



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



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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”



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

Documenti NATO su OSINT

- * La sintesi delle direttive NATO si può trovare in tre pubblicazioni dove sono elencate metodologie 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/>



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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
 - * ...



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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!

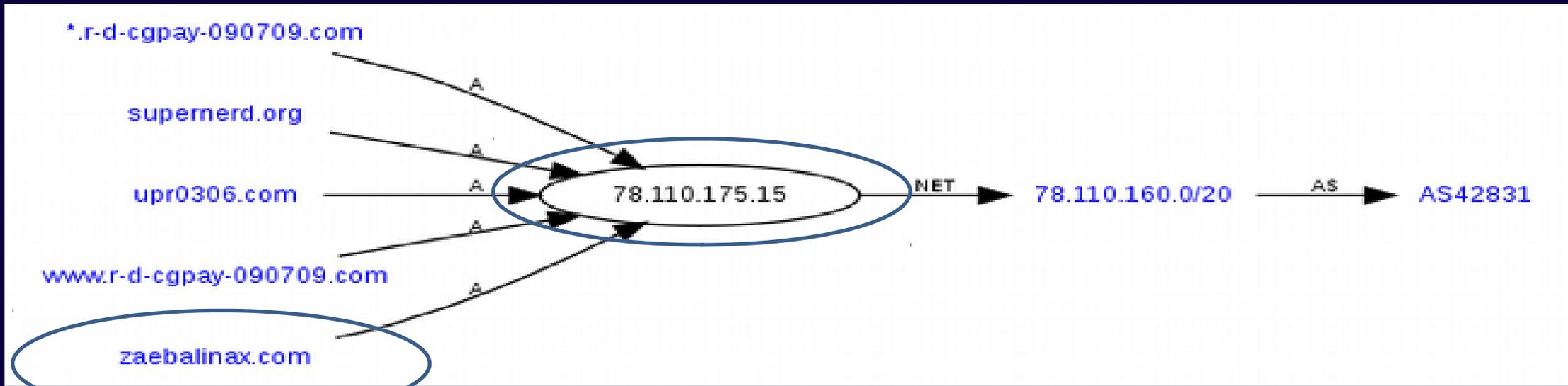


19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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`



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

OSINT vs Koobface

*Oops...

330000р.	
Год выпуска	2000
Пробег	139000км.
Объем двигателя	1895см ³
Тип двигателя	Бензин инжектор
Мощность	105л.с.
КПП	Ручная
Привод	Задний
Руль	Левый
Тип кузова	Хэтчбек
Цвет	Серебряный металлик
Описание	Автомобиль в идеальном состоянии. Более подробная информация по телефону.
Город	Москва
Владелец	Антон
Телефон	+799219910190



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

The art of OSINT

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



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

Le basi: i motori di ricerca



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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>



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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

