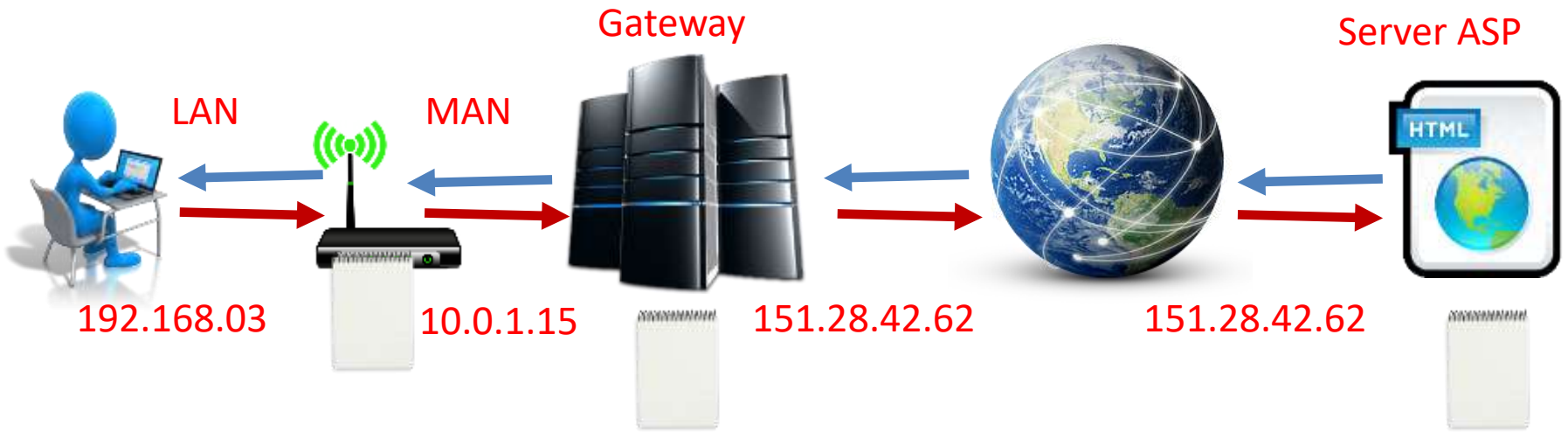
Le indagini telematiche: tracciamento e OSINT

Corrado Federici
corrado.federici@unibo.it

INDAGINI TELEMATICHE: IL TRACCIAMENTO

Con il temine «*tracciamento*» si intende l'insieme delle attività tec-inv:

- realizzate sulla base dell'**analisi dei documenti** (file di *log*) forniti da soggetti terzi (ASP, ISP, Aziende, Enti…) coinvolti nell'evento
- finalizzate all'**identificazione del contratto di connettività** ed eventualmente il rispettivo dispositivo, mediante il quale è stata presumibilmente posta in essere la condotta oggetto d'indagine



INDAGINI TELEMATICHE

La Piramide di privacy

Granularità

Efficacia

INDAGINI TELEMATICHE

Basic Subscriber Information (BSI)

- Sono i dati forniti dall'utente in sede di registrazione (Nome, Cognome, Email), metodi di pagamento (es. carta di credito) ed utenze telefoniche dichiarate e/o verificate, IP di registrazione
- I dati vengono comunicati dal *provider* (*voluntary disclosure*) con decreto di esibizione solo se l'utente ricade nella giurisdizione dell'AG
- Per esempio in Italia non possiamo di norma chiedere dati di registrazione associati ad un profilo venezuelano. Tuttavia tale regola non trova una generale applicazione

Traffic Data Log

- Riportano alcune specifiche operazioni, senza però fornirne i dettagli, come ad esempio il *login* e/o *logout*, oppure tentativo di *reset password* ad un dato *account*.
- Tali elementi non hanno la stessa granularità informativa che caratterizza un file di log di un *web server*, dove vengono specificate ad esempio la pagina di provenienza, l'*useragent*, l'esito del comando HTTP

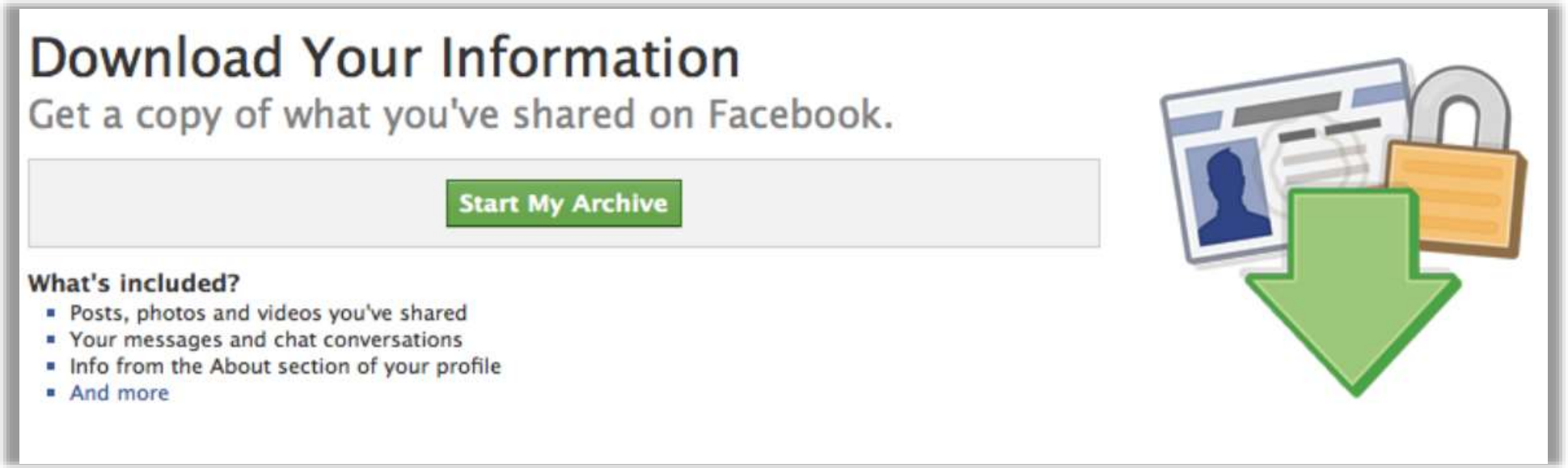
Activity Log

Sono dei log dettagliati contenenti dati di natura applicativa oltre a quelli di tracciamento

ip	agent	uri	time
ip1664.com	msnbot/1.0 (+http://search.msn.com/msnbot.htm)	/robots.txt	18868620
ip1664.com	msnbot/1.0 (+http://search.msn.com/msnbot.htm)	/gpspubs/sigkdd-kdd99-panel.html	18868620
ip1115.unr	Mozilla/4.0 (compatible; MSIE 5.5; Windows 98; SAFEXPLORER TL)	/news/99/n23/i12.html	18868621
ip2283.unr	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/dmcourse/data_mining_course/assignmer	18868621
ip2283.unr	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/dmcourse/dm.css	18868621
ip1389.net	Mozilla/4.0 (compatible; MSIE 6.0; X11; Linux i686; en) Opera 8.5	/gpspubs/kdd99-est-ben-lift/sld021.htm	18868622
ip1389.net	Mozilla/4.0 (compatible; MSIE 6.0; X11; Linux i686; en) Opera 8.5	/gpspubs/kdd99-est-ben-lift/img021.gif	18868622
ip1389.net	Mozilla/4.0 (compatible; MSIE 6.0; X11; Linux i686; en) Opera 8.5	/favicon.ico	18868622
ip1946.com	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ys	/news/2001/n10/15i.html	18868622
ip992.unr	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT; MS Search 4.0 Robot)	/aps/bt4-a.sol_crm.re.html	18868622
ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/	18868624
ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/kdr.css	18868624
ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/images/KDnuggets_logo.gif	18868624
ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/images/kdnuggets.co.jp.gif	18868624
ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/aps/aw1.js	18868624
ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/images/newy.gif	18868624
ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/aps/bt4-a.ind.gif	18868624
ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/aps/f-spss-h2.ind.gif	18868624
ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/aps/t-salf-sd12.c12.gif	18868624

Content Data

Sono i dati generati e riconducibili all'utente i quali vengono assunti al dibattimento per il tramite la cooperazione internazionale (art. 727 c.p.p.), o volontariamente da parte del *provider* (art. 234-bis c.p.p.), ovvero tramite perquisizione informatica (artt. 247 co. 1-bis e 352 co. 1-bis c.p.p.).

