

Social **N**etwork **A**nalysis (**SNA**) e **O**pen **S**ource **INT**elligence (**OSINT**) nelle attività d'indagine

RELATORI

Dott. Alessandro MASSARO

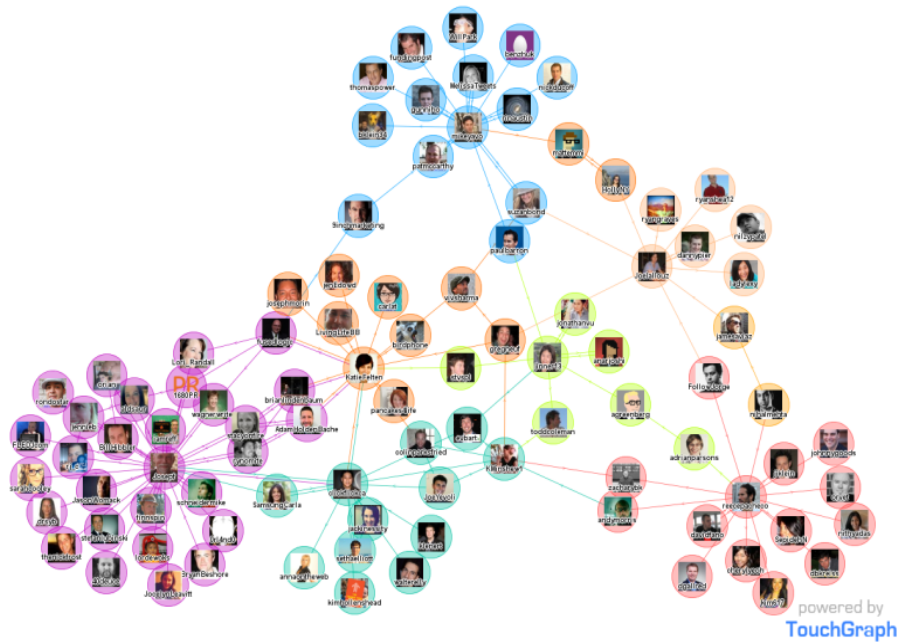
Dott. Ing. Fabio MELE

Come possono essere d'aiuto la SNA e l'OSINT nelle attività di ricerca delle informazioni?

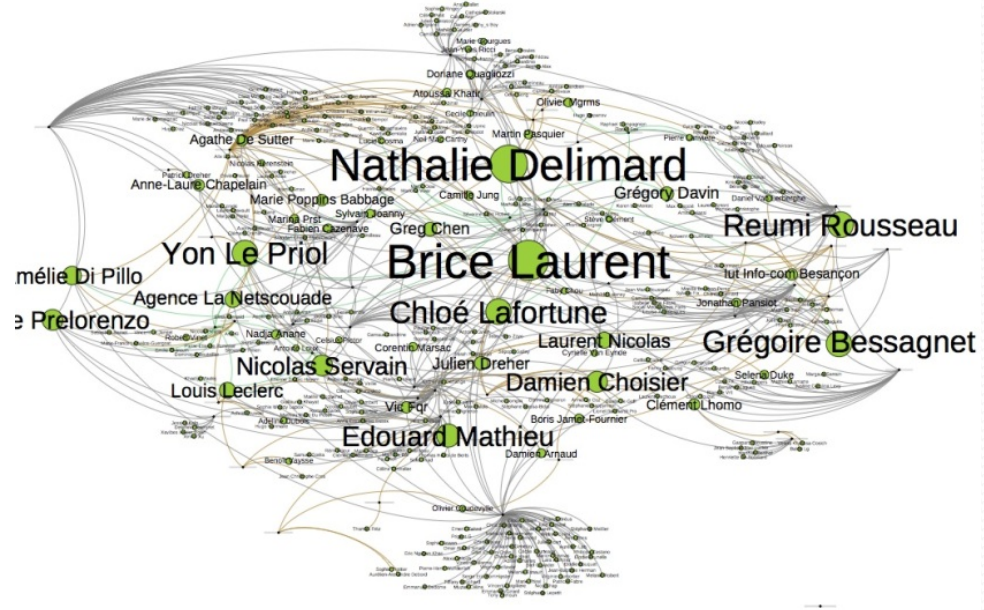
- La Social Network Analysis (analisi delle reti sociali), visualizza i collegamenti (ARCHI) tra i vari soggetti (NODI) sfruttando la “Teoria delle Reti”. L'insieme degli archi e dei nodi prende il nome di GRAFI.
- L'applicazione della SNA viene utilizzata in diversi campi che spaziano dalla sociologia, alla psicologia, al marketing, all'economia, alla genetica fino ad arrivare al giornalismo investigativo ed alle investigazioni.

Esempi di grafici

GRAFO SOCIAL NETWORK



GRAFO SOCIAL MEDIA INFLUENCER



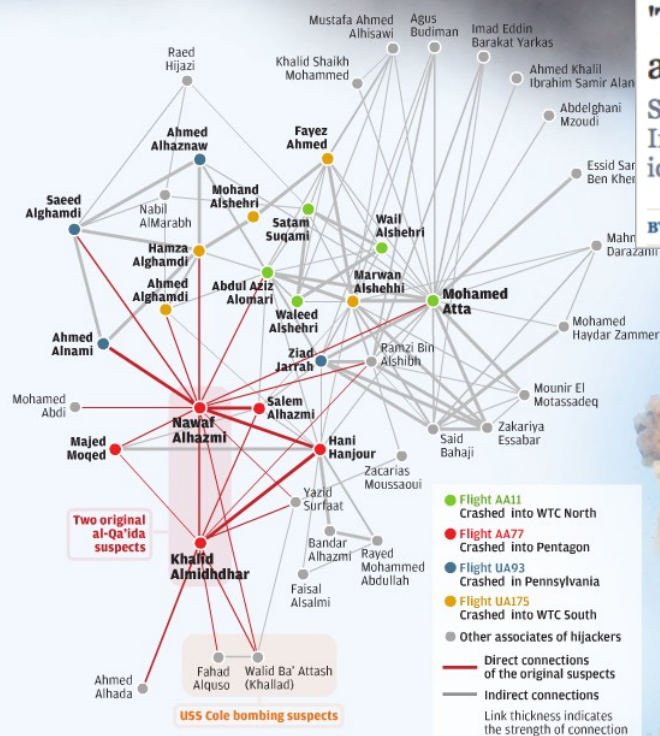
Come possono essere d'aiuto la SNA e L'OSINT nelle attività di ricerca delle informazioni?

