change to policies, programmes and legislation.

Operational intelligence: Typically provides an investigative team with hypotheses and inferences concerning specific elements of illegal operations of any sort. These will include hypotheses and inferences about specific criminal networks, individuals or groups involved in unlawful activities, discussing their methods, capabilities, vulnerabilities, limitations and intentions that could be used for effective law enforcement action.

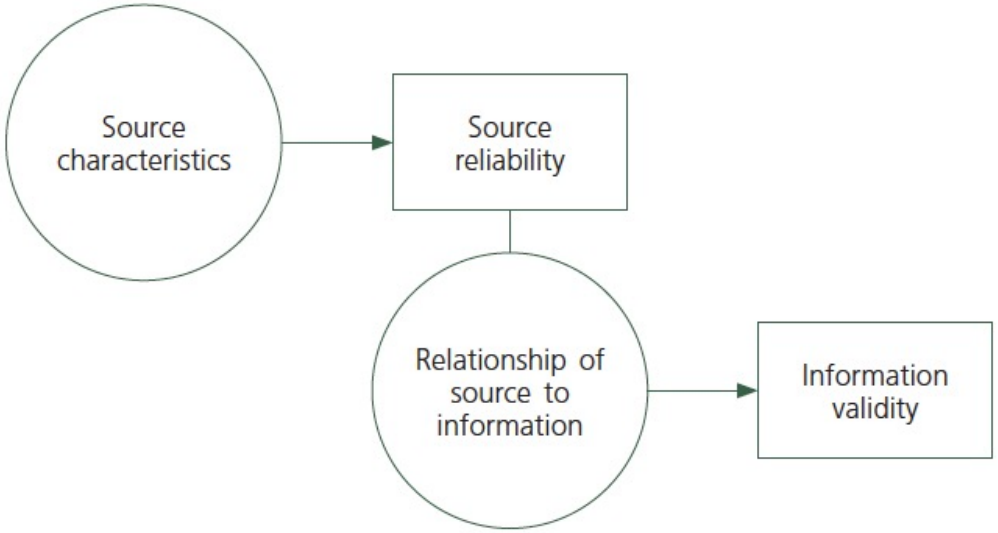
Information + Evaluation = Intelligence



Data integration

- ✓ **Link charting**
- *relationships among entities featuring in the investigation*
- ✓ **Event charting**
- *chronological relationships among entities or sequences of events*
- ✓ **Commodity flow charting**
- *to explore the movement of money, narcotics, stolen goods or other commodities*
- ✓ **Activity charting**
- *to identify activities involved in a criminal operation*
- ✓ **Financial profiling**
- *to identify concealed income of individuals or business entities and to identify indicators of economic crime*
- ✓ **Frequency charting**
- *to organize, summarize and interpret quantitative information*
- ✓ **Data correlation**
- *to illustrate relationships between different variables*

Processo di valutazione



Three fundamental principles apply to evaluation:

1. It must not be influenced by personal feelings but be based on professional judgement.
2. Evaluation of the source must be made separately to the information.
3. It must be carried out as close to the source as possible.

Processo di valutazione

Percezione del contesto

Il processo di percezione collega le persone al loro ambiente ed è fondamentale per una comprensione accurata del mondo che ci circonda.

Un'analisi accurata d'intelligence richiede una percezione accurata.

Key individual or individuals - WHO?

Criminal activities - WHAT?

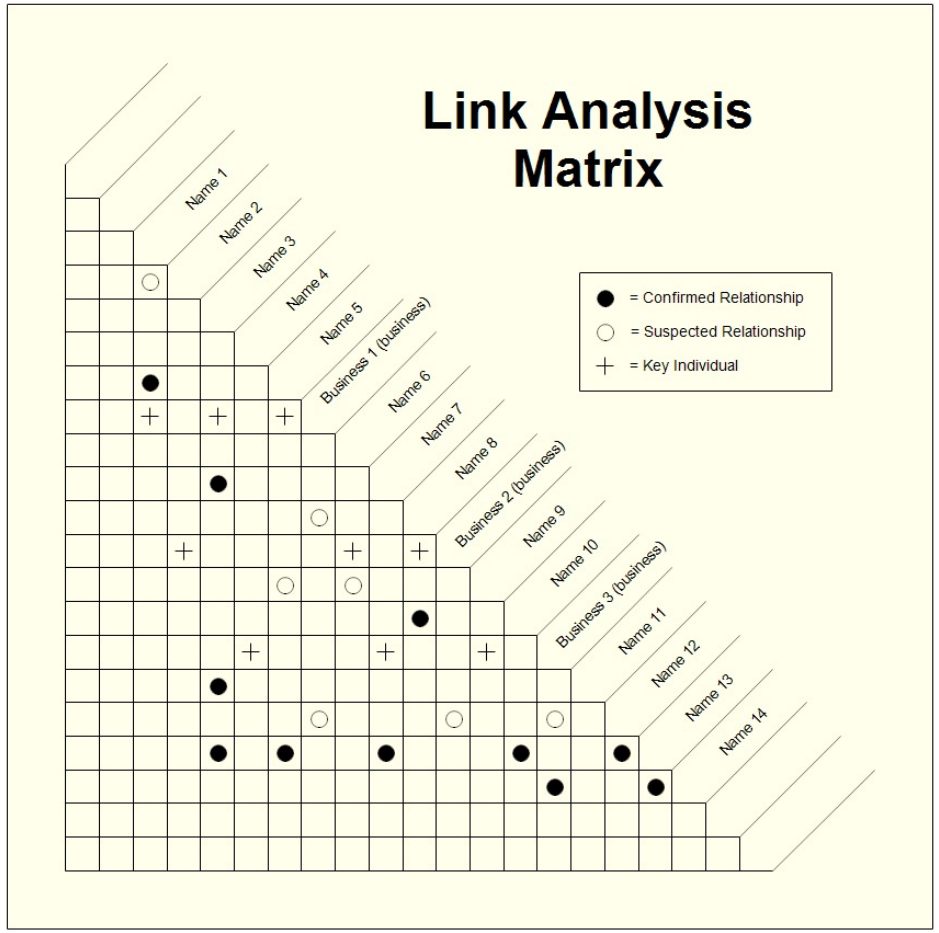
Geographical scope - WHERE?

