PERFECTLY IMPERFECT

19-20-21 agosto
2016

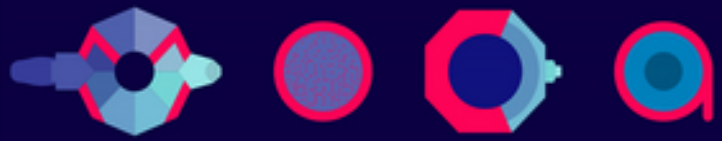
Parco Ex Caserma Cocco
Pescara

OSINT
Open Source Intelligence

i tuoi dati in piazza

Paolo ‘aspy’ Giardini

About: paolo ‘aspy’ giardini



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

Di cosa parleremo

- Introduzione a OSINT
  - Definizione di OSINT
  - Chi utilizza OSINT e perché
- Cosa, dove, come cercare
  - Motori, servizi, ed altri luoghi
  - Social networks, relazioni, cerchie, e tutto il resto
  - Geolocalizzazione, Metadata, Analisi delle Immagini
- Alcuni esempi reali
- Conclusioni

Definizioni

OSINT= Open Source INTelligence

“Open Source” si riferisce alla ricerca di informazioni tratte da “fonti liberamente disponibili”

(non all'open source software)

Si differenzia dalla attività di Intelligence in quanto le informazioni non sono ottenute “illegalmente”

Documenti NATO su OSINT

- La sintesi delle direttive NATO si può trovare in tre pubblicazioni dove sono elencate metologie e fonti:
  - NATO Open Source Intelligence Handbook v.1.2
  - NATO Open Source Intelligence reader
  - Intelligence Exploitation of the Internet

Link: http://www.phibetaiota.net/2009/07/2422/

Cosa si può fare con OSINT

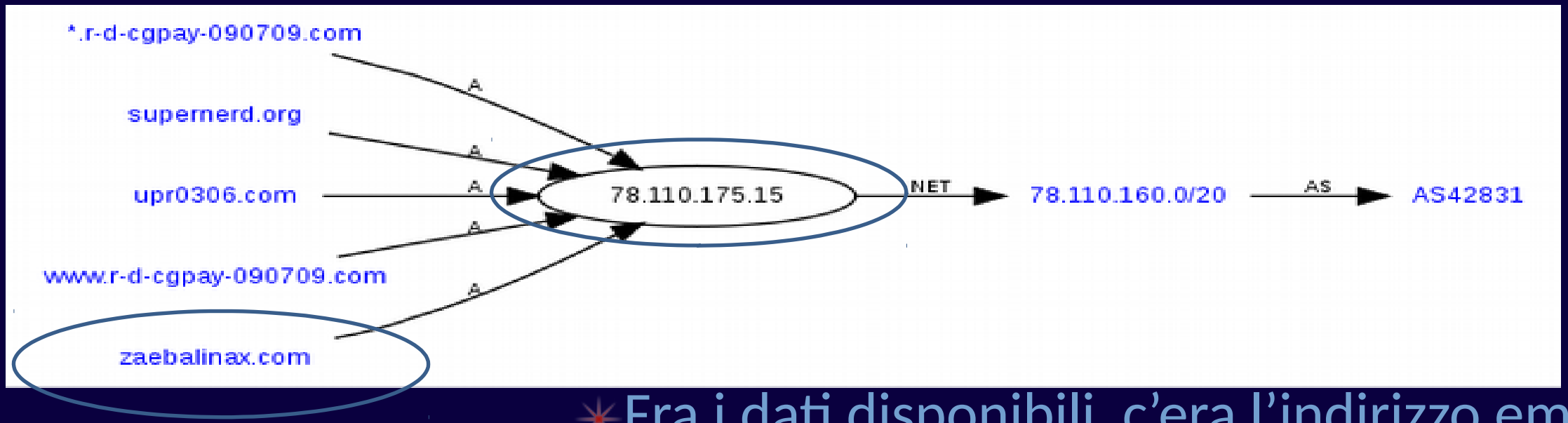
- Ricerca di informazioni su persone
- Ricerca di informazioni su aziende
- Identificare ed analizzare gruppi di varia natura
- Informazioni militari non classificate
- Ricerca informazioni scientifiche ed accademiche
- Analisi informazioni economiche
- Indagini di varia natura
- Ricerca informazioni propedeutiche a ...
- Per esempio:
  - Ricerca dipendenti scontenti (es. su Facebook)
  - Ricerca informazioni diffuse inavvertitamente
  - ...

Un esempio reale

- OSINT e Forze dell'Ordine
  - Conoscete Koobface? (https://it.wikipedia.org/wiki/Koobface)
  - Un singolo errore ha permesso ad un ricercatore dotato di pazienza e perseveranza di scoprire il numero di telefono, il nome, l'indirizzo del botnet master!

OSINT vs Koobface

- Partendo dall'analisi dell'infrastruttura di Koobface, Danchev ha semplicemente cercato tutti i domini riconducibili allo stesso IP



- Fra i dati disponibili c'era l'indirizzo email del proprietario: **krotreal@gmail.com**

OSINT vs Koobface

- Anche I criminali amano i gattini...

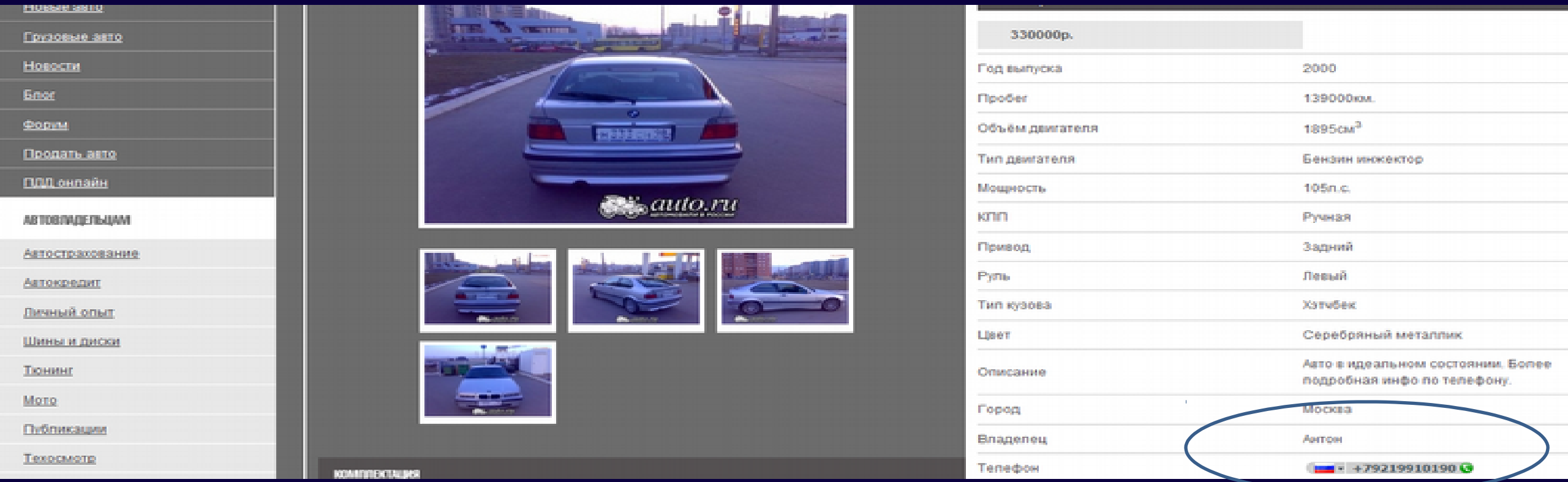
Sphynx (kitten) (St. Petersburg)
E-mail: krotreal@gmail.com