How two names and a sheaf of newspaper cuttings revealed the 9/11 team

This social network of the 19 hijackers behind the 9/11 attacks in the United States, and their associates, was drawn up at the end of 2001. Valdis Krebs, a commercial consultant in network analysis, started with newspaper reports of the two original terrorist suspects, Nawaf Alhazmi and Khalid Almihdhar. He then plotted the position of the other hijackers and associates. His analysis highlighted the central role played by Mohamed Atta. It also shows the close associations between the "Hamburg cell" that Atta set up, as well as the close links with the two original suspects - critical information that may have helped to avert an attack had it been known.



Emergency services attend the scene after Flight AA77 crashes into the Pentagon



'Terrorist Facebook' – the new weapon against al-Qa'ida

Social networking is not just for the MySpace generation. Intelligence agencies are adopting a controversial new technique to identify terrorist masterminds

BY STEVE CONNOR, SCIENCE EDITOR WEDNESDAY 19 AUGUST 2009



The second plane, Flight UA175, crashes into the South Tower of the World Trade Center

Come possono essere d'aiuto la SNA e L'OSINT nelle attività di ricerca delle informazioni?

Miliziani dell'Is fanno un selfie e in 24 ore arrivano 3 missili

Una base jihadista è stata bombardata dall'Us Air Force dopo esser stata localizzata con una fotografia postata su Twitter. Lo rivelano gli stessi vertici militari, spiegando anche come l'intelligence sta usando i social media

di ALESSANDRA BORELLA

http://www.repubblica.it/esteri/2015/06/05/news/militante_dell_is_si_fa_un_selfie_e_24_ore_arrivano_3_missili-116096314/

Lo leggo dopo 05 giugno 2015

5,8 mila

Consiglia Condividi

Tweet

21

G+

0

LinkedIn

0

Pinterest



Era uno dei quartieri generali dello Stato Islamico, distrutto da un raid americano in meno di un giorno dopo essere stato individuato grazie a un selfie su Twitter. L'Is colpisce con i social media e con i social media viene colpito.

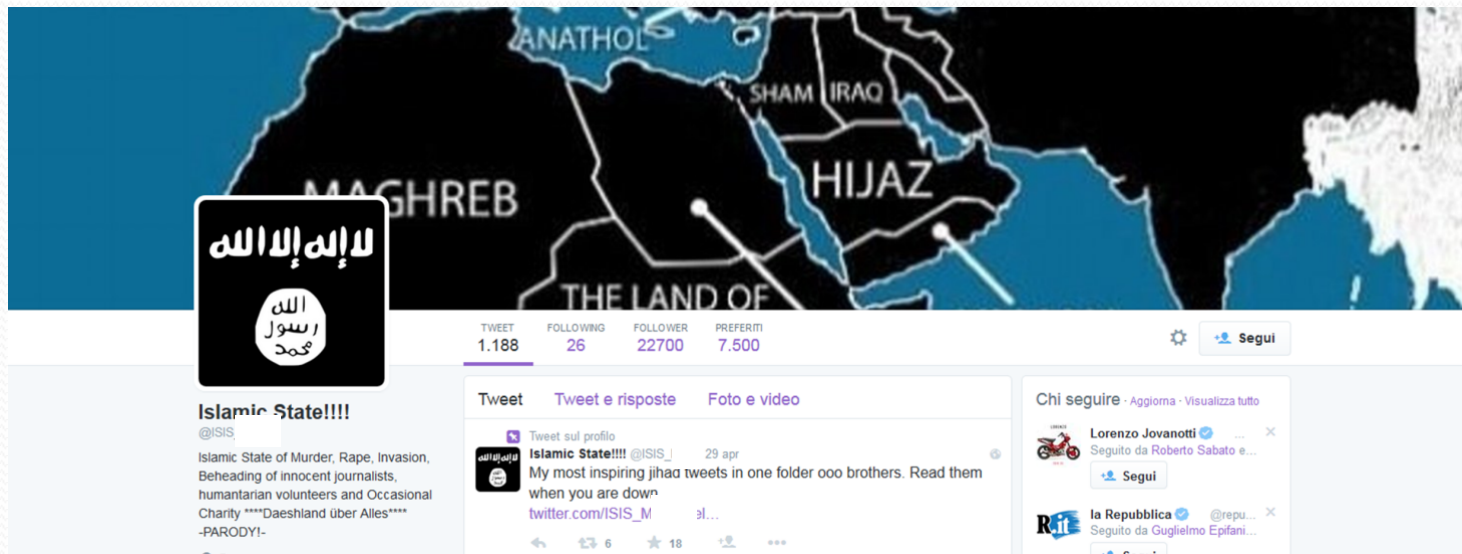
I servizi di intelligence dell'Us Air Force, basati a Hurlburt Field, in Florida, hanno trovato sul social network lo scatto di alcuni militanti jihadisti all'interno di una base, durante una ricerca di routine sui militanti dell'Is sul web. Poi sono riusciti a identificare altre immagini degli uomini, alcune delle quali fornivano le informazioni necessarie a localizzare con precisione dove si trovassero. In

L'estrazione delle informazioni dai Social Network

- NodeXL è un template Open Source di Excel creato dalla Microsoft Resource in collaborazione con alcune Università Americane.
- NodeXL permette di analizzare qualsiasi tipo di network creando delle relazioni in base ad elementi comuni. Tramite i dati in input crea un grafico che viene sviluppato con algoritmi matematici, già inclusi nel plug-in.
- NodeXL si interfaccia tramite le API con Twitter Facebook ed altri social network.

Case study: ISIS_M***

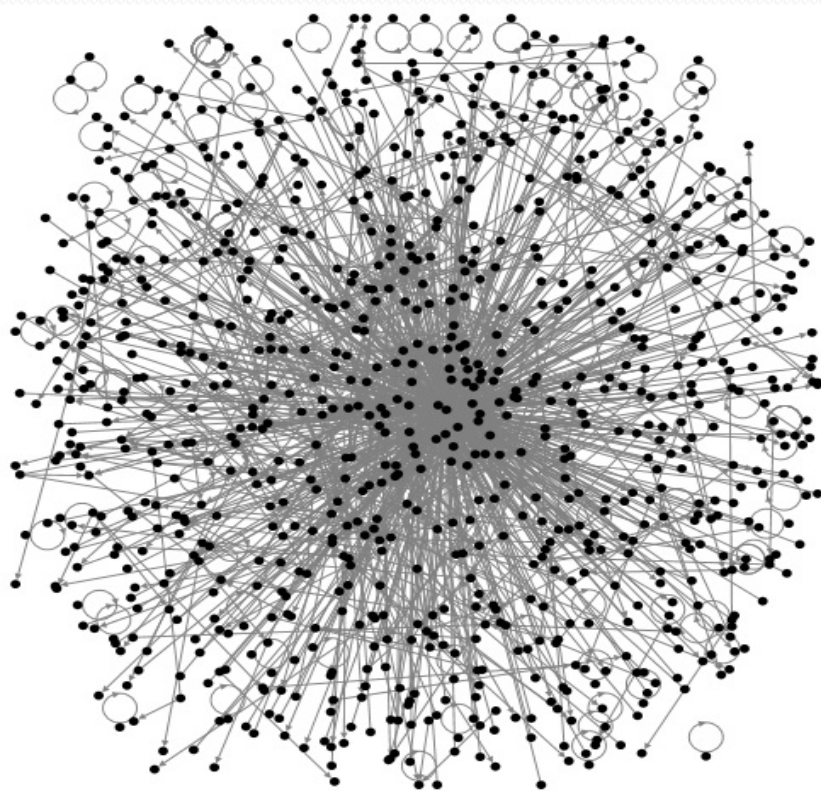
- Analisi del profilo Twitter “ISIS_M***” uno dei canali ufficiali dello Stato Islamico (IS).