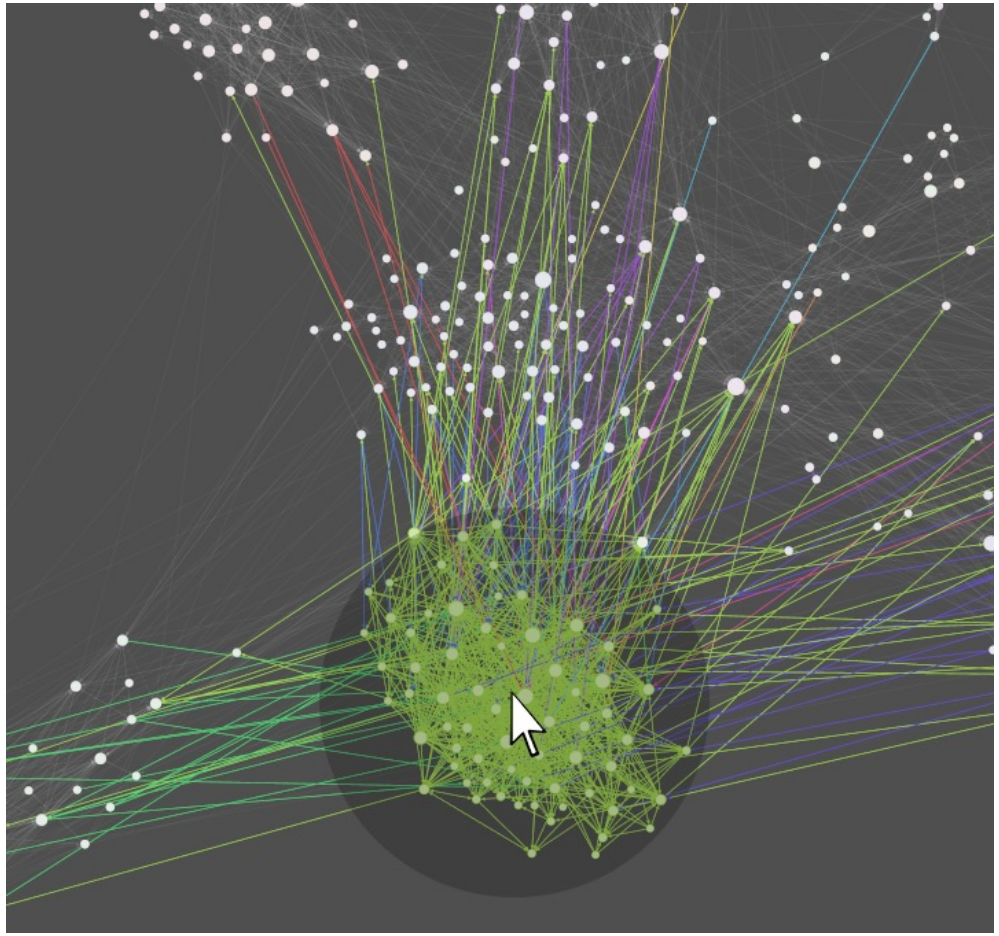
Motive - WHY?

Time-frame - WHEN?

Method of operation - HOW?

Association matrix





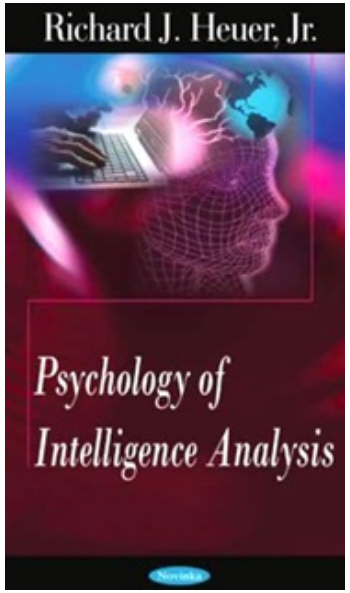
Percezione e realtà

Bias cognitivi

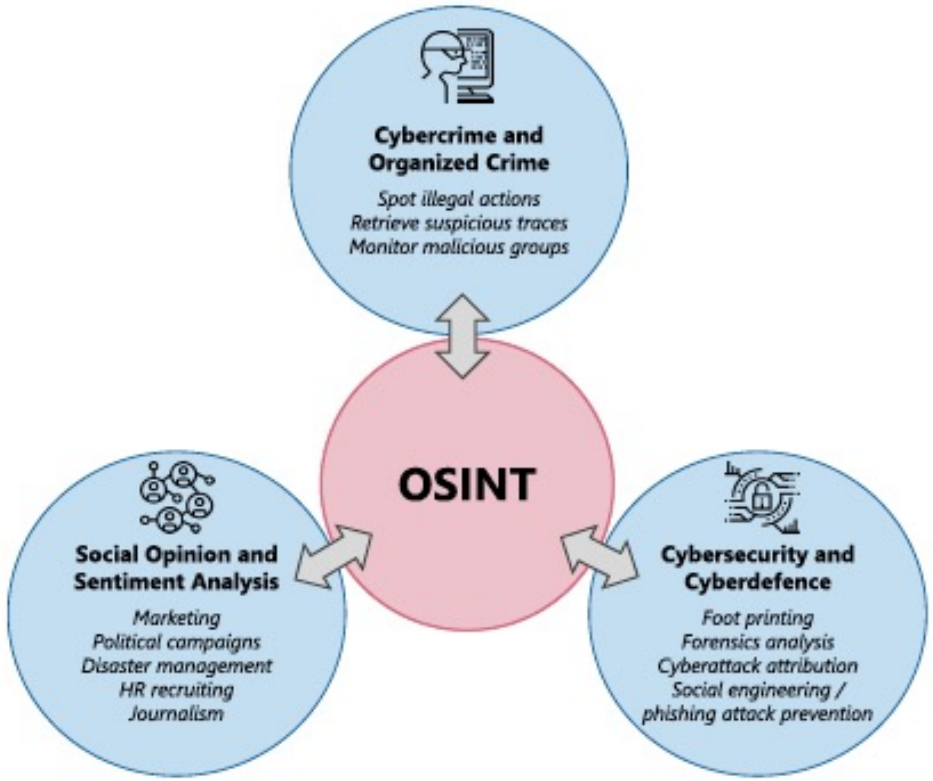
- **Processo passivo**: i nostri sensi vengono colpiti dagli eventi e ne interpretano soggettivamente la dimensione, mediante interferenza
- **Processo attivo**: registrare un evento consapevolmente

