

UNIVERSITA' DEGLI STUDI DI MILANO
Facoltà di Giurisprudenza
Cattedre di "Informatica Giuridica" e
"Informatica Avanzata"

CORSO DI PERFEZIONAMENTO IN
COMPUTER FORENSICS E DATA
PROTECTION

NodeXL: l'amo delle Reti Sociali

tesi a cura di
Dott. Alessandro MASSARO
Dott. Ing. Fabio MELE



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

Open Source INTelligence

- Internet è diventata la piazza virtuale da dove passano e restano impigliate milioni di informazioni.
- Per poter aver accesso alle informazioni della rete si possono utilizzare le fonti di pubblico accesso ovvero le OSINT.
- L'OSINT raccoglie e analizza le varie informazioni contenute nei mezzi di comunicazione.

Dott. Alessandro MASSARO
Dott. Ing. Fabio MELE

Come estrapolo le informazioni? NodeXL

- L' Open Source Intelligence permette di estrapolare tutte le informazioni, ma per filtrarle e ottenere i dati di nostro interesse ci serviamo delle **Analisi delle Reti Sociali** o **SNA**.
- **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, sia virtuale che reale, 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.

Dott. Alessandro MASSARO
Dott. Ing. Fabio MELE

NodeXL e la “pratica” applicazione: i cinguettii dell'ISIS nell'amo della rete

- NodeXL può essere impiegato in innumerevoli campi che vanno dalle scienze sociali al marketing ma anche dagli addetti alle investigazioni.
- La vera **potenzialità** di NodeXL è la possibilità di poter estrarre dati non solo da *social network* ma anche da *email* e *browser* ed *altri tipi di software*.
- Per interfacciarsi con vari social network NodeXL utilizza un importatore che scarica i dati di profili di utenti o gruppi, in maniera semplice, creando poi delle relazioni tra i vari dati ritrovati. Questi dati vengono a loro volta tradotti sotto forma di grafico.

Dott. Alessandro MASSARO
Dott. Ing. Fabio MELE

NodeXL e la “pratica” applicazione: i cinguettii dell'ISIS nell'amo della rete

- **CASO REALE:** Abbiamo analizzato in questo elaborato il profilo Twitter “ISIS_ [redacted]” uno dei canali ufficiali di scambio di informazioni dello Stato Islamico (IS).



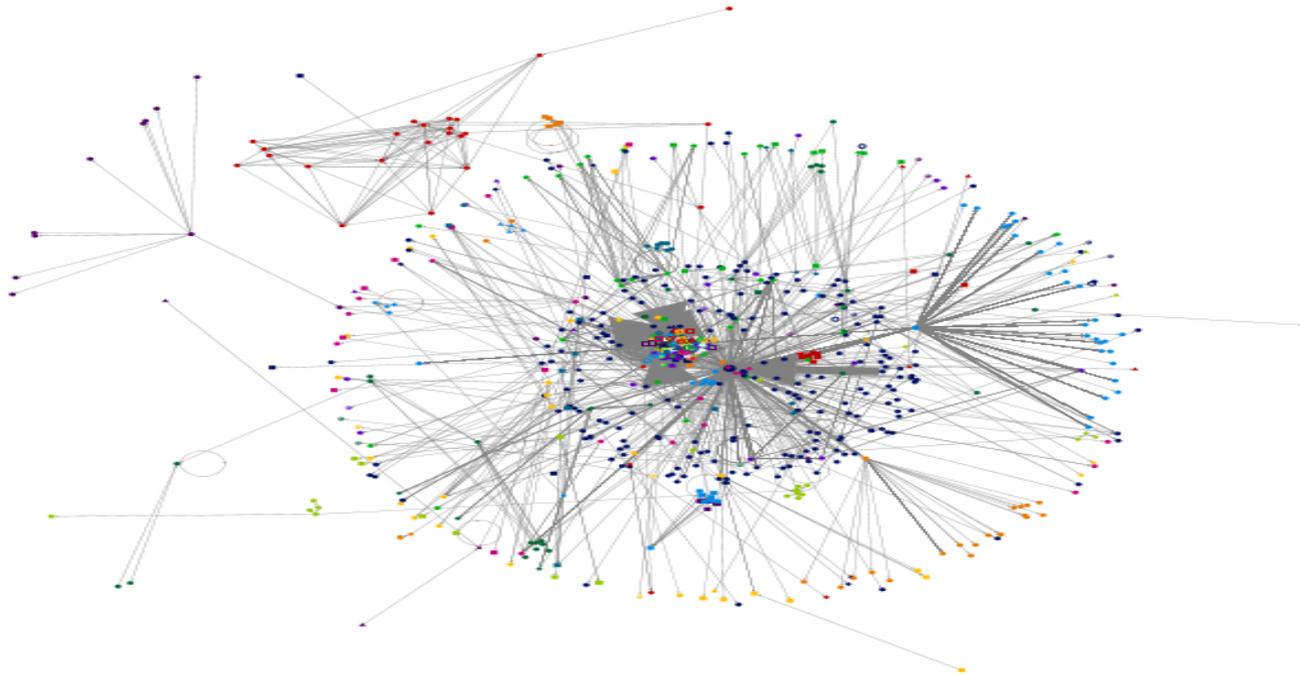
Dott. Alessandro MASSARO
Dott. Ing. Fabio MELE