Case study: ISIS_M***

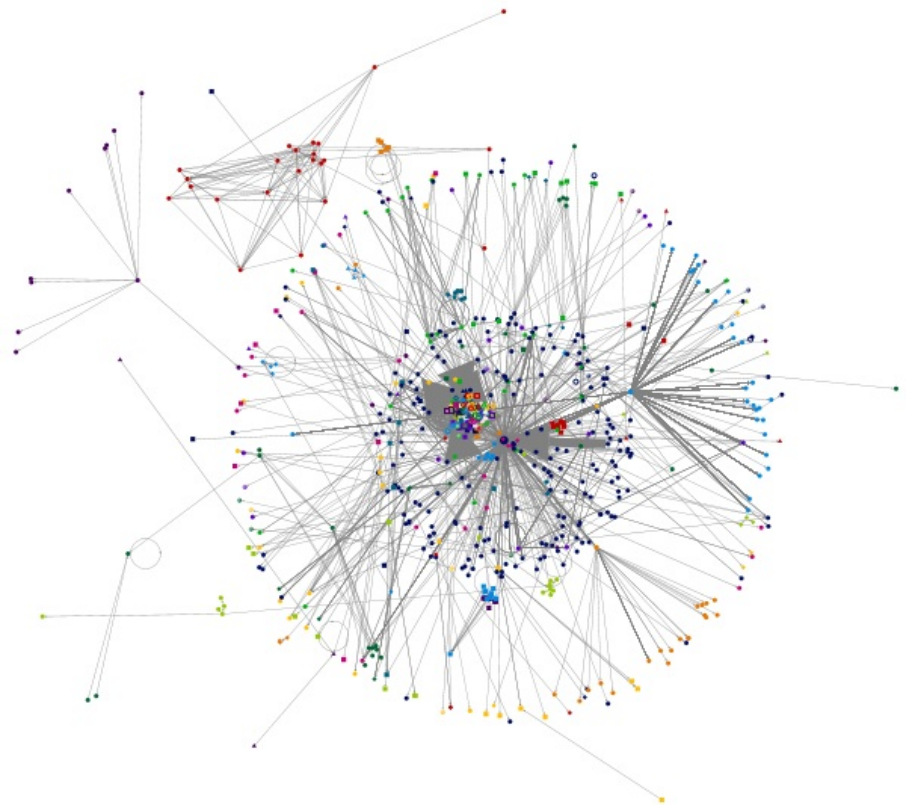
Grafo della rete

GRAFO NON FILTRATO



Created with NodeXL (<http://nodexl.codeplex.com>)

GRAFO FILTRATO



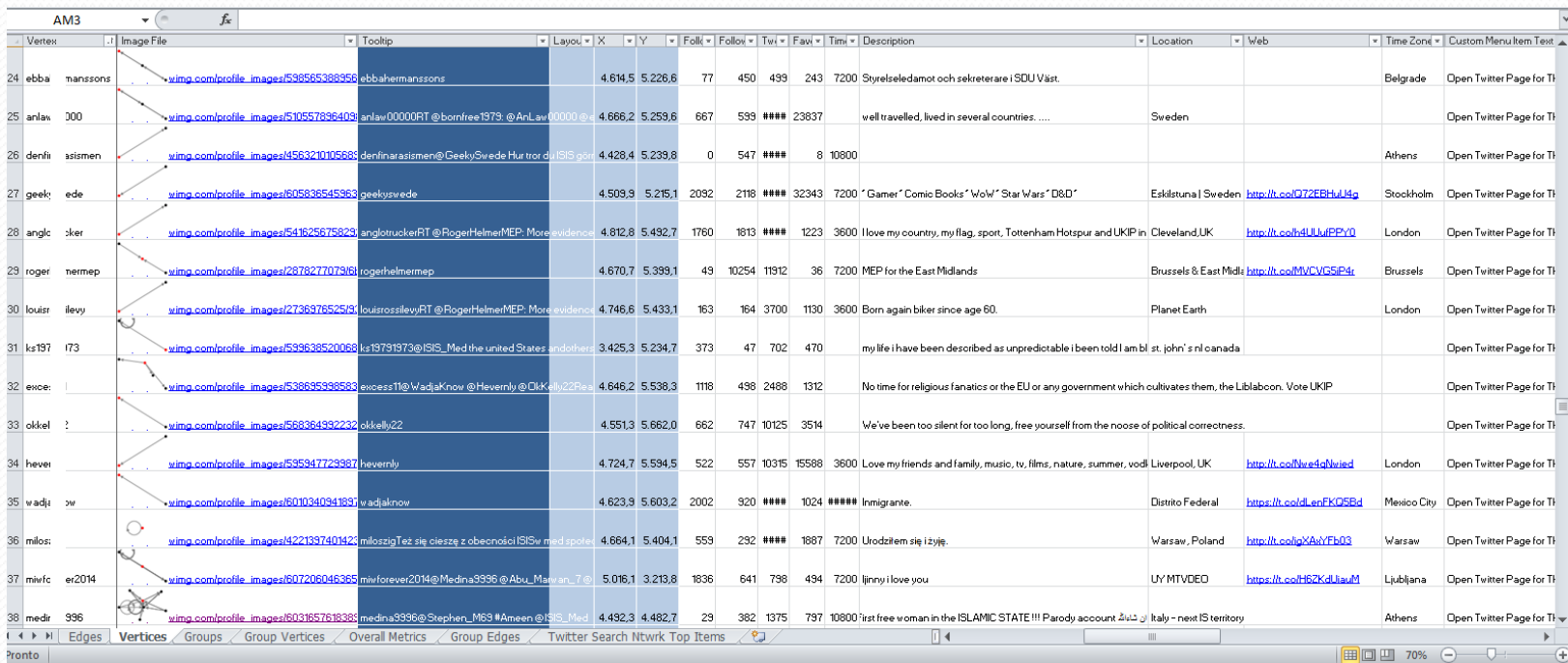
Created with NodeXL (<http://nodexl.codeplex.com>)