Percezione e realtà

Le impressioni resistono ai cambiamenti

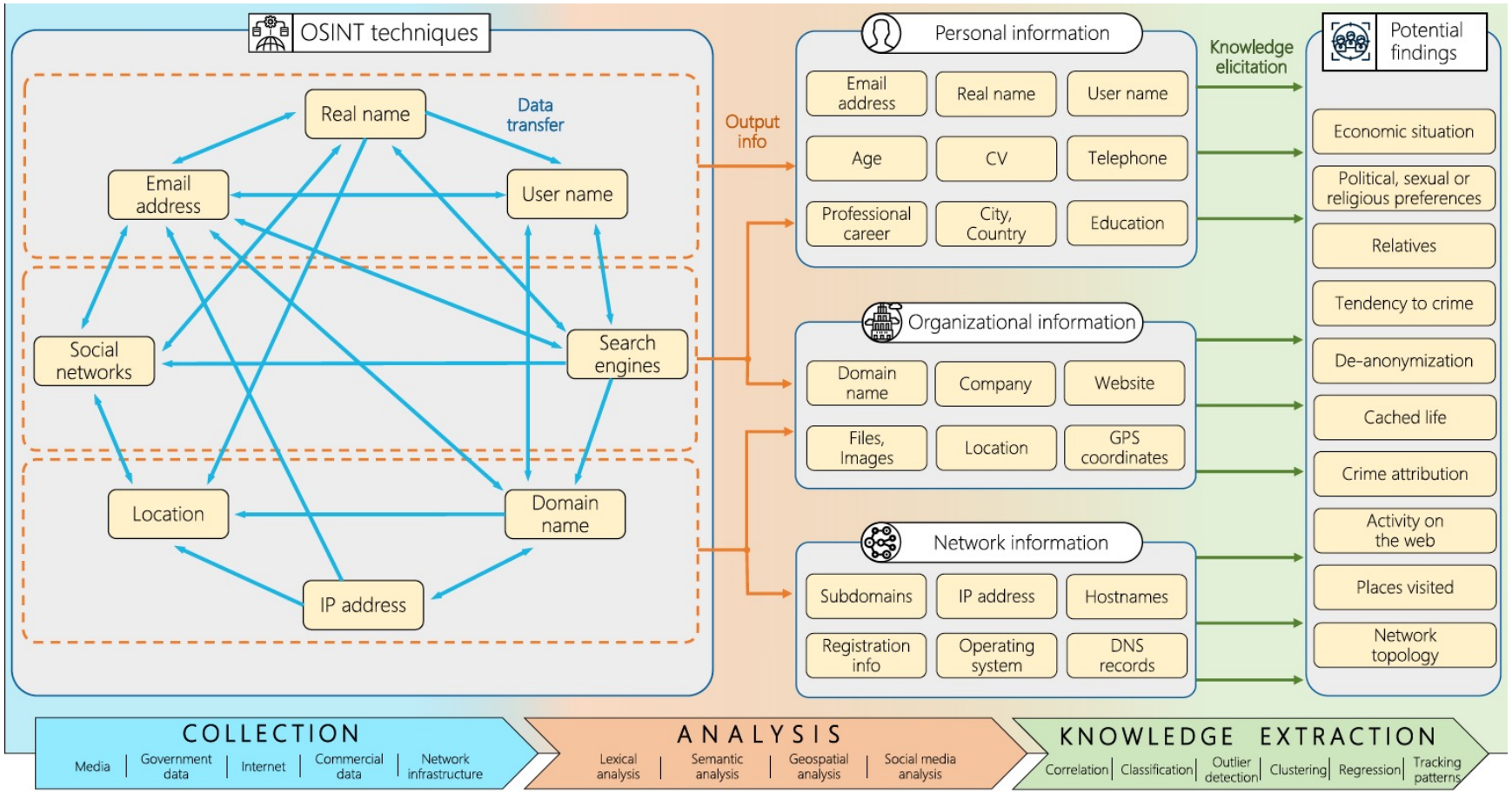


Open Source Intelligence



Pros ✓	Cons ✗
Huge amount of available information	Complexity of data management
High capacity of computing	Unstructured information
Big data and machine learning	Misinformation
Complementary types of data	Data sources reliability
Flexible purpose and wide scope	Strong ethical/legal considerations

Open Source Intelligence



Statistics

Source https://gs.statcounter.com

Desktop SEM

Google	bing	Yahoo!	DuckDuckGo	Ecosia	YANDEX
89.67%	7.04%	2.3%	0.55%	0.25%	0.08%

Desktop Search Engine Market Share in Italy - September 2021

Google	bing	Yahoo!	DuckDuckGo	Ecosia	StartPage
81.73%	11.04%	4.2%	2.49%	0.17%	0.08%

Desktop Search Engine Market Share in United States Of America - September 2021

Google	YANDEX	Mail.ru	bing	DuckDuckGo	Yahoo!
50.07%	46.72%	1.65%	0.7%	0.42%	0.33%