Sale Sphynx kittens.
Kittens are pedigree.
Fully immunized.
Kittens are very playful and funny.
Girl - a pure black color,
boy - a black iridescent with in tum.
Anton.
Tel. +79219910190

09/05/2007

OSINT vs Koobface

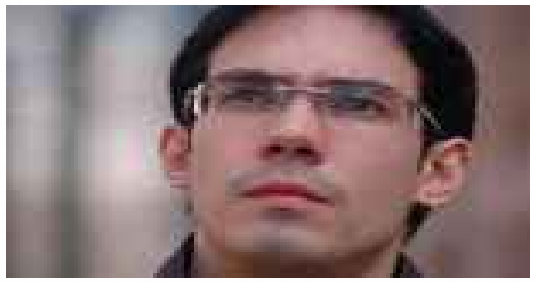
- Oops...



OSINT vs Koobface

- Nella tana del coniglio ^

Real name: Anton Nikolaevich Korotchenko (Антон Николаевич Коротченко)
City of origin: St. Petersburg
Primary address: Omskaya st. 26-61; St. Petersburg; Leningradskaya oblast,197343
Associated phone numbers obtained through OSINT analysis, not whois records:
+79219910190
+380505450601
050-545-06-01
ICQ - 444374
Emails: krotreal@yahoo.com
krotreal@gmail.com
krotreal@mail.ru
krotreal@livejournal.com
newfider@rambler.ru
WM identification (WEB MONEY) : 425099205053
Twitter account: @KrotReal; @Real_Koobface
Flickr account: KrotReal
Vkontakte.ru Account: KrotReal; tonystarx
Foursquare Account: KrotReal



The art of OSINT

Il gioco sta tutto nell'individuare le **connessioni** tra le informazioni, quasi come i detective dei film ;)

Possibili fonti

- Motori di ricerca
- Social networks
- Chat (skype, IRC, chat private,...)
- Blog, mailing lists, forum
- Siti di vendita, annunci, scambio
- Siti image e video sharing
- Siti di incontri
- Giornali, Pubblica Amministrazione, ordini professionali, camere di commercio
- Archivi pubblici, organizzazioni governative e non governative
- Siti istituzionali, Grey Literature, Deep WEB
- Servizi specializzati nella ricerca, valutazione e vendita info
- Informazioni tecniche dalla rete Internet

Metodi

- Prima di tutto: analizzare le informazioni in proprio possesso, quindi:
- Ricerca per parole chiave
- Analisi delle immagini
- Correlazione informazioni
- Analisi dell'ambiente
- Analisi dei contatti
- Analisi informazioni tecniche internet

Le basi: i motori di ricerca

Google dorks

- Le Google Dorks possono essere usate sia per scopi OSINT che per raccogliere informazioni propedeutiche ad attacchi.
- Es. installazioni di sw vulnerabili, information disclosure, ricerche all'interno di uno specifico sito, cercare uno specifico tipo di file …

- http://www.exploit-db.com/google-dorks/
- http://www.hackersforcharity.org/ghdb/
- http://gabrieleromanato.altervista.org/traduzioni/googleguide.pdf

Google dorks esempi

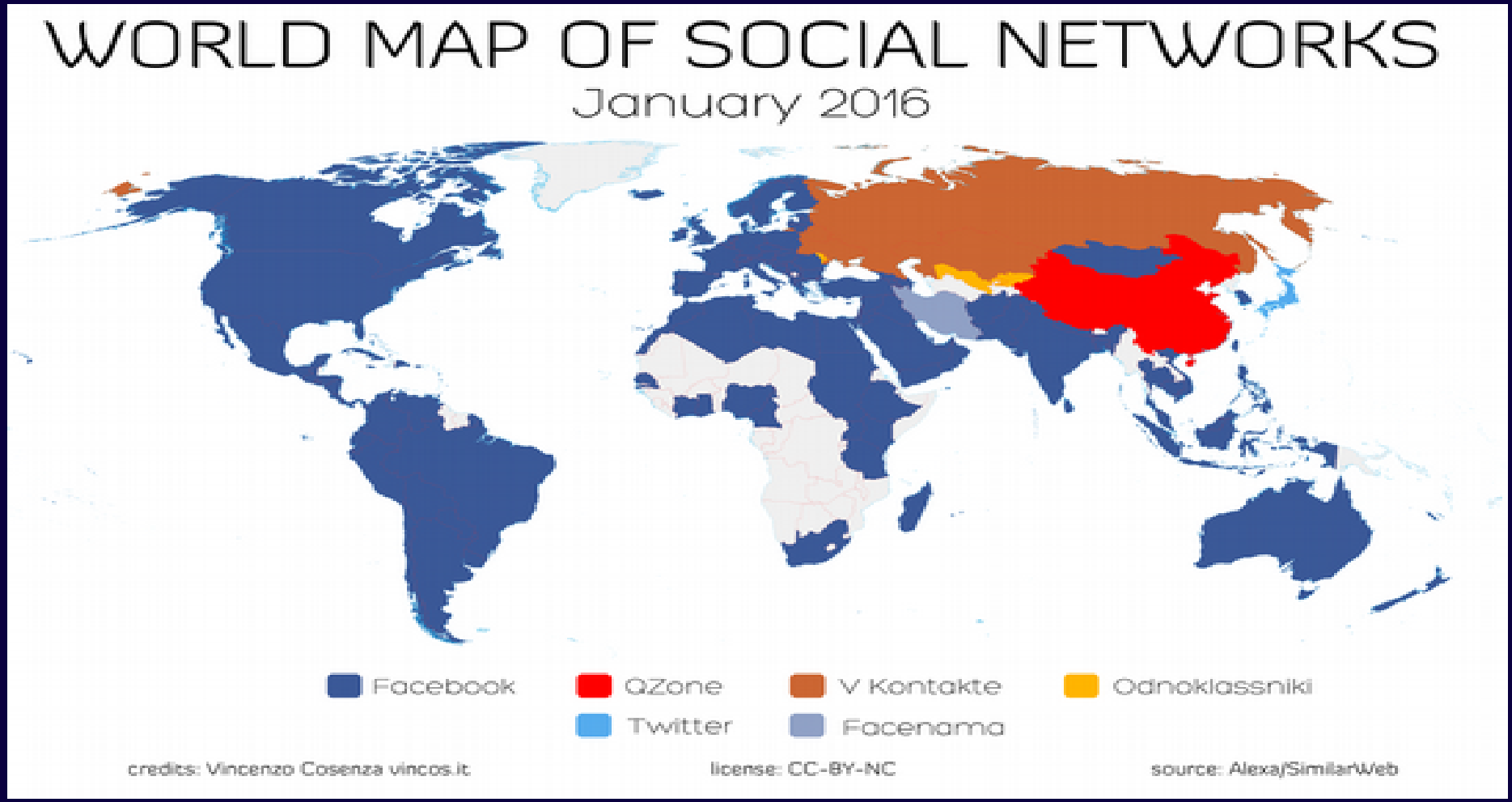
Usando le “chiavi” giuste è possibile effettuare ricerche molto specifiche