Informazioni acquisite con NodeXL

- Tipo di relazione tra i vari utenti
 - @Mentions, @Replies, Tweet
- Informazioni sul profilo completo di ogni singolo utente
 - Link del profilo e dell'immagine del profilo
 - Tooltip
 - Follower, Following, twitter generati
 - Time Zone, Location
 - Geolocalizzazione

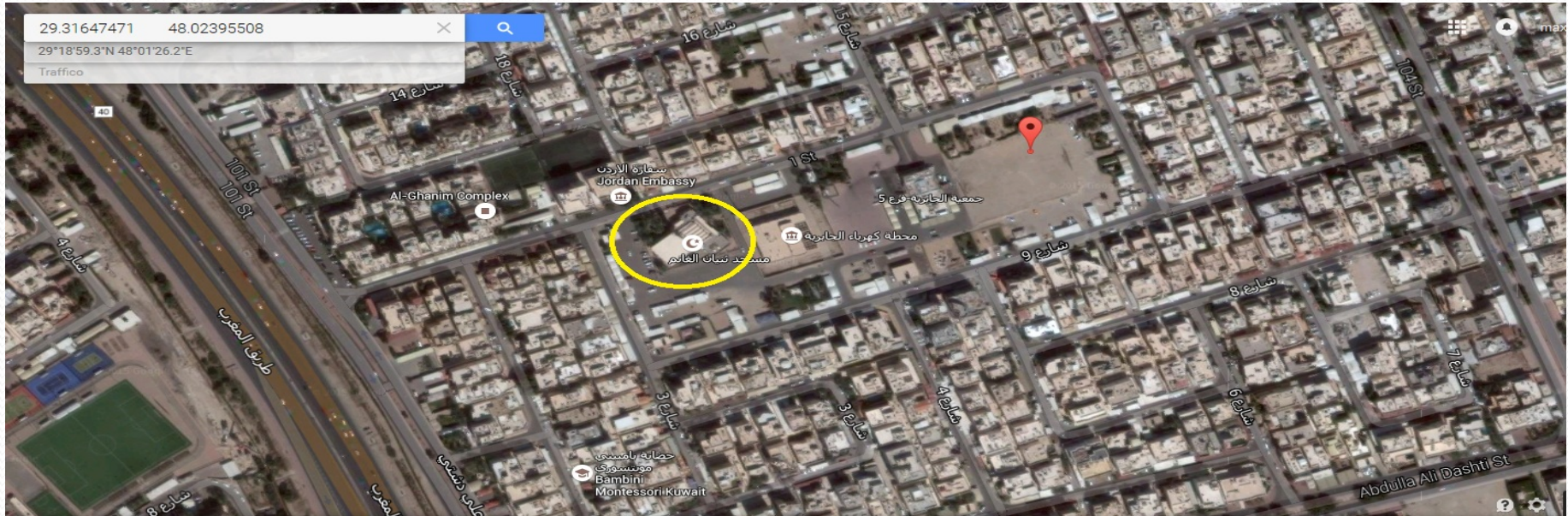
Informazioni acquisite con NodeXL

- Informazioni sul profilo completo dell'utente

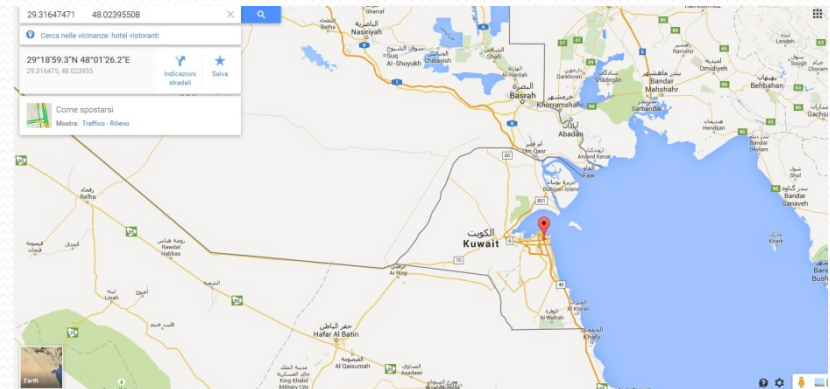


Vertex	Image File	Tooltip	Layout	X	Y	Follw	Follow	Retw	Fav	Time	Description	Location	Web	Time Zone	Custom Menu Item Text
24	ebba manssons	ximg.com/profile_images/538565388958/ebbahermanssons		4.614,5	5.226,6	77	450	439	243	7200	Styrelseledamot och sekreterare i SDU Väst.			Belgrade	Open Twitter Page for Ti
25	anlaw 000	ximg.com/profile_images/510557896409/anlaw00000RT @bornfree1979 @AnLaw00000 @e		4.666,2	5.253,6	667	539	####	23837		well travelled, lived in several countries.	Sweden			Open Twitter Page for Ti
26	denlin asismen	ximg.com/profile_images/4563210105688/denlinasismen@GeelySvede Hur tror du ISIS gör		4.428,4	5.239,8	0	547	####	8	10800				Athens	Open Twitter Page for Ti
27	geeky ede	ximg.com/profile_images/605838545363/geekysvede		4.509,9	5.215,1	2092	218	####	32343	7200	"Gamer" Comic Books "Wow" Star Wars "D&D"	Eskilstuna Sweden	http://t.co/Q72ERHJ4g	Stockholm	Open Twitter Page for Ti
28	anglcrker	ximg.com/profile_images/541625675823/anglcruckerRT @RogerHelmerMEP: More evidence		4.812,8	5.492,7	1760	1813	####	1223	3600	I love my country, my flag, sport, Tottenham Hotspur and UKIP in	Cleveland,UK	http://t.co/h4UJwFPYQ	London	Open Twitter Page for Ti
29	roger nermep	ximg.com/profile_images/2878277079161/rogerhelmermep		4.670,7	5.339,1	49	10254	11912	36	7200	MEP for the East Midlands	Brussels & East Midl	http://t.co/MVCVGSIP4	Brussels	Open Twitter Page for Ti
30	louisr illevy	ximg.com/profile_images/273697652593/louiscrosslevyRT @RogerHelmerMEP: More evidence		4.746,6	5.433,1	163	164	3700	1130	3600	Born again biker since age 60.	Planet Earth		London	Open Twitter Page for Ti
31	ks197173	ximg.com/profile_images/533638520068/ks1971973@ISIS_Med the united States and others		3.425,3	5.234,7	373	47	702	470		my life i have been described as unpredictable i been told I am bl st. john' s nl canada				Open Twitter Page for Ti
32	excess11	ximg.com/profile_images/5386395939583/excess11@Waduknow @Heavenly @DKelly22Re		4.646,2	5.538,3	1118	498	2488	1312		No time for religious fanatics or the EU or any government which cultivates them, the Liblabcon. Vote UKIP				Open Twitter Page for Ti
33	okkel 2	ximg.com/profile_images/568364939222/okkelly22		4.551,3	5.662,0	662	747	10125	3514		We've been too silent for too long. free yourself from the noose of political correctness.				Open Twitter Page for Ti
34	hevenly	ximg.com/profile_images/535347729387/hevenly		4.724,7	5.534,5	522	557	10315	15588	3600	Love my friends and family, music, tv, films, nature, summer, vodi	Liverpool, UK	http://t.co/Nve4qWvied	London	Open Twitter Page for Ti
35	waduknow	ximg.com/profile_images/6101340341831/waduknow		4.623,9	5.603,2	2002	320	####	1024	####	Immigrante.	Distrito Federal	https://t.co/denFKO5Bd	Mexico City	Open Twitter Page for Ti
36	milosz	ximg.com/profile_images/4221397401422/miloszTeż się cieszę z obecności ISIS w mediach społ		4.664,1	5.404,1	559	292	####	1887	7200	Urodziłem się i żyję.	Warsaw, Poland	http://t.co/hg5AcyFK03	Warsaw	Open Twitter Page for Ti
37	miwifer2014	ximg.com/profile_images/607206045365/miwifer2014@Medina3996 @Abu_Marwan_U7 @		5.016,1	3.213,8	1836	641	798	494	7200	Ijnniyi love you	UY MTVDEO	https://t.co/t62KdUiaaM	Ljubljana	Open Twitter Page for Ti
38	medira996	ximg.com/profile_images/6031657618388/medira996@Stephen_M69 #Ameen @ISIS_Med		4.492,3	4.482,7	29	382	1375	737	10800	1st free woman in the ISLAMIC STATE !!! Parody account	Italy - next IS territory		Athens	Open Twitter Page for Ti