Desktop Search Engine Market Share in Russian Federation - September 2021

Google	bing	Yahoo!	Ask Jeeves	DuckDuckGo	YANDEX
98.28%	1.43%	0.19%	0.03%	0.02%	0.02%

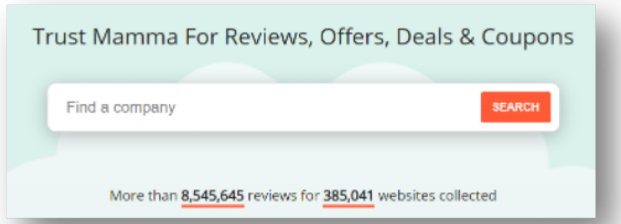
Desktop Search Engine Market Share in Islamic Republic Of Iran - September 2021

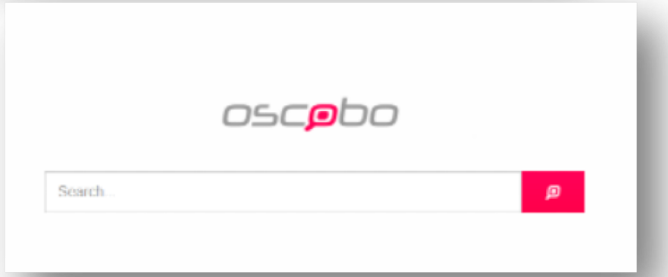
Baidu	Sogou	bing	Haosou	Google	YANDEX
40.24%	29.54%	13.94%	7.92%	7.9%	0.3%

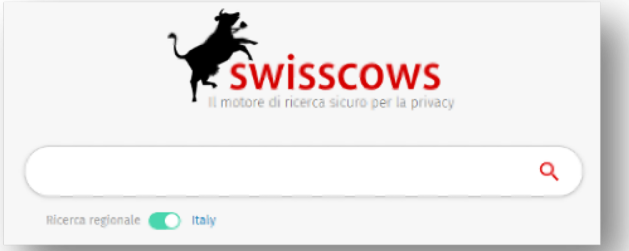
Desktop Search Engine Market Share in China - September 2021

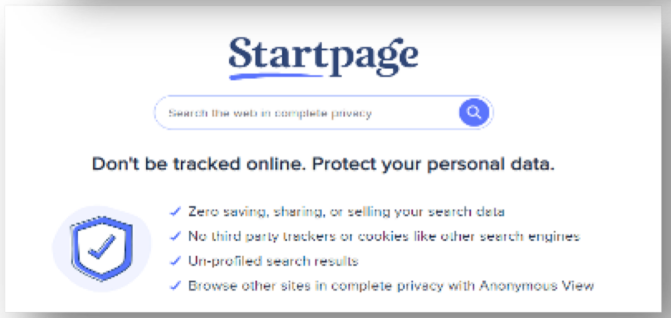
Source https://gs.statcounter.com

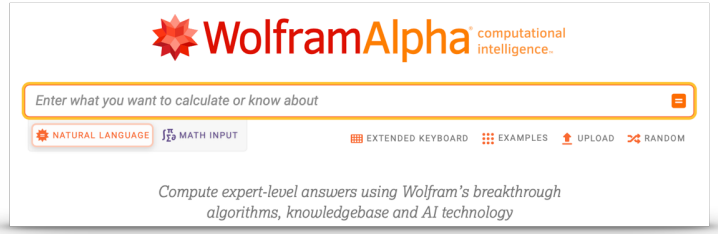
Search Enginges

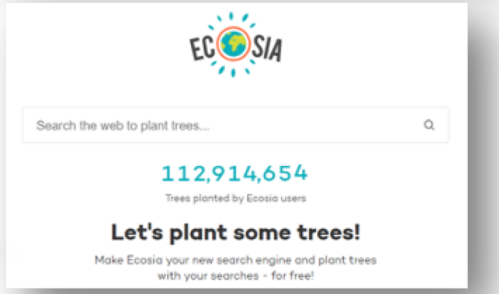








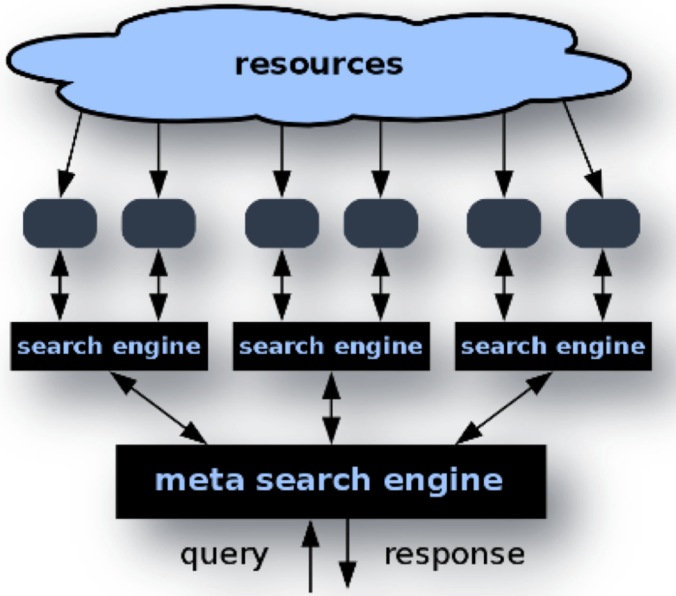




Metamotori

Interfaccia informatica che svolge la sua interrogazione su più motori di ricerca contemporaneamente

100SearchEngines https://www.100searchengines.com
SearchAll https://www.searchall.net
All-in-One http://all-io.net
SonicRun http://www.sonicrun.com
Weboasis https://weboas.is/
Etools http://www.etools.ch
Zapmeta http://www.zapmeta.com
FaganFinder https://www.faganfinder.com
The Lookup http://the-lookup.com
Search https://search-it.netlify.app
DADgogo http://dadgogo.com