- inurl:phpbb1.txt
- site:clusit.it filetype:pdf
- site:governo.it filetype:doc
- Allintext:frode informatica carta credito

https://support.google.com/websearch/answer/2466433?hl=it
https://www.google.com/advanced_search

Social networks

- “The Big Ones”
  - Facebook
  - Twitter
  - Google+
- “The Dinosaurs”
  - Myspace
- Media/Vanity
  - Instagram
  - Flickr
  - Vine
  - Foursquare
  - Youtube
- Country based
  - Weibo (Cina)
  - Vkontakte (Russia)
  - Tuenti (Spagna)
  - Qzone (Cina)
- Professional
  - Linkedin



Non dimenticare ORKUT(*): chiuso ma l’archivio è online

*Orkut è stato il più diffuso SN in Brasile ed India

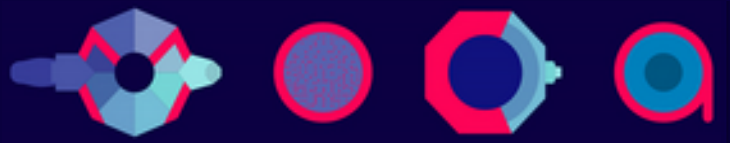
Facebook

- Facebook, con I suoi milioni di utenti, è terreno di caccia fertile
- FB Graph Search è una funzionalità introdotta nel 2013 ed in continua evoluzione
- E’ possibile effettuare ricerche di parole chiave
- E’ possibile creare “query”specifiche
- La struttura della richiesta cambia con le versioni del motore interno

Facebook Graph Search

E’ possibile effettuare ricerche con un linguaggio simile a quello umano:

- People who work at FIAT USA
- people who like a.c. milan
- people who live in milan, italy and like beatles
- pages liked by Matteo Renzi
- movies liked by people who like Matteo Renzi



Facebook Graph Search

E’ possibile effettuare ricerche avanzate tramite speciali le speciali funzioni messe a disposizione da FB Graph search

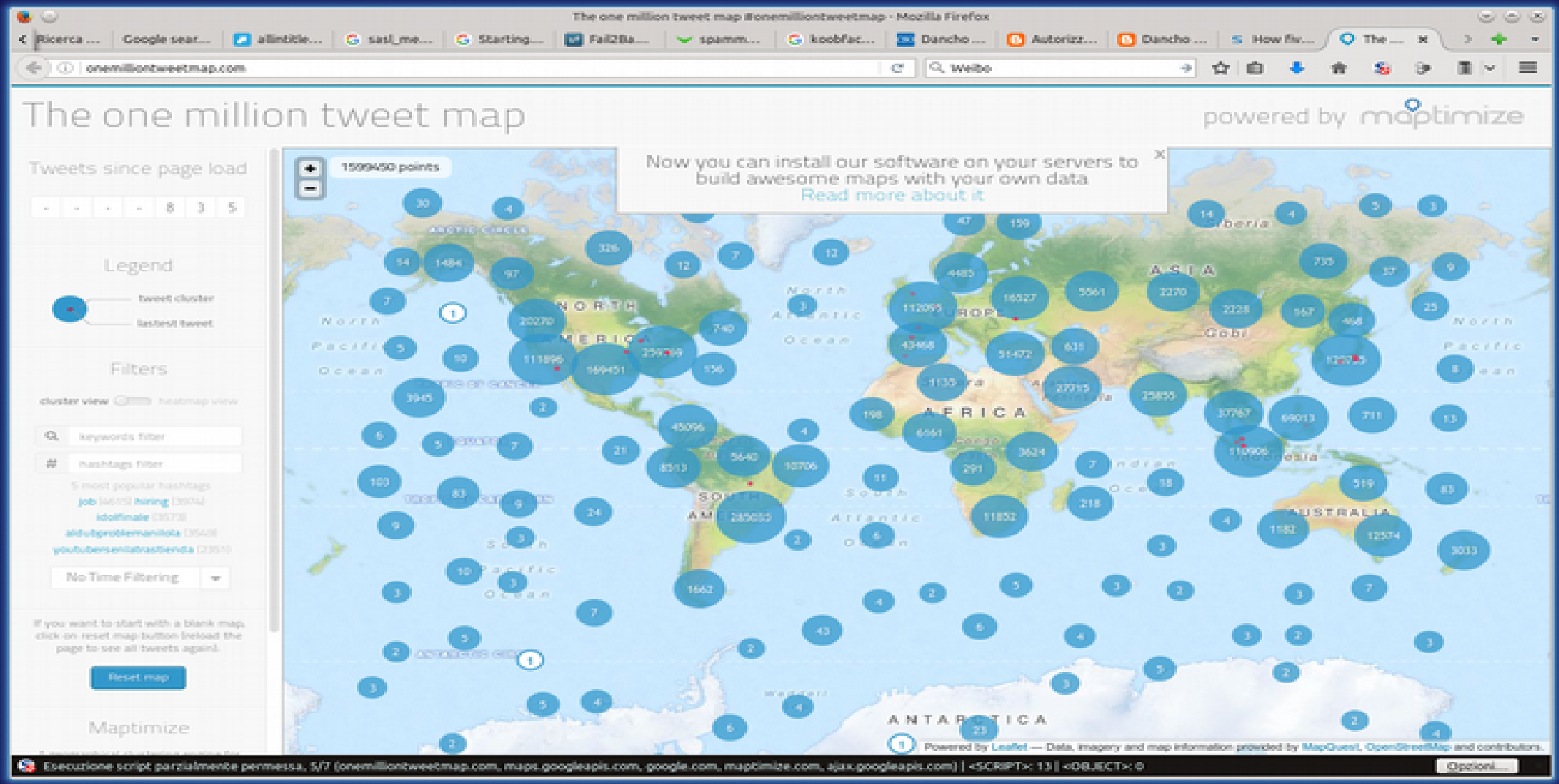
- https://www.facebook.com/friendship/username1/username2/
- https://www.facebook.com/search/USERID1/photos-liked
- https://www.facebook.com/search/USERID/photos-of
- https://www.facebook.com/search/USERID/friends
- https://www.facebook.com/search/USERID/friends/pages-liked