Informazioni acquisite con NodeXL



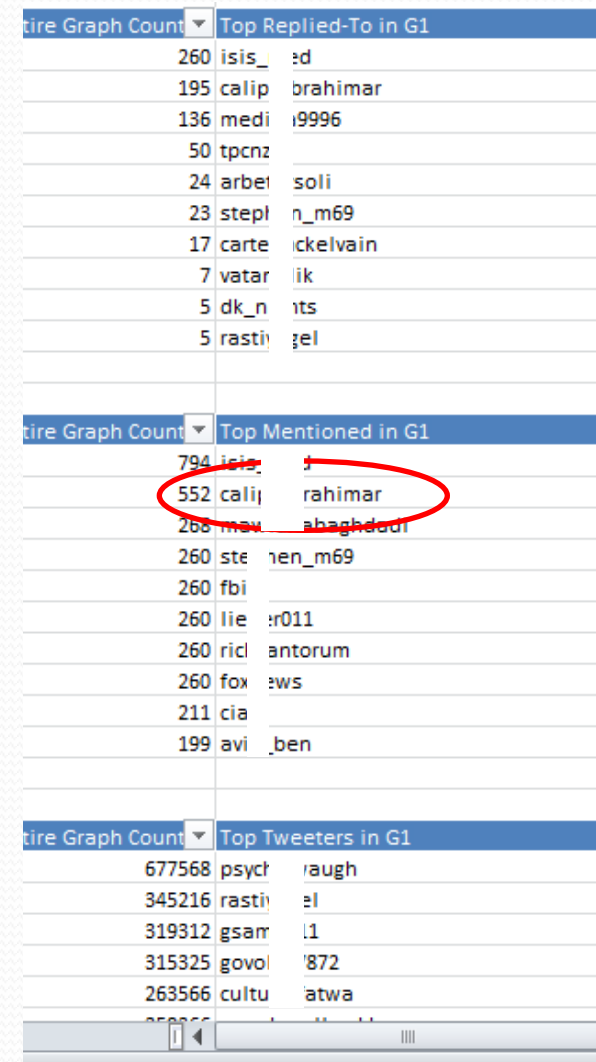
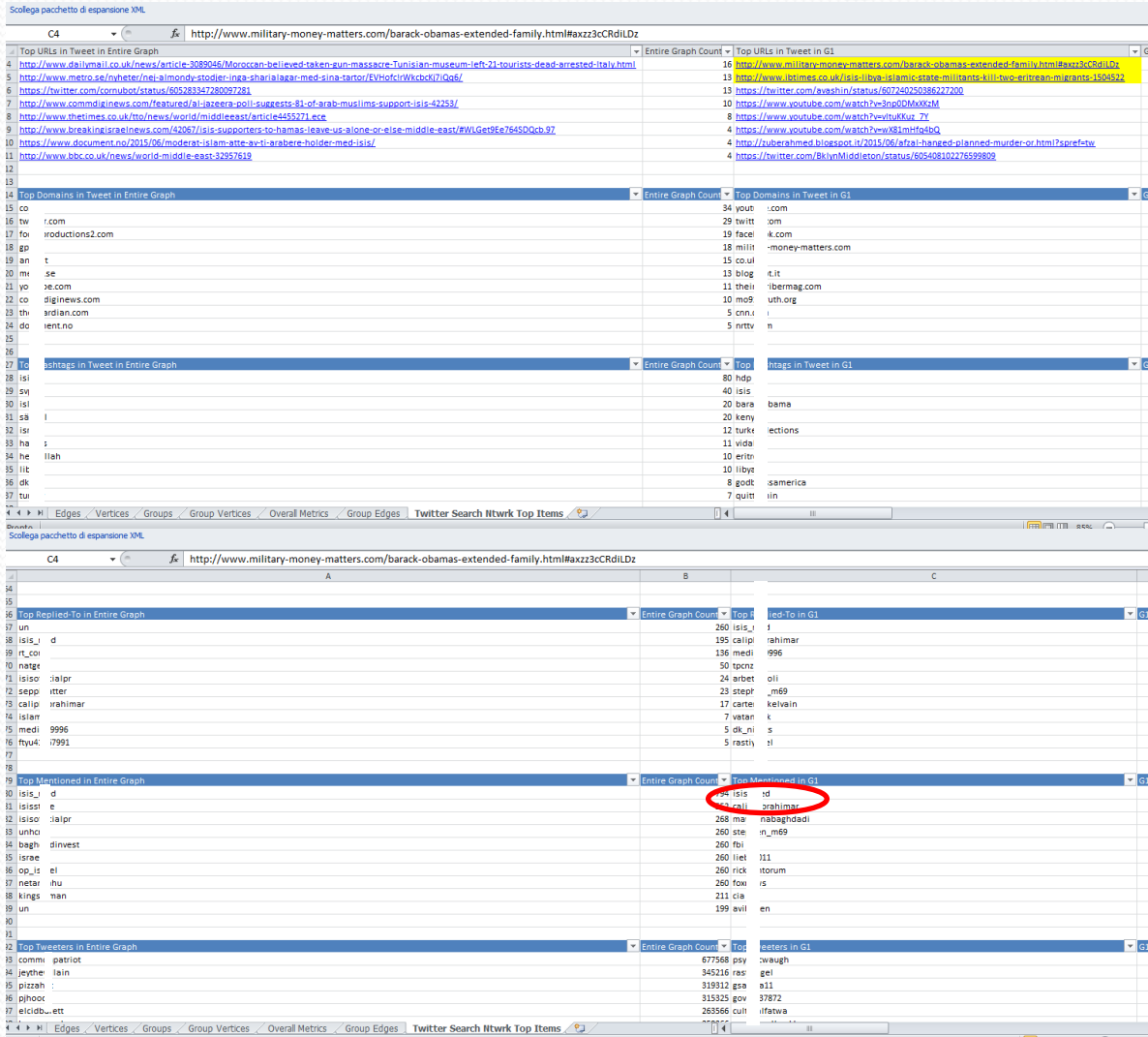
Vertex 1	Latitude	Longitude	Imported ID	In-Reply-To Tweet ID	Reciproq
256 itsme_1e			60549097354049945L		No
257 elcidb			60549407623498547		No
258 wibble			60550416453013504		No
259 mf26			60550971000822988	60494963269584486	No
260 mf26			60550971000822988	60494963269584486	No
261 mf26			60550971000822988	60494963269584486	No
262 mf26			60550971000822988	60494963269584486	No
263 mishagu			60551045266425856		No
264 malekhesk	2931647471	4802395508	605510674064621568		No
265 malekhe	2931647471	4802395508	60551067406462156		No
266 malekhe	2931647471	4802395508	60551067406462156		No
267 med_ic			60554684036945920		No
268 hussamsic			6055485492379156		No