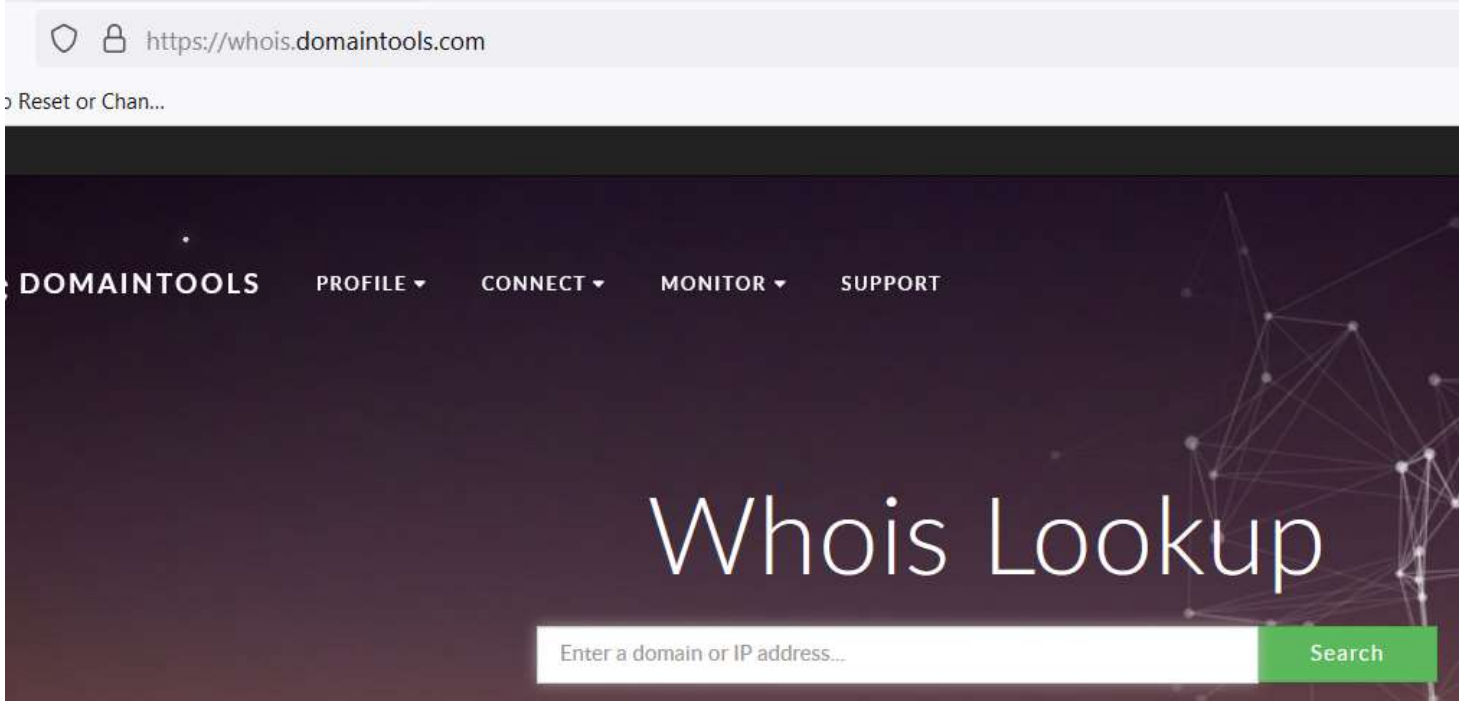


INDAGINI TELEMATICHE

Whois

Il protocollo Whois consente:

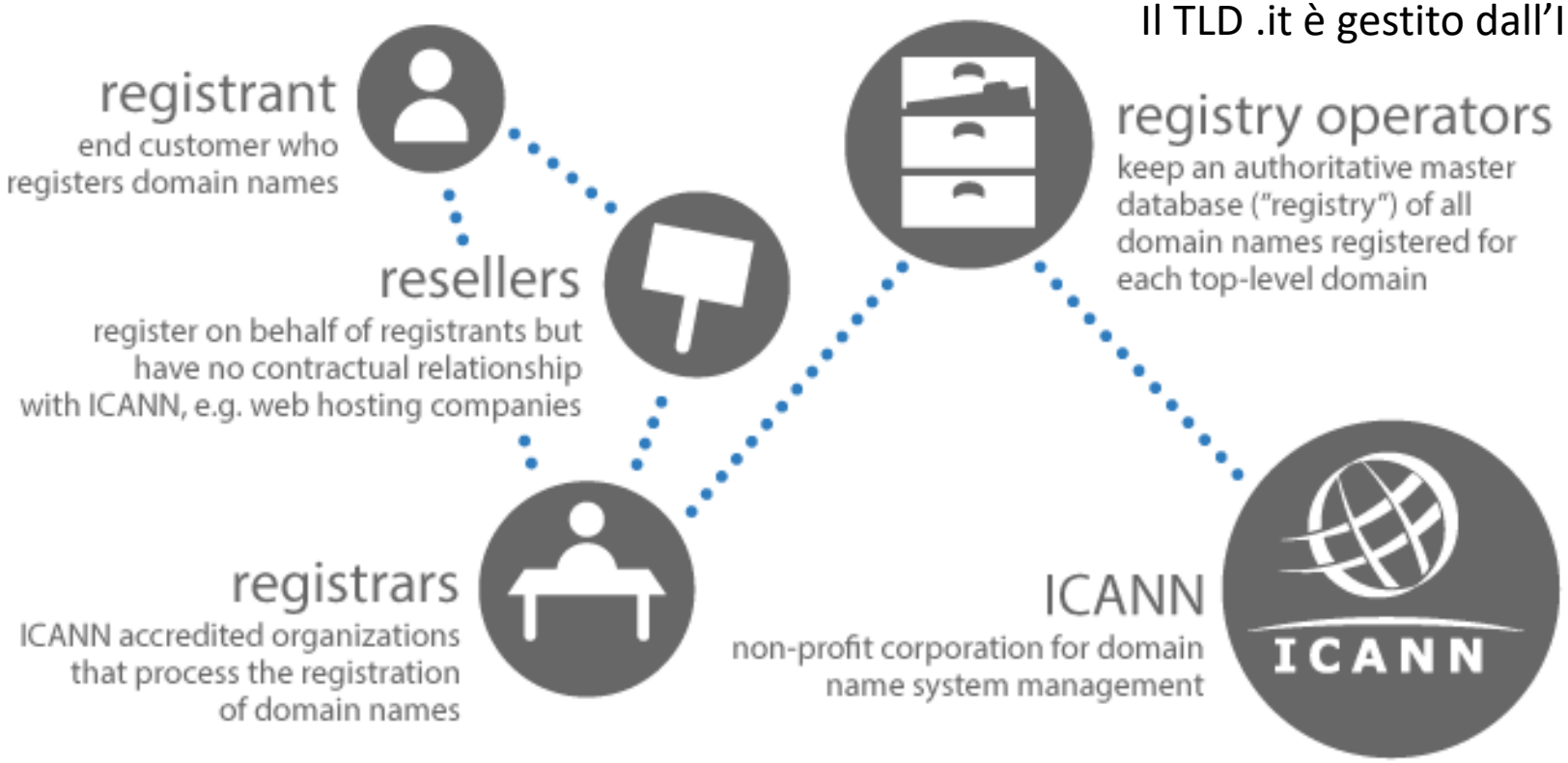
- di stabilire a quale *Service Provider* appartenga un determinato indirizzo IP (es. 78.5.138.198)
- I dati di registrazione di un dominio (whois mydomain.com)
- ottenere informazioni sulle persone fisiche o giuridiche che lo gestiscono
- stato di attivazione e rispettivo periodo




```
ugo@ugo-VirtualBox:~$ whois microsoft.com
   Domain Name: MICROSOFT.COM
   Registry Domain ID: 2724960_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2021-03-12T23:25:32Z
   Creation Date: 1991-05-02T04:00:00Z
   Registry Expiry Date: 2022-05-03T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints(
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://
```