Twitter Search

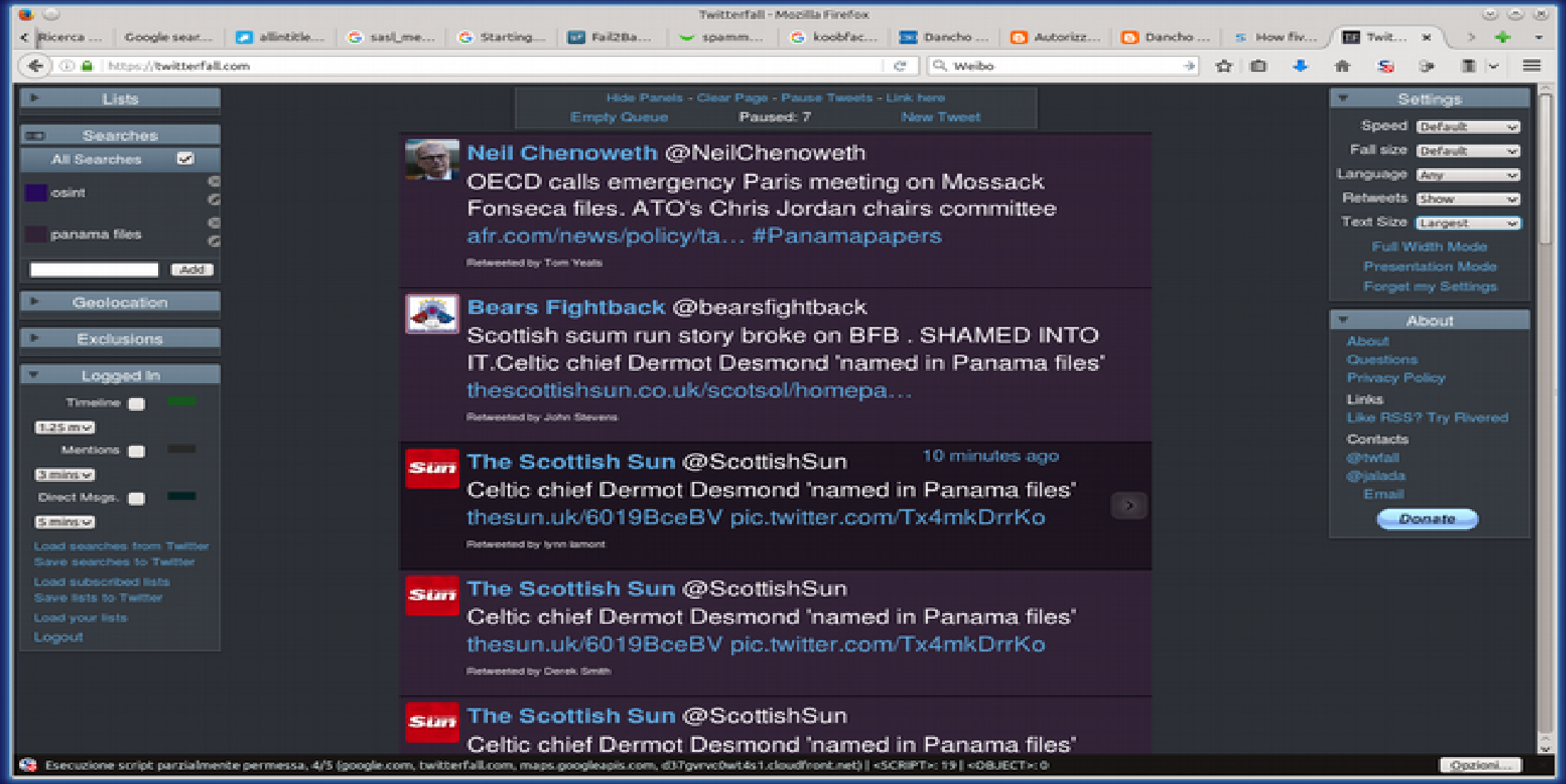
- Anche Twitter, con i suoi milioni di utenti, è un grande serbatoio di informazioni
- Oltre agli strumenti interni, ne esistono anche alcuni online che sfruttano le sue API

- https://twitter.com/search-advanced
- http://onemilliontweetmap.com/
- https://twitterfall.com