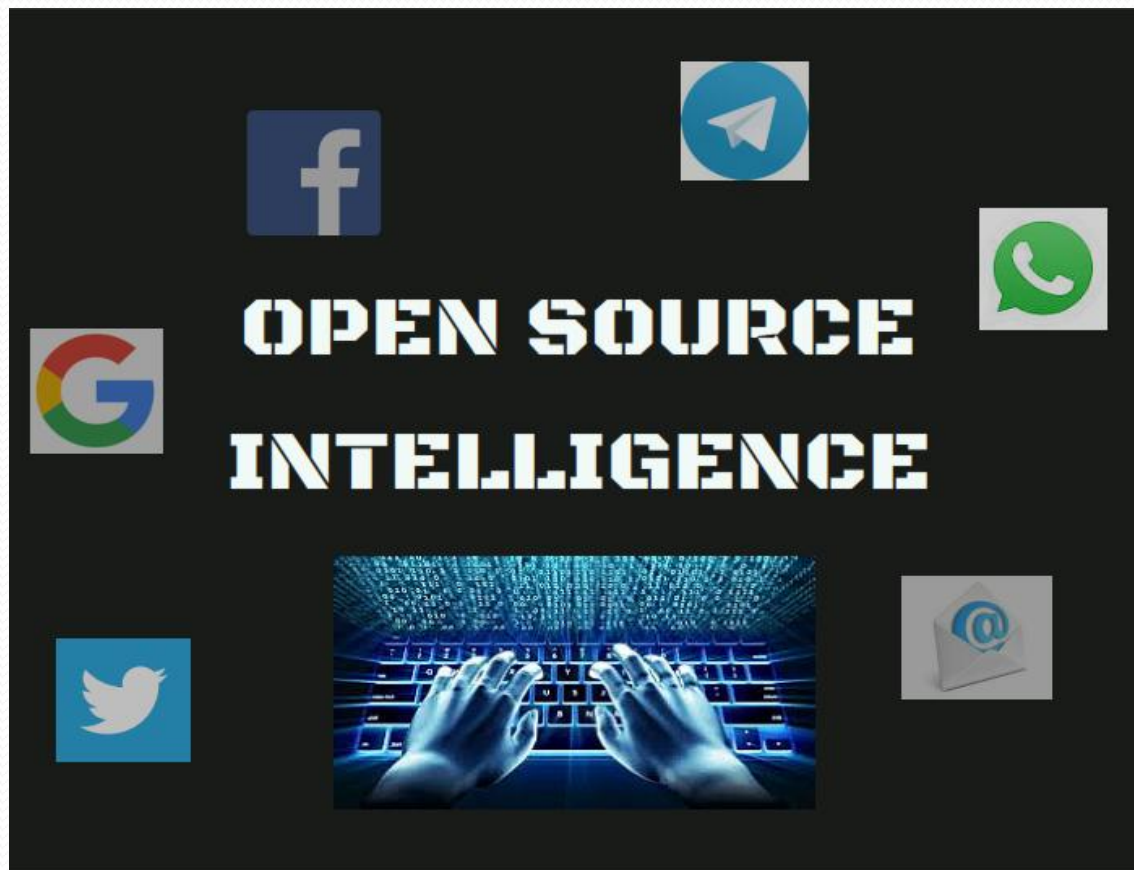
Informazioni acquisite con NodeXL

- Infine NodeXL permette di effettuare l'analisi delle informazioni presenti nella rete generando delle statistiche ed estraendo:
 - Top degli URL della rete
 - Top dei domini
 - Top delle parole e delle coppie di parole
 - Hashtag, menzioni, tweet