INDAGINI TELEMATICHE

Il TLD .it è gestito dall'IIT del CNR di Pisa

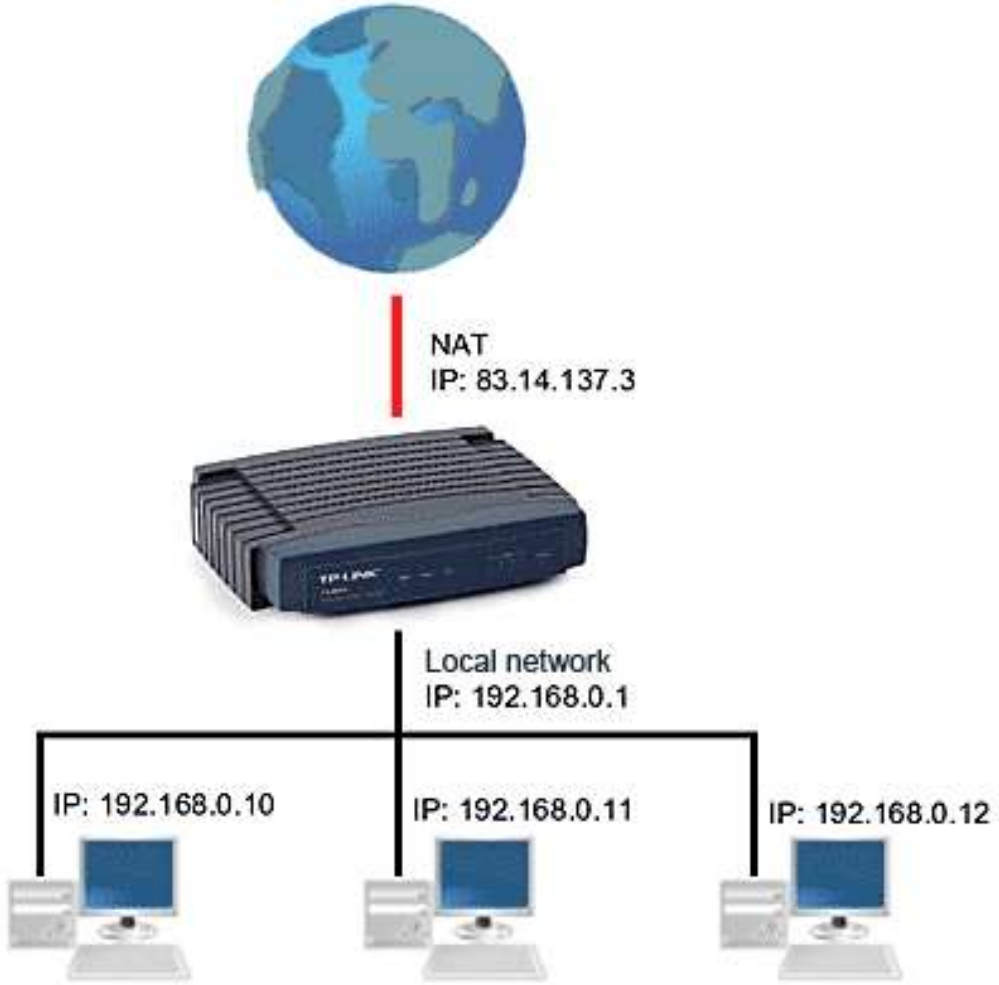


domain registry process

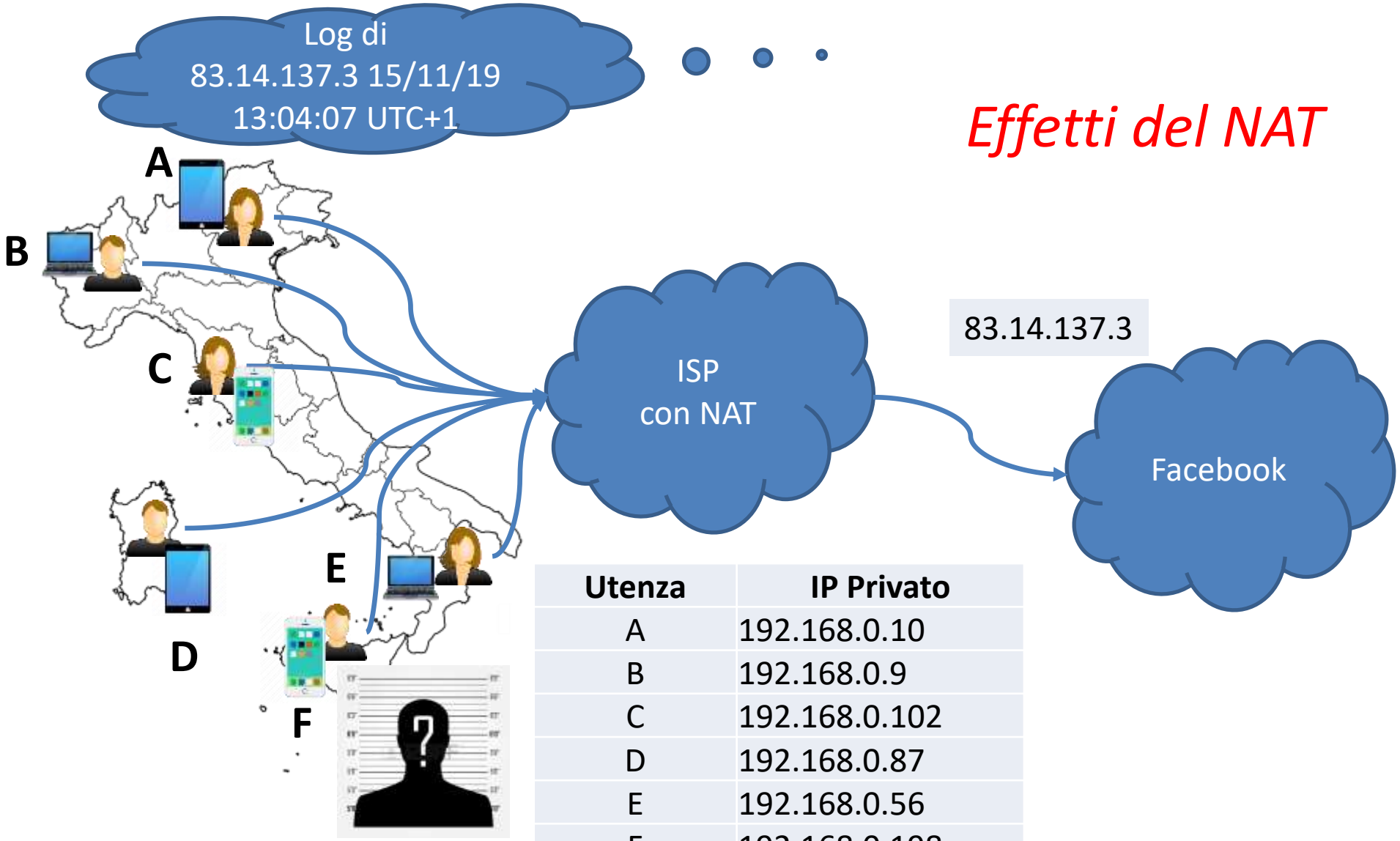
Internet Corporation for Assigned Names and Numbers

Network Address Translaton

- Il NAT consente all'ISP di sopperire alla scarsità di indirizzi IP pubblici (v.4) da attribuire ai propri clienti in ogni istante
- In alcune circostanze, tale soluzione si è rilevata una vera a propria tecnica di *antiforensics*, in quanto non consente l'identificazione univoca dell'utente o abbonato (art. 5 D.Lgs. 109/2008), costringendo così l'investigatore a lavorare su una pletora di utenze «*potenzialmente indiziarie*».
- Tale rischio può essere mitigato se si dispone di numerose registrazioni dall'IP di interesse oppure quando si abbiano informazioni anche sulla porta (sorgente) ad esso associata



INDAGINI TELEMATICHE



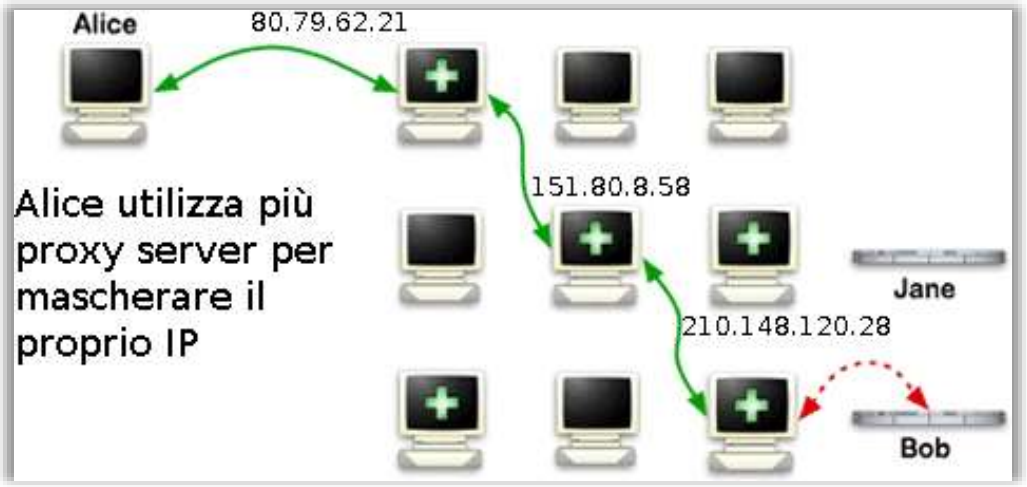
Effetti del NAT

Utenza	IP Privato
A	192.168.0.10
B	192.168.0.9
C	192.168.0.102
D	192.168.0.87
E	192.168.0.56
F	192.168.0.198