Motori decentralizzati

Utilizzo della tecnologia del registro distribuito – blockchain

Almonit http://almonit.eth.link

IPFS Search https://ipfs-search.com

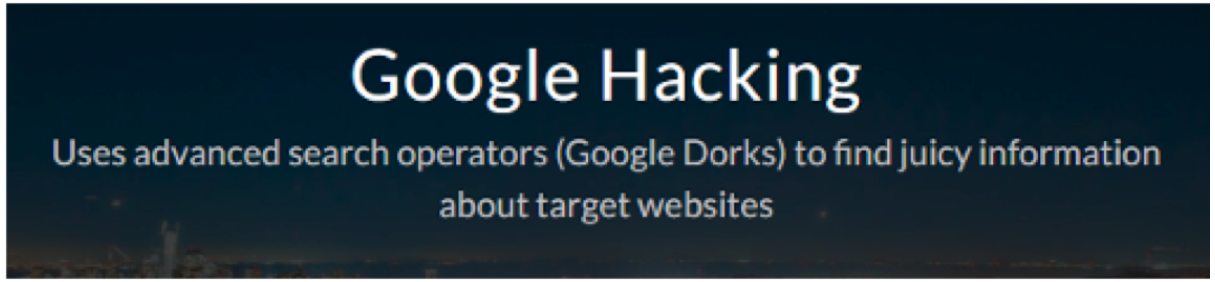
Presearch https://presearch.org

Susper https://susper.com

Yacy https://yacy.net

- controllo dell'utilizzo e condivisione delle informazioni
- protezione informazioni consumatori
- piattaforma decentralizzata
- ecosistema che consente agli utenti di trarre potenzialmente profitto dalle ricerche
- matching appropriato

- intitle
- allintitle
- inurl
- allinurl
- filetype
- intext
- allintext
- text
- site
- book
- movie
- inanchor
- numrange
- daterange
- author
- group
- insubject
- msgid
- site
- weather
- phonebook
- link



Social Media Intelligence

Tecnica di ricerca di informazioni tramite il monitoraggio e l'analisi dei contenuti scambiati attraverso i Social Media

- Informazioni crowd-sourced
- Supporto decision-making process
- Aspetti etici e GDPR

Social Media search and monitoring

Tool	Link
AIDR	http://aidr.qcri.org/
buzzglobe	https://buzzglobe.com/
CrowdTangle	https://www.crowdtangle.com
Evolve Social Search	https://bonobos.github.io/evolve-social-search/
Isearchsocial	https://isearchsocial.com
Spyderfoot	https://www.spiderfoot.net
SocialPath	https://github.com/woj-ciech/SocialPath
UVRX	http://www.uvrx.com/social.html
Data visualization	https://osintcombine.tools https://gephi.org
TweetBeaver	https://tweetbeaver.com/index.php

Hashtag

A word or phrase preceded by a hash sign # that classifies or categorizes the accompanying text.

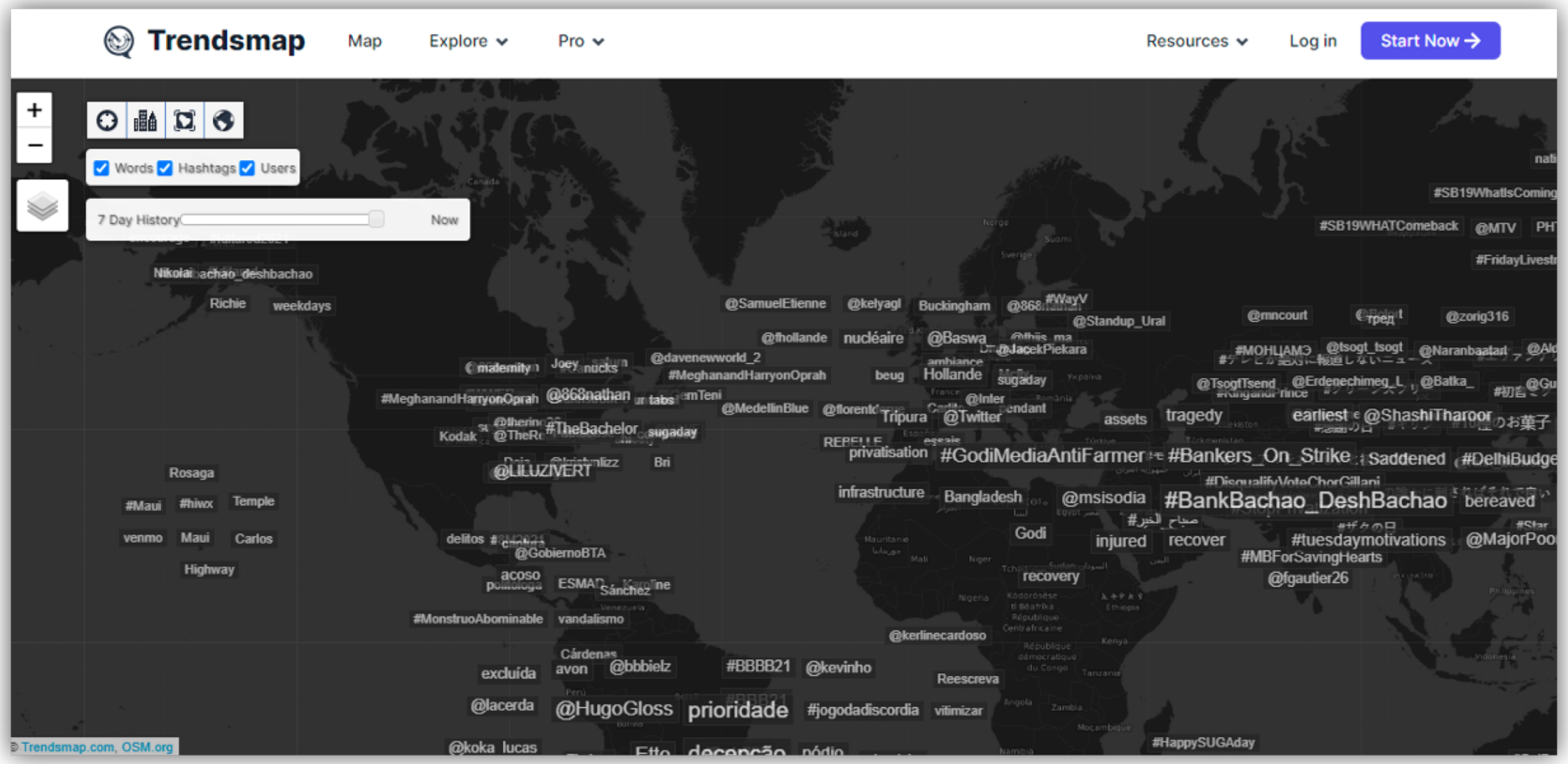
è usato per indicizzare parole chiave o argomenti e per essere dunque individuato