Twitter: the one million tweet map



Twitterfall



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

Comunità virtuali

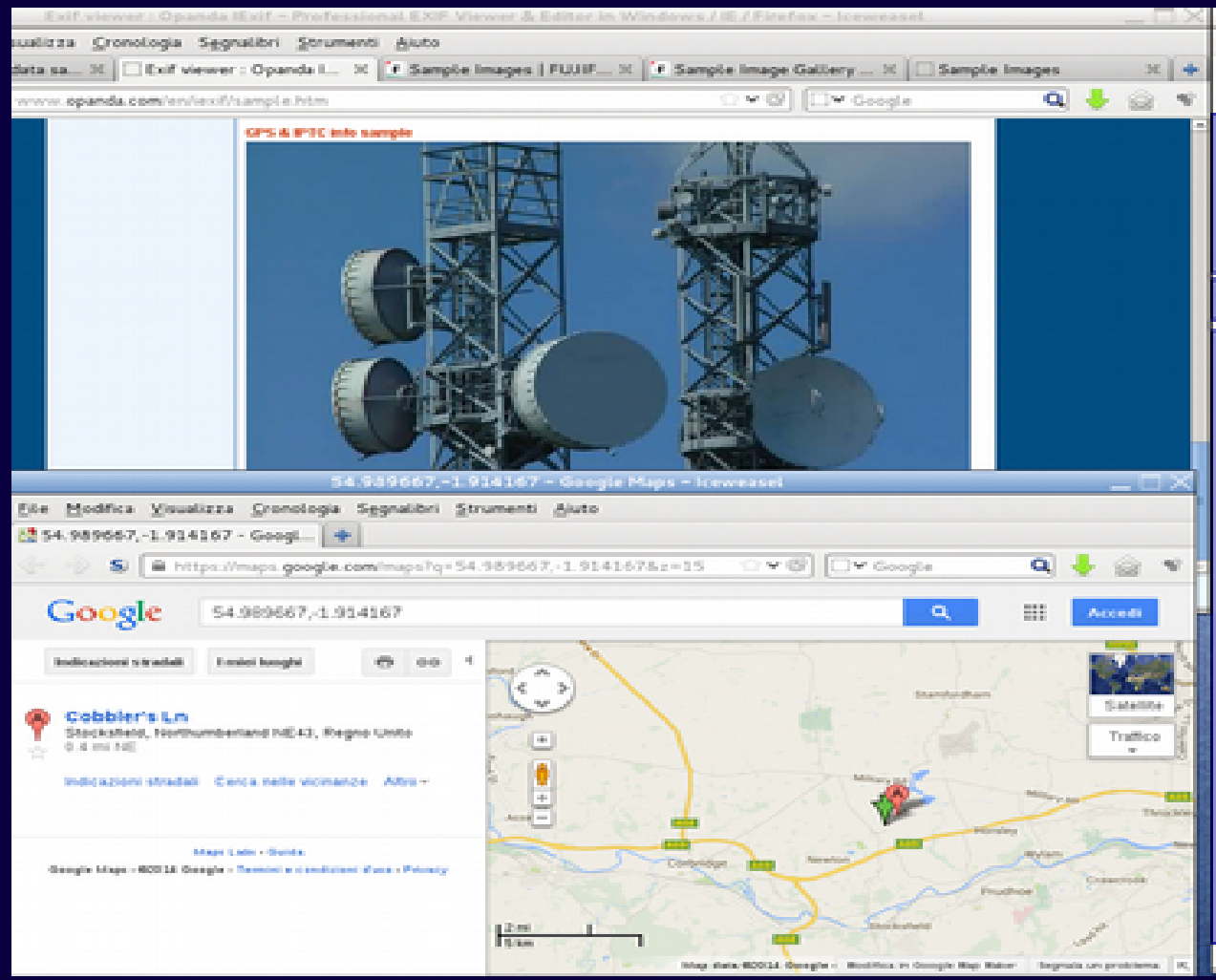
- “Everything that doesn’t fit into Social Networks”
  - Forums
  - Mailing lists
  - Blogs (senza contare i microblogging)
  - Online chat rooms (IRC)
  - Gaming - Playstation, Xbox Live, Steam
  - Virtual worlds
  - Dating sites
  - …

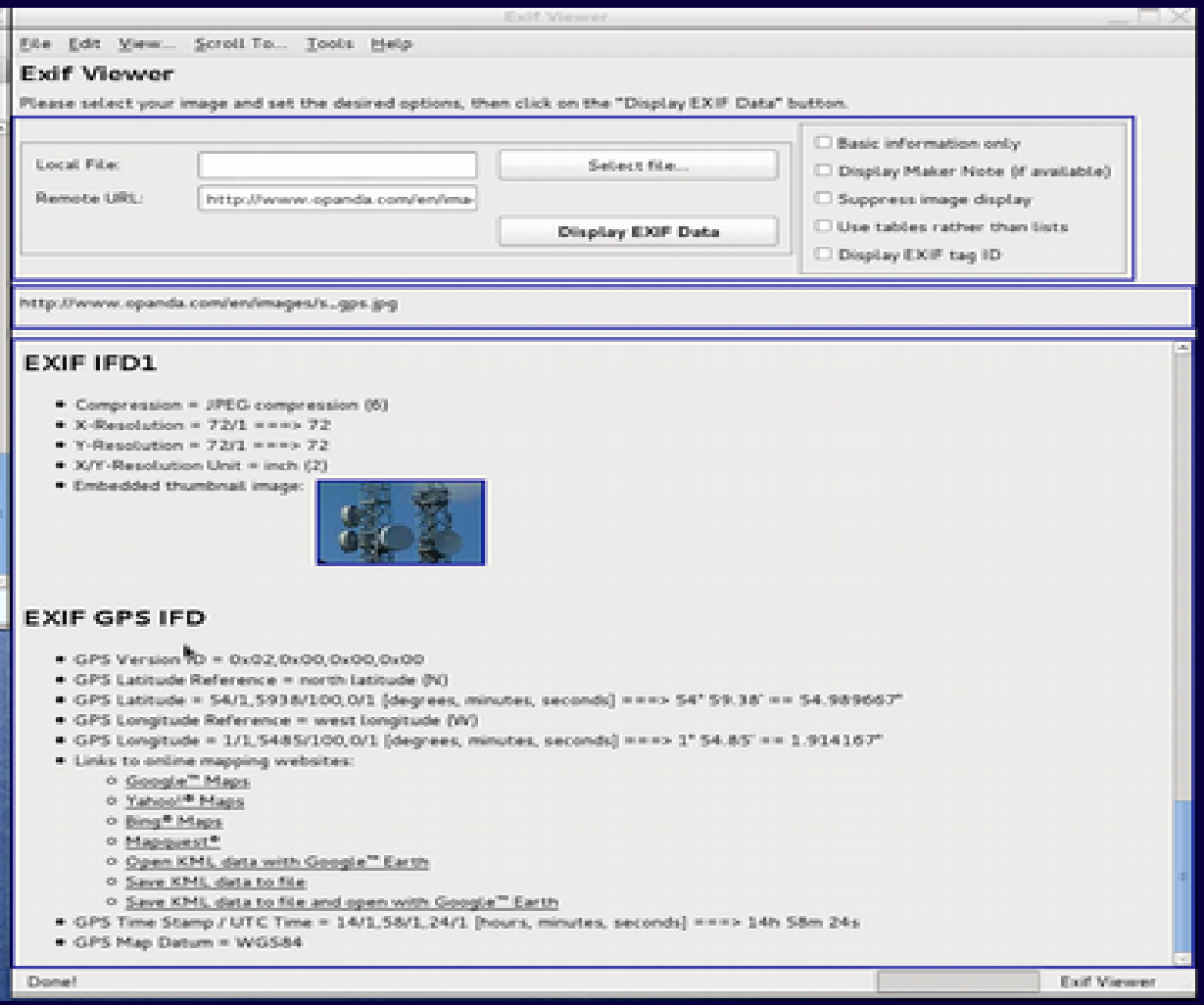
Quello che le foto...