Occultamento

Alle difficoltà rappresentate dal NAT si aggiungono i meccanismi di occultamento sia a livello di rete che applicativo:

- Wifi hot spots aperti
- Proxy
- Tor Browser
- Virtual Private Network

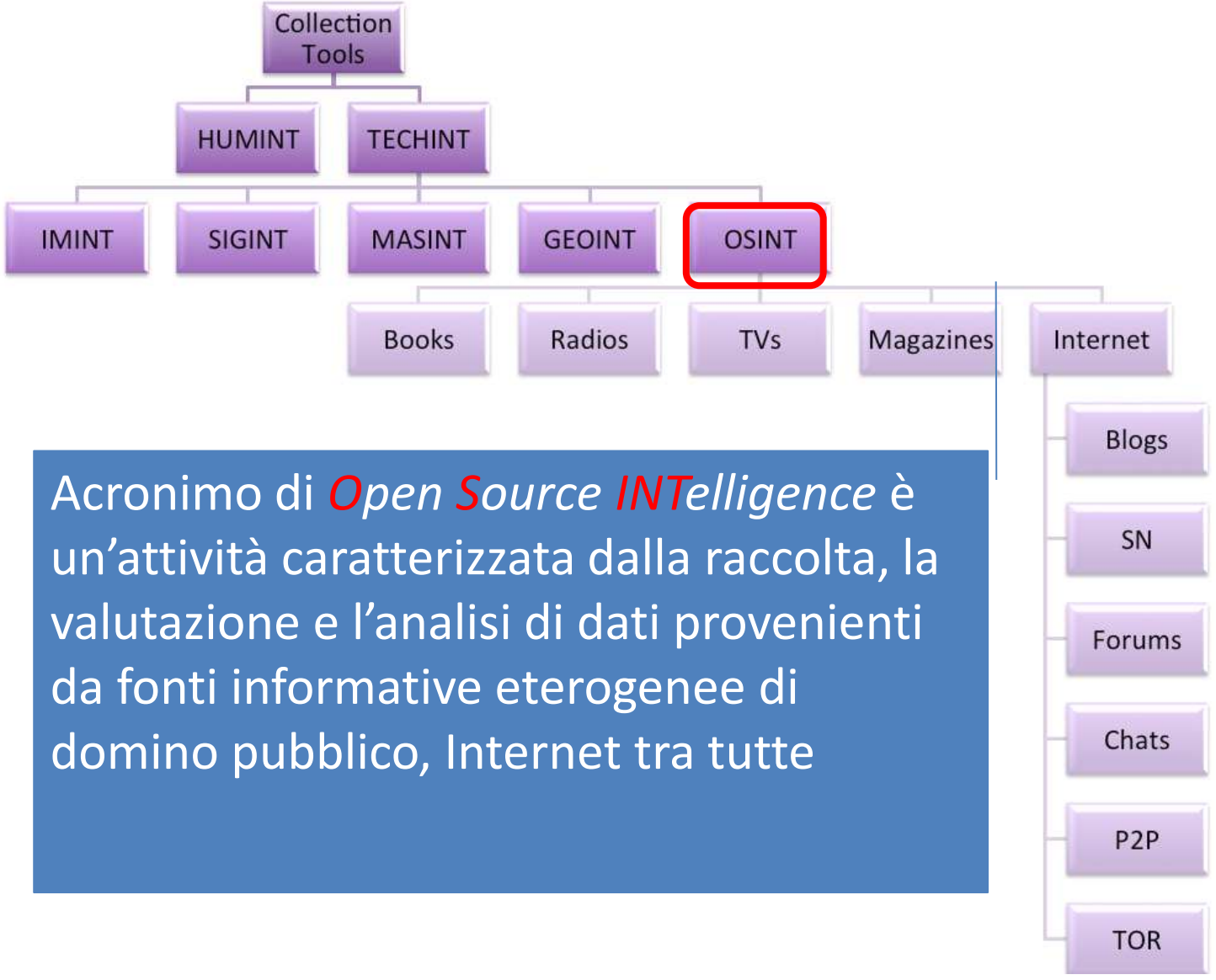


NordVPN

ProtonVPN

SwissVPN

OSINT



Acronimo di *Open Source INTelligence* è un'attività caratterizzata dalla raccolta, la valutazione e l'analisi di dati provenienti da fonti informative eterogenee di domino pubblico, Internet tra tutte

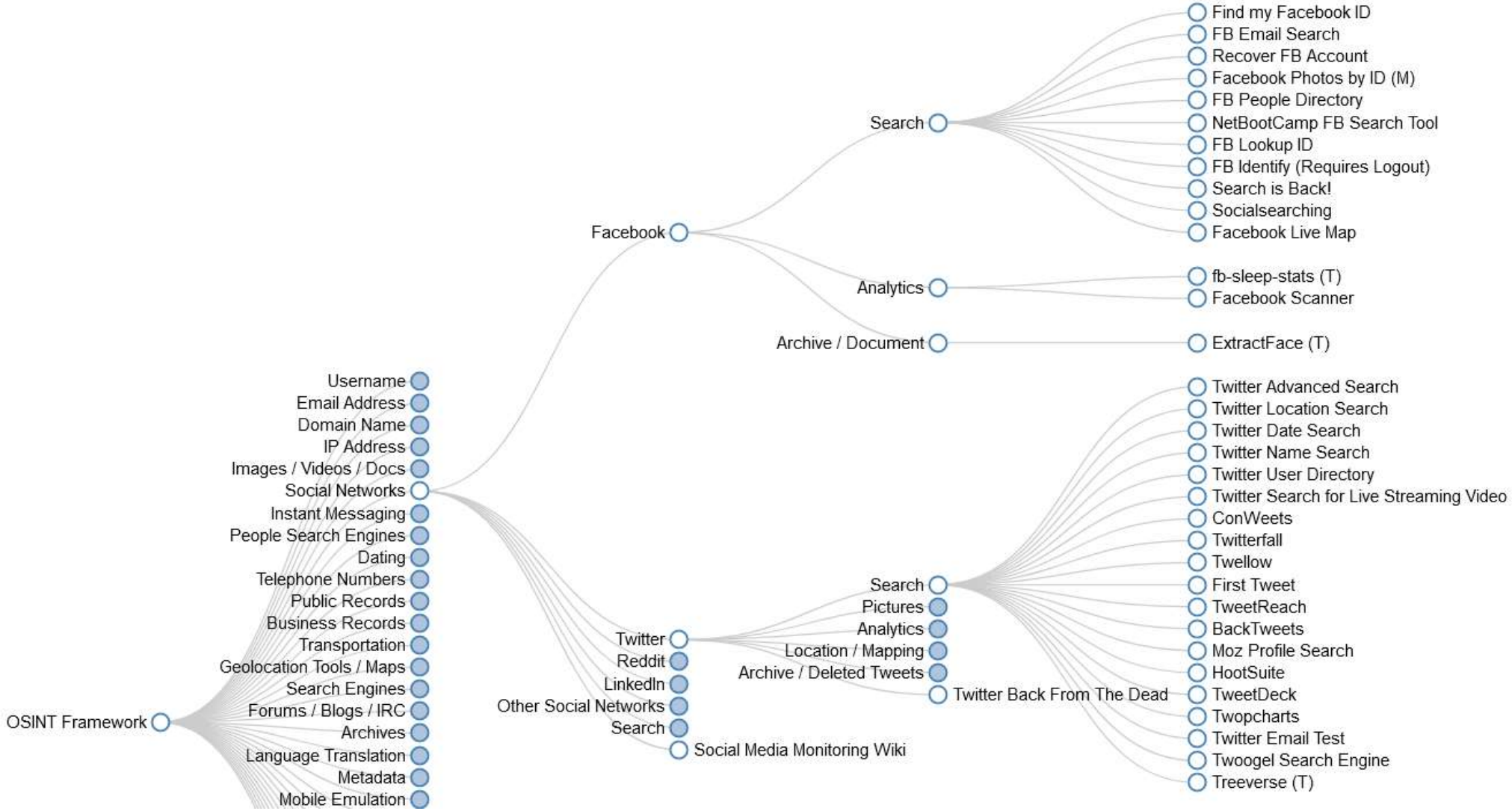
OSINT

Esiste una procedura standard per l'OSINT?