Need to be there for a reason

5W+H

Tool	Link
All Hashtag	https://www.all-hashtag.com
Best Hashtags	http://best-hashtags.com
Display Purposes	https://displaypurposes.com
Hashtag Directory	https://www.thehashtagdirectory.com
Hashtag Hub	https://hashtaghub.herokuapp.com
Hashtatit	https://www.hashatit.com
#onemilliontweetmap	https://onemilliontweetmap.com
SMAT Streamlit	https://www.smat-app.com
Social Bearing	https://www.socialbearing.com
Tagdef	https://tagdef.com/it/
TagsFinder	https://www.tagsfinder.com/it-it/
Twubs	https://twubs.com

Twitter Trendsmap



Hashtag analysis

Twitter Visualization

Fact vs. Fiction

Misinformation (mis-, meaning wrong or mistaken)
“false informazioni che vengono diffuse, indipendentemente dall'intento di fuorviare.”

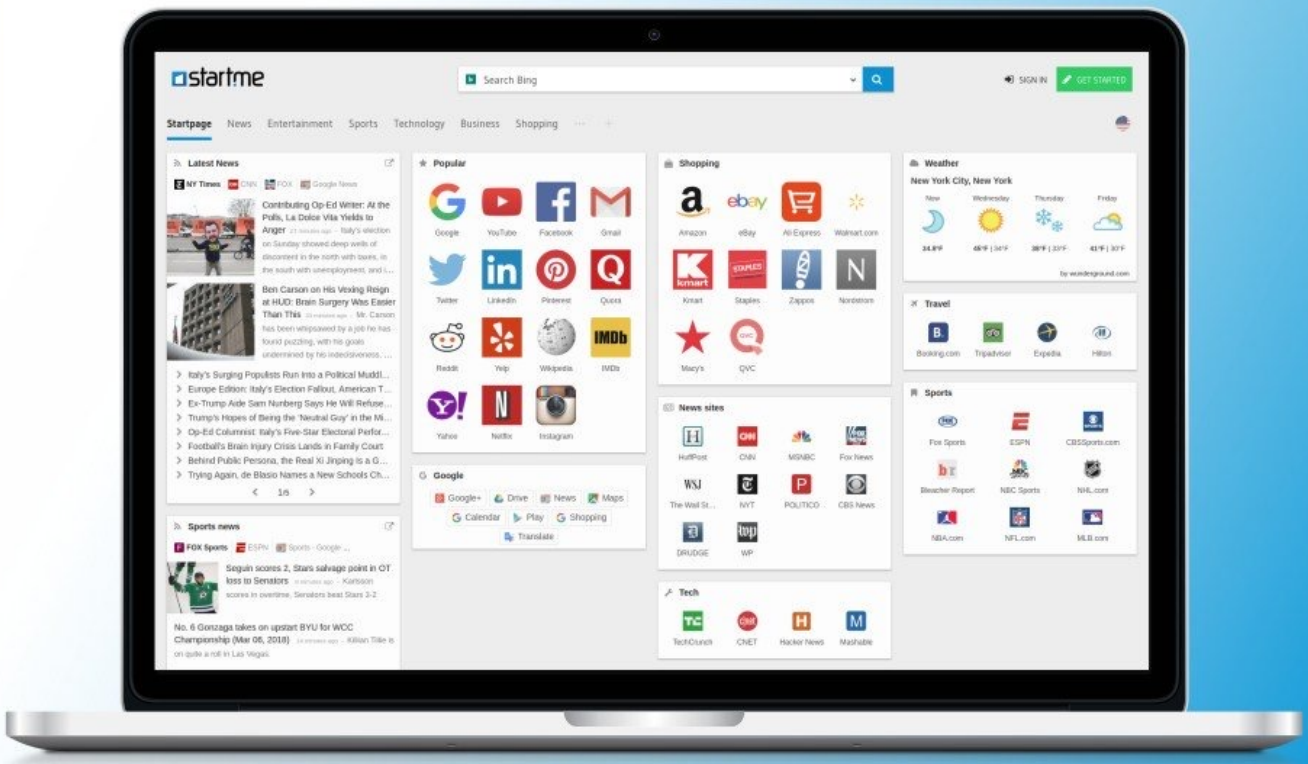
Disinformation (dis-, reversal or negative instance of the word that follows)
“informazioni false o fuorvianti che vengono diffuse deliberatamente per ingannare.”