NodeXL e la “pratica” applicazione: i cinguettii dell'ISIS nell'amo della rete

- **CASO REALE:** Quindi tramite l'importatore ci siamo collegati al profilo ISIS [REDACTED] ed abbiamo impostato alcune configurazioni automatiche, dopo alcuni minuti, tutti i dati sono stati caricati nel software, la rete analizzata era composta da circa 10,000 nodi e da 1000 attori.
- Per una migliore analisi dei risultati, abbiamo configurato alcuni parametri per filtrare i dati. Quindi eliminando quelli meno importanti, cioè quei nodi che hanno basse connessioni, abbiamo impostato il centro del grafico ed organizzato i vari gruppi con algoritmi matematici già inclusi nel plug-in. Una volta concluse queste operazioni, la rete ottenuta è la seguente.

Dott. Alessandro MASSARO
Dott. Ing. Fabio MELE

NodeXL e la “pratica” applicazione: i cinguettii dell'ISIS nell'amo della rete



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

Dott. Alessandro MASSARO
Dott. Ing. Fabio MELE

NodeXL e la “pratica” applicazione: i cinguettii dell'ISIS nell'amo della rete

DATI INTERESSANTI REPERITI:

- CONNESSIONI CON FBI – CIA - POLICENATIONALF (EDGE 159-171-)

ALCUNI SOGGETTI MENZIONANO (@) LE FORZE DI POLIZIA PER
INDIRIZZARE ALCUNI MESSAGGI



Dott. Alessandro MASSARO
Dott. Ing. Fabio MELE

NodeXL e la “pratica” applicazione: i cinguettii dell'ISIS nell'amo della rete

DATI INTERESSANTI REPERITI:

- LINK WEB RELATIVO AL PRESIDENTE DEGLI USA, BARACK OBAMA (Top URL G1)

VIENE INDICATA LA STORIA DELLE ORIGINI DELLA FAMIGLIA DI BARACK OBAMA

The screenshot shows the website 'Military MONEY MATTERS' with the tagline 'Take Command of Your Finances!'. The main article is titled 'Barack Obama's Extended Family'. The text of the article reads: 'Barack Obama's extended family paints a colorful picture, and it's one he'd probably prefer you not see. Attempting to research his family, including all his father's wives and mistresses, and all his half-siblings, is enough to confuse any voter. Obama shares a father with seven half-siblings, and a mother with one. That's quite an extended family.'

The page includes a sidebar with navigation links such as 'Home', 'Site Info', 'Money Matters', 'Debt Matters', and 'Credit Matters'. There are also social media links for Facebook, Twitter, and YouTube, and a 'Live Well' section featuring a book cover titled 'NEVER FEEL POOR AGAIN on your Military Paycheck'.

Dott. Alessandro MASSARO
Dott. Ing. Fabio MELE

NodeXL e la “pratica” applicazione: i cinguettii dell'ISIS nell'amo della rete

DATI INTERESSANTI REPERITI:

- TWEET CON COMUNICAZIONE DI SERVIZIO SUL DISTRETTO A LUCI ROSSE (Edge 5 Ghostfane29-isis_ [REDACTED])

Abu Qutata” era stato inviato quattro settimane fa per il reclutamento e non ha fatto più ritorno raccomandando di fare attenzione al quartiere a luci rosse perché probabilmente lì ci sono i Peshmerga .