- I dati EXIF possono rivelare:
  - Fotocamera utilizzata, caratteristiche della foto
    - Utilità: poter ricondurre una foto ad una macchina/utente
  - Data ed ora dello scatto
  - Posizione geografica
- Uno dei tanti tools (ci sono anche tool online)
  https://addons.mozilla.org/it/firefox/addon/exif-viewer/

NB: la maggior parte dei siti (Facebook, ecc) rimuovono tutti i dati EXIF o almeno i dati GPS

Quello che le foto...Exif viewer





19-20-21 agosto 2016

Parco Ex Caserma Cocco
Pescara

Analisi delle immagini

- Da una immagine si possono avere molte **informazioni** oltre a quelle dei dati EXIF
  - Esaminare il soggetto, l'ambiente, le persone, la situazione, il contesto
  - Esaminare dove è stata reperita (sito web , social, ...)
  - Individuare altre informazioni disponibili in rete effettuando una ricerca *"per immagine"*

    https://www.tineye.com/
  - Provate I servizi come "Stolen camera finder"

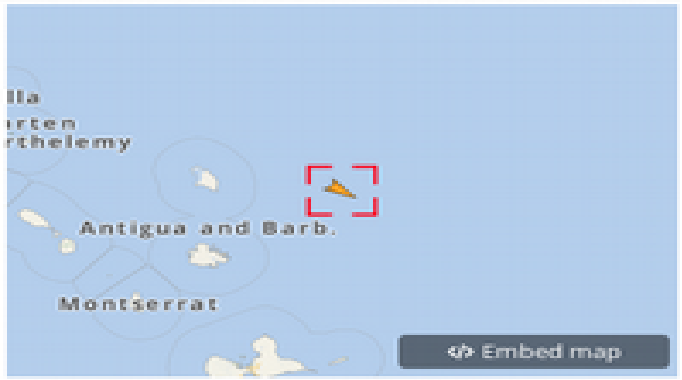
    http://www.stolencamerafinder.com/

Analizziamo le immagini

Analizziamo le immagini

Analizziamo le immagini

SAIQ map position



SAIQ AIS Data

Ultima segnalazione:	Feb 29, 2016 13:13 UTC
Tipo di imbarcazione:	Crude Oil Tanker
Bandiera:	Panama
Destinazione:	SIKKA
ETA:	Apr 02, 12:00
Lat/Lon:	17.53946 N/61.01841 W
Rotta/Velocità:	129.3 ° / 11.6 kn.
Pescaggio attuale:	21.6 m
Identificativo di chiamata:	3EZD4
IMO / MMSI:	9406166 / 355705000

Last updated:	Mar 30, 2016
IMO number:	9406166
Call sign:	3EZD4
Summer DWT:	299999.00 MT
Built:	Apr 13, 2011
Owner:	SAIQ MARITIME TRANSPORTATION COMPANY S.A
Operator:	OMAN SHIP MANAGEMENT COMPANY S.A.O.C.

SAIQ Master Data

Costruita:	2011	GT:	156935 t
Dimensione:	330 x 60 m	NT:	99000 t
Pescaggio:	21.5 m	DWT:	299999 t
TEU:	Premium users only	Crude (bbl):	Premium users or
Builder:	Premium users only	Owner:	Premium users or
Place of build:	Premium users only	Manager:	Premium users or

Ultimi cinque porti di scalo come sono stati riportati da AIS

Data / Ora	Porto / Nazione
Feb 01, 2016, 09:04 UTC	GIBRALTAR, GIBRALTAR
Oct 08, 2015, 11:01 UTC	RAS TANURA, SAUDI ARABIA
Apr 23, 2015, 08:04 UTC	JU'AYMAH CRUDE & LPG TERMINALS, SAU

SAIQ

Show vessel's track
Possible Destinations
Distance to...
Port Calls
Vessel Details
Add to fleet

Changed from **ST EUSTATIUS** on **2016-02-29 06:59**

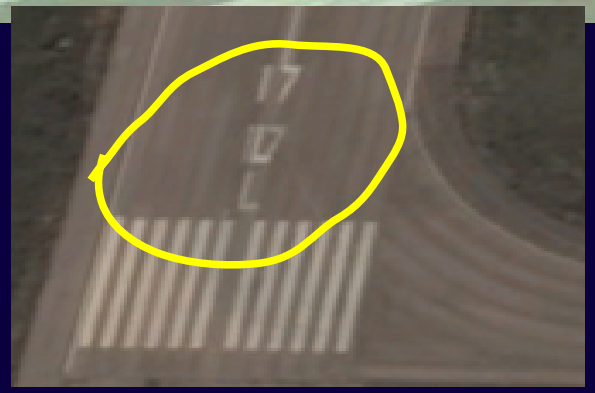
MMSI 355705000	21.6 m
Type Crude Oil Tanker	Destination SIKKA
Size 330 x 60 m	ETA 2016-04-02 12:00 UTC
Flag Panama[PA]	Data Received 2016-02-29 13:59
Position -31.19198° / 32.05032°	Status Under way using engine
Course 46.5°	Station ---
Speed 10.2 Knots	Position Received 2016-03-23 14:43:00

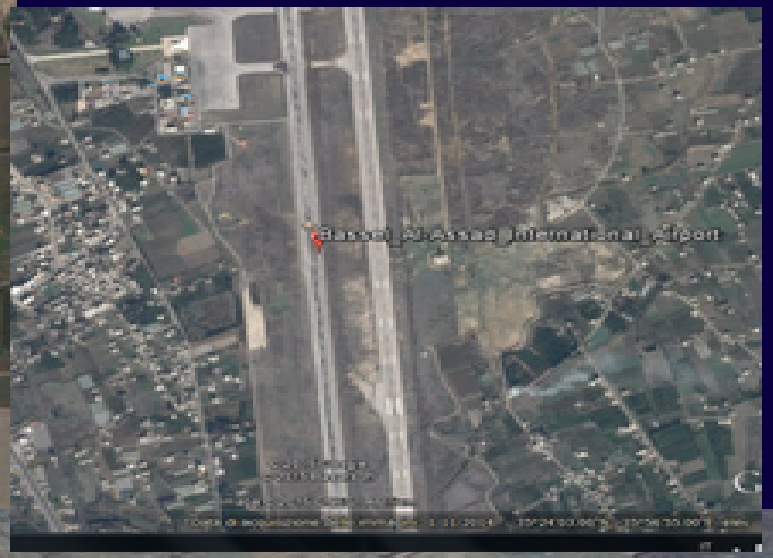
Un esempio

Ecco un post su twitter del 21 settembre 2015:
#Syria : Supposedly first pic of Russian jets on ground from the ground at #Latakia airport
https://twitter.com/finriswolf/status/646210662973091840
Come possiamo verificare l'esattezza dell'informazione?