Intenzione di ingannare

https://www.state.gov/disarming-disinformation/

Start.me

startme



Data Collation and Data Processing Tools

Tool	Link
Atavi	https://atavi.com
Bookmark OS	https://bookmarkos.com
Clipix	https://www.clipix.com
eLink	https://elink.io/dashboard
Email This	https://www.emailthis.me/
FAVable	https://www.favable.com
Flipboard	https://flipboard.com
Zotero	https://www.zotero.org
Zulu	https://tryzulu.com

Business Information

Aleph	https://aleph.occrp.org
AllStocksLink	http://www.allstocks.com/links
Biznar	https://biznar.com
Bizstats Uk	https://www.bizstats.co.uk
Bizstats	http://www.bizstats.com
Bureau Van Dijk	http://www.bvdinfo.com
Buzzfile	https://www.buzzfile.com/Home/Basic
Cedar Rose	https://www.cedar-rose.com
Comparably	https://www.comparably.com
CompeteShark	https://competeshark.com
Corporate Information	https://www.corporateinformation.com

Business Information

Corporation Wiki	https://www.corporationwiki.com
CorpWatch	http://www.corpwatch.org
Crunchbase	https://www.crunchbase.com
Dun & Bradstreet	https://www.dnb.com
Euromonitor	https://www.euromonitor.com
Factiva	https://global.factiva.com
GuideStar	https://www.guidestar.org
Infobel	https://www.infobel.com
National US Corp Dir.	https://corporation.directory
Owler	https://corp.owler.com
Plunkett Research	https://www.plunkettresearch.com

Business Information

Corporation Wiki	https://www.corporationwiki.com
CorpWatch	http://www.corpwatch.org
Crunchbase	https://www.crunchbase.com
Dun & Bradstreet	https://www.dnb.com
Euromonitor	https://www.euromonitor.com
Factiva	https://global.factiva.com
GuideStar	https://www.guidestar.org
Infobel	https://www.infobel.com
National US Corp Dir.	https://corporation.directory
Owler	https://corp.owler.com
Plunkett Research	https://www.plunkettresearch.com

OSINT services

Email address OSINT service	URL	Main output
Hunter	`hunter.io`	Validity and availability
Have I Been Pwned	`haveibeenpwned.com`	Appearance in public data breaches
Pipl	`pipl.com`	Personal information about the owner

Username OSINT service	URL	Main output
KnowEm	`knowem.com`	Presence in social networks, domains and online communities
Name Chk	`namechk.com`	
Name Checkr	`namecheckr.com`	
User Search	`usersearch.org`	
NameVine	`namevine.com`	Suggestions of alternative similar usernames
Lullar	`com.lullar.com`	Availability in social networks

OSINT services

Real name OSINT service	URL	Main output
Pipl	pipl.com	Personal information
That's Them	thatsthem.com	Personal details, education, professional career, skills, locations, and relatives.
Spokeo	spokeo.com	
Fast People Search	fastpeoplesearch.com	
Nuwber	nuwber.com	
Cubib	cubib.com	
Peek You	peekyou.com	
Yasni	yasni.com	Social networks profiles
Family Search	familysearch.org	Kinship information, relatives
GENi	geni.com	
Family Tree Now	familytreenow.com	
True People Search	truepeoplesearch.com	

OSINT services

Location OSINT service	URL	Main output
Google Maps	`google.com/maps`	Locations from GPS coordinates
Wikimapia	`wikimapia.org`	
Bing Maps	`bing.com/maps`	
GPS Coordinates	`gps-coordinates.net`	GPS coordinates from location
Historic Aerials	`historicaerials.com`	Historic images of the past
Terra Servers	`terraserver.com`	
Land Viewer	`eos.com`	

IP address OSINT service	URL	Main output
IP Location	`iplocation.net`	Location, domain and ISP
ViewDNS	`viewdns.info`	Technical network-based information
That's Them	`thatsthem.com/reverse-ip-lookup`	Individual or company information
I Know What You Download	`iknowwhatyoudownload.com`	Torrent files

OSINT services

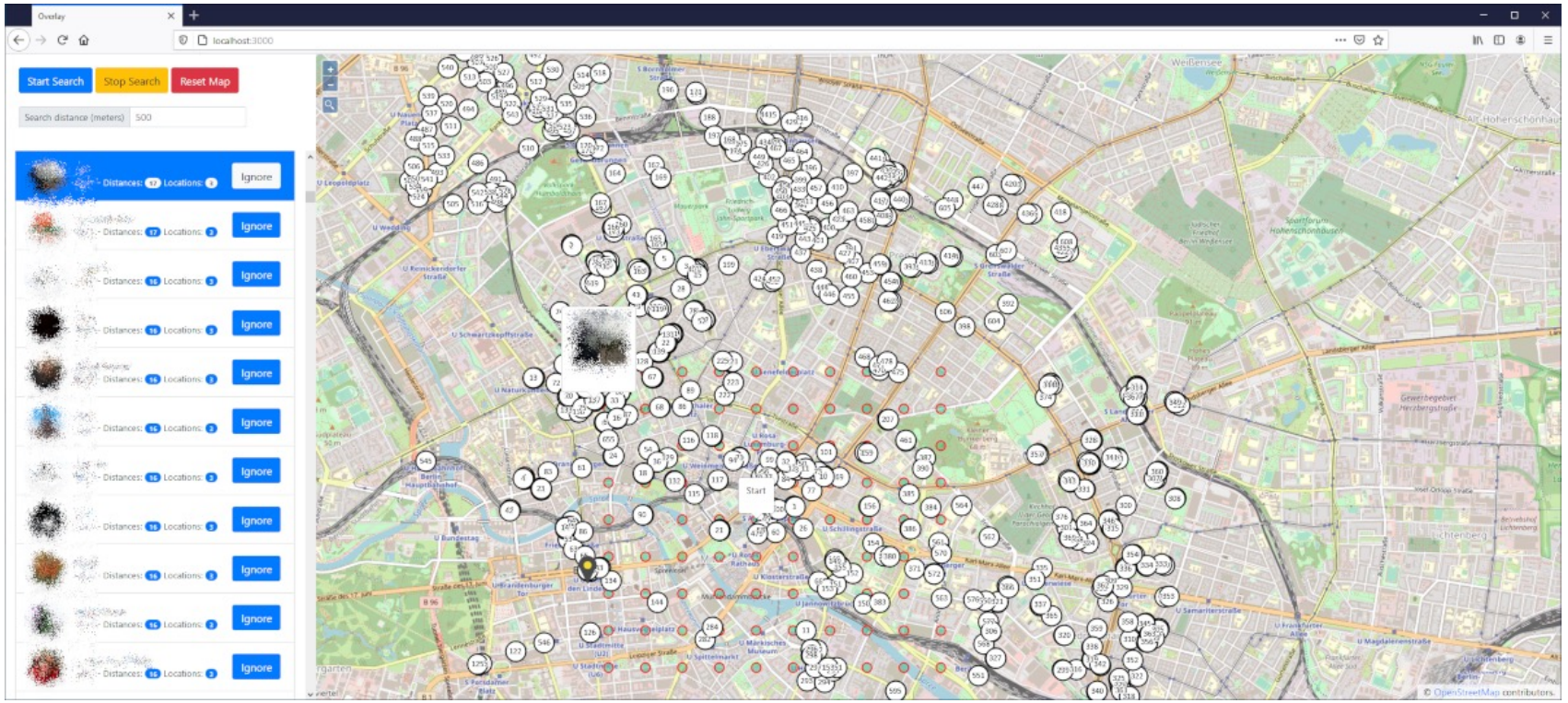
Domain name OSINT service	URL	Main output
DNS Trails	securitytrails.com/dns-trails	DNS records and related domains
Whoisoly	whoisology.com	Personal or company information
Wayback Machine	web.archive.org/web	Backups of websites
Visual Site Mapper	visualsitemapper.com	Map of subdomains
Threat Crowd	threatcrowd.org	
Whois	who.is	Registration info and DNS records
Alexa	alexa.com	Traffic statics
SimilarWeb	similarweb.com	
FindSubdomains	findsubdomains.com	Subdomains

Main features

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

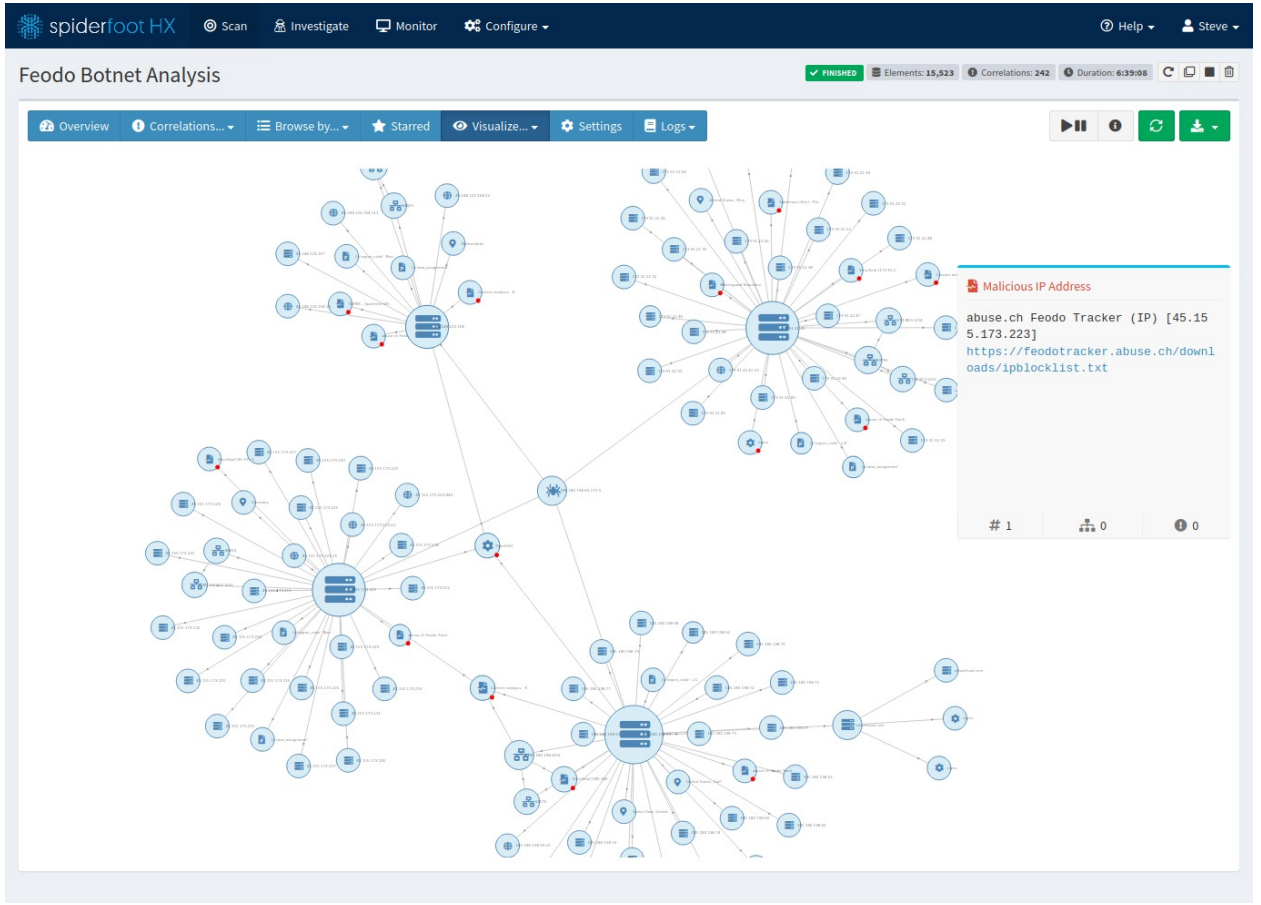
Wifi geolocation data

Telegram nearby



Digital images forensics

OSINT without APIs



DOTT. GIOVANNI D'ALASCIO

Università degli Studi di Roma Tor Vergata

https://www.linkedin.com/in/gdalascio