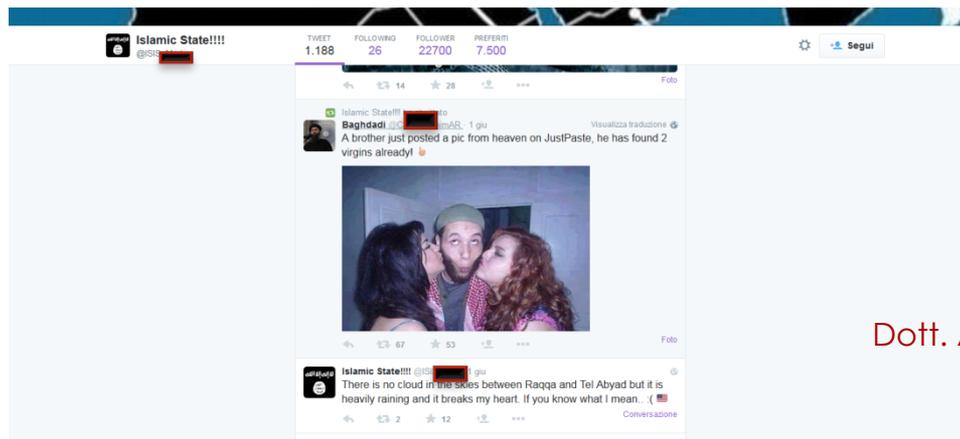


Dott. Alessandro MASSARO
Dott. Ing. Fabio MELE

NodeXL e la “pratica” applicazione: i cinguettii dell'ISIS nell'amo della rete

DATI INTERESSANTI REPERITI:

- TWEET A SFONDO SESSUALE (Edge 6508 Chaliphbrahim-isis_med)
@CaliphIbrahimAR: A brother just posted a pic from heaven on JustPaste, he has found 2 virgins already!.



Dott. Alessandro MASSARO
Dott. Ing. Fabio MELE

NodeXL e la “pratica” applicazione: i cinguettii dell'ISIS nell'amo della rete

DATI INTERESSANTI REPERITI:

o TWEET NON ESISTENTE (Edge 6462 fbi-isis [REDACTED])

In questo caso il link corrispondente alla pagina non viene trovato, ma NodeXL ha comunque estrapolato tutti i dati necessari all'identificazione del nodo difatti questo è il suo contenuto: [@CarterMcKelvain Behheading target acquired. @lieber011 @RickSantorum @FoxNews @FBI @CIA](#)

Vertex 1	Vertex 2	Color	Width	Opacity	Label	Relationship	Relationship ID	Tweet
442 spin	isis					Replies to	42160.39046	@ISIS don't worry ya sheikh. according to the pamphlet by sheikh kaygusuz, it's hahal for competent one on t
443 spin	isis					Replies to	42161.91197	@ISIS valiahi haram :(https://t.co/TzJerdy84
444 isis	spinosa_zakir					Mentions	42161.9762	RT @spinosa_zakir: @ISIS valiahi haram :(https://t.co/TzJerdy84
445 isis	elcotemya					Replies to	42162.03331	@elcotemya bililyorum abn
446 liebe	cia					Mentions	42162.04689	Graduation was great but leave it to @RickSantorum to make an ISIS joke on stage in front of everyone @FoxNews
447 liebe	cia					Mentions	42162.05102	RT @CarterMcKelvain: @lieber011 @RickSantorum @FoxNews @ISIS FBI @CIA this is how you get put on a l
448 liebe	cia					Mentions	42162.05299	RT @CarterMcKelvain: @ISIS @lieber011 @RickSantorum @FoxNews @FBI @CIA Too bad my head is ENCRYPT
449 liebe	cia					Mentions	42162.05318	@CarterMcKelvain @ISIS @lieber011 @RickSantorum @FoxNews @FBI @CIA Too bad my head is ENCRYPT
450 carte	mcKelvain					Mentions	42162.05072	@lieber011 @RickSantorum @FoxNews @ISIS @FBI @CIA this is how you get put on a list
451 carte	mcKelvain					Mentions	42162.05193	@lieber011 @RickSantorum @FoxNews @FBI @CIA oh god I'm loling so hard
452 carte	mcKelvain					Mentions	42162.05287	@ISIS @lieber011 @RickSantorum @FoxNews @FBI @CIA Too bad my head is ENCRYPTED! HAI Cant decrypt m
453 isis	cia					Mentions	42162.05172	@CarterMcKelvain Behheading target acquired. @lieber011 @RickSantorum @FoxNews @FBI @CIA
454 isis	cia					Mentions	42162.0524	@CarterMcKelvain I hate LOLing people. Target 2 locked. @lieber011 @RickSantorum @FoxNews @FBI @CIA
455 liebe	fbi					Mentions	42162.04689	Graduation was great but leave it to @RickSantorum to make an ISIS joke on stage in front of everyone @FoxNews
456 liebe	fbi					Mentions	42162.05102	RT @CarterMcKelvain: @lieber011 @RickSantorum @FoxNews @ISIS @lieber011 @CIA this is how you get put on a l
457 liebe	fbi					Mentions	42162.05299	RT @CarterMcKelvain: @ISIS @lieber011 @RickSantorum @FoxNews @FBI @CIA Too bad my head is ENCRYPT
458 liebe	fbi					Mentions	42162.05318	@CarterMcKelvain @ISIS @lieber011 @RickSantorum @FoxNews @FBI @CIA Too bad my head is ENCRYPT
459 carte	mcKelvain					Mentions	42162.05072	@lieber011 @RickSantorum @FoxNews @ISIS @FBI @CIA this is how you get put on a list
460 carte	mcKelvain					Mentions	42162.05193	@lieber011 @RickSantorum @FoxNews @FBI @CIA oh god I'm loling so hard
461 carte	mcKelvain					Mentions	42162.05287	@ISIS @lieber011 @RickSantorum @FoxNews @FBI @CIA Too bad my head is ENCRYPTED! HAI Cant decrypt m
462 isis	cia					Mentions	42162.05172	@CarterMcKelvain Behheading target acquired. @lieber011 @RickSantorum @FoxNews @FBI @CIA
463 isis	fbi					Mentions	42162.0524	@CarterMcKelvain I hate LOLing people. Target 2 locked. @lieber011 @RickSantorum @FoxNews @FBI @CIA
464 liebe	foxnews					Mentions	42162.04689	Graduation was great but leave it to @RickSantorum to make an ISIS joke on stage in front of everyone @FoxNews

Dott. Alessandro MASSARO
Dott. Ing. Fabio MELE

NodeXL e la “pratica” applicazione: i cinguettii dell'ISIS nell'amo della rete

DATI INTERESSANTI REPERITI:

- **TWEET CON COORDINATE GEOGRAFICHE** (Edge 264 malekheskey)

Uno dei dati più interessanti ritrovati in questo caso pratico sono le coordinate geografiche. NodeXL, le memorizza al suo interno, ovviamente solo se l'utente Twitter ha abilitato questa impostazione sul proprio smartphone.

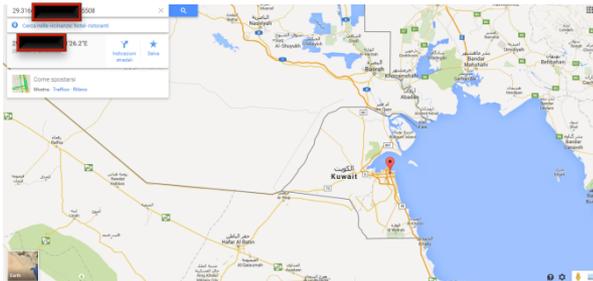
Vertex 1	Latitude	Longitude	Imported ID	In-Reply-To Tweet ID	Reciproci	X	Y	Z	AA	AB	AC
256			605490973540499456		No						
257			605494076234985472		No						
258			605504164530135040		No						
259			605509710008229888	604949632695844864	No						
260			605509710008229888	604949632695844864	No						
261			605509710008229888	604949632695844864	No						
262			605509710008229888	604949632695844864	No						
263			605510452664258560		No						
264	2931647471	4802395508	605510674064621568		No						
265	2931647471	4802395508	605510674064621568		No						
266	2931647471	4802395508	605510674064621568		No						
267			605546840369459200		No						
268			605548549237915648		No						

Dott. Alessandro MASSARO
Dott. Ing. Fabio MELE

NodeXL e la “pratica” applicazione: i cinguettii dell'ISIS nell'amo della rete

DATI INTERESSANTI REPERITI:

- TWEET CON COORDINATE GEOGRAFICHE (Edge 264 malekheskey)



Dott. Alessandro MASSARO
Dott. Ing. Fabio MELE

NodeXL e la “pratica” applicazione: i cinguettii dell'ISIS nell'amo della rete

CONCLUSIONI:

- NodeXL è uno strumento molto potente che attraverso l'analisi delle reti sociali potrebbe affiancarsi agli attuali metodi investigativi tradizionali ed essere di ausilio alle forze di Intelligence per la lotta al terrorismo e alla criminalità organizzata
- Allo stato attuale questo template non è diffuso nel nostro Paese, pur essendo uno strumento gratuito e di facile utilizzo.

Grazie per l'attenzione

Dott. Alessandro MASSARO
Dott. Ing. Fabio MELE