1. Cerco su wikipedia l'aeroporto di Latakia,Bassel Al-Assad
2. Aprendo la pagina di Wikipedia posso avere le geo coordinate
3. Click su geo coordinate per aprire la pagina web con i link a servizi di mappe https://tools.wmflabs.org
4. Click su servizio scelto (es. Google Earth)
5. Esamino i segni sulla pista dell'aeroporto e li confronto con quelli presenti nelle immagini di Google Earth
6. Confronto il panorama (colline) sulla foto con le immagini di Google Earth
7. Confronto l'edificio che sembra una antenna radar sulla foto con le immagini di Google Earth
8. Posso infine identificare il tipo di aerei ritratti

Un esempio

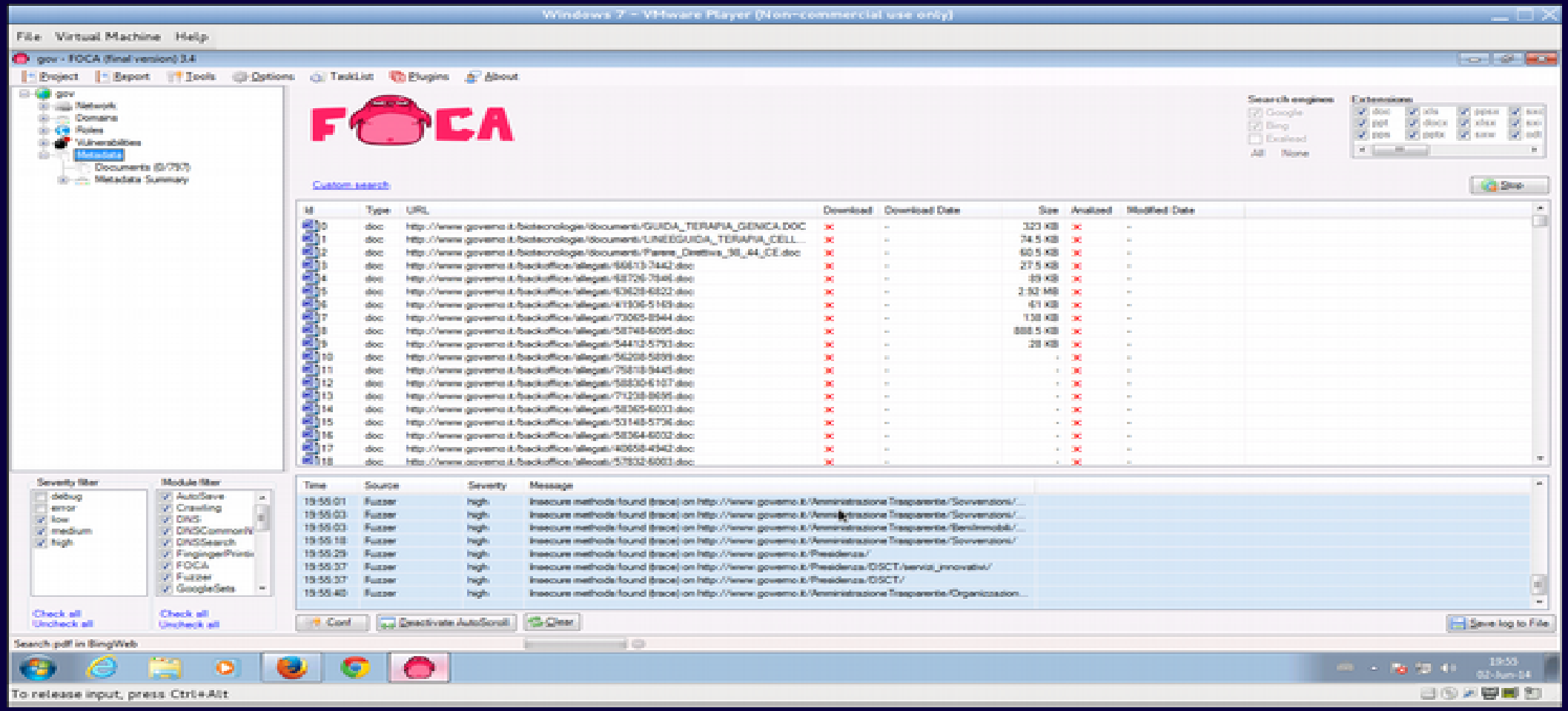




Metadati

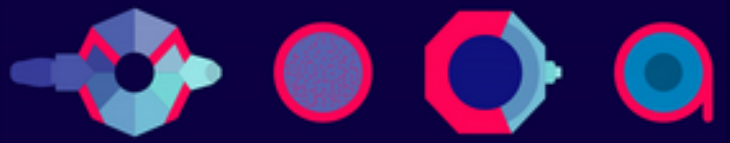
- I metadati sono le informazioni nascoste all'interno dei file
- L'analisi dei metadati di un file può portare interessanti risultati: nome utente, data creazione, versione software, utili ad esempio per restringere il campo di indagine

Fear the FOCA



Geolocalizzazione

- Riuscire a posizionare fisicamente il luogo dove si trova il soggetto di una ricerca può avere un valore inestimabile
- Esistono strumenti in grado, a seconda del contesto, di indicare più o meno precisamente la località dalla quale è stata effettuata un contatto su una rete (mobile, Internet)