- Generalmente "**NO**"
- OSINT è un'attività complessa e soggetta a molte variabili
- Tuttavia esistono schemi procedurali definiti o strumenti che automatizzano la ricerca o portali che raggruppano i siti che offrono strumenti di OSINT

OSINT FRAMEWORK

https://osintframework.com/



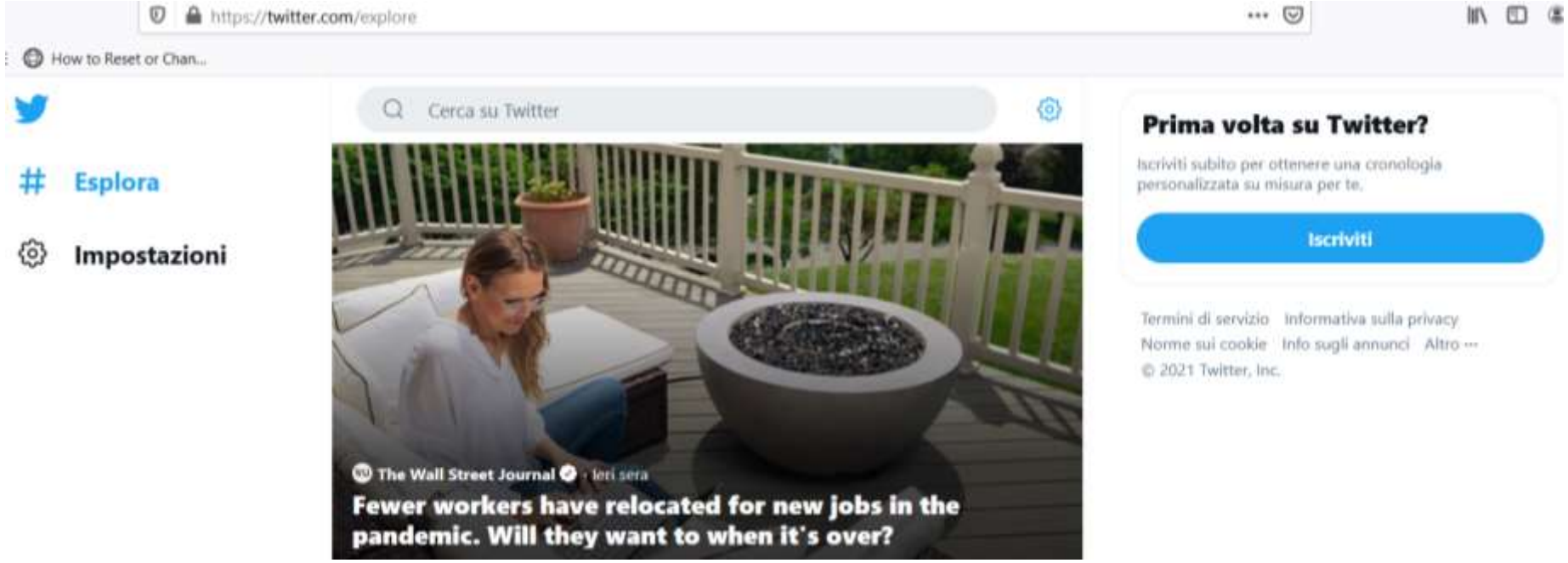
I Social Media

- Con il termine *Social Media* si intende l'insieme delle tecnologie utilizzate per creare una comunità di utenti in grado di condividere contenuti testuali e multimediali
- I dati che una volta erano patrimonio di una ristretta cerchia di sodali ora possono essere facilmente condivisi con un più ampio numero di persone o anche essere resi pubblici
- I *Social Network* possono pertanto rappresentare una miniera d'oro per i cercatori di informazioni anche perché di norma le persone condividono più di quanto si rendano conto e spesso si scordano di averlo fatto
- I grandi social media provider utilizzando molte tecniche (anche di IA) per rilevare se le ricerche sono fatte da una persona o da un bot

TWITTER

- Il modulo di ricerca "*base*" di Twitter è utile per:
  - *News generiche*
  - *Gossip*
  - *Trend* (argomenti più seguiti) identificabili tramite gli *hashtag,*
- Non richiede il logon come Facebook, ma può essere poco preciso

https://twitter.com/explore



TWITTER

Ricerca di base con operatori

Query	Trova Tweet...
Bmw 320	che contiene sia “*Bmw*" che “*320*". Operatore predefinito
“aria fritta"	che contiene la frase esatta “aria fritta"
cheese OR Brexit	che contiene “cheese" oppure “*Brexit*" (o entrambi).
auto –diesel	che contiene "*auto*" ma non "*diesel*"
#occupygezi	che contiene l'*hashtag* "*occupygezi*"
from:corrado	inviato da “*corrado*"
@Agenzia_Ansa	che contiene un riferimento all'utente "*Agenzia_Ansa*"

TWITTER

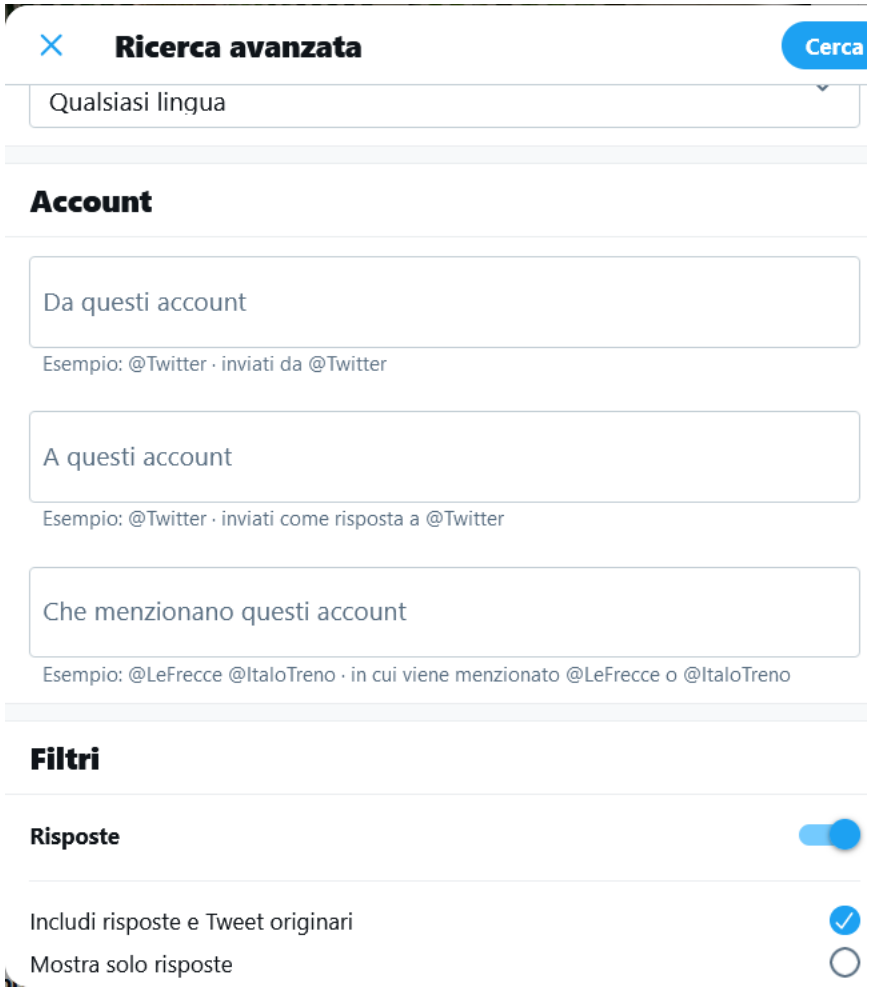
Ricerca di base con operatori

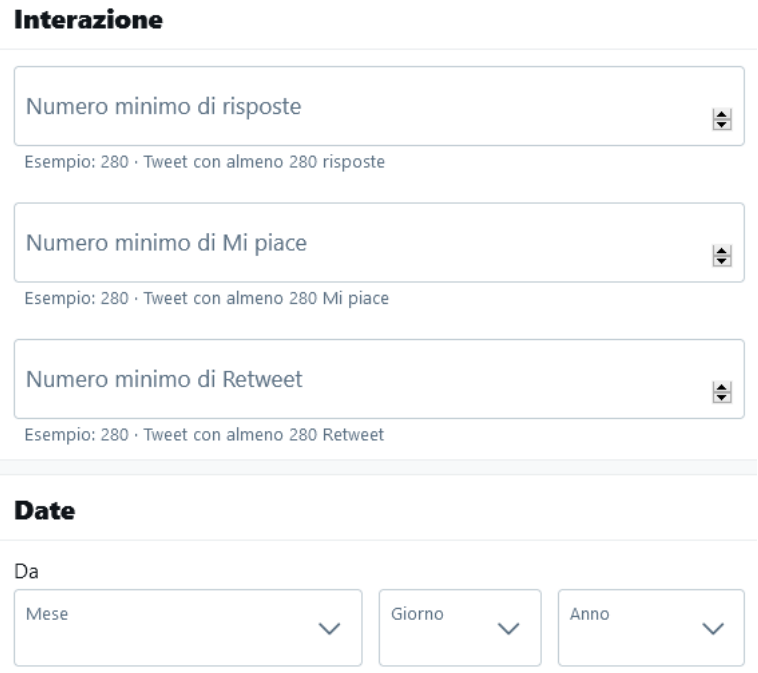
Query	Trova Tweet...
"flash mob"near:“Bologna"	che contiene la frase esatta "*flash mob*" ed è stato inviato vicino a “*Bologna*".
near:Bologna within:15km	inviato a meno di 15 chilometri da “*Bologna*".
cioccolata since:2015-07-25	che contiene “*cioccolata*" e inviato a partire dal "*2015-07-25*" (anno-mese-giorno).
bicicletta until:2010-12-27	che contiene "*mafia*" ed è stato inviato entro il "*2015-07-25*".
film -romantico :)	che contiene "*film*", ma non "*romantico*" e con una connotazione positiva.
volo :(	che contiene "*volo*" e con una connotazione negativa.
traffico ?	che contiene "*traffico*" e pone una domanda.

TWITTER

Ricerca avanzata

https://twitter.com/search-advanced





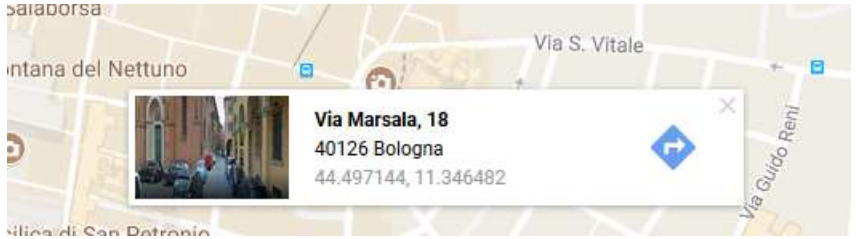
TWITTER

Ricerca spaziale

- Può tornare utile sapere quali utenti hanno pubblicato un Tweet in una data zona ove è avvenuto un evento di interesse
- Twitter consente una ricerca all'interno di aree centrate attorno ad un punto definito dalle coordinate GPS

TWITTER

Ricerca spaziale

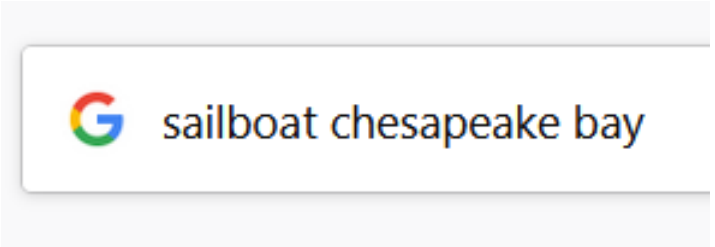


https://twitter.com/search?q=geocode:40.712776,-74.005974,10km

GOOGLE

Operator Examples	
Operator Example	**Finds Pages Containing**
sailboat chesapeake bay	the words **sailboat**, **Chesapeake** and **Bay**
*sloop **OR** yawl*	either the word **sloop** or the word **yawl**
"To each his own"	the exact phrase **to each his own**
virus -computer	the word **virus** but NOT the word **computer**
Star Wars Episode +III	This movie title, including the roman numeral III
~boat loan	loan info for both the word **boat** and its synonyms: **canoe**, **ferry**, etc.
define:sarcastic	definitions of the word **sarcastic** from the Web
mac * x	the words **Mac** and **X** separated by exactly one word
I'm Feeling Lucky *(Google link)*	Takes you directly to first web page returned for your query

Ricerca di base

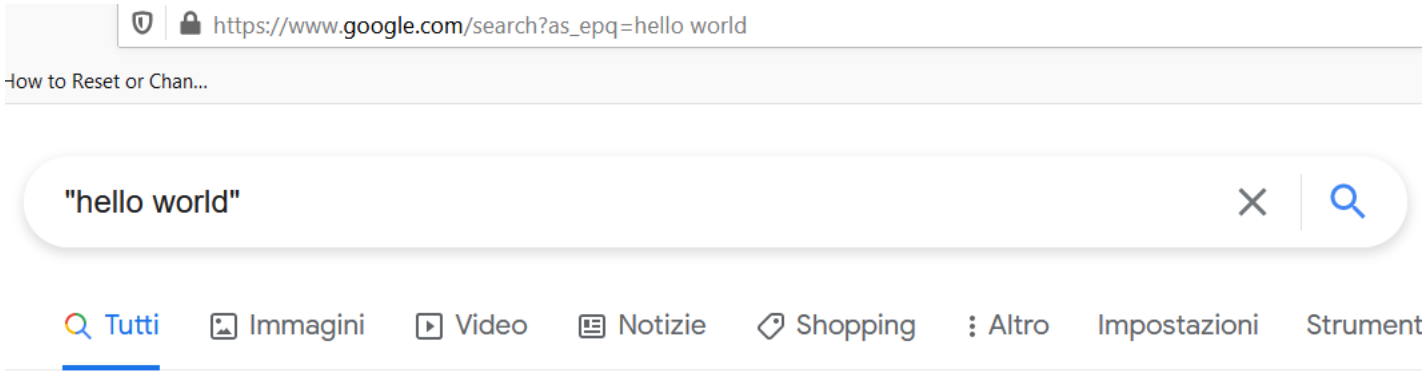


https://www.sans.org/security-resources/GoogleCheatSheet.pdf

GOOGLE

Parametri della query

Search Parameters		
Search Parameters	**Value**	**Description of Use in Google Search URLs**
q	the search term	The search term
filter	0 or 1	If **filter** is set to 0, show potentially duplicate results.
as_epq	a search phrase	The value submitted is as an exact phrase. No need to surround with quotes.
as_ft	i = include e = exclude	The file type indicated by **as_filetype** is included or excluded in the search.
as_filetype	a file extension	The file type is included or excluded in the search indicated by **as_ft**.
as_occt	any = anywhere title = page title body = text of page url = in the page URL links = in links to the page	Find the search term in the specified location.
as_dt	i = include e = exclude	The site or domain indicated by **as_sitesearch** is included or excluded in the search.
as_sitesearch	site or domain	The file type is included or excluded in the search indicated by **as_dt** .
as_qdr	m3 = three months m6 = six months y = past year	Locate pages updated with in the specified time frame.



https://www.sans.org/security-resources/GoogleCheatSheet.pdf

GOOGLE

Ricerca avanzata

Advanced Operators		
Advanced Operators	**Meaning**	**What To Type Into Search Box** ***(& Description of Results)***
site:	Search only one website	**conference site:www.sans.org** *(Search SANS site for conference info)*
[#]...[#] or numrange:	Search within a range of numbers	**plasma television $1000...1500** *(Search for plasma televisions between $1000 and $1500)*
date:	Search only a range of months	**hockey date: 3** *(Search for hockey references within past 3 months; 6 and 12-month date-restrict options also available)*
safesearch:	Exclude adult-content	**safesearch: sex education** *(Search for sex education material without returning adult sites)*
link:	linked pages	**link:www.sans.org** *(Find pages that link to the SANS website)*
info:	Info about a page	**info:www.sans.org** *(Find information about the SANS website)*
related:	Related pages	**related:www.stanford.edu** *(Find websites related to the Stanford website)*
intitle:	Searches for strings in the title of the page	**intitle:conference** *(Find pages with "conference" in the page title)*
allintitle:	Searches for all strings within the page title	**allintitle:conference SANS** *(Find pages with "conference" and "SANS" in the page title. Doesn't combine well with other operators)*
inurl:	Searches for strings in the URL	**inurl:conference** *(Find pages with the string "conference" in the URL)*
allinurl:	Searches for all strings within the URL	**allinurl:conference SANS** *(Find pages with "conference" and "SANS" in the URL. Doesn't combine well with other operators)*