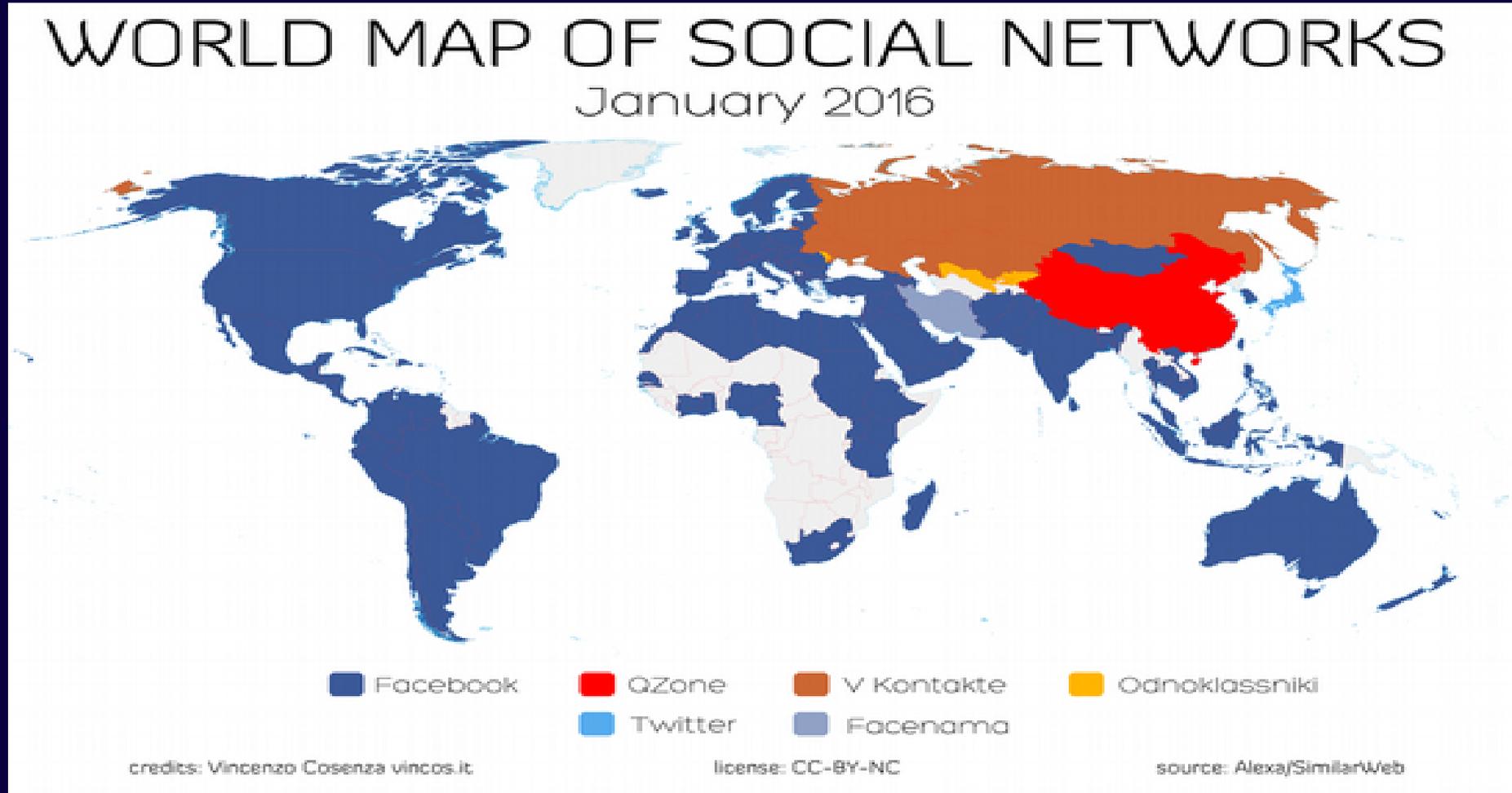


19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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>



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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>



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

Twitter: the one million tweet map

The screenshot shows a web browser window displaying the website "The one million tweet map". The browser's address bar shows the URL "onemilliontweetmap.com". The page title is "The one million tweet map" and it is "powered by maptimize".

The main content is a world map with numerous blue circular markers of varying sizes, each containing a number representing the number of tweets in that cluster. The map is titled "1500450 points". A text box on the map says: "Now you can install our software on your servers to build awesome maps with your own data. Read more about it".

On the left side, there is a sidebar with the following sections:

- Tweets since page load:** A row of buttons with numbers: "-", "-", "-", "-", "8", "3", "5".
- Legend:** A blue circle icon labeled "tweet cluster" and a red dot icon labeled "fastest tweet".
- Filters:** Includes "cluster view" (selected) and "heatmap view", a "keywords filter" input field, a "hashtags filter" input field, and a list of "5 most popular hashtags": "job (3004)", "hiring (2904)", "idolfinale (2572)", "aldubproblemanicola (2540)", and "youtuberorientalastrenda (2310)". There is also a "No Time Filtering" dropdown menu.
- Reset map:** A button with the text "Reset map".
- Maptimize:** The logo for the mapping service.

At the bottom of the browser window, there is a status bar with the text: "Esecuzione script parzialmente permessa, 5/7 (onemilliontweetmap.com, maps.googleapis.com, google.com, maptimize.com, ajax.googleapis.com) | <SCRIPT>: 13 | <OBJECT>: 0".