Informazioni acquisite con NodeXL



Attività di OSINT



Attività di OSINT

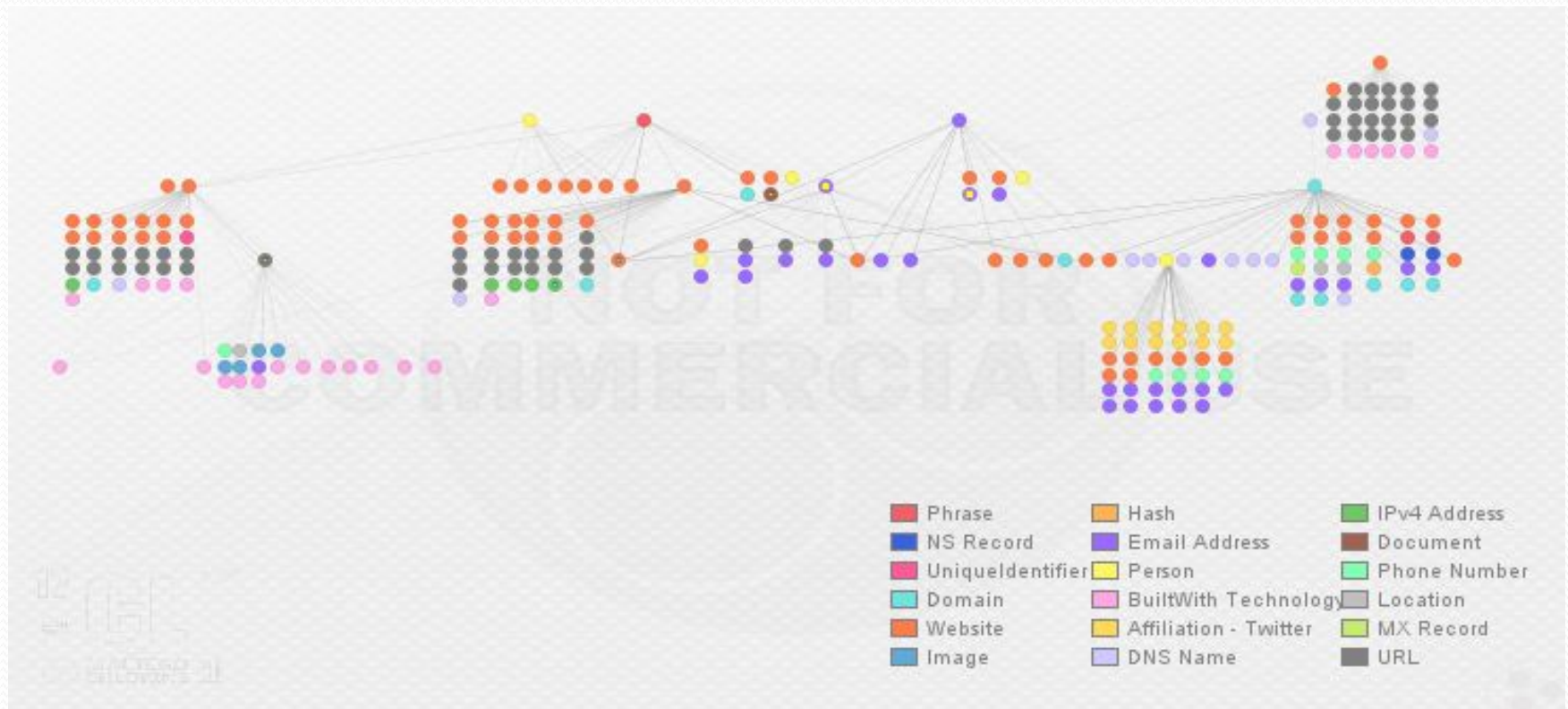


Attività di OSINT

- **OSINT**, acronimo di **Open Source INTelligence**, è l'attività di raccolta di informazioni mediante la consultazione di fonti di pubblico accesso.
- Lo strumento maggiormente utilizzato per questa attività è Maltego.
- Maltego è un tool, che permette di raccogliere informazioni e di raggrupparle graficamente:
 - Siti web, Social network, wiki, Blog
 - Dati pubblici tra cui articoli di stampa, dati demografici ecc.
 - Dati geolocalizzati, ed immagini anche satellitari
 - ... e molto altro ancora.

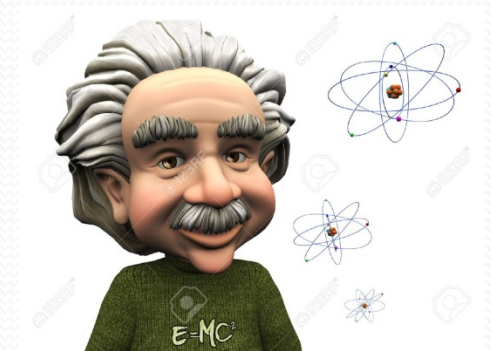
Attività di OSINT su «caliphiB****»

GRAFICO DATI MALTEGO



Attività di OSINT su «caliphiB****»

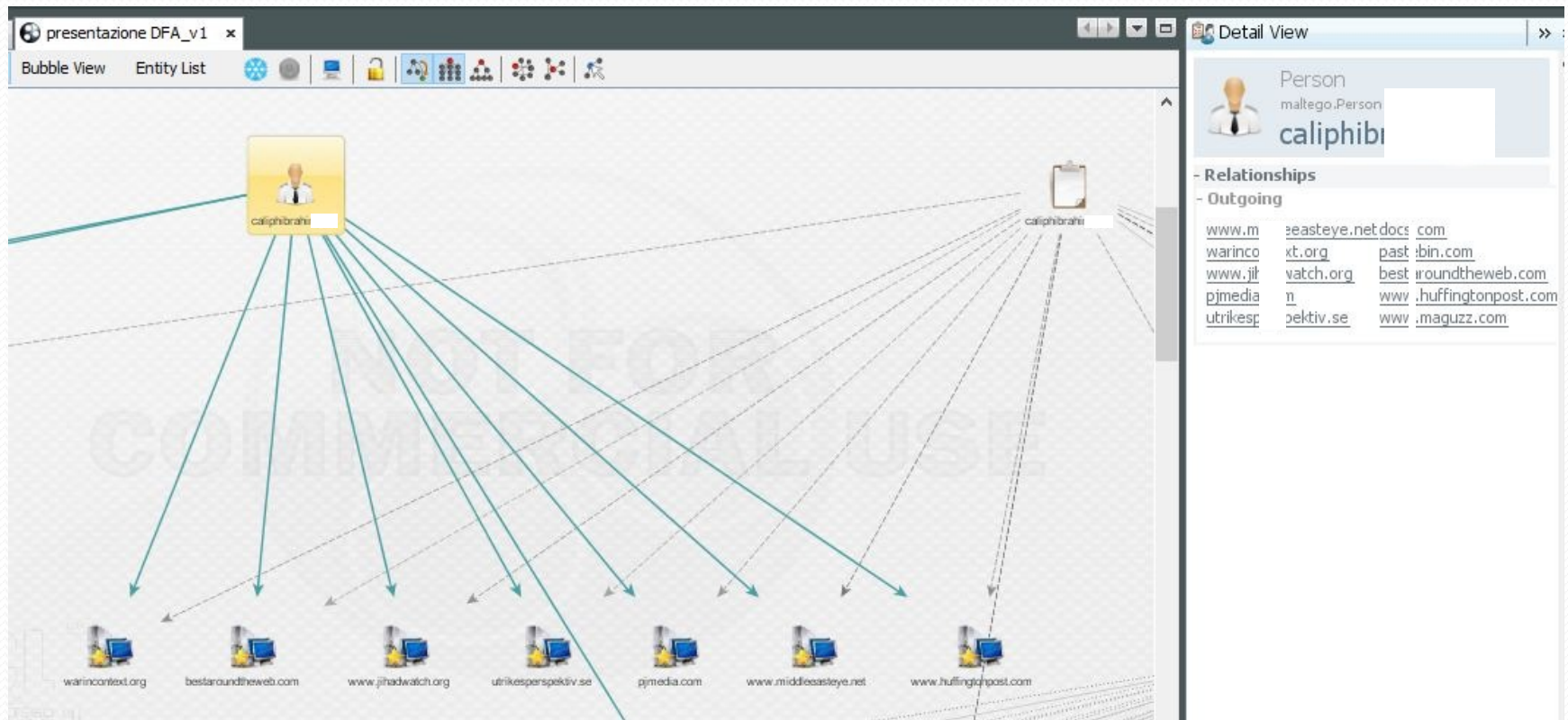
- Attraverso il grafico generato da Maltego l'operatore ha la possibilità di effettuare un'analisi, al fine di evidenziare le correlazioni pertinenti eliminando, quindi, le informazioni superflue e di scarso interesse per la ricerca.



«Il calcolatore è straordinariamente veloce, accurato e stupido.
Gli uomini sono incredibilmente lenti, imprecisi e creativi.
L'insieme dei due costituisce una forza incalcolabile»

A. Einstein

Attività di OSINT su «caliphiB****»

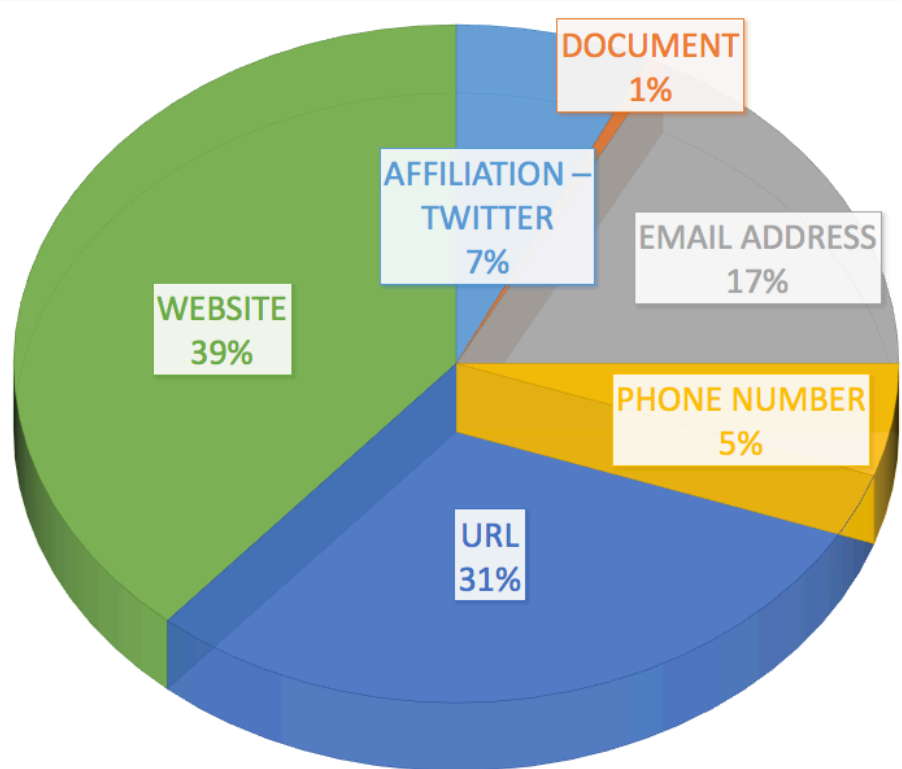


Dott. Alessandro MASSARO
Dott. Ing. Fabio MELE



Attività di OSINT su «caliphiB****»

- Dalla ricerca con Maltego sono emersi :



DATI RILEVANTI ESTRATTI DA MALTEGO

Attività di OSINT su «caliphiB****»

OSINT su immagini :

- GOOGLE
- YANDEX
- TINEYE
- TWICSY (Twitter)

IMMAGINE ORIGINALE DA TWITTER



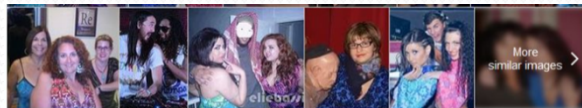
<http://twicsy.com>

<http://tineye.com>

<https://www.yandex.com>

Attività di OSINT su «caliphiB****»

YANDEX



Sites where the image is displayed



assek Facebook
book.com/Voyage.No.Limits



Facebook اتج-----اد صفح-----ات شم-----ال افريقى-----ا هن-----ال-----ورثا
http://ru-r
ebook.com/Nord.afrique.anti.5wanjiya
الاع-----وان
اتج-----اد صفح-----ات شم-----ال افريقى-----ا هن-----ال-----ورثا

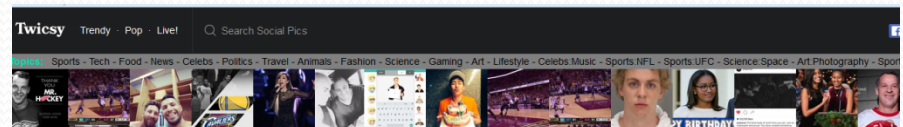


D7ak M: assek Facebook
http://tr-tr book.com/Voyage.No.Limits
Fotograf: التحية و



Facebook اتح-----اد صفح-----ات شم-----ال افريقا-----اض-----ال-----جرذا
http://ru-r ebook.com/Nord.afrique.anti.5wanjiya

TWICSY











Yehia Amin
 @Yehiaamin

Follow

RELATED PICS



Yehiaamin: @AhmedFouad_Negm بلغ الكلام ده يا كبير <http://t.co/vKYmTuA5gp> - 2013-02-28 19:04:37

TWITTER



Attività di OSINT su «caliphiB****»

Tools di OSINT su Skype :

- SKYPEGRAB.NET
- permette di effettuare delle ricerche per reperire informazioni sugli utenti Skype
- E-mail → Username
- Username → E-mail
- Username → Indirizzi IP

The screenshot shows the SKYPEGRAB.NET website interface. At the top, there is a dark header with the text "Email to Skype". Below this, there is a search form with a label "email:" and a text input field containing "owa[REDACTED]@gmail.com". To the right of the input field is a CAPTCHA image showing the digits "029". Below the CAPTCHA is a button labeled "CAPTCHA". Underneath the CAPTCHA is a dark bar with the text "Resolve". Below this bar is a light gray box containing the results under the heading "Usernames:". The results listed are "owa[REDACTED]125", "owa[REDACTED]ri8", and "live:owa[REDACTED]dri_2".

Conclusioni SNA ed OSINT

L'attività ci ha permesso di acquisire:

- Grafo di rete completo di relazioni e di profili utenti
- Siti web
- Gruppi di Google plus
- Social network (Twitter, Facebook)
- Documenti condivisi
- Immagini condivise e reverse image
- Indirizzi e-mail
- Username Skype
- Indirizzi IP

Conclusioni SNA ed OSINT

“Se riveli al vento i tuoi segreti, non devi poi rimproverare al vento di rivelarli agli alberi.”

Kahlil Gibran

Grazie



Quest'opera è distribuita con licenza Creative Commons **Attribuzione**
- Non commerciale - Non opere derivate CC BY-NC-ND