GOOGLE

Ricerca avanzata

Advanced Operators		
Advanced Operators	**Meaning**	**What To Type Into Search Box** ***(& Description of Results)***
filetype: or **ext:**	Searches for files with that file extension	**filetype:ppt** *(Find files with the "ppt" file extension. ".ppt" are MS PowerPoint files.)*
cache:	Display the Google cache of the page	**cache:www.sans.org** *(Show the cached version of the page without performing the search)*
phonebook: or **rphonebook:** or **bphonebook**	Display all, residential, business phone listings	**phonebook:Rick Smith MD** *(Find all phone book listing for Rick Smith in Maryland. Cannot combine with other searches)*
author:	Searches for the author of a newsgroup post	**author:Rick** *(Find all newsgroup postings with "Rick" in the author name or email address. Must be used with a Google Group search)*
insubject:	Search only in the subject of a newsgroup post	**insubject:Mac OS X** *(Find all newsgroup postings with "Mac OS X" in the subject of the post. Must be used with a Google Group search)*
define:	Various definitions of the word or phrase	**define:sarcastic** *(Get the definition of the word sarcastic)*
stock:	Get information on a stock abbreviation	**stock:AAPL** *(Get the stock information for Apple Computer, Inc.)*

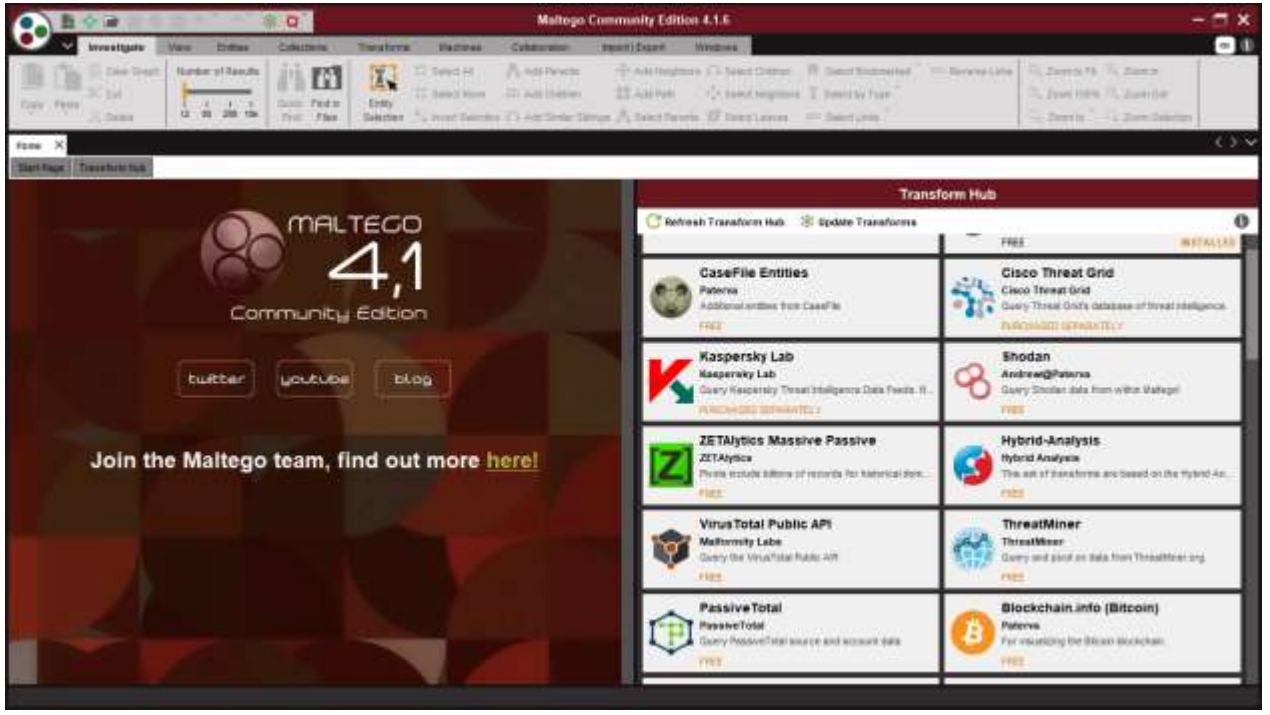
https://www.sans.org/security-resources/GoogleCheatSheet.pdf

STRUMENTI PER L'OSINT: MALTEGO

- Maltego è un applicativo di node graphics disponibile in 3 versioni client:

CE CL XL

- E' basato sul concetto di "Trasformata", moduli di codice scritti in qualunque linguaggio di programmazione che, a partire da un parametro di ricerca iniziale, acquisiscono i dati da un InfoProvider e li passano a Maltego per la visualizzazione
- Le trasformate si possono installare da un marketplace oppure localmente



STRUMENTI PER L'OSINT: MALTEGO

Le trasformate del Marketplace

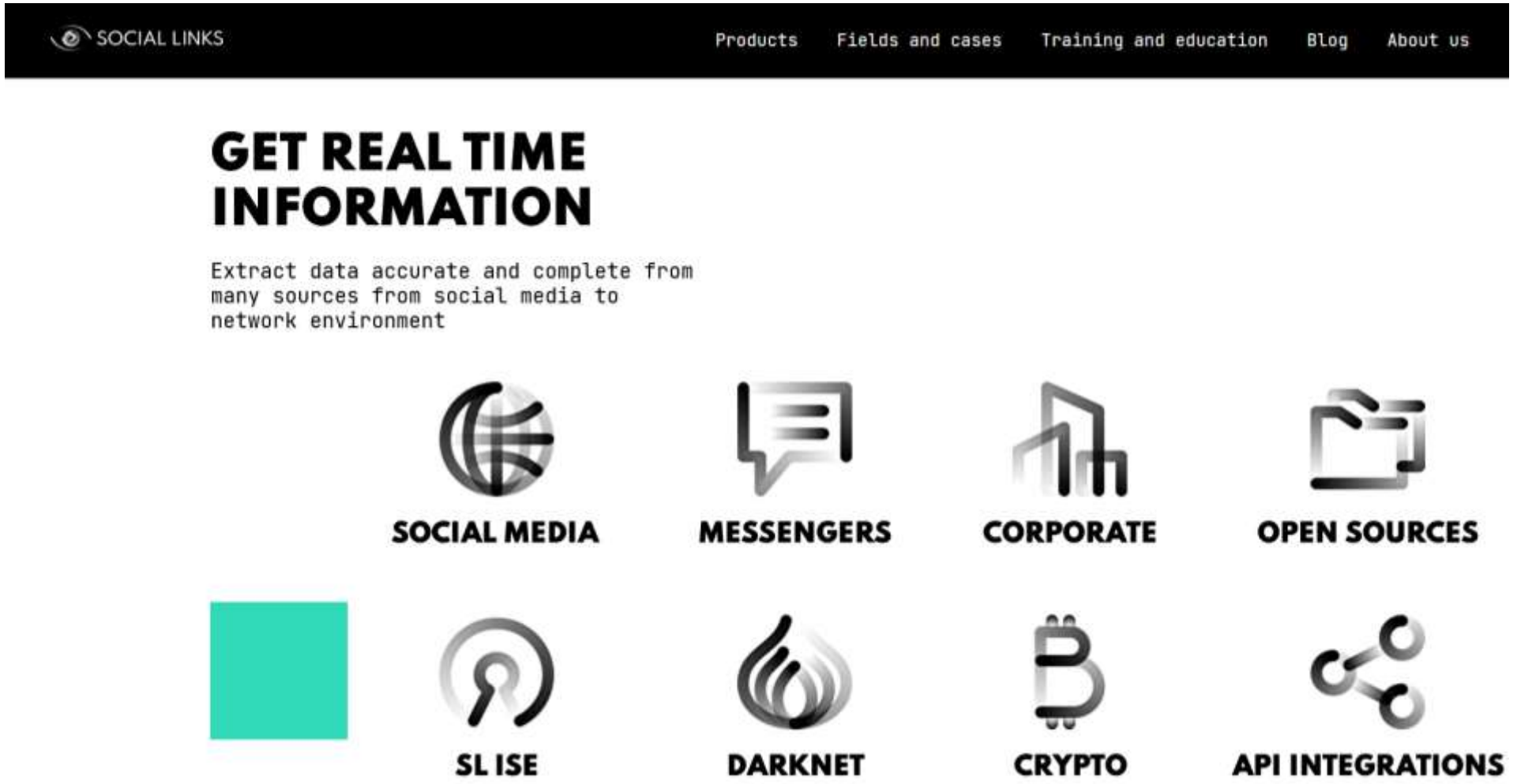
Pro

- Immediatamente disponibili
- Aggiornate durante il periodo di licenza dagli Info providers
- Ampia copertura di ambiti

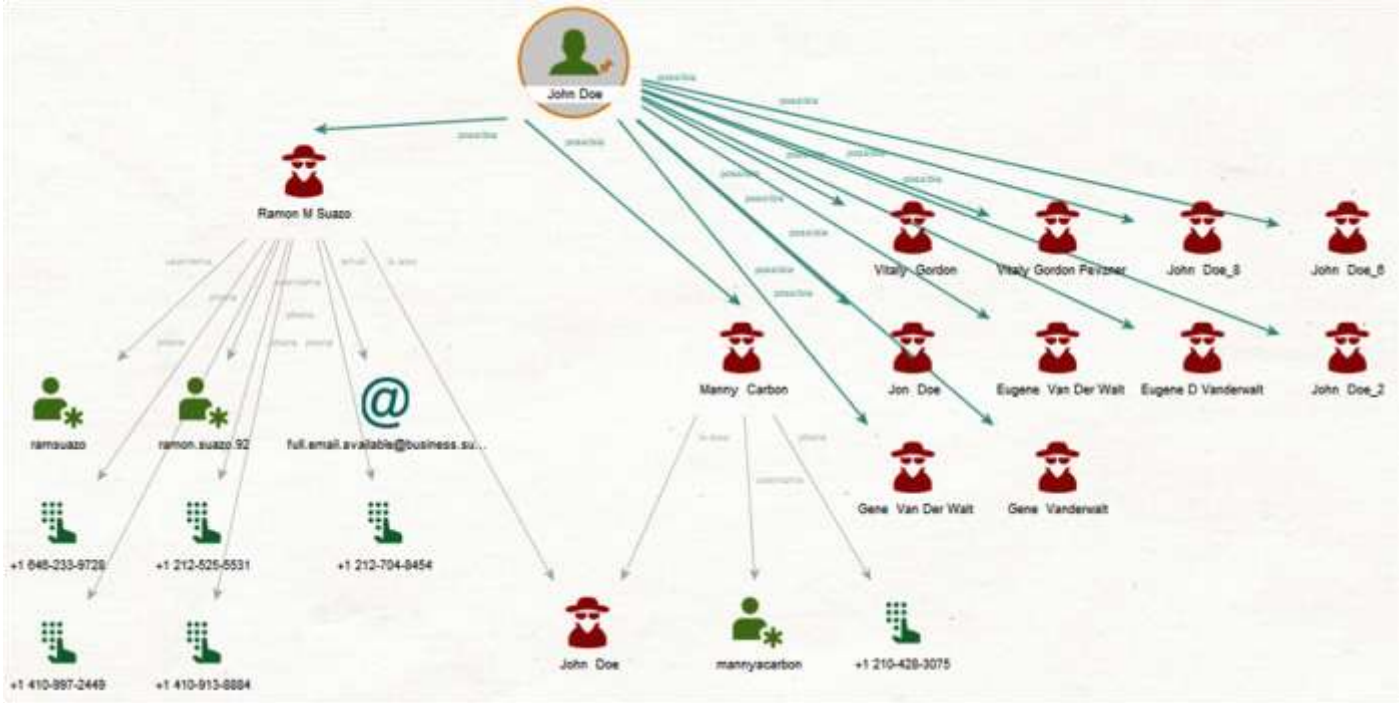
Contro

- Discovery delle informazioni
- Perdita di controllo
- Costi

ESEMPIO DI INFO PROVIDER: SOCIAL LINKS



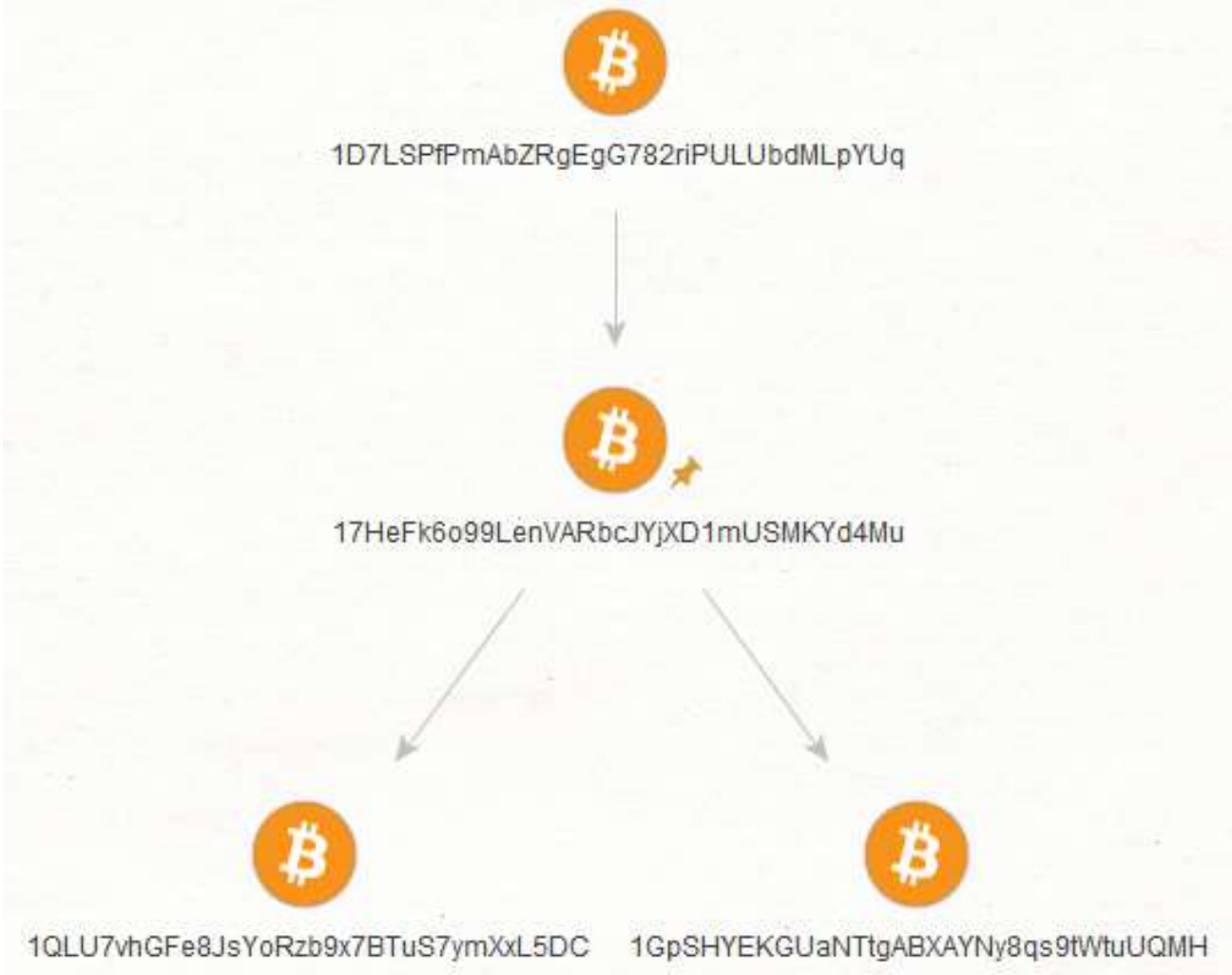
STRUMENTI PER L'OSINT: MALTEGO



Maltego è ormai lo strumento di riferimento per la visualizzazione grafica di relazioni tra entità:

- **Persone o Gruppi di persone**
- **Enti, aziende, associazioni, organizzazioni**
- **Siti Web, Domini DNS, email, indirizzi IP, certificati digitali**
- **Documenti**
- **Criptovalute**
- **Utenze telefoniche**

MALTEGO: TRANSAZIONI BITCOIN



STRUMENTI PER L'OSINT: MALTEGO

Entità di partenza in un'indagine

- ✓ indirizzo posta elettronica (*email*)
- ✓ nome utente (*username*)
- ✓ nome reale (*real name*)
- ✓ utenza telefonica (*telephone number*)
- ✓ nome di dominio (*domain name*)
- ✓ Indirizzo ip di un host
- ✓ Certificato digitale di un host
- ✓ Indirizzo Bitcoin
- ✓ Un oggetto pubblico nel Cloud

1BzroGk1d4A3HyZ4wCBYhkt8ZcqhmhyJu8