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

Twitterfall

Twitterfall - Mozilla Firefox
https://twitterfall.com

Hide Panels - Clear Page - Pause Tweets - Link here
Empty Queue Paused: 7 New Tweet

Neil Chenoweth @NeilChenoweth
OECD calls emergency Paris meeting on Mossack Fonseca files. ATO's Chris Jordan chairs committee
afr.com/news/policy/ta... #Panamapapers
Retweeted by Tom Yeats

Bears Fightback @bearsfightback
Scottish scum run story broke on BFB . SHAMED INTO IT.Celtic chief Dermot Desmond 'named in Panama files'
thescottishsun.co.uk/scotsol/homepa...
Retweeted by John Stevens

The Scottish Sun @ScottishSun 10 minutes ago
Celtic chief Dermot Desmond 'named in Panama files'
thesun.uk/6019BceBV pic.twitter.com/Tx4mkDrrKo
Retweeted by Lynn Lamont

The Scottish Sun @ScottishSun
Celtic chief Dermot Desmond 'named in Panama files'
thesun.uk/6019BceBV pic.twitter.com/Tx4mkDrrKo
Retweeted by Derek Smith

The Scottish Sun @ScottishSun
Celtic chief Dermot Desmond 'named in Panama files'

Esecuzione script parzialmente permessa, 4/5 [google.com, twitterfall.com, maps.googleapis.com, d07gvrvcbw4x1.cloudfront.net] <SCRIPT>: 19 | <OBJECT>: 0

Settings
Speed Default
Fall size Default
Language Any
Retweets Show
Text Size Largest
Full Width Mode
Presentation Mode
Forget my Settings

About
About
Questions
Privacy Policy
Links
Like RSS? Try Rivered
Contacts
@twfall
@jalada
Email
Donate



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
 - * ...



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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/>

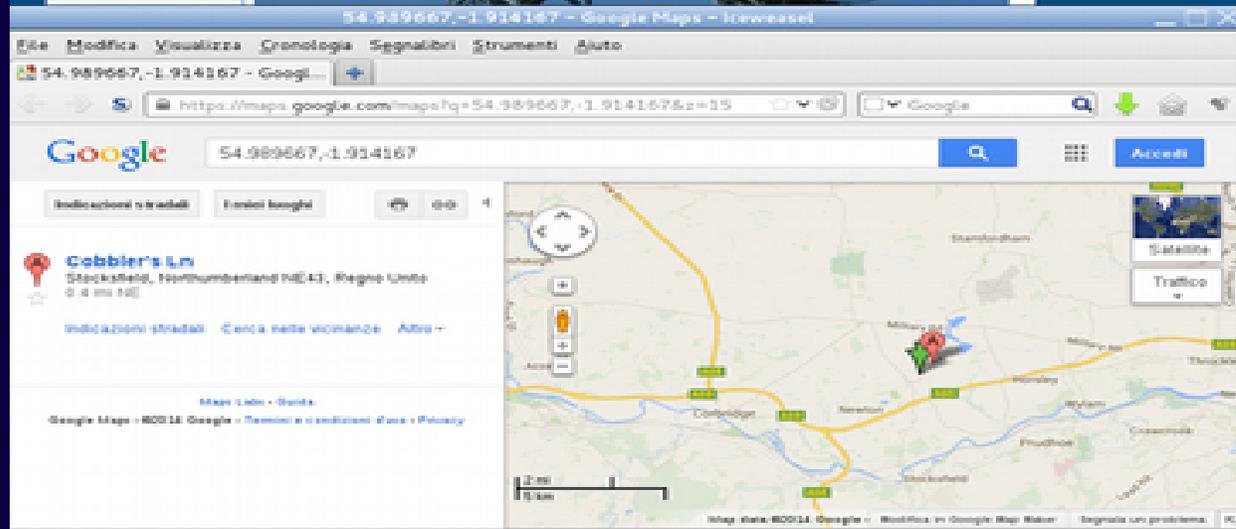
NB: la maggior parte dei siti (Facebook, ecc) rimuovono tutti i dati EXIF o almeno i dati GPS



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

Quello che le foto...Exif viewer



Exif Viewer

Please select your image and set the desired options, then click on the "Display EXIF Data" button.

Local File:

Remote URL:

Basic information only
 Display Maker Note (if available)
 Suppress image display
 Use tables rather than lists
 Display EXIF tag ID

<http://www.opanda.com/en/images/e...gps.jpg>

EXIF IFD1

- Compression = JPEG compression (8)
- X-Resolution = 72/1 ==> 72
- Y-Resolution = 72/1 ==> 72
- X/Y-Resolution Unit = inch (2)
- Embedded thumbnail image: 

EXIF GPS IFD

- GPS Version ID = 0x02,0x00,0x00,0x00
- GPS Latitude Reference = north latitude (N)
- GPS Latitude = 54/1,5938/100,0/1 [degrees, minutes, seconds] ==> 54° 59.38' == 54.989667°
- GPS Longitude Reference = west longitude (W)
- GPS Longitude = 1/1,5485/100,0/1 [degrees, minutes, seconds] ==> 1° 54.85' == 1.914167°
- Links to online mapping websites:
 - [Google™ Maps](#)
 - [Yahoo!™ Maps](#)
 - [Bing® Maps](#)
 - [Mapquest™](#)
 - [Open KML data with Google™ Earth](#)
 - [Save KML data to file](#)
 - [Save KML data to file and open with Google™ Earth](#)
- GPS Time Stamp / UTC Time = 14/1,58/1,24/1 [hours, minutes, seconds] ==> 14h 58m 24s
- GPS Map Datum = WGS84

Done!



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/>



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

Analizziamo le immagini



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

Analizziamo le immagini



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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:	3E2D4
IMO / MMSI:	9406166 / 355705000

Last updated:	Mar 30, 2016
IMO number:	9406166
Call sign:	3E2D4
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 (bbt):	Premium users only
Builder:	Premium users only	Owner:	Premium users only
Place of build:	Premium users only	Manager:	Premium users only

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, SAUDI ARABIA

SAIQ

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



MMSI: 355705000
Type: Crude Oil Tanker
Size: 330 x 60 m
Flag: Panama[PA]

Position: -31.19198° / 32.05032°
Course: 46.5°
Speed: 10.2 Knots

Destination: SIKKA
ETA: 2016-04-02 12:00 UTC
Data Received: 2016-02-29 13:59

Status: Under way using engine
Station: ---
Position Received: 2016-03-23 14:43:00

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



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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?

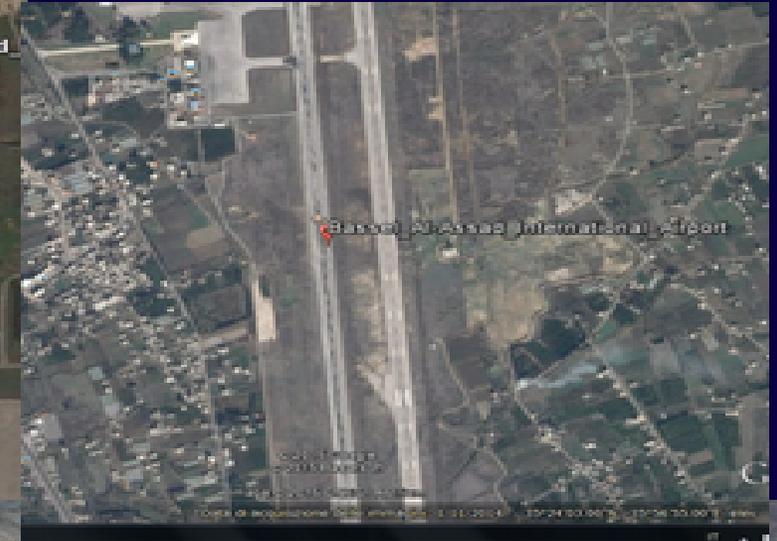
1. Cerco su wikipedia l'aeroporto di Latakia, Bassel Al-Assad
2. Aprendo la pagina di Wikipedia posso avere le geo coordinate
3. Click su geo coordinate per aprire la pagina web con i link a servizi di mappe
<https://tools.wmflabs.org>
4. Click su servizio scelto (es. Google Earth)
5. Esamino i segni 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



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

Un esempio



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

Fear the FOCA

File Virtual Machine Help

gov - FOCA (final version) 3.4

Project Report Tools Options TaskList Engines About

gov

- Network
- Domains
- Roles
- Vulnerabilities
- Metadata
 - Documents (8/797)
 - Metadata Summary

Search engines: Google, Bing, Ecindex, All, None

Extensions: doc, ppt, xls, docx, pptx, xlsx, xlsx, xml, xml, xml, xml

Custom search

ID	Type	URL	Download	Download Date	Size	Analyzed	Modified Date
0	doc	http://www.governo.it/biotecnologie/documenti/GUIDA_TERAPIA_GENICA.DOC	OK	--	323 KB	OK	--
1	doc	http://www.governo.it/biotecnologie/documenti/LINEEGUIDA_TERAPIA_CELL...	OK	--	24.5 KB	OK	--
2	doc	http://www.governo.it/biotecnologie/documenti/Parere_Direttiva_M_4_CG.doc	OK	--	60.5 KB	OK	--
3	doc	http://www.governo.it/backoffice/illegal/56613-5442.doc	OK	--	27.5 KB	OK	--
4	doc	http://www.governo.it/backoffice/illegal/63726-7146.doc	OK	--	69 KB	OK	--
5	doc	http://www.governo.it/backoffice/illegal/63628-6323.doc	OK	--	1.93 MB	OK	--
6	doc	http://www.governo.it/backoffice/illegal/41306-5145.doc	OK	--	61 KB	OK	--
7	doc	http://www.governo.it/backoffice/illegal/73005-8044.doc	OK	--	138 KB	OK	--
8	doc	http://www.governo.it/backoffice/illegal/58748-6005.doc	OK	--	888.5 KB	OK	--
9	doc	http://www.governo.it/backoffice/illegal/54413-5193.doc	OK	--	28 KB	OK	--
10	doc	http://www.governo.it/backoffice/illegal/56208-5699.doc	OK	--	1 KB	OK	--
11	doc	http://www.governo.it/backoffice/illegal/75818-8443.doc	OK	--	1 KB	OK	--
12	doc	http://www.governo.it/backoffice/illegal/58304-6107.doc	OK	--	1 KB	OK	--
13	doc	http://www.governo.it/backoffice/illegal/71238-8435.doc	OK	--	1 KB	OK	--
14	doc	http://www.governo.it/backoffice/illegal/58365-6003.doc	OK	--	1 KB	OK	--
15	doc	http://www.governo.it/backoffice/illegal/53148-5196.doc	OK	--	1 KB	OK	--
16	doc	http://www.governo.it/backoffice/illegal/58364-6003.doc	OK	--	1 KB	OK	--
17	doc	http://www.governo.it/backoffice/illegal/40608-4042.doc	OK	--	1 KB	OK	--
18	doc	http://www.governo.it/backoffice/illegal/57832-6003.doc	OK	--	1 KB	OK	--

Time Source Severity Message

19:58:01	Fuzzer	high	Insecure methods found (brace) on http://www.governo.it/Administratore Trasparente/Sovvenzioni/...
19:58:03	Fuzzer	high	Insecure methods found (brace) on http://www.governo.it/Amministrazione Trasparente/Sovvenzioni/...
19:58:03	Fuzzer	high	Insecure methods found (brace) on http://www.governo.it/Administratore Trasparente/Sovvenzioni/...
19:58:18	Fuzzer	high	Insecure methods found (brace) on http://www.governo.it/Administratore Trasparente/Sovvenzioni/...
19:58:29	Fuzzer	high	Insecure methods found (brace) on http://www.governo.it/Presidenza/
19:58:37	Fuzzer	high	Insecure methods found (brace) on http://www.governo.it/Presidenza/DSCT/servizi_innovativi/
19:58:37	Fuzzer	high	Insecure methods found (brace) on http://www.governo.it/Presidenza/DSCT/
19:58:40	Fuzzer	high	Insecure methods found (brace) on http://www.governo.it/Administratore Trasparente/Organizzazion...

Severita filter: debug, error, low, medium, high

Module filter: AutoSave, Creating, DNS, DNSCommonW, DNSSearch, Fingerprint, FOCA, Fuzzer, GoogleSets

Check all / Uncheck all

Conf Deactivate AutoScroll Clear Save log to File

Search pdf in BingWeb

To release input, press Ctrl+Alt



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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)



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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
 - *...



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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/>



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

Un esempio

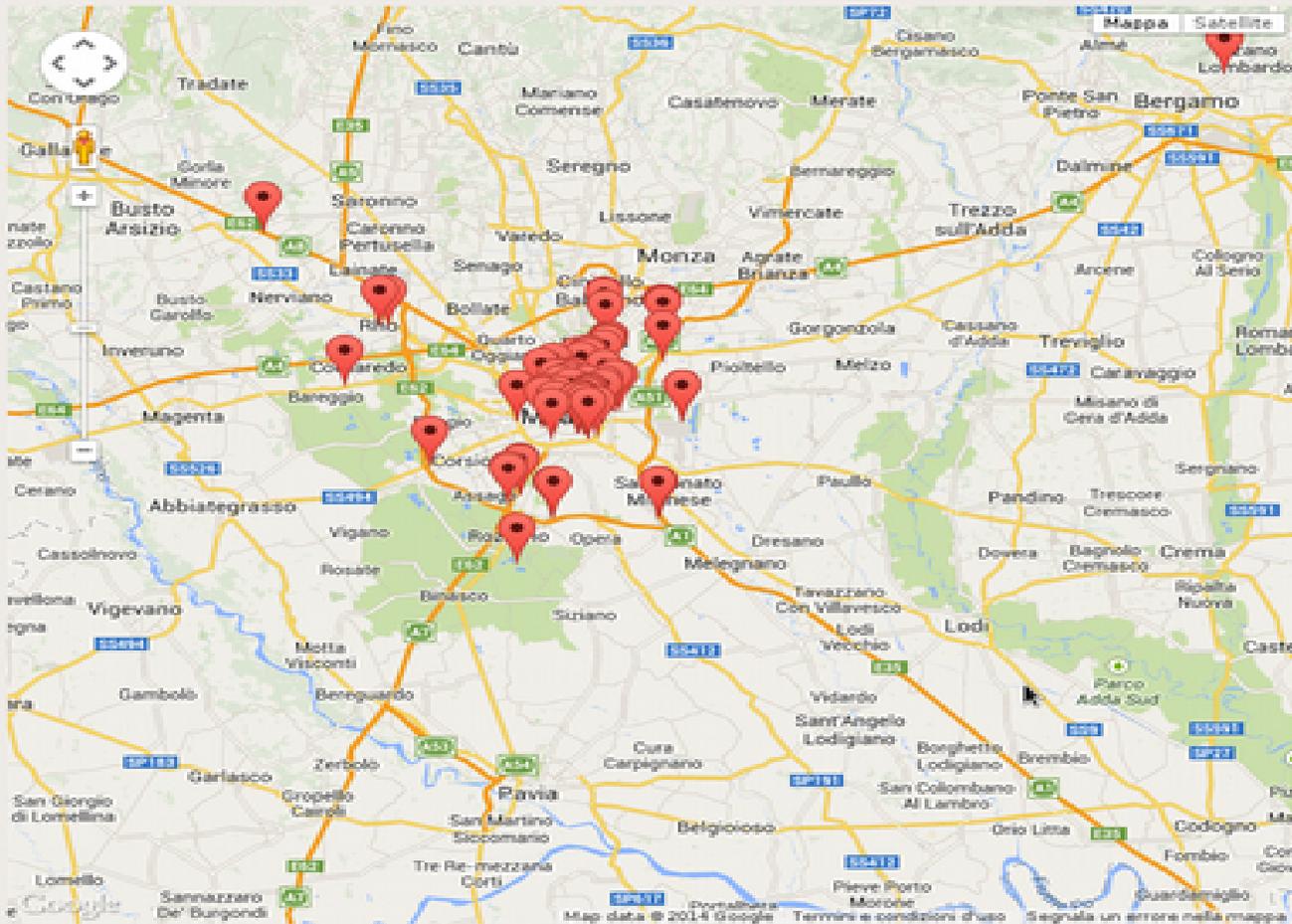
creepy.py - Geolocation OSINT tool (come superutente)

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 M.
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:



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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*



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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/ilektrojohncreepy/>) **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



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

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](http://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>



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara

OSINT

Open Source Intelligence

Grazie per la vostra attenzione

Paolo 'aspy' Giardini



19-20-21 agosto
2016

Parco Ex Caserma Cocco
Pescara