Un esempio

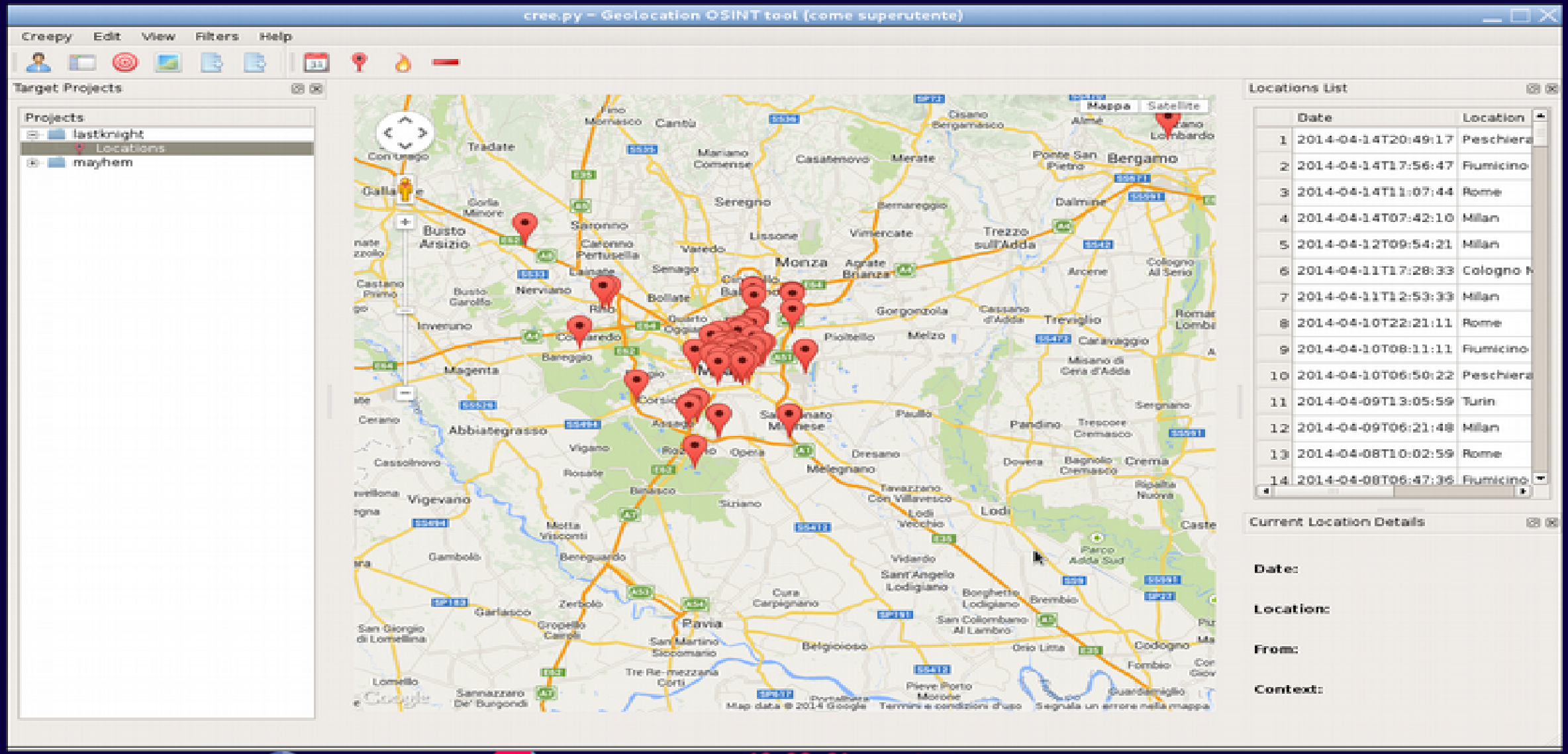
- E’ possibile effettuare una geolocalizzazione a partire da:
  - Un indirizzo IP
  - Un numero di telefono o di cellulare
  - Un indirizzo Skype
  - Un account Twitter
  - Un account Instagram
  - Una foto postata
  - Una rete WiFi
  - …

Creepy

- Creepy permette di risalire alla posizione geografica di un soggetto in base ai dati rivelati dai social networks quali Twitter o dai metadati di immagini tratte da Flickr, Instagram, Google plus

http://www.geocreepy.com/
http://github.com/ilektrojohn/creepy/

Un esempio


cree.py – Geolocation OSINT tool (come superutente)
Creepy
Edit
View
Filters
Help
Target Projects
Projects
lastknight
Locations
mayhem
Locations List
Date
Location
1 2014-04-14T20:49:17 Peschiera
2 2014-04-14T17:56:47 Fiumicino
3 2014-04-14T11:07:44 Rome
4 2014-04-14T07:42:10 Milan
5 2014-04-12T09:54:21 Milan
6 2014-04-11T17:28:33 Cologno
7 2014-04-11T12:53:33 Milan
8 2014-04-10T22:21:11 Rome
9 2014-04-10T08:11:11 Fiumicino
10 2014-04-10T06:50:22 Peschiera
11 2014-04-09T13:05:59 Turin
12 2014-04-09T06:21:48 Milan
13 2014-04-08T10:02:59 Rome
14 2014-04-08T06:47:36 Fiumicino
Current Location Details
Date:
Location:
From:
Context:
Mappa
Satellite

Conclusioni

Il mondo dell'OSINT è molto, molto più vasto
di quanto abbiamo visto oggi
Le metodologie utilizzabili evolvono ogni giorno
I risultati spesso sono sopra le aspettative

Molto spesso
sono proprio i dati pubblicati dagli stessi utenti
a permettere questi risultati

Software

- XMIND (http://www.xmind.net/) **XMind** is the most professional and popular mind mapping tool
- FOCA (https://www.elevenpaths.com/labstools/foca/index.html) **FOCA** (Fingerprinting Organizations with Collected Archives) is a tool used mainly to find metadata and hidden information in the documents it scans.
- MALTEGO (https://www.paterva.com/web6/products/maltego.php) **Maltego** is a unique platform developed to deliver a clear threat picture to the environment that an organization owns and operates.
- CREEPY (http://github.com/ilektrojohn/creepy/) **Creepy** is a Geolocation OSINT Tool. Offers geolocation information gathering through social networking platforms
- EXIF VIEWER (https://addons.mozilla.org/it/firefox/addon/exif-viewer/) **Exif Viewer** is an add-on for Firefox. Displays the Exif and IPTC data in local and remote JPEG images
- TOR BROWSER (https://www.torproject.org/projects/torbrowser.html.en) The **Tor Browser** lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software

Strumenti e documentazione

- http://www.phibetaiota.net/wp-content/uploads/2014/01/Ben-Benavides-Social-Web-Sites-A-Guide.pdf
- http://www.phibetaiota.net/2014/01/ben-benavides-exploring-social-media-web-sites-a-guide-for-the-open-source-analyst/
- http://www.onstrat.com/osint/
- site://www.css.ethz.ch osint
- http://www.phibetaiota.net/wp-content/uploads/2013/07/2013-07-11-OSINT-2ool-Kit-On-The-Go-Bag-O-Tradecraft.pdf
- http://www.difesaonline.it/index.php/it/15-notizie/approfondimenti/280-la-demodoxalogia-l-osint-open-source-intelligence-italiana
- http://rr.reuser.biz/
- https://twitter.com/OSINTCenter

OSINT
Open Source Intelligence

Grazie per la vostra attenzione

Paolo ‘aspy’ Giardini

19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara