

# Analisi delle Fonti Aperte OSINT

Ing. Selene Giupponi

# # whois Selene



## Selene Giupponi:

- **Managing Director Europe, Resecurity Inc.**
- **Computer Engineering Degree + II Level Master in Computer Forensics & Digital Investigations**
- General Secretary and Member @ **IISFA** (INFORMATION SYSTEM FORENSICS ASSOCIATION, ITALIAN CHAPTER)
- Active Member of the **IT Engineer Commission**, Engineers Association of the Latina Province
- **Digital Forensics Court Trial Witness** on e-crimes and ICT enhanced crimes
- Consultant for multiple **Law Enforcement agencies** around the world
- Advisor @ **European Courage Focus Group** – Cyber Terrorism & Cybercrime
- **ITU** Roster of Experts Official Member
- **HTCC** HIGH TECH CRIME CONSORTIUM Member
- Co-Founder at **The Security Brokers**
- Trainer at **NATO, INTERPOL**
- **CIFI** – Certified Information Forensics Investigator
- Certified Trainer for **SPEKTOR & UFED**
- **ECISO** Board of Directors Member



# Agenda

- **Introduzione a OSINT**
  - Chi utilizza OSINT e perché
- **Cosa e Dove cercare**
  - Motori, servizi, ed altri luoghi
  - Social network, relazioni, cerchie, e tutto il resto
- **La cassetta degli attrezzi**
  - Uso dei motori di ricerca
  - Strumenti, Tecniche, Network analisi, Metadata
  - Sock Puppet e Social Network
- **Sicurezza e contromisure**

# Categorie di Intelligence

HUMAn INTelligence (HUMINT)

COMMunications INTelligence (COMINT)

SIGnal INTelligence (SIGINT)

MeAsurements & Signatures INTelligence (MASINT)

TECHnical INTelligence (TECHINT)

FINancial INTelligence (FININT)

GEOspatial INTelligence (GEOINT)

IMagery INTelligence (IMINT) talvolta definita come PHOTo INTelligence (PHOTINT)

**OSINT – Open Source INTelligence**

# Definizioni – OSINT

- 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”

# Definizioni – OSINT

“I define OSINT as the finding, gathering, exploitation, validation, analysis and sharing with intelligence-seeking clients of publicly available print and electronic data from unclassified, non-secret (often«gray literature») sources”

(Fleisher, 2008)

# Definizioni – OSINT

- Cosa è e cosa non è?
- Secondo il testo “NATO Open Source Intelligence Handbook”, esistono quattro distinte categorie di “open source information and intelligence”
- **Open Source Data (OSD):** “Data is the raw print, broadcast, oral debriefing, or other form of information from a primary source.”
- **Open Source Information (OSI):** “OSI is comprised of the raw data that can be put together, generally by an editorial process that provides some filtering and validation as well as presentation management.”

# Definizioni – OSINT

- **Open Source Intelligence (OSINT):** “OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience, generally the commander and his/her immediate staff, in order to address a specific question.”
- **Validated OSINT (OSINT-V):** “OSINT-V is information to which a very high degree of certainty can be attributed. It can only be produced by an all-source intelligence professional, with access to classified intelligence sources ...”



# Definizioni – OSINT

- Sembra “burocraticinese”, ma descrive la definizione e la necessità di OSINT a livello strategico di pianificazione militare o di intelligence
- Il "nostro" OSINT è molto più pratico e serve a scopi tecnici o tattici.
- Spesso viene utilizzato per una valutazione di sicurezza

# La necessità di informazioni

- La ricerca di informazioni utili al proprio scopo ha da sempre avuto enorme importanza nella storia
- Nel 6 ° secolo AC, Sun Tzu scrisse "conosci il tuo nemico" (L'arte della guerra)
- Si vis pacem, para bellum (Vegezio)
- «se vuoi la pace, prepara la guerra»
- Senza andare troppo indietro nel tempo, basti pensare alla guerra fredda ed al ruolo dello spionaggio in quel periodo
- Qualunque attacco necessita di preparazione e di informazioni su cui basare la strategia

# Briciole di storia

- **Open Source Spy Games**

- 1939: il governo britannico ha chiesto alla BBC di monitorare i supporti di stampa estera e trasmissioni radiofoniche

<http://www.bbc.co.uk/news/uk-england-berkshire-36712152>

- Per anni, nel periodo della guerra fredda, la Stasi (DDR) ha analizzato riviste occidentali, libri, giornali e trasmissioni radio della Germania ovest alla ricerca di informazioni

<https://rijmenants.blogspot.it/2009/03/stasi-sigint-operations.html>

# Una esplosione di dati

- L'evoluzione dei mezzi di comunicazione ha visto come conseguenza la produzione di enormi quantità di informazioni
- Giornali, libri, radio, tv, ..., Internet
- Più informazioni accessibili a “tutti” -> più open source intelligence identificabile
- Più fonti da analizzare e validare

# Il problema

- In particolare, “l'esplosione” in internet dei servizi offerti ha permesso a milioni di persone, di aziende, di enti di rendere disponibili “volontariamente” informazioni che li riguardano.
- Molte volte anche “quelle informazioni” che forse era meglio non divulgare...
- Queste informazioni sono a disposizione di tutti

# Ad esempio

- Sappiamo bene che ogni servizio Internet raccoglie, per un motivo o per l'altro, informazioni sui suoi utenti(log, statistiche, etc.)
- Come se non bastasse, milioni di utenti pubblicano sui social networks ogni genere di notizie.
- Lo fanno anche i vostri colleghi, dipendenti, competitor,...
- E voi?

# Il perché dell'OSINT

- E' in questa infinita messe di dati che opera l'esperto di OSINT
- Ricercare, esaminare, correlare le informazioni pubblicamente disponibili permette di ottenere informazioni sull'organizzazione, sui progetti, sui processi aziendali, sulle persone
- Informazioni utili a competitor o criminali

# Il lato utile dell'OSINT

- Le informazioni recuperabili tramite OSINT non sono utilizzabili soltanto per fini “negativi”
- Possono essere utilmente impiegate per supportare decisioni strategiche, valutare campagne di marketing, verificare il “sentiment” e la reputazione online
- Possono essere impiegate per migliorare la sicurezza dell'organizzazione



# Chi utilizza OSINT?

- Aziende
- Recruiter
- Governi, politici
- Counterintelligence
- Intelligence
- Polizia
- Giornalisti (d'inchiesta)

# Ma anche...

- Investigatori privati
- Stalker
- Criminalità organizzata
- Concorrenza sleale
- Buontemponi
- Troll
- Criminali informatici

# Ma non solo...

- Utilizzando risorse liberamente accessibili, I **bloggers di Arkenstone** provano a ricostruire la gerarchia di comando e l'ordine di battaglia dell'esercito Iraniano
- Che strumenti utilizzano?
- Google Earth
- Ricerca di nuova costruzioni / fortificazioni
- Classici media Iraniani
- Parate militari, eventi, comunicati, ...
- “grey literature”

# Ma non solo...

Title: Partial Demolition of the 130th Brigade's (NEZAJA) Old Garrison  
Location: Bojnourd, N. Khorasan, Iran Lat: 37.481565° Long: 57.326135°  
Imagery Date: See Inset Source: Google Earth



Red shading indicates building razed between 12/2012-10/2013



<http://thearkenstone.blogspot.it/2014/05/> - coord. Google earth 37°28'53.92"N 57°19'35.61"E

# Esempi di OSINT in diretta TV





# Esempi di OSINT in diretta TV



# Esempi di OSINT in diretta TV



# Quanto è importante?

- Si pensi che il governo USA, la NATO, il Governo Italiano, solo per citare qualche nome, hanno dedicato e dedicano sforzi ed energie ad OSINT
- Come già detto, in ambito US Army e NATO e, l'OSINT consiste nella “raccolta, selezione, distillazione e diffusione di informazioni non classificate ad una comunità ristretta ed in relazione a specifici argomenti”



# NATO OSINT

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

# NATO OSINT

“During the week of 5–9 May 2014, the cross-panel Task Group SAS–IST–102 on “Intelligence Exploitation of Social Media” met at the NATO Collaboration Support Office (CSO) to hold their second official team meeting. This joint effort between subject matter experts from both the System Analysis and Studies (SAS) Panel and the Intelligence Systems and Technology (IST) Panel is focused on Open Source Intelligence (OSINT) and its employment in obtaining Information Superiority (IS), one of the primary issues for military dominance. **The exploitation of all relevant information from various sources is a key factor for NATO’s IS, and an integral part of this is to glean actionable intelligence from a wide variety of sources.**”

- <https://www.sto.nato.int/SitePages/newsitem.aspx?ID=2162>
- <http://www.natoschool.nato.int/Academics/Resident-Courses/Course-Catalogue>

# OSINT: quali risultati?

- Dipende:
  - Dall'argomento
  - Dalla capacità dell'operatore
  - Dalla attendibilità delle fonti
    - Anche una “non informazione” è una informazione
- **In generale, se si ha abbastanza tempo, i risultati sono soddisfacenti**

# OSINT: problemi?

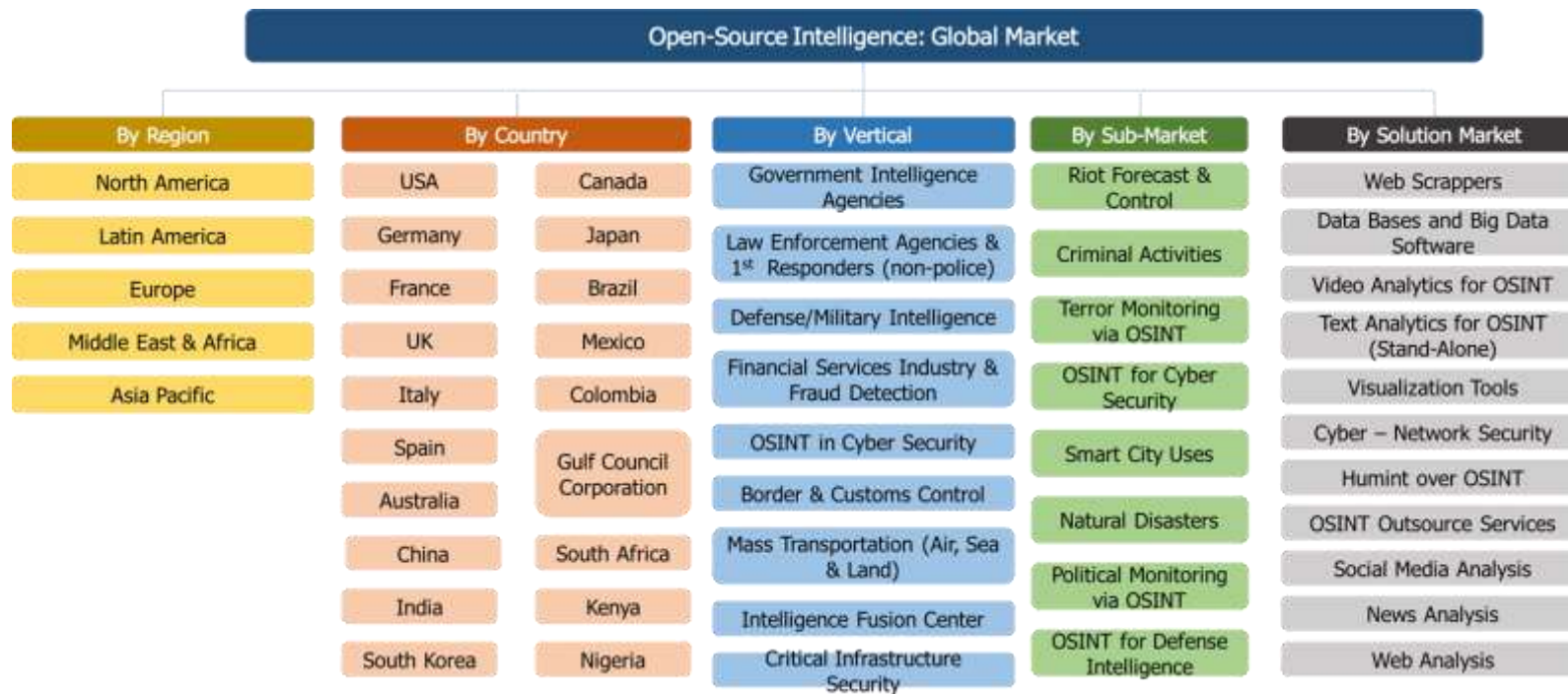
- Linguaggio/barriere culturali
- Troppa fiducia nei tools automatici
- Disinformazione
  1. Le informazioni possono essere false
  2. Le informazioni possono essere manipolate
  3. Impossibilità di accesso legale all'informazione

# Cosa si può fare con OSINT

- Risorse Umane
  - Ricerca dipendenti scontenti (es. su Facebook)
  - Verifica curriculum di possibili nuovi dipendenti
- Ricerca di informazioni personali
- Ricerca informazioni su concorrenti
- Analisi economiche
- Antiriciclaggio
- Analisi di marketing
- Identificazione e controllo gruppi di varia natura
- Informazioni militari non classificate

# Mercato dell'OSINT

L'immagine sottostante elenca e suddivide il mercato globale dell'OSINT per segmenti:



# Cosa si può fare con OSINT

- Ricerca scientifica ed accademica
- Ricerca informazioni propedeutiche ad un attacco
- OSINT e Forze dell'Ordine
  - Conoscete Koobface? (<https://it.wikipedia.org/wiki/Koobface>)

## Koobface

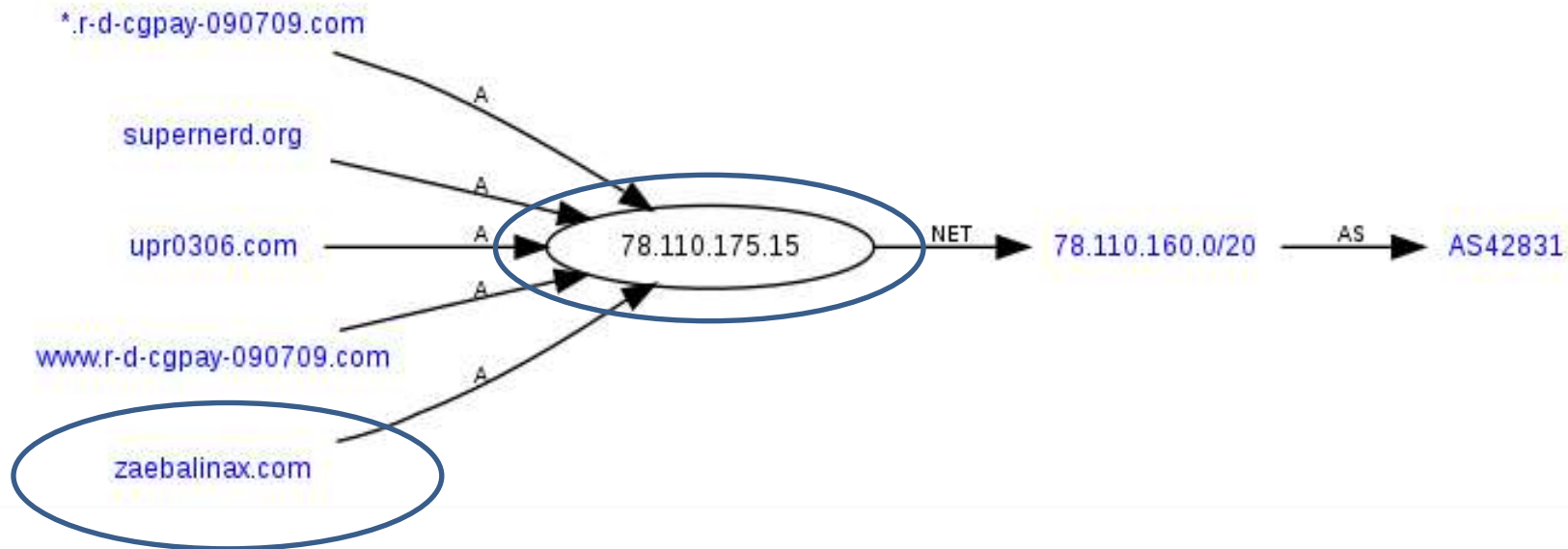
Da Wikipedia, l'enciclopedia libera.

**Koobface** è un [worm](#) informatico che colpisce gli utenti della [rete sociale](#) di [Facebook](#). Koobface dopo l'infezione, rimanda la connessione internet su pagine di [Rogueware](#) o pubblicitarie, inoltre, in uno stadio più avanzato, tenta di ottenere informazioni sensibili dalle vittime come numeri di carta di credito o dati di accesso a forum, social network e caselle e-mail. Spesso le password degli utenti infetti vengono sostituite con "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!  
(<https://ddanchev.blogspot.com/2012/01/whos-behind-koobface-botnet-osint.html>)

# OSINT vs. Koobface

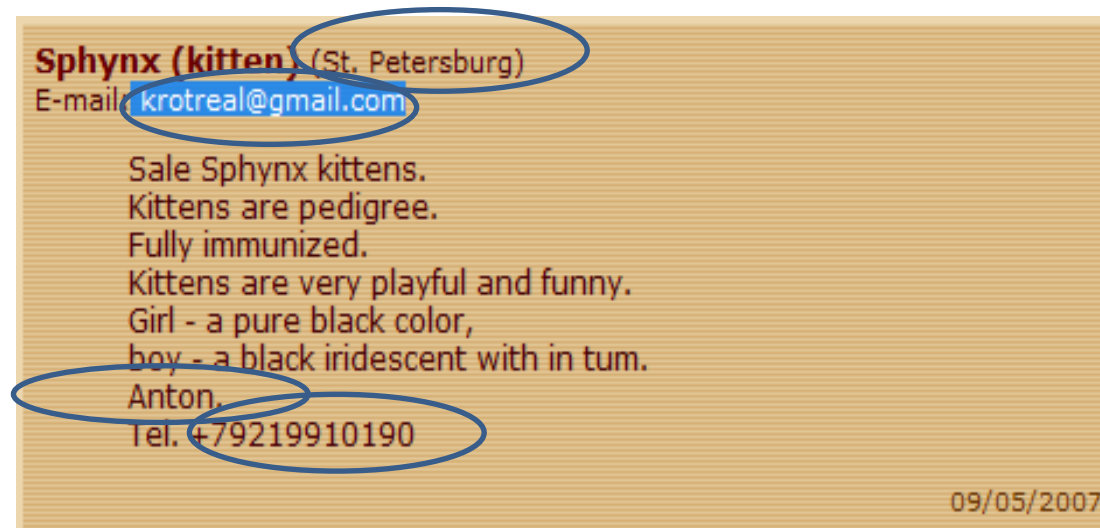
- Partendo dall'analisi dell'infrastruttura di Koobface, Danchev ha semplicemente cercato tutti i domini riconducibili allo stesso IP





# OSINT vs. Koobface

- In questo modo Danchev ha trovato un dominio registrato con una email diversa dalle altre
  - krotreal@gmail.com
- Anche I criminali amano i gattini...



# OSINT vs. Koobface

- Oops...

Новые авто

Грузовые авто

Новости

Блог

Форум

Продать авто

ПДД онлайн

АВТОВЛАДЕЛЬЦАМ

Автострахование

Автокредит

Личный опыт



Шины и диски

Тюнинг

Мото



Публикации

Техосмотр



КОМПЛЕКТАЦИЯ

3300000р.

Год выпуска	2000
Пробег	139000км.
Объем двигателя	1895см <sup>3</sup>
Тип двигателя	Бензин инжектор
Мощность	105л.с.
КПП	Ручная
Привод	Задний
Руль	Левый
Тип кузова	Хэтчбек
Цвет	Серебряный металлик
Описание	Авто в идеальном состоянии. Более подробная инфо по телефону.
Город	Москва
Владелец	Антон
Телефон	 +79219910190 

# 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](#)



<http://ddanchev.blogspot.it/2012/01/whos-behind-koobface-botnet-osint.html>

# OSINT vs. Koobface

- Cosa ci insegna questa vicenda?
  - Essere pigri è male
  - La sicurezza non è retroattiva
- Puoi essere furbo, ma...
  - Basta un solo errore: un file nel posto sbagliato, un pacchetto di troppo, un file non sanitizzato,...

# Modalità di fare OSINT

- **Manuale** - la ricerca viene effettuata direttamente dall'operatore
  - Le scelte vengono fatte sul momento
  - Raccolta e confronto oneroso, difficilmente “scalabile” ed elevato rischio di “perdere” informazioni
  - Qualità del dato e validazione analista su molteplici basi di dati
- **Automatica** - la ricerca viene effettuata tramite strumenti parametrizzabili
  - Deve essere effettuata una scrematura a posteriori
  - Potenzialmente molto efficace, facilmente “scalabile” ed integrabile, richiede enormi investimenti (HW e SW), le tecnologie sono in rapida convergenza
  - Rischio di falsi positivi dovuti a AI non evoluta come analista

# Modalità di fare OSINT

- **La mia soluzione:**
  - Mix di operazioni automatiche e manuali validate ed analizzate dall'occhio critico dell'analista
- **Perché?**
  - Benefici dall'uso di tecniche automatiche per l'individuazione o la connessione di dati, parte critica e di eliminazione del rumore da parte dell'analista

# The Art of OSINT

- Tools e API possono automatizzare molte attività ma una gran parte dei risultati sono basati sull'intuito
- Il Software è perfetto per l'automazione dei compiti ripetitivi e per l'estrazione dei contenuti, ma estrarre “contesti” è molto più difficile
- **Esperienza (anche conoscenza dell'argomento e dei tool utilizzati), intuito ed istinto sono ciò che separa buoni risultati da risultati scadenti**
- Per esempio: trovare un username conduce ad altri profili (del target, delle sue cerchie) con altri dati. Questo può condurre al nome reale, che può condurre all'indirizzo fisico o alla geolocalizzazione del target, e via così..

# The Art of OSINT

- Il gioco sta “tutto” nell’individuare le connessioni tra le informazioni, quasi come i detective dei film ;)





# Link Analysis & Mind Mapper

- **Link analysis...analisi delle connessioni tra entità**
  - Nella teoria delle reti, l'analisi dei collegamenti è una tecnica di analisi dei dati utilizzata per valutare le relazioni tra i nodi. Le relazioni possono essere identificate tra vari tipi di nodi, tra cui organizzazioni, persone e transazioni. (source Wikipedia)
- **Mind Mapper...mappa mentale**
  - Una mappa mentale è una forma di rappresentazione grafica del pensiero teorizzata dal cognitivista inglese Tony Buzan, a partire da alcune riflessioni sulle tecniche per prendere appunti (source Wikipedia)

# Mind Mapper

- Un ausilio nelle attività di investigazioni OSINT potrebbe essere l'utilizzo di un programma per il “mind mapping”
  - **VYM -View Your Mind (multiplatforma)**
    - <http://sourceforge.net/projects/vym/>
  - **Xmind (multiplatforma)**
    - <http://www.xmind.net/>
  - **Freemind (multiplatforma)**
    - <http://freemind.sourceforge.net/>
  - **Mindmaple (Windows)**
    - <http://www.mindmaple.com/>

# Esercizio 1

- Oggi vedremo molti tool e tecniche ma lo scopo del corso è che imparare a pensare come un detective / troubleshooter / analista.
- Adesso ditemi: Chi è quest'uomo?

[https://thehackernews.com/2014/06/fifa-world-cup-security-team\\_26.html](https://thehackernews.com/2014/06/fifa-world-cup-security-team_26.html)



# Agenda

- **Introduzione a OSINT**
  - Chi utilizza OSINT e perché
- **Cosa e Dove cercare**
  - Motori, servizi, ed altri luoghi
  - Social network, relazioni, cerchie, e tutto il resto
- **La cassetta degli attrezzi**
  - Uso dei motori di ricerca
  - Strumenti, Tecniche, Network analisi, Metadata
  - Sock Puppet e Social Network
- **Sicurezza e contromisure**

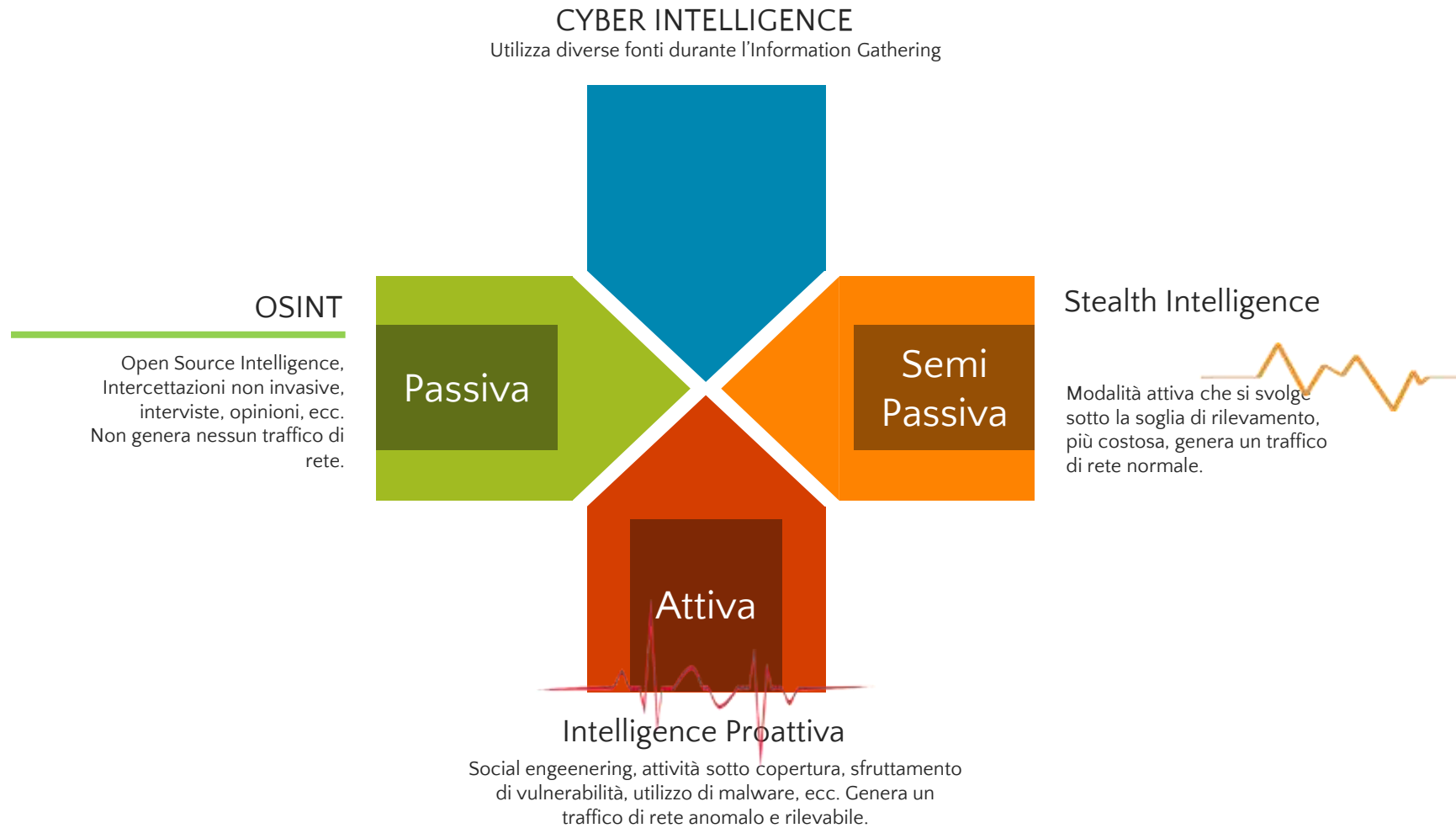
# Profiling & Scoping

- Molto semplicemente, dovete definire:
  - **Target**
  - **Obbiettivi**
  - **Regole di ingaggio**
- Ricordate che lo scopo di OSINT è di produrre **informazioni utilizzabili** al fine di **prendere decisioni** o **definire strategie**, non riempire pagine e pagine di report
- **Come pianifico la mia investigazione o attività OSINT?**

# Pianificazione delle fasi - OSINT



# Che tipo di OSINT effettuare?



# Classificazione delle fonti

- INFORMAZIONI GENERALI (info provenienti dal web o dai media)
- INFORMAZIONI A PAGAMENTO (database commerciali o siti a pagamento)
- ESPERTI (interviste e opinioni di esperti, tecnici, specialisti, ecc.)
- DOCUMENTI “GRAY” (brevetti, report, pubblicazioni ad uso interno, atti di convegni, ecc.)
- O.D.S. (Open Source Data): Dati grezzi, generici, generati da registrazioni, fotografie, immagini satellitari, in generale tutta la documentazione pubblicata su canali pubblici da fonti non attendibili
- O.S.I.F. (Open Source Information): Informazione pubblica che ha subito un processo di filtraggio e convalida, come giornali, libri, comunicazioni e divulgazioni da fonti attendibili
- L'O.S.I.N.T. è l'unione di ODS e OSIF, consiste in informazioni filtrate, cercate, selezionate e destinate a soddisfare una specifica richiesta informativa



# Come vengono trattate le fonti?

- Le informazioni contenute nelle fonti pubbliche vengono “trattate” attraverso la conoscenza di:
  - **STRUMENTI DI HACKING** (ottenere informazioni sulle identità digitali)
  - **AVANZATO USO DEI MOTORI DI RICERCA** (usando ad esempio GHDB)
  - **UTILIZZO DI PORTALI DI INVESTIGAZIONI ON LINE** (informazioni istituzionali su persone fisiche o giuridiche, partecipazioni azionarie/societarie, proprietà immobiliari, ecc.)

# 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, 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

- Ricerca per parole chiave
- Analisi delle immagini
- Correlazione informazioni
- Analisi dell'ambiente
- Analisi dei contatti
- Analisi informazioni tecniche internet

# La ricerca di informazioni

- Analizzare le informazioni in proprio possesso sul Target
- Valutare gli **ambiti di ricerca** (Ambiente di lavoro? Contatti ed amicizie?)
- Definire la **priorità** delle ricerche
- Individuare **keyword**
- **Si ma cosa cercare? tutto?**

# Cosa cercare?

- Dipende dal soggetto della ricerca
- Dipende dalla domanda a cui si deve rispondere
- Le keyword e gli argomenti possono cambiare (anzi, cambiano!) durante l'analisi in base ai risultati
- E' fondamentale correlare le risposte per individuare nuove direzioni di ricerca

# Cosa serve?

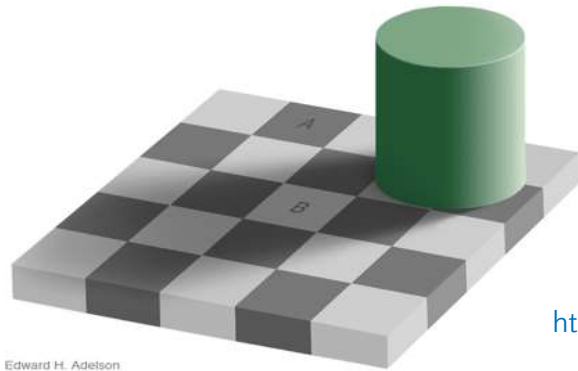
- Fantasia
- Immaginazione
- Capacità logiche
- Conoscenze tecniche
- Informazioni di partenza
- Qualche buon tool

# Alcune problematiche

- **Troppe informazioni**
  - Può essere difficile individuare “la pista giusta”
  - anche per difficoltà linguistiche
- **Affidabilità delle informazioni**
  - Capire se l'informazione è vera, falsa, manipolata
    1. Potrebbe essere stata creata volutamente falsa
    2. Potrebbe trattarsi di fake profile
    3. Potrebbe essere di seconda o terza mano
    4. Interpretazioni personali, anche le nostre!

# Cognitive BIAS

- E' un pattern sistematico di deviazione dalla norma o dalla razionalità nel giudizio.
  - In psicologia indica una tendenza a creare la propria realtà soggettiva, non necessariamente corrispondente all'evidenza, sviluppata sulla base dell'interpretazione delle informazioni in possesso, anche se non logicamente o semanticamente connesse tra loro, che porta dunque a un errore di valutazione o a mancanza di oggettività di giudizio (source Wikipedia)

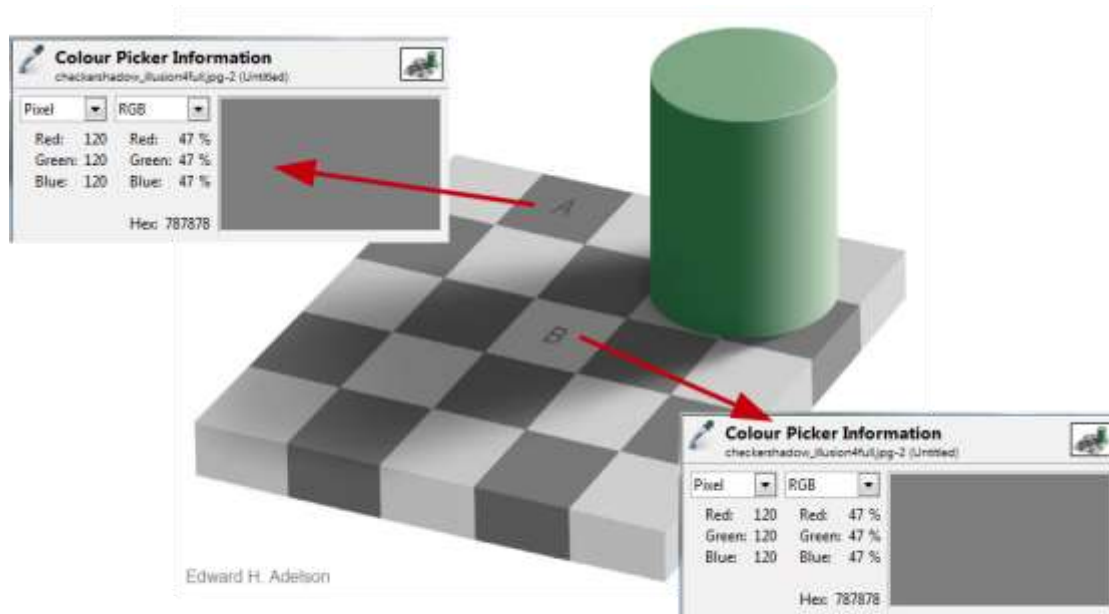


<http://persci.mit.edu/gallery/checkershadow>



# Cognitive BIAS

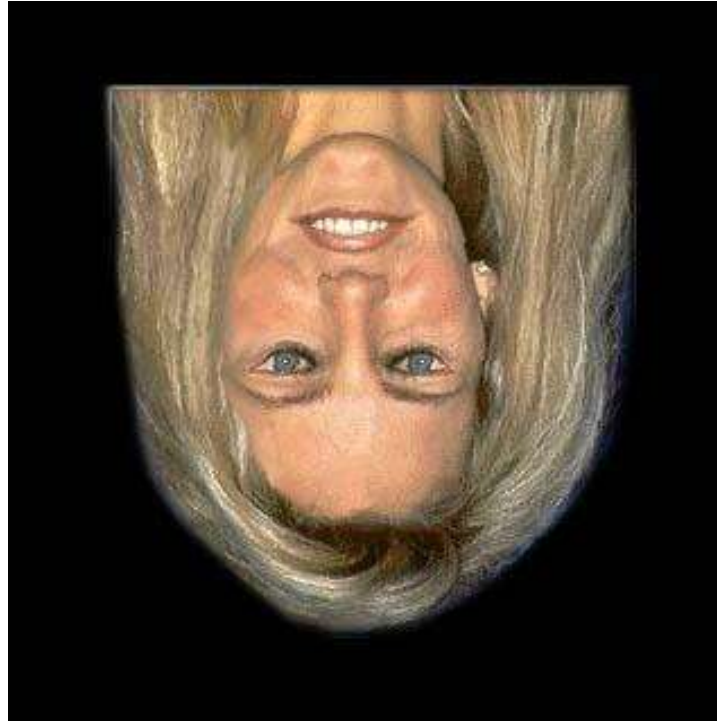
Facciamo attenzione prima di fornire giudizi...



<http://persci.mit.edu/gallery/checkershadow>

# Esempi di Cognitive BIAS

Facciamo attenzione prima di fornire giudizi...



Thompson (1980) - Thatcher Illusion

# Esempi di Cognitive BIAS

Facciamo attenzione prima di fornire giudizi...



Thompson (1980) - Thatcher Illusion

<https://ninetyninenews.wordpress.com/2016/09/26/il-sorriso-della-thatcher/>

# Esempi di Cognitive BIAS

Effetto Thatcher..



<https://youtu.be/jdADSx8Jpfl>

# Esempi di Cognitive BIAS



# Esempi di Cognitive BIAS

- Il contesto è tutto
- Non bisogna fermarsi alle apparenze



# Profilazione

- La creazione di un profilo del soggetto aiuta a definire gli ambiti di ricerca:
  - Lavoro, amici, famiglia, hobby
  - Prodotti, mercato, clienti, fornitori
  - Localizzazione geografica
  - Studi, interessi



# Le basi: motori di ricerca





# Le basi: motori di ricerca

- **Motori di ricerca generic**
  - es. Google, Bing
- **Motori di ricerca specifici**
  - es. ricerche su social network o su username
- **Cataloghi**
  - es. Library of Congress Online Catalog
- **Motori di ricerca specializzati su persone**
  - es. Pipl
- **Motori di ricerca interni dei siti**

# Le basi: motori di ricerca

- **Primo problema:**
- Si tende ad assumere che i motori di ricerca siano infallibili
- **Ma come funziona un motore di ricerca?**
- **Ci sono tre parti che compongono un motore di ricerca**
  - Uno spider/crawler
  - Un database che indicizza i risultati del lavoro dello spider
  - Un motore di backend che analizza le richieste ed i contenuti del database, assegnando il “rank” e fornendo i risultati in base ad algoritmi proprietari che cambiano continuamente

# Le basi: motori di ricerca

- **Secondo problema:**

- Si tende ad assumere che un motore di ricerca valga l'altro ed usare sempre lo stesso od al massimo ad usarne uno o due...
- Sbagliato!

"When the researchers ran 12,570 different queries through search engines at Yahoo, Google, MSN and Ask Jeeves, they found that **only 1.1 percent** of the results appeared on all four engines, while **84.9 percent** of the top results were unique to one engine. **Only 2.6 percent** of the results were shared by three search providers, and **11.4 percent** were delivered by two search engines."

# Le basi: motori di ricerca

- Cosa sto cercando di dirvi?
  - Può esservi una notevole differenza fra i risultati di differenti motori di ricerca
  - E' indispensabile abituarsi ad usare più motori, effettuate ricerche su motori specializzati ed utilizzare le funzioni specifiche di ciascun motore
- Vedremo fra poco come sfruttare le caratteristiche di alcuni motori di ricerca per ottenere il massimo dei risultati...

# Le basi: motori di ricerca

## Una tabella di esempio

	<b>Google</b> <a href="http://www.google.com">www.google.com</a>	<b>Bing</b> <a href="http://www.bing.com">www.bing.com</a>	<b>DuckDuckGo</b> <a href="http://duckduckgo.com/">http://duckduckgo.com/</a>
<b>Default search</b>	Automatically looks for synonyms and variations on your terms. Drops words from your search if the number of results is low or zero.	Automatically looks for synonyms and variations on your term. Usually searches on all of your words but has started to drop terms if the number of results is low.	All of your words but drops terms if the number of results is low or zero.
<b>Wild card or truncation</b>	Not user specified. Google automatically looks for variations and synonyms. (But see Proximity and asterisk below).	Not user specified. Automatically looks for synonyms and variations.	No
<b>Alternative terms or variations</b>	Use OR for example <code>oil OR petroleum</code>	Use OR for example <code>oil OR petroleum</code>	Use OR for example <code>oil OR petroleum</code>
<b>Suggests other search strategies and related terms</b>	Suggests searches as you type. Also offers related searches at the bottom of your results page.	Suggests searches as you type in your search. 'Related Searches' at the bottom or to the right of your results page.	Suggests searches as you type.
<b>Phrases</b>	"..." for example <code>"climate change"</code>	"..." for example <code>"climate change"</code>	"..." for example <code>"climate change"</code>
<b>Proximity</b>	Use the asterisk to stand in for one or more words in a phrase for example <code>solar * panels</code>	<code>near:n</code> listed in Bing's documentation but no longer seems to work.	No
<b>Exclude pages with a word</b>	Precede words with a minus sign (-) For example <code>cabbage -red</code>	Precede words with a minus sign (-) or use NOT For example <code>cabbage -red</code> <code>cabbage NOT red</code>	Precede words with a minus sign (-) For example <code>cabbage -red</code>

# Le basi: motori di ricerca



# Le basi: motori di ricerca

- **Google, Yahoo e Bing sono rivolti agli utenti USA, mentre Baidu è rivolto agli utenti cinesi.**
  - L'operatore deve imparare a sfruttare tutti i motori di ricerca e le loro particolarità legate alla nazionalità
  - Da notare: la maggior parte degli strumenti di ricerca al di fuori degli USA raccolgono e memorizzano dati principalmente o esclusivamente dalla loro regione o paese. Si possono trovare dei dati su Yandex, ma non su google.com (o anche google.ru)
  - Linguaggio: I motori di ricerca internazionali devono offrire la possibilità di cercare nella lingua madre
  - le query condotte nel set di caratteri non latini possono produrre risultati più specifici.

# Esercizio 1: motori di ricerca

- Provate ad effettuare la stessa ricerca su differenti motori
  - Ad esempio, cercate “berlin ballroom” su:
    1. yandex.ru
    2. Baidu.com
    3. Google.it
    4. Google.de
- Otteniamo gli stessi risultati?

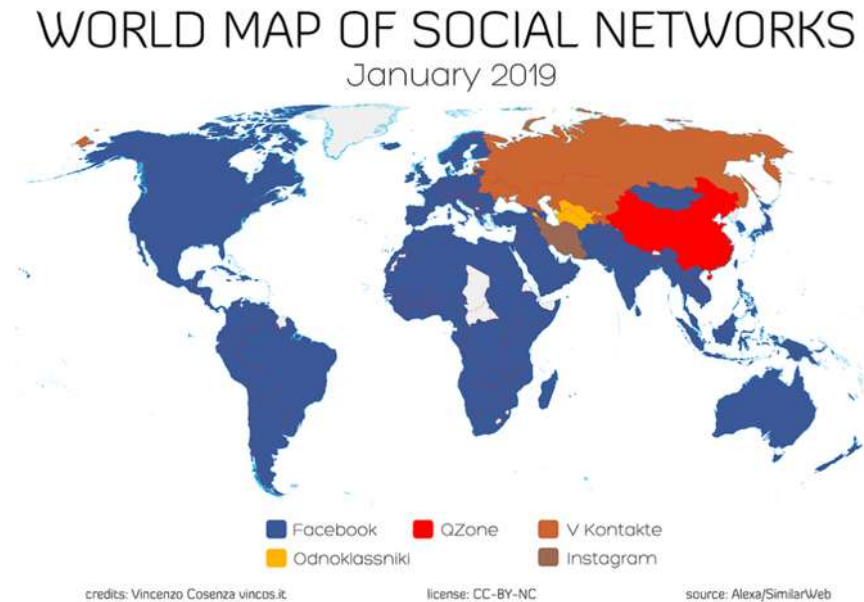


# Cerchie, amici, follower...

- I profili social sono una fonte notevole di dati da analizzare
- Una analisi dei contatti conduce spesso ad ulteriori direzioni di indagine
- Utile in questo senso FB Graph Search
  - attenzione però, perché dopo lo scandalo di Cambridge Analytica, Facebook cambia le tipologie di ricerca e i risultati ottenibili molto spesso

# Social Network

- **The Big Ones”**
  - Facebook
  - Twitter
  - Google+
- **“The Dinosaurs”**
  - Myspace
- **Media/Vanity**
  - Instagram
  - Flickr
  - Vine
  - Foursquare
  - YouTube
- **International**
  - Weibo
  - VKontakte
  - Tuenti
  - Qzone
- **Professional**
  - LinkedIn

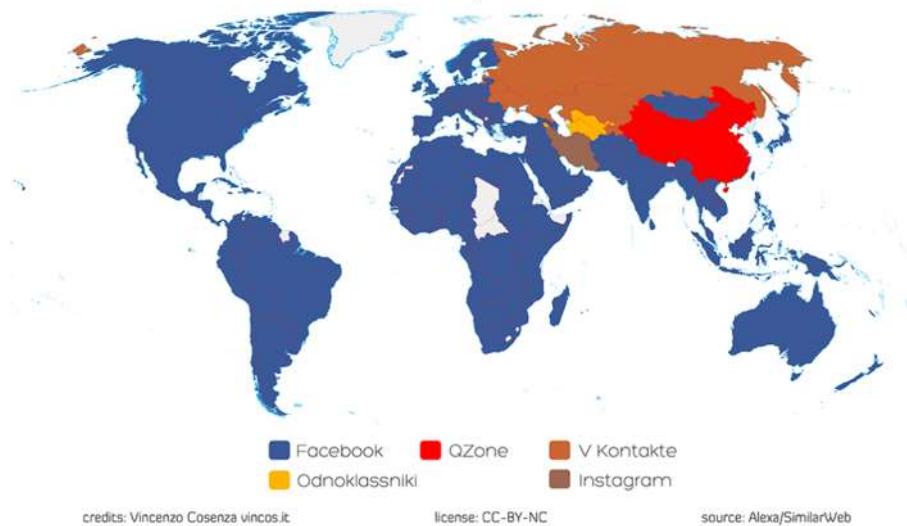


Non dimenticare ORKUT(\*): chiuso ma l'archivio è online

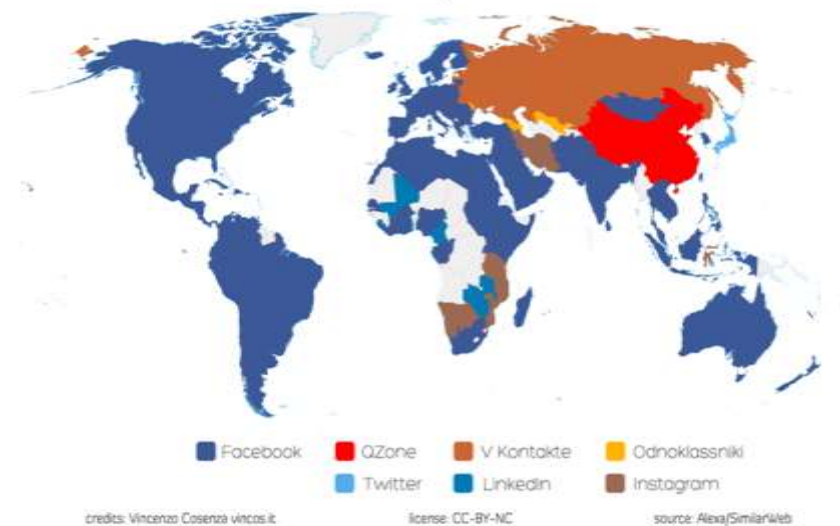
\*Orkut è stato il più diffuso SN in Brasile ed India

# Social Network...sempre in evoluzione

WORLD MAP OF SOCIAL NETWORKS  
January 2019



WORLD MAP OF SOCIAL NETWORKS  
January 2017



# Comunità virtuali

- “Everything that doesn’t fit into Social Networks” ovvero tutto quello che non è Social Network ma anni addietro era l’internet dove poter scambiare postare informazioni o comunicare con altri utenti...
  - Forums
  - Mailing lists
  - Blogs (senza contare i microblogging)
  - Online chat rooms (IRC)
  - Gaming – Playstation, Xbox Live, Steam
  - Virtual worlds

# Selected Source: People

- Se il target è una persona
- **Motori di ricerca**
  - [www.spokeo.com](http://www.spokeo.com)
  - [www.peakyou.com](http://www.peakyou.com)
  - [www.lullar.com](http://www.lullar.com)
  - [www.pipl.com](http://www.pipl.com)

- **Siti di dating**
  1. [www.badoo.com](http://www.badoo.com)
  2. [www.twoo.com](http://www.twoo.com)
  3. [www.adultfriendfinder.com](http://www.adultfriendfinder.com)
  4. [www.nirvam.com](http://www.nirvam.com)
  5. [www.datingwebsites.it](http://www.datingwebsites.it)

**E tanti altri...**

# Esercizio 2

- **Chi è Mark W. Gillette?**
  - Ditemi tutto quello che potete trovare sulla sua presenza sui social network e sulle sue esperienze lavorative
- **Paolo Rossi: dalla coppa del mondo a.... ?**
  - Ditemi tutto quello che potete trovare sulla sua vita dopo il calcio.
- **Angela Merkel è stata nel 2014 a Pechino con una delegazione di imprenditori.**
  - Quali aziende e ed industrie sono state rappresentate in questo viaggio?
  - Potete usare fonti in inglese, tedesco, cinese...

# Selected Source: Paste Site

- I “Paste Site” sono popolari, facili da usare e (più o meno) anonimi
- Vengono utilizzati per una serie di attività:
  - White: Condividere configurazioni, crash dumps, codice, IRC logs, etc...
  - Black: postare leaked files, dati rubati, dump di databases, “doxing”, credenziali sottratte, etc...
  - Ad esempio, si trovano molti annunci per vendita di CC e credenziali rubate
  - Esempi di aggregatori
    1. <https://netbootcamp.org/pastesearch.html#gsc.tab=0>
    2. il più famoso: <https://pastebin.com>

# Selected Source: Wikipedia

- **Wikipedia è semplicemente enorme**
  - 1 560 171 voci in italiano | 5 957 519 voci in inglese
  - oltre 290 lingue
  - Wikipedia è uno sforzo della comunità, e tutte le attività (le modifiche, aggiunte, soppressioni, ecc.) sono legate a un nome utente o un indirizzo IP.
- **A volte una persona di interesse è un utilizzatore fisso di Wikipedia, ad esempio un contribuatore**
- **A volte possiamo "decodificare" persone di interesse dai suoi contributi su Wikipedia (interessante per argomenti di nicchia)**



# Selected Source: Wikipedia

- Attenzione, A volte le persone diffondono menzogne e disinformazione via Wikipedia o commettono errori di giudizio
  - Il 2 agosto 2013, un editor legato al Senato degli Stati Uniti con l'IP 156.33.241.5 ha modificato la pagina di Wikipedia di Edward Snowden cambiando la sua descrizione da "dissidente" a "traditore»

*Wikipedia is a staple of the Internet user's information diet. Because of this, Wikipedia is also laden with manipulation, forgery, and the downright unscrupulous.“*

# Selected Source: Wikipedia

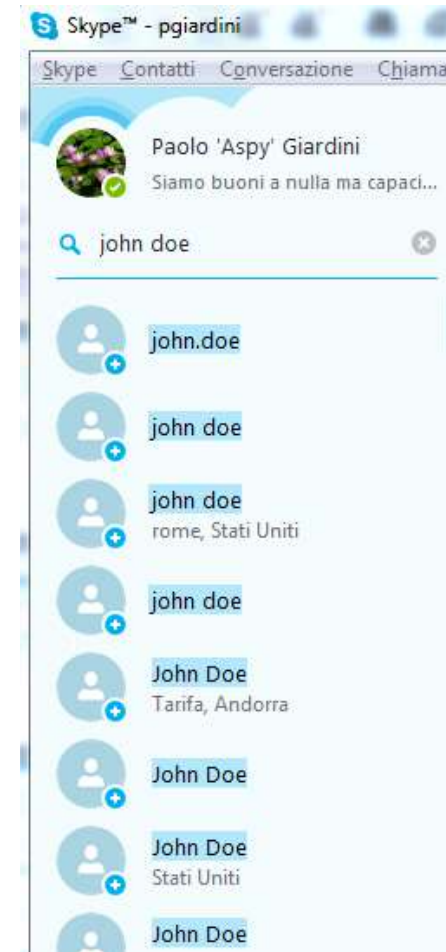
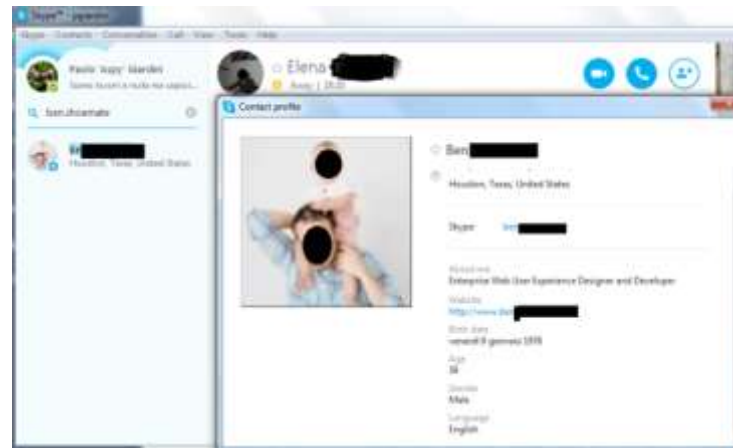
- Wikiscanner (RIP)
  - "Alert me when an IP from the US Congress is editing zh.wikipedia.org"
  - "Alert me when an IP from Urumqi University is editing articles on the situation in Xinjiang."
- wikiwatchdog.com
  - Permette di individuare quali articoli sono stati modificati da un IP

# Esercizio 3

- Chi è l'utente di Wikipedia "Rincewind42"?
- E' maschio o femmina?
- Dove è nato?
- Dove risiede attualmente?
- Che lavoro svolge?
- Quali sono i suoi interessi?

# Skype

- Usando il programma Skype, provate ad aggiungere un contatto
  - Spesso gli utenti inseriscono molte informazioni personali



# Skype

- Alcuni suggerimenti
- Provate a fare una ricerca su un motore cercando una e-mail o uno Skype-id del target
- Se avete una e-mail potete cercare un utente Skype
- Con ID Skype potete:
  - Leggere le informazioni pubbliche del profilo
  - Cercare l'IP dal quale il target si collega
  - Effettuare una ricerca per immagine del profilo
  - Geo-localizzare l'IP del target

# Skype

- **Alcuni tool online disponibili**

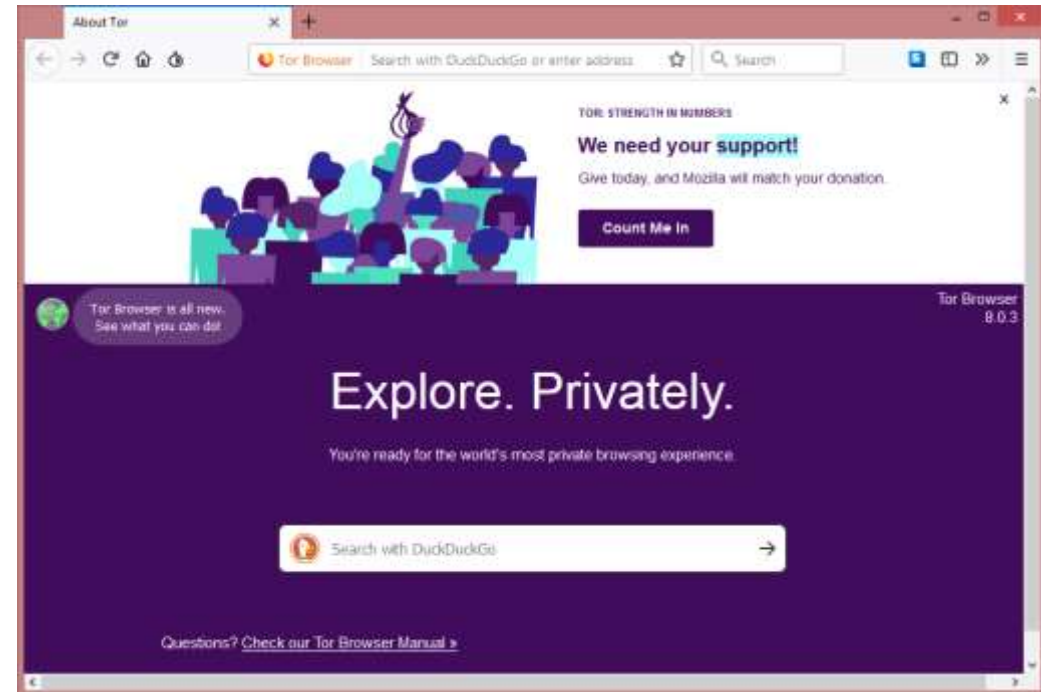
1. <https://webresolver.nl>
2. <http://resolvethem.com>
3. <http://www.skypeipresolver.net/skypedb.php>
4. <http://mostwantedhf.info/index.php>

- **Per approfondire:**

1. <http://www.automatingosint.com/blog/2016/05/expanding-skype-forensics-with-osint-email-accounts/>
2. <https://www.kitploit.com/2019/02/osint-spy-search-using-osint-open.html>
3. Dump all the contacts and messages from skype database

# Esercizio 4

- Tor
- Download, installazione e uso
- Cercare le seguenti risorse e navigare su
  1. Google
  2. Facebook
  3. ANAC



# I2P

- I2P è una rete di copertura anonima, una rete dentro la rete.
  - Il suo scopo è di proteggere le comunicazioni dal controllo a tappeto e dal monitoraggio di terze parti come gli ISP.
- <https://geti2p.net/it/>





# Freenet

- Freenet è una rete decentralizzata, creata per resistere alla censura, che sfrutta le risorse (banda passante, spazio su disco) dei suoi utenti per permettere la pubblicazione e la fruizione di qualsiasi tipo di informazione.
  - Freenet è stata costruita pensando ad anonimato e sicurezza, non alla velocità di trasmissione.
- Freenet è un software libero distribuito con GNU General Public License; essendo scritto in Java può funzionare su tutti i sistemi operativi dotati di Java Virtual Machine.
  - <https://freenetproject.org/>

# Motori di ricerca del Dark Web

- Torch
- Duck Duck go
- Onion URL Repository
- Uncensored Hidden Wiki
- The WWW Virtual Library
- notEvil
- ParaZite
- TorLinks
- StartPage
- AHMIA
- Haystak
- Visitor
- DarkWeb
- Onionland
- Deeplink
- PirateBay
- Abiko
- FreshOnions
- Candle
- Grams
- Multivac
- Atlayo

# Agenda

- **Introduzione a OSINT**
  - Chi utilizza OSINT e perché
- **Cosa e Dove cercare**
  - Motori, servizi, ed altri luoghi
  - Social network, relazioni, cerchie, e tutto il resto
- **La cassetta degli attrezzi**
  - Uso dei motori di ricerca
  - Strumenti, Tecniche, Network analisi, Metadata
  - Sock Puppet e Social Network
- **Sicurezza e contromisure**

# Strumenti

- Non esistono bacchette magiche
- Esistono però degli ottimi strumenti per le operazioni ripetitive e di routine
- Ovviamente ogni risultato deve essere valutato singolarmente e nel contesto

# Motori di ricerca: Google

- E' impossibile parlare di motori di ricerca senza nominare Google
- Nel bene o nel male Google domina il mercato nel settore delle ricerche “convenzionali
- Google ha alcune caratteristiche uniche nell'effettuare ricerche
  - Se si ricerca un termine con caratteri accentati, Google cerca anche per stringhe senza caratteri accentati
    - Es. “México” e “Mexico” sono equivalenti.
  - Se si vuole ricercare esclusivamente "México", deve essere usato l'operatore "+".

# Motori di ricerca: Google

- Ma...non è tutto oro quel che luccica
- I risultati cambiano a seconda se si utilizza una versione localizzata di Google
  - [google.com](http://google.com)/[google.fr](http://google.fr)/[google.de](http://google.de)/[google.pt](http://google.pt)/etc...
- I risultati cambiano in base alla lingua selezionata
- I risultati cambiano in base al paese dal quale siete collegati
  - risultati differenti per IP Cinesi, Norvegesi, Americani,...



# Motori di ricerca: Google Operator

- **AND** le parole devono essere presenti
- es. green AND blue
- **OR** almeno uno delle parole deve essere presente
- es. green OR blue
- AND / OR devono essere scritti in maiuscolo
- - (**Minus**)
- per escludere risultati
- \* (**Asterisk**)
- wildcard, include delle derivazioni
- "" (**Quotes**)
- per cercare una parola o frase in maniera specifica

# Motori di ricerca: Google Operator

- **How to search on Google**
  - [https://support.google.com/websearch/answer/134479?hl=en&ref\\_topic=3081620](https://support.google.com/websearch/answer/134479?hl=en&ref_topic=3081620)
- **Google Guide**
  - <http://www.googleguide.com/>
- **Search Operators Cheat Sheet**
  - <https://www.searchlaboratory.com/wp-content/uploads/2012/11/searchoperators.pdf>



# Google Dorks

- Le ricerche su Google possono essere fatte indicando specifiche parole chiave che istruiscono il motore affinché imposti speciali filtri.
- Le ricerche effettuate usando queste parole chiave sono dette “google dorks”
- Un ausilio sono i form per le ricerche avanzate
  - [https://www.google.com/advanced\\_search](https://www.google.com/advanced_search)
  - [https://www.google.com/advanced\\_image\\_search](https://www.google.com/advanced_image_search)

# Google Dorks

- **Intext**
  - Searches for the occurrences of keywords inside the text of the page
- **Allintext**
  - Searches for occurrences of all the keywords given inside the text of the page all at time
- **Inurl**
  - Searches for a URL matching one of the keywords
- **Allinurl**
  - Searches for a URL matching all the keywords in the query
- **Intitle**
  - Searches for occurrences of keywords in page title
- **Allintitle**
  - Searches for occurrences of keywords in page title all at a time
- **Site**
  - Specifically searches that particular site and lists all the results for that site
- **filetype**
  - Searches for a particular filetype mentioned in the query
- **Link**
  - Searches for external links to pages
- **Numrange**
  - Used to locate specific numbers in your searches
- **Daterange**
  - Used to search within a particular date range
- **Related**
  - Lists web pages that are similar to the web page you specify
- **Cache**
  - Searches into pages cached by google
- **Info**
  - Information about site
- **Location**
  - Show only pages from selected country

# Google Dorks Resources

- Le ricerche su Google possono essere fatte indicando specifiche parole chiave che istruiscono il motore affinché imposti speciali filtri.
- Le ricerche effettuate usando queste parole chiave sono dette “google dorks”
- Un ausilio sono i form per le ricerche avanzate
  - [https://www.google.com/advanced\\_search](https://www.google.com/advanced_search)
  - [https://www.google.com/advanced\\_image\\_search](https://www.google.com/advanced_image_search)

# Google Dorks Esempi

- `inurl:phpbb1.txt`
- `xamppdirpasswd.txt filetype:txt`
- `Instagram password filetype:txt`
- `site:clusit.it filetype:pdf`
- `site:uniroma2.it filetype:xls`

# Non esiste solo Google

- Effettuare ricerche anche con altri motori amplia le possibilità di trovare informazioni utili
  - Bing
  - Baidu
  - Yandex
  - Yahoo
  - Virgilio
  - E tanti altri...
- Basta Google! Ecco gli altri motori di ricerca
  - <https://www.ninjacademy.it/google-altri-motori-di-ricerca/>

# Motori di ricerca: Bing

- Bing è spesso indicato come il fratello minore di Google...
- Gestisce almeno il 20% di tutte le ricerche effettuate al mondo
- Possiede alcuni operatori che non sono presenti in altri motori di ricerca
  - **linkfromdomain:**
    - Riporta le pagine linkate da uno specifico dominio
  - **Ip:**
    - Riporta i siti ospitati sullo stesso IP.
    - Utile ad esempio per individuare quali siti sono presenti sullo stesso server

# Motori di ricerca: Bing

- **contains:FILETYPE**
  1. L'operatore contains: riporta le pagine che contengono link ad altri documenti del tipo specificato (documenti e file multimediali come musica, video, PDF, ecc)
  2. filetype: riporta pagine create nel formato specificato
    - Es. filetype:pdf
- **Bing Miscellanea: LOC: e LOCATION:**
  1. Entrambi riportano pagine web da un paese specifico
  2. La ricerca può essere ulteriormente rifinita specificando il linguaggio



# Motori di ricerca: Bing

- **Es. “Software Company” loc:in**
  - Riporta le aziende software in India
- **“MSOFTX” loc:cn**
  - cerca siti pertinenti allo switch Huawei’s MSOFTX localizzati in Cina
- **Se si vuole specificare il linguaggio:**
  - “MSOFTX” loc:cn language:en
- **Bing Miscellanea: feed: e hashtag:**
  - L’operatore feed: riporta i feed RSS od Atom in un sito per un particolare termine di ricerca
  - L’operatore hasfeed: riporta i siti con link al feed indicato
- **Advanced Operator Reference**
  - <http://msdn.microsoft.com/en-us/library/ff795620>



# Motori di ricerca: Baidu

- 3° motore più grande al mondo (primo in Cina)
- Supporta molti degli operatori standard:
  - site:
  - domain:
  - inurl:
  - allinurl:
  - intitle:
  - allintitle:
  - filetype:
- **Affiliated sites:**
  - [www.baidu.jp](http://www.baidu.jp)
  - Baidu Thailand, Egypt...



# Motori di ricerca: Yandex

1. Il più popolare motore in Russia
2. Molto potente, con operatori “personalizzati”
3. Esempi
  - Ricerca per file del tipo specificato
    - Mime=”html/pdf/doc/ppt/xls/rtf/swf”
  - Mostra tutti i siti indicizzati con dominio \*.ro
    - rhost:ro.\*
  - Mostra tutti i siti indicizzati con dominio \*.edu
    - rhost:edu.\*
  - Mostra tutti i siti indicizzati con dominio \*.edu, che contenga nella URL il termine ftp
    - rhost:edu.\* inurl:ftp

# Motori di ricerca: Yandex

- Ricerca pagine scritte nel linguaggio specificato
  1. lang="ru/uk/be/en/fr/de"
  2. RU = Russo
  3. UK = Ucraino
  4. BE = Bielorusso
  5. EN = Inglese
  6. FR = Francese
  7. DE = Tedesco
- Ricerca siti contenenti "ballistics" in lingua Ucraina
  - ballistics lang="uk"



# Esercizio 5

- Adesso che conoscete le basi dell'utilizzo dei motori di ricerca, effettuate le seguenti ricerche:
  - Trovate quanti più curriculum vitae dei dipendenti INPS
  - Trovate nome e posizione di personale della Marina Greca (Hellenic Navy)

# Effettuare più ricerche

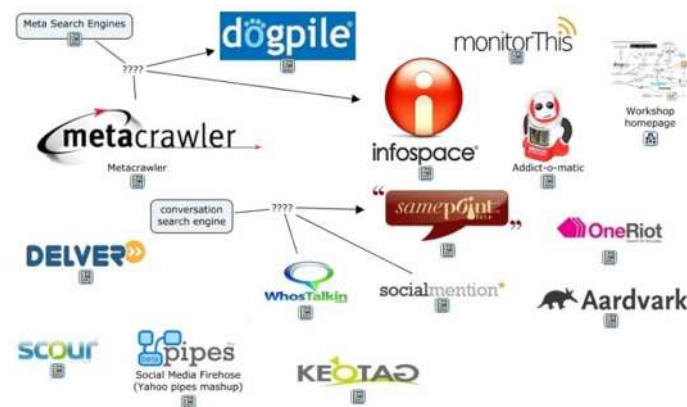
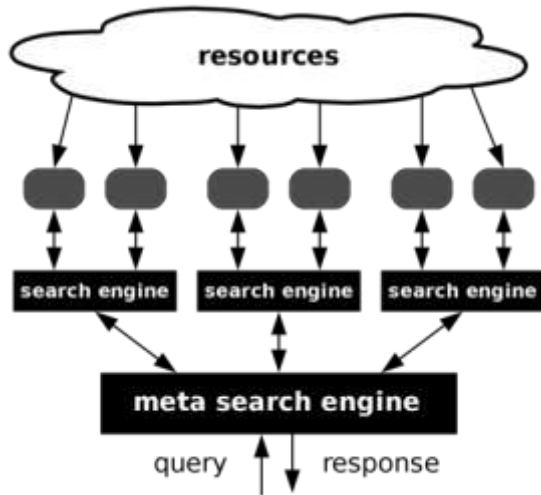
- Gli algoritmi di indicizzazione possono cambiare i risultati di una ricerca anche a distanza di poco tempo
- I risultati per una stessa parola chiave cambiano in base alla nazione di provenienza della richiesta
  - Si può modificare l'IP utilizzando proxy, VPN, TOR
- Provate la stessa ricerca su **google.it, fr, de, com,...**
  - <https://support.google.com/websearch/answer/2466433?hl=en>

# Motori di ricerca e privacy

- Esistono motori di ricerca che non registrano le query effettuate ne altre informazioni sui client
  - <https://duckduckgo.com/>
  - <https://www.ixquick.com/>
  - <https://startpage.com/>

# Meta Search Engine

- Un motore di ricerca definito metasearch utilizza altri motori di ricerca e aggrega i loro dati



## Esempi sono

- All-in-One, AllTheInternet, Etools, FaganFinder, Goofram, iZito, Nextaris, Metabear, Myallsearch, Qwant, Sputtr, Trovando, WebOasis, Zapmeta

# Elenchi telefonici

- A parte i servizi come pagine gialle e pagine bianche può essere utile esaminare gli elenchi telefonici interni (aziende, università, ecc.)
- Sono disponibili online elenchi telefonici internazionali. Ad esempio:
  - <http://www.infobel.com>
  - <http://www.paginebianche.it/>
- Un operatore OSINT ha la sua lista di elenchi
  - Createvi e tenete aggiornata la Vostra lista
  - Vengono aggiornati spesso tali elenchi



# Esercizio 6

- Analizzate il sito della vostra azienda per valutare quali file sono esposti su internet
- Allargate il campo di ricerca ricercando qualunque informazione relativa alla vostra azienda

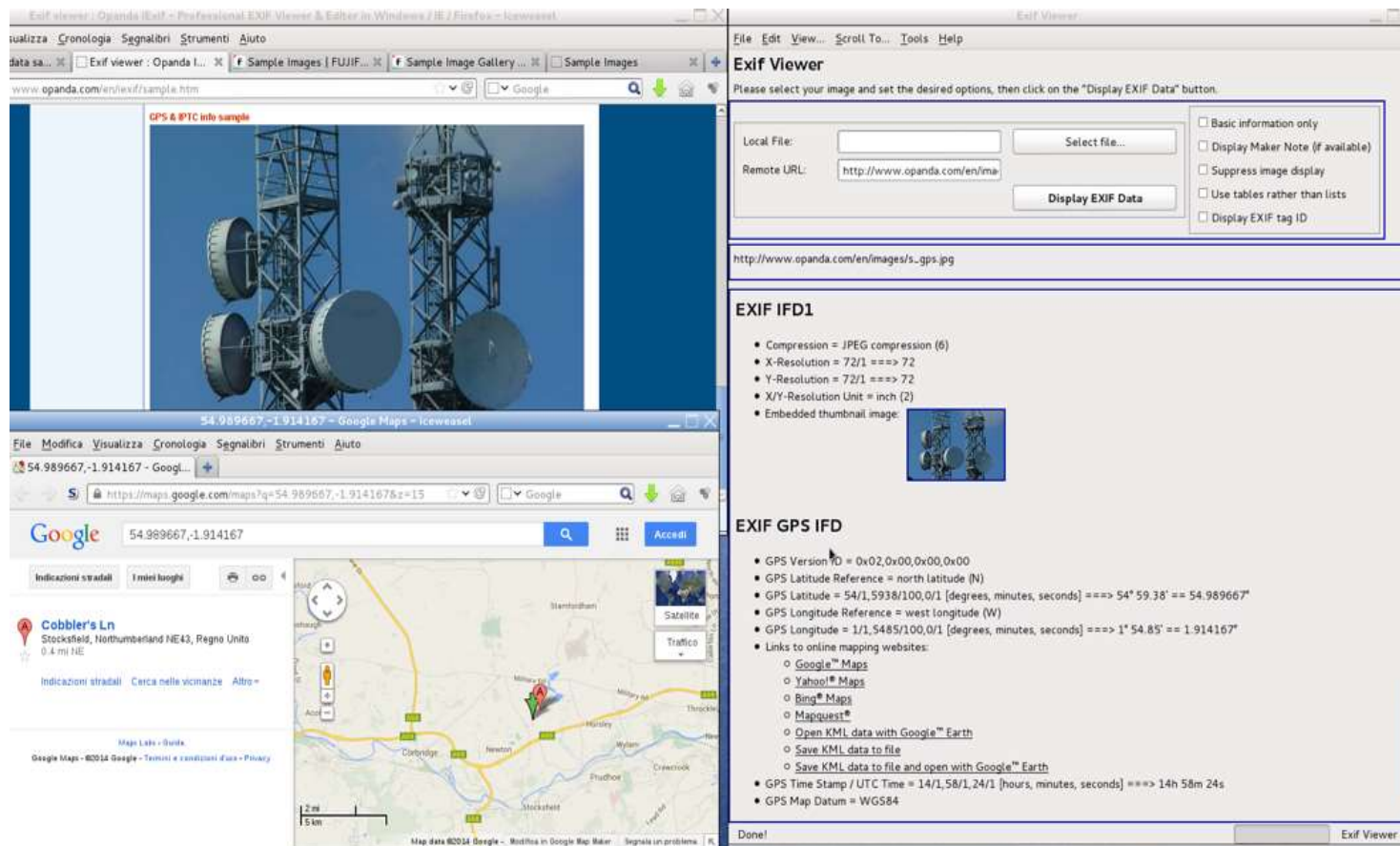
# Analizziamo le immagini



# Quello che le foto...

- I dati EXIF possono rivelare:
  1. Fotocamera utilizzata, caratteristiche delle foto
    1. Utilità: poter ricondurre una foto ad una macchina/utente
  2. Data ed ora
  3. Localizzazione geografica
- Uno dei tanti tool (anche online)
  1. <https://addons.mozilla.org/it/firefox/addon/exif-viewer/>
  2. NB: la maggior parte dei siti (Facebook, ecc.) rimuovono tutti i dati EXIF o almeno i dati GPS

# EXIF Viewer



# Ricerca per immagini

- Nel marzo 2013 uno studio ha dimostrato che la maggior parte dei social media più popolari rimuovono gli EXIF data.
  - <http://www.embeddedmetadata.org/social-media-test-results.php>








		Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	Exif	IPTC IIM	IPTC XMP
Tested in March 2013										
<b>Facebook -</b> <a href="http://www.facebook.com">www.facebook.com</a> Tested in June 2013	Metadata not shown anymore, all embedded metadata stripped-off from image files.									
		Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	IPTC	IPTC IIM	IPTC XMP
<b>Flickr FREE account-</b> <a href="http://www.flickr.com">www.flickr.com</a> Tested in June 2013 (PRO account may show other results)	A few metadata fields shown, 'by' was overridden, for any downscaled rendition all embedded metadata are stripped-off from image files, only the Original rendition keeps all metadata.									
		Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	Exif	IPTC IIM	IPTC XMP
					Exif	IPTC IIM	IPTC XMP	Exif	IPTC IIM	IPTC XMP
<b>Google+ -</b> <a href="http://plus.google.com">plus.google.com</a> Tested in March 2013	Primarily Exif metadata shown, all embedded fields are preserved.									
		Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	Exif	IPTC IIM	IPTC XMP
<b>Img.ly -</b> <a href="http://www.img.ly">www.img.ly</a> Tested in October 2012	No metadata shown, all embedded fields are preserved in the Save As image files.									
		Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	Exif	IPTC IIM	IPTC XMP
<b>Instagram -</b> <a href="http://instagram.com">instagram.com</a> Tested in June 2013	Image taken by a smartphone, metadata edited with an app, then posted at Instagram: No metadata are shown, all metadata stripped-off from Save As files.									
		Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	Exif	IPTC IIM	IPTC XMP

# Ricerca per immagini

- **Da una immagine si possono avere molte informazioni oltre a quelle EXIF**
  - Esaminare l'ambiente, le persone, la situazione, il contesto
  - Esaminare dove è stata reperita (sito, social, ...)
  - Individuare altre informazioni disponibili in rete effettuando una ricerca “per immagine”
  - Attenzione, se usate una immagine trovata su internet per un fake profile, ci sono ottime possibilità che TinEye trovi l'originale!
  - Provate i servizi come “Stolen camera finder”

# Ricerca per immagini

- Avendo una immagine, ad esempio da un profilo, si può fare una “Reverse Image Search”
- Alcune risorse utili per ricerca immagini
  - <https://images.google.com>
  - <https://yandex.com/images/>
  - <https://www.bing.com/images>
  - <http://www.tineye.com/>

	 Elements Identified	 Faces	 Structures	 Places	 Digital/ Logos	 Alternate Sizes	 Flipped or Altered
Google	1	Neutral	Great	Great	Great	Good	Neutral
Yandex	2+	Great	Great	Great	Good	Good	Good
Bing	3+	Good	Good	Good	Good	Neutral	Great
TinEye	1	Neutral	Neutral	Neutral	Great	Great	Good

# Ricerca per immagini – Esempio

Ecco un post su Twitter

<https://twitter.com/finriswolf/status/646210662973091840>

 **Not a spy**  
@finriswolf [Segui](#)

[#Syria](#) : Supposedly first pic of Russian jets on ground from the ground at [#Latakia](#) airport



23:33 - 21 set 2015

Come possiamo verificare l'esattezza dell'informazione?





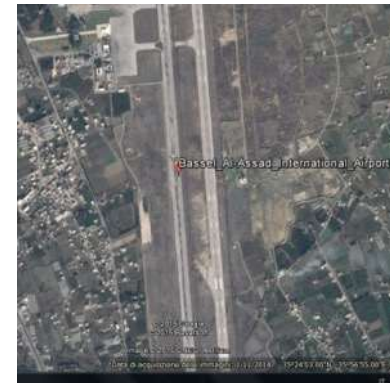
# Ricerca per immagini – Esempio

- Cerco su Wikipedia l'aeroporto di Latakia, Bassel Al-Assad
  - Aprendo la pagina di Wikipedia posso avere le geo-coordinate

## Aeroporti civili [ modifica | modifica wikitesto ]

- Aeroporto internazionale di Aleppo - 36°10′51″N 37°13′28″E﻿ / ﻿36.18083°N 37.22444°E﻿ / 36.18083; 37.22444
- Aeroporto internazionale Basil al-Asad (Laodicea) - 35°24′04″N 35°56′55″E﻿ / ﻿35.40111°N 35.94861°E﻿ / 35.40111; 35.94861
- Aeroporto internazionale di Damasco - 33°24′41″N 36°30′56″E﻿ / ﻿33.41139°N 36.51556°E﻿ / 33.41139; 36.51556

- Click su geo coordinate per aprire una lista di mappe <https://tools.wmflabs.org>
- Click su servizio scelto (Google Map)
- Esamino i segni sulla pista dell'aeroporto e li confronto con quelli presenti nelle immagini di Google Map



# Ricerca per immagini - Esempio

- Confronto il panorama (colline) sulla foto con le immagini su Google Map
- Confronto l'edificio che sembra una antenna radar sulla foto on photo con le immagini su Google Map
- Posso identificare il tipo di aerei ritratti



# Analizziamo una immagine



# Esercizio 7

- Cosa ci dice questa immagine?
- Provate ad analizzare l'immagine mostrata ed individuare le informazioni in essa contenute, quelle che possiamo estrapolare e quelle che possiamo trovare effettuando una ricerca



# Esercizio 7



# Maritime OSINT

- Come trovare le informazioni e tracciare le navi?
- Alcune risorse utili
  - <https://www.vesselfinder.com>
  - <http://maritime-connector.com>
  - <http://www.marinetraffic.com/it/>
  - <http://www.shipfinder.com>
- **Ottimo articolo con molte altre risorse**
  - OSINT on the Ocean: Maritime Intelligence Gathering Techniques
  - <https://medium.com/@raebaker/osint-on-the-ocean-maritime-intelligence-gathering-techniques-2ee39e554fe1>



# Esercizio 8

- Chi è l'uomo a sinistra della foto?
- Chi è l'uomo sulla destra nella foto?
- Chi ha preso la foto?
- Per chi lavora il fotografo?
- Dove è stata scattata la foto?
- Che tipo di fotocamera ha preso questa foto?
- Quando è stata scattata la foto?
- Fornire tre utenti Flickr che hanno inviato le foto da questa posizione.
- Qual è il nome utente di Twitter della persona a destra?
- Qual è la data di nascita della persona a destra?
- Qual è il nome della madre?
- Qual è il suo numero di telefono?
- Qual è il suo indirizzo di casa?
- Quale giornalista ha usato questa foto in un articolo di Forbes?
- Qual è la data di nascita della persona a sinistra?



# Wayback Machine

- “Internet non dimentica” è un luogo comune che ha un certo fondamento
- “Wayback Machine” è un progetto con lo scopo di archiviare e rendere disponibili pagine web e le loro modifiche nel tempo
- Questo permette (a volte) di recuperare interessanti informazioni
  - Vecchie informazioni pubblicate, vecchie rubriche telefoniche, vecchi dati che possono essere comparati con i dati attuali...
- Il più famoso è <http://archive.org>



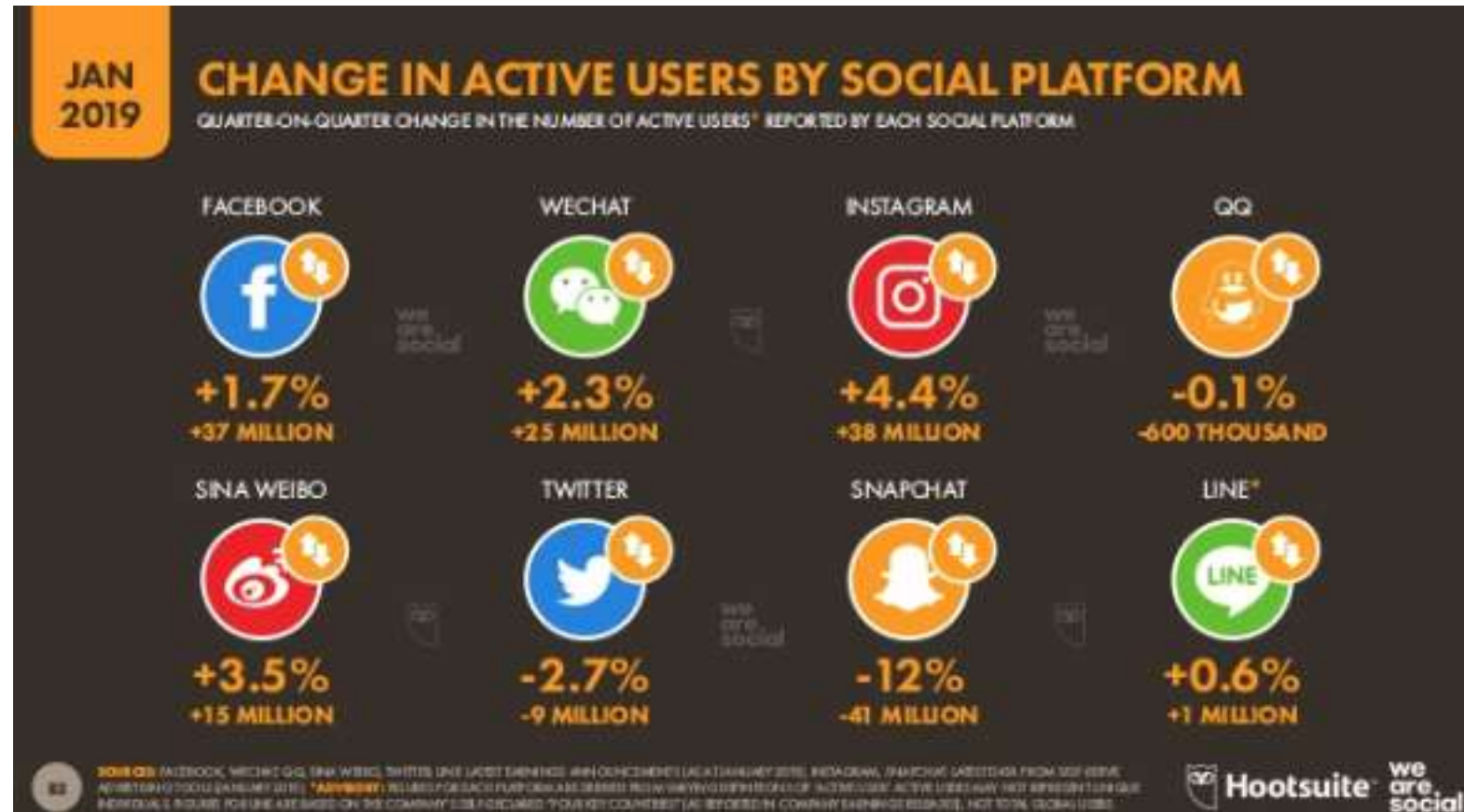
# Alternative a Wayback Machine

- [Archive.is](#)
- [Screenshots.com](#)
- [DomainTools](#)
- [iTools](#)
- [Alexa](#)

# Social Network



# Social Network



# Twitter

- **Twitter, con i suoi milioni di utenti, è un grande serbatoio di informazioni**
  1. Twitter utilizza il carattere “@” per identificare un profilo
  2. Non è obbligatorio usare un nome reale per creare un account, ma è necessaria email e numero di telefono
- **Twitter ha il suo motore di ricerca interno**
  - Usando il box di ricerca in top page
  - Usando i form nelle pagine dedicate:
    1. <https://twitter.com/search-home>
    2. <https://twitter.com/search-advanced>
    3. Usando una URL creata ad hoc:
      - <https://twitter.com/search?q=keywords>



# Twitter

- Quando si usa il box di ricerca è possibile filtrare i risultati usando i filtri preimpostati:
  - Popolari
  - Più recenti (ultime due settimane)
  - Persone
  - Foto
  - Video
  - Notizie
  - Trasmissioni (Periscope)



# Twitter

- **Elencare le informazioni per ogni profilo:**
  - [Twitter.com/username/likes](https://twitter.com/username/likes)
  - [Twitter.com/username/followers](https://twitter.com/username/followers)
  - [Twitter.com/username/following](https://twitter.com/username/following)
  - [Twitter.com/username/media](https://twitter.com/username/media)
  - [Twitter.com/username/with\\_replies](https://twitter.com/username/with_replies)
  - [Twitter.com/username/lists](https://twitter.com/username/lists)



# Twitter Search

- Oltre agli strumenti interni, ne esistono anche alcuni online che sfruttano le sue API
  - <http://onemilliontweetmap.com>
  - <https://twitterfall.com>
  - <https://followerwonk.com/bio>
  - <http://geosocialfootprint.com>
  - <http://omnicity.com/ot>
  - <http://mentionmapp.com>
  - <http://www.twitonomy.com>



# Twitter Tool: Tinfoleak

<https://tinfoleak.com>

## Search for Twitter users leaks



- Basic information about a Twitter user (name, picture, location, followers, etc.)
- Devices and operating systems used by the Twitter user
- Applications and social networks used by the Twitter user
- Place and geolocation coordinates to generate a tracking map of locations visited
- Show user tweets in Google Earth!
- Download all pics from a Twitter user
- Hashtags used by the Twitter user and when are used (date and time)
- User mentions by the the Twitter user and when are occurred (date and time)
- Topics used by the Twitter user



# Instagram

- E' possibile effettuare ricerche su Instagram usando il box di ricerca che ha una funzione di auto completamento
- Esistono servizi online per effettuare ricerche
  1. <http://www.imgrum.org/search?query=keyword>
  2. <https://tofo.me>
  3. <http://mininsta.net/>
  4. <https://websta.me>
  5. <http://www.thepicta.com>
- Ovviamente sono sempre utilizzabili i motori di ricerca
- Si possono valutare le connessioni tramite i "like" ecc...



# Come funziona Facebook

- Ogni profilo, foto, post, commento, pagina, ecc. in FB è un oggetto referenziato in un database
- Ogni oggetto del database è identificato da un **ID numerico**
- Tramite questo ID è possibile mettere in relazione ogni oggetto presente su FB
- Usando Facebook Graph Search è possibile creare query mirate e molto dettagliate



# Facebook: individuare il profile ID

Avendo la URL del profilo:

1. <https://findmyfbid.com>
2. <https://lookup-id.com>
3. <https://seotoolstation.com/bulk-facebook-id-finder>

Si può individuare un user ID analizzando le URL delle foto

1. <https://www.facebook.com/photo.php?fbid=10154851531324251&set=pb.725584250.-2207520000.1467299078.&type=3&theater>
2. <https://www.facebook.com/photo.php?fbid=10152715060201101&set=a.10151932269991101.1073741826.523266100&type=3&theater>



# Facebook: usare lo User ID

Prendiamo un profilo FB

- <https://www.facebook.com/zuck>

Individuiamo lo User ID (4)

Proviamo ad usarlo:

- <https://www.facebook.com/4>

Oppure:

- <https://www.facebook.com/profile.php?id=4>

**In pratica, lo User ID corrisponde al profilo utente**



# Facebook Graph Search

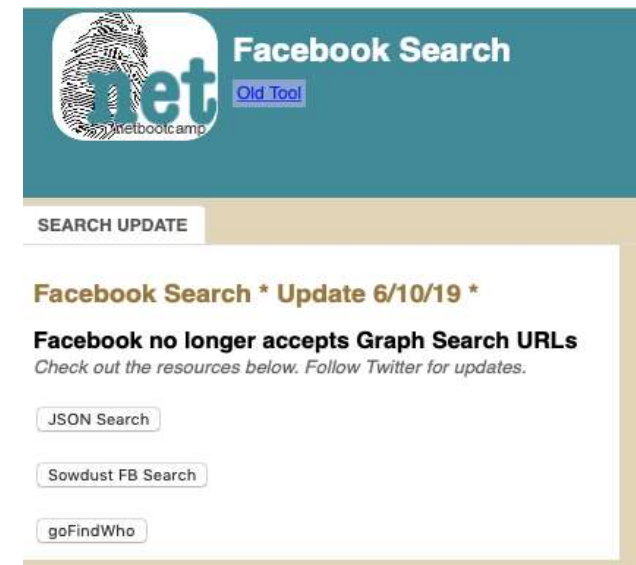
- E' una funzionalità introdotta nel 2013
- Vi sono vari metodi per effettuare le ricerche sul database di Facebook
- Usando il box di ricerca è possibile cercare pressoché qualunque keyword
- E' possibile impostare la categoria di risultati per mezzo dei pulsanti presenti sotto il box
- E' possibile rifinire i risultati impostando opportunamente le opzioni sulla sinistra dei risultati
- Da ottobre 2019, Facebook ci ha reso la vita ancora più difficile nell'effettuare le ricerche...



# Ricerche su Facebook

## Ecco come avviare (in parte)

- <https://gist.github.com/nemec/2ba8afa589032f20e2d6509512381114>
- <https://sowdust.github.io/fb-search/>
- <https://gofindwho.com>
- <https://www.aware-online.com/osint-tools/facebook-search-tool/>
- <https://graph.tips/beta/>
- <https://whopostedwhat.com>
- <https://intelx.io/tools?tab=facebook>
- <https://searchisback.com>
- <https://plessas.net/facebookmatrix>



# Agenda

- **Introduzione a OSINT**
  - Chi utilizza OSINT e perché
- **Cosa e Dove cercare**
  - Motori, servizi, ed altri luoghi
  - Social network, relazioni, cerchie, e tutto il resto
- **La cassetta degli attrezzi**
  - Uso dei motori di ricerca
  - Strumenti, Tecniche, Network analisi, Metadata
  - Sock Puppet e Social Network
- **Sicurezza e contromisure**

# Metadata





# Cosa sono i Metadati

I metadati sono le informazioni nascoste all'interno dei file detti anche «data about data»

L'analisi dei metadati di un file può portare interessanti risultati utili ad esempio per restringere il campo di indagine, come:

- nome utente
- data creazione
- versione software

# Fear the FOCA!

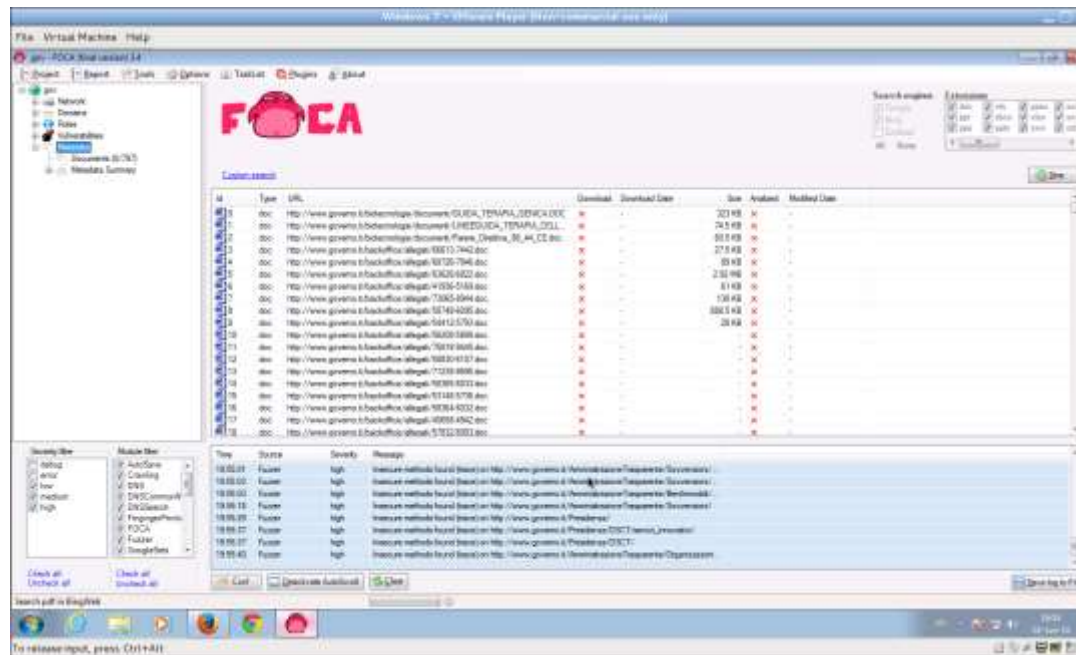
- FOCA (Fingerprinting Organizations with Collected Archives) è uno strumento utilizzato principalmente per trovare i metadati e le informazioni nascoste nei documenti esaminati
- Se questi documenti sono linkati su pagine web possono essere scaricati e analizzati con FOCA.
  1. FOCA gira sotto Windows / Wine o su macchina virtuale
  2. <https://www.elevenpaths.com/labs/tools/foca/index.html>

# Fear the FOCA!

- FOCA effettua ricerche con Google, Bing Exealed per trovare documenti “office” presenti sul sito indicato
- Quindi scarica i documenti e ne estrae i metadati:
  - File creator
  - Timestamps
  - Usernames in full paths (C:\Documents and Settings\Joe)
  - Operating systems, software versions
  - Printers, Shared printers, Shared folders
  - Local and remote disk
  - NetBIOS names, Hostname, IP address
  - Mobile phone, camera models

# Fear the FOCA!

- FOCA ha anche alcune funzioni “particolari” come:
  - search for basic SQL injection, open directory listings, perform zone transfers, flag insecure HTTP methods, perform DNS cache snooping, flag "juicy files", etc...



# Esercizio 10

- A caccia di Metadata...
  1. Università di Tor Vergata?
  2. Il vostro sito personale?
  3. o quello della vostra azienda?

# Maltengo

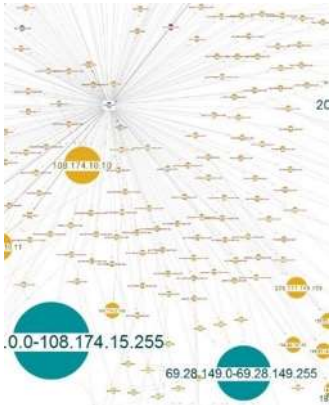
- MALTEGO è un software sviluppato dalla società Paterva, che offre la possibilità di raccogliere informazioni tramite la consultazione di dati pubblicamente accessibili e raggrupparle, in formato grafico attraverso l'utilizzo di trasformazioni.
  - Effettua ricerche e connessioni fra informazioni liberamente disponibili e rappresenta i risultati in forma grafica
    1. solo link analysis no social network analysis (SNA) – analisi delle reti sociali
  - Il cuore del programma sono le “trasformazioni” ovvero dei «plugin» che effettuano le ricerche e le correlazioni

# Maltengo

- Paterva Maltego è disponibile in due versioni, Community e su licenza annuale
  1. <https://www.paterva.com>
  2. <https://www.maltego.com>
- Effettuata la registrazione per la versione “Community” si possono provare le trasformazioni disponibili ma con alcune limitazioni.
- La community mette a disposizione degli utenti ulteriori «trasformazioni» sviluppate dagli utilizzatori

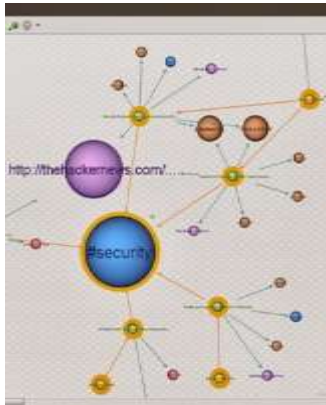
# Maltengo

- Alcuni esempi delle sue funzionalità:



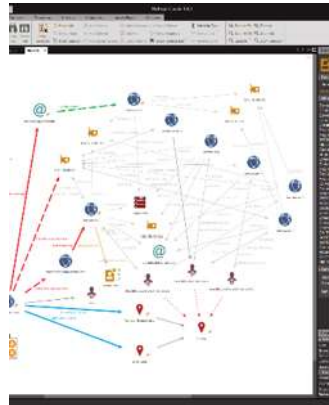
## Network Footprinting

footprint of the domain  
linkedin.com



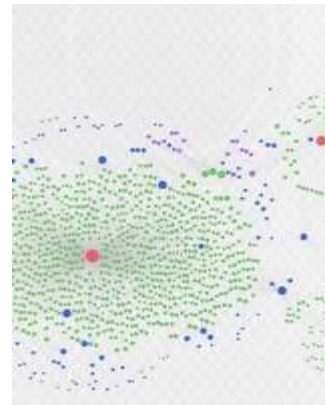
## Social Network Monitoring

keywords, links and  
hashtags  
shared by popular security  
based Twitter users



## Cyber Crime Investigation

anonymous online DDOS  
attack site



## Malware Attribution

Angler and Bedep  
distribution networks and  
domains registered

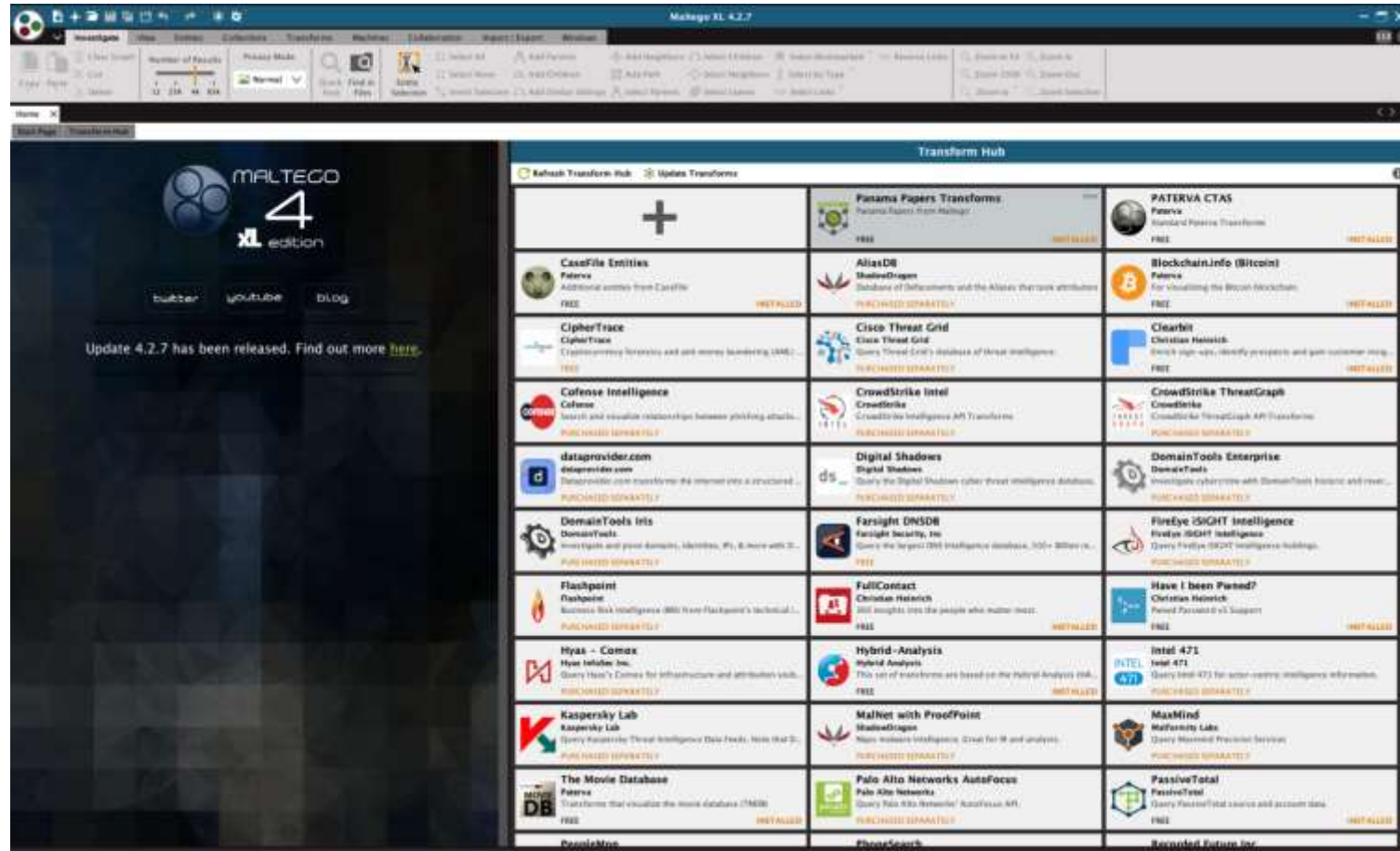


## Website Correlation With Tracking Codes

Google Analytics tracking  
code

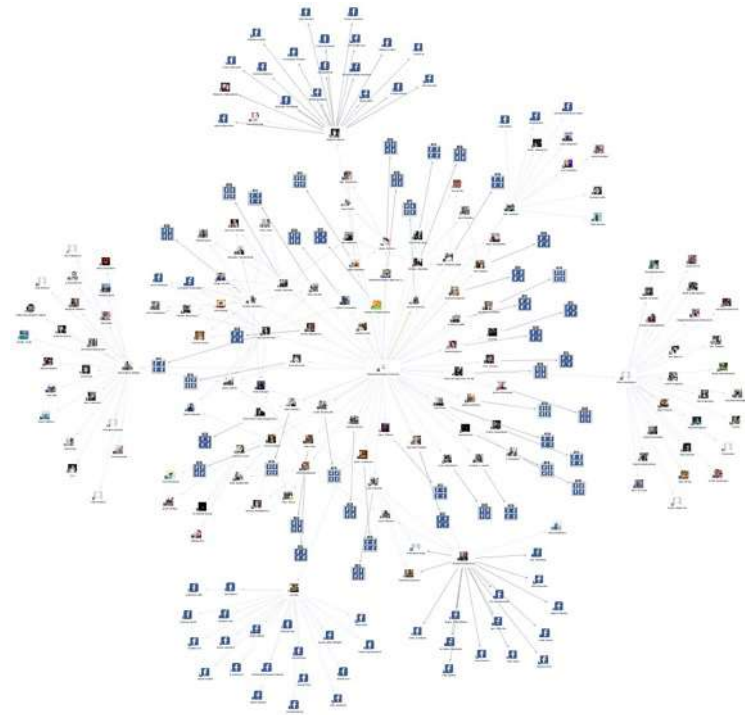


# Maltengo



# Maltengo: Social Links

- One workplace for search & visualization
- Social Links - Commercial plugin for Maltego Classic & XL by Paterva

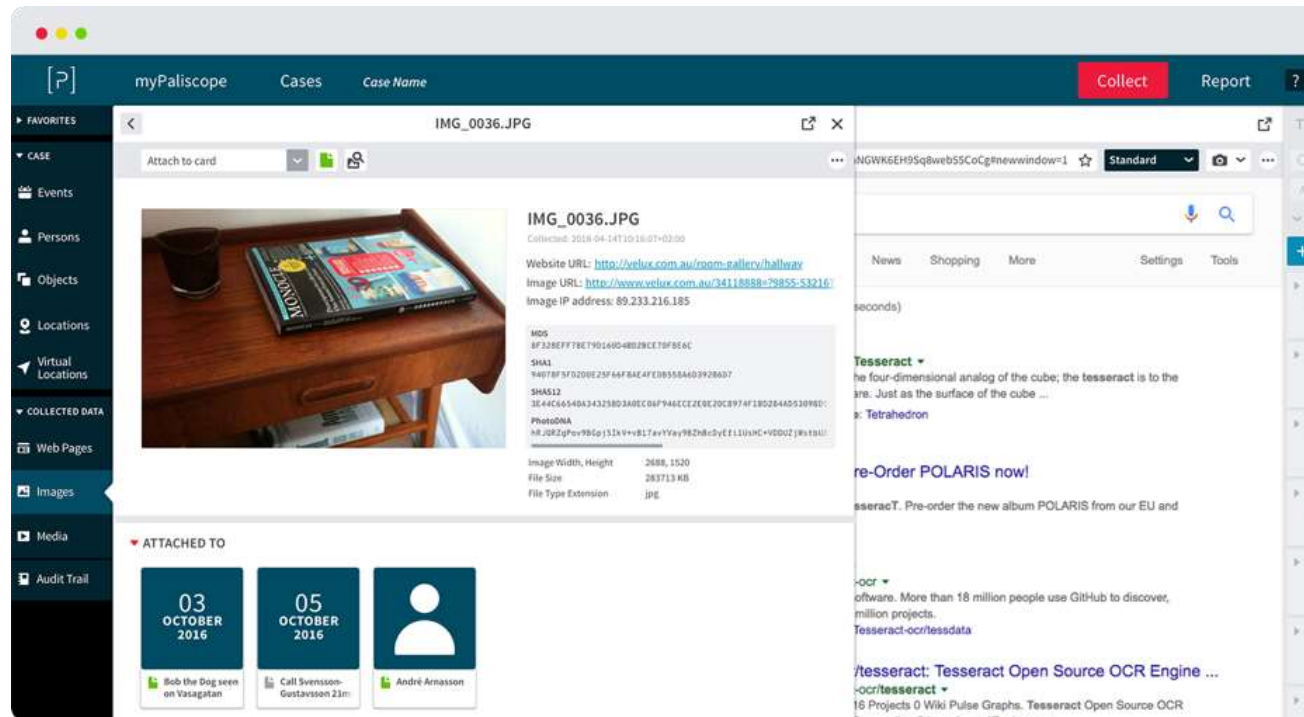


# Maltengo: Social Links

- **Socials:** Facebook, Instagram, LinkedIn, Twitter, Skype, Xing, Foursquare, Badoo, Blogger, Classmates, Flickr, Github, FullContact, MyMail, Myspace, Odnoklassniki, Snapchat, Sqoop, V Kontakte, Youtube, Photobucket, Deviantart, Pinterest, Tinypic, Imageshack and others.
- **Messengers:** Telegram, Signal and others.
- **DarkNet:** 30+ forums and marketplaces without authorization.
- **Corporate:** CompaniesHouse, Companies OC, Google Companies, OCCRP, Offshores.
- **Integration** with 3rd party services: Pipl, Bitcoinwhoswho, Securitytrails, Censys, Shodan, ZoomEye and others.
- **Social Links** data base with 7 TB of e-mails, aliases, names, phone numbers.
- **Cryptocurrency:** Ethereum platform analysis, Bitcoinwhoswho, TokenView;
- **Some more sources:** DocumentCloud, Ebay, Torrents, TruePeopleSearch, Wikileaks, dating sites such as Match, Chemistry, Fling, Meetup, okcupid, ask.fm, rsvp.com.au and others.

# Paliscope

- Paliscope is an online investigation tool for collecting open source data in an easy, fast and secure way.



# Geolocalizzazione

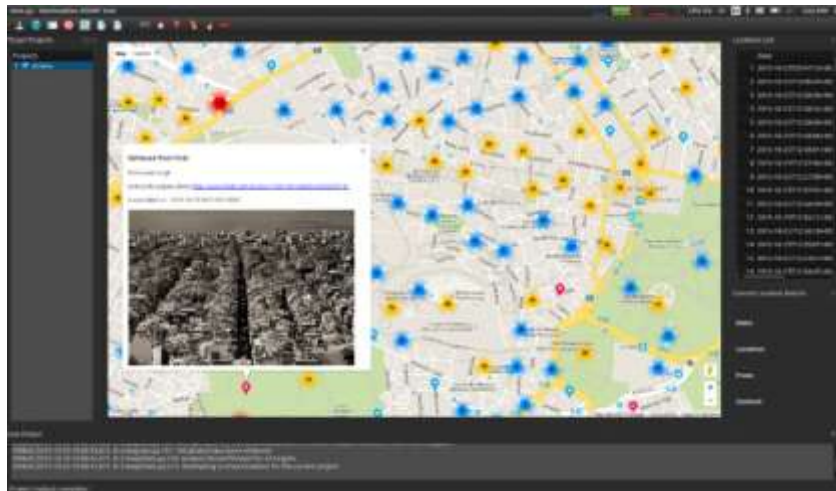
- Riuscire a posizionare fisicamente il luogo dove si trova il soggetto di una ricerca può avere un valore inestimabile
- Esistono strumenti in grado, a seconda del contesto, di indicare più o meno precisamente la località dalla quale è stata effettuata un contatto su una rete (mobile, Internet)

# Infosniper

- [www.infosniper.net](http://www.infosniper.net)
  1. “infoSNIPER offers free as well as commercial web API geolocation services.”
  2. Inserendo un IP viene mostrata la posizione su una mappa google, yahoo, microsoft
  3. Ad esempio un IP può essere recuperato da un header di una mail o da un log di un sito web

# 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 o Instagram, se presenti
  - <http://www.geocreepy.com>
  - <http://github.com/ilektrojohn/creepy/>



# Fonti non convenzionali

- Abitazione, azienda, dintorni
- Google Street view
- **Foto satellitari**
- Google Map, Earth
- **Video**
- Youtube, Vimeo
- **Ma anche IBAN...**



# Fonti non convenzionali

- E' possibile analizzare un IBAN per cercare informazioni, compresa posizione geografica

1. <http://www.mutuissimo.it/iban.asp>
2. <http://it.ibancalculator.com/>

VERIFICA IBAN

Stato: IT | IBAN: IT17601016000 | Verifica

✓ Esatto! Codice formalmente corretto.

IBAN - ITALY - FORMAT				
Country code	IBAN check digits	CIN (Check char)	ABI (National bank code)	BBAN (Branch code) Numero di conto corrente (Account number)
ISO 3166-1	IT	07601	01600	
FORMATO CARTACEO		FORMATO DIGITALE		
IBAN IT: IT17601016000		IT 0760101600		

Dati della filiale

Abi: 07601 Cab: 01600  
Banca: POSTE ITALIANE SPA  
Filiale: MILANO  
Indirizzo: P.ZZA CORDUSIO, 4 MILANO 20100 MI

Telefono | Agenda | Risorse | Wikipedia



# Esercizio 11



**Maks Czuperski** ✓

@MaksCzuperski

Segui

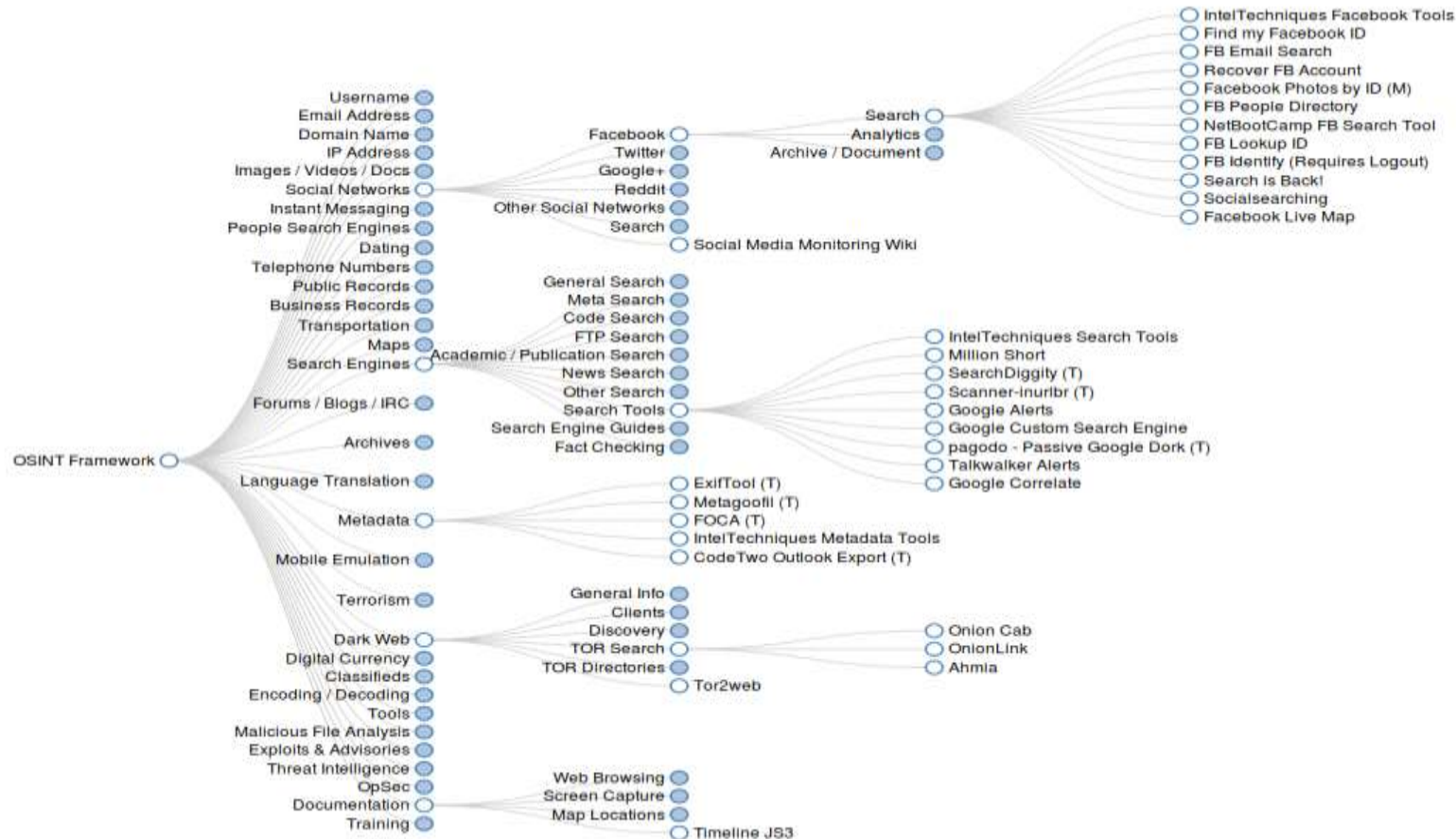


[#DigitalSherlocks](#) out there!—Where am I?



03:43 - 12 gen 2017

# Osint Framework



<http://osintframework.com>

# Analisi delle fonti

- La valutazione delle fonti è un fattore importante del processo OSINT.
- Ci sono delle domande che ci dobbiamo porre per determinare l'affidabilità delle fonti
  1. Who
  2. When
  3. Where
  4. What
  5. Why

# Analisi delle fonti

- **Who:** Chi ha creato l'informazione?
  1. E' una fonte autorevole?
  2. La fonte ha pubblicato altre informazioni? Come sono state giudicate?
- **When:** Quando è stata pubblicata l'informazione?
  1. Definite la data ed il contesto dell'informazione
- **Where:** Dove è stata pubblicata l'informazione?
  1. Il sito/pagina web è autorevole?
  2. E' una fonte privata o pubblica?
  3. Dove è situata (nazione/sito web/ecc.)?
- **What:** Quale è il contenuto dell'informazione ?
  1. E' confermato da altre fonti?
- **Why:** Perché è stata rilasciata questa informazione?
  1. Cercate di comprendere le motivazioni della pubblicazione

# OSINT Report

- **Un report deve essere:**
  - Chiaro
  - Completo
  - Contenere un riepilogo breve per non specialisti (executive report)
  - Indicare le fonti
  - Specificare le metodologie utilizzate
  - Suggestire ulteriori direzioni da esplorare

# OSINT Report: quali informazioni

- **Ad esempio, un report OSINT su una persona può comprendere:**
  - Informazioni personali e familiari
  - Immagini del soggetto (ma non solo)
  - Interessi e hobby
  - Contatti (email, telefono, indirizzo, profili)
  - Studi
  - Lingue conosciute
  - Esperienze professionali
  - Lavoro attuale
  - Business partner
  - Associazioni
  - Persone esterne di rilevante importanza
  - Link a materiali e documenti
  - Annotazioni dell'operatore

# Strumenti di reportistica

- Potreste avere bisogno di acquisire come prova ciò che è mostrato in una pagina web
- Un metodo è quello di salvare la pagina e firmarla digitalmente così da avere il contenuto con la data/ora dell'acquisizione
- Ci sono strumenti che fanno questo automaticamente



# Strumenti di reportistica

- Hashbot è uno strumento per acquisire e validare tramite firma digitale verificabile nel tempo lo stato di una pagina web o di un documento in internet.
  1. <https://www.hashbot.com>
- FAW è il primo browser concepito per l'acquisizione forense delle pagine web
  1. <http://www.fawproject.com/it/default.aspx>
- Altro strumento forense, X1 Social Discovery
  1. <https://www.x1.com/products/x1-social-discovery>
- Se la firma digitale non è richiesta:
  1. <http://www.printfriendly.com>

# Agenda

- **Introduzione a OSINT**
  - Chi utilizza OSINT e perché
- **Cosa e Dove cercare**
  - Motori, servizi, ed altri luoghi
  - Social network, relazioni, cerchie, e tutto il resto
- **La cassetta degli attrezzi**
  - Uso dei motori di ricerca
  - Strumenti, Tecniche, Network analisi, Metadata
  - Sock Puppet e Social Network
- **Sicurezza e contromisure**

# Cosa è un Fake Profile?

- Un “sock puppet” è un falso profilo o falsa identità utilizzato per vari motivi
- La chiave è la plausibilità
- Le caratteristiche devono essere ritagliate sul target



# Cosa è un Fake Profile?



Admiral James Stavridis was targeted by cyber-spies on Facebook who set up fake accounts in his name. Photograph: Yves Logghe/AP

# Fake Profile: perché?

- Perché usare un fake profile?
- Nascondere la propria identità reale
- Per la propria (e altrui) sicurezza
- Per assumere l'identità di un'altra persona
- Per creare confusione
- Per presentarsi in maniera credibile
- Per introdursi in un gruppo
- ...
- ma attenzione al suo utilizzo sostituzione di persona (art. 494 cod. pen.)

# Fake Profile: chi?

- Chi utilizza Fake Profile?
- Giornalisti, investigatori
- Interessati a manipolare l'opinione pubblica
- Analisti OSINT
- I Cattivi: stalker, spammer, cyber criminali
- Agenzie (NSA)?
- In breve: chiunque...

# Fake Profile: esempi

1. Sock Puppet sono stati utilizzati:
2. Per influenzare la gente
  - Elezioni in Corea del Sud, Stati Uniti, Italia...
3. Per distruggere organizzazioni
  - Palantir/HBGary (prossima slide)
4. Per spionaggio
  - Il caso dell'Ammiraglio James Stavridis

# Fake Profile: il caso Team Themis

## 1. Giocare sporco con Sock Puppet:

- Il “ Team Themis” (HBGary, Berico, Palantir) ha pianificato una operazione per screditare e diffamare Wikileaks.
- In un'altra operazione il bersaglio erano i sindacati di lavoratori che si opponevano alla Camera di Commercio degli Stati Uniti
- Entrambi i progetti prevedevano l'infiltrazione nei social network per rilasciare documenti falsi, creare "fughe di notizie" con informazioni imbarazzanti sulla vita personale degli attivisti



# Background

1. In base al tipo di attività, deve essere definito il profilo personale del Vostro “alter ego”
2. Sesso, nome, storia
3. E-mail, sito web personale, su quali siti è presente
4. Profili sui Social networks
5. Lavoro, Contatti, Famiglia, ecc.
6. Se è un profilo aziendale:
7. Prodotti, staff, clienti, ...
8. Sito web, email, indirizzo, telefono,...

# Rischi

- E' facile bruciare un Fake Profile
- C'è il rischio di divulgare le proprie informazioni personali reali
- Si può fallire lo scopo ed essere scoperti, in questo caso:
  1. Discredito personale
  2. Discredito dell'organizzazione
  3. Altri rischi personali

# Individua i Fake Profile

1. Esamine le foto postate. Sono compatibili?
  - Verificatele con TinEye!
2. Il profilo è aggiornato spesso?
3. Verificate la lista degli “amici”
  - es. Solo donne? Mmm ...
4. Esamine le informazioni personali
  - Scuola, lavoro, ...
5. La data di nascita?
6. Esamine tutti i post ed i commenti

# Fake Profiles generator

1. Una buona parte dei profile sui social networks sono gestiti da bot (per attività di intelligence, marketing, disinformazione, manipolazione dell'opinione pubblica)
2. Nel suo rapporto annuale 2013, FB stima in almeno 100 milioni i profile "duplicati"

## Esistono decine di generatori di fake profile

1. <http://www.datafakegenerator.com/generador.php>
2. <http://www.name-list.net/>
3. <http://www.fakenamegenerator.com/>
4. <http://www.pearltrees.com/djager/false-facebook-text-message/id3277486>
5. <http://www.classtools.net/FB/home-page>

# Agenda

- **Introduzione a OSINT**
  - Chi utilizza OSINT e perché
- **Cosa e Dove cercare**
  - Motori, servizi, ed altri luoghi
  - Social network, relazioni, cerchie, e tutto il resto
- **La cassetta degli attrezzi**
  - Uso dei motori di ricerca
  - Strumenti, Tecniche, Network analisi, Metadata
  - Sock Puppet e Social Network
- **Sicurezza e contromisure**

# Anonimato e sicurezza

- A cosa si deve prestare attenzione durante una sessione OSINT?
  - **Profilazione**
    - Esistono decine di sistemi per profilare un utente od un sistema
    - <https://panopticlick.eff.org/>
  - **Traffico**
    - Alcune attività OSINT generano una grande quantità di traffico che può essere sospetto od analizzato
  - **Dati personali**
    - Non tradirsi, ad esempio con post non valutati attentamente

# Anonimato e sicurezza

- **A cosa si deve prestare attenzione durante una sessione OSINT?**
  - Lasciare trapelare o scoprire la propria identità
    1. “Oops, mi sono collegato al mio fake profile da una WiFi pubblica senza proteggermi...”
    2. “Oops, ho dimenticato di citare una mail/ho usato un indirizzo sbagliato”
    3. “Oops, Ho dimenticato di attivare la VPN...”
  - Ambienti ostili
    1. Analisi del traffico, perdita o sequestro dell’hardware
  - Malware
- **Lo storico delle ricerche effettuate rimane per sempre!**

# Anonimato e sicurezza

- La prima preoccupazione deve essere di proteggere la propria identità
- Due livelli di protezione
  - Fisica (indirizzo IP)
  - Logica (dati personali reali)



# Protezione logica

- **Qualsiasi cosa che usiate può parlare di voi**
  - Indirizzi e-mail
  - Foto
  - Sistema operativo utilizzato, lingua, timezone
  - Browser, addon, fonts utilizzati
  - Contatti su social
  - Siti preferiti
  - Cookies
- **Hint: non usate la vostra CC per acquistare una VPN!**
- **Ancora più importante se usate un fake profile!**

# Protezione logica

- L'indirizzo IP dal quale vi collegate rivela troppe cose per poterlo divulgare tranquillamente
- È buona cosa utilizzare sistemi che nascondano il proprio IP
  - VPN, proxy, TOR

# Virtual Machine

- L'utilizzo di machine virtuali dedicate fornisce un livello addizionale di sicurezza fra voi ed il target
- Separate sempre la ricerca dall'analisi
- Sono disponibili vari software free per la virtualizzazione, ad esempio:
  - **VMware Player**
  - <https://my.vmware.com/web/vmware/downloads>
  - **VirtualBox**
  - <https://www.virtualbox.org/>

# Suggerimenti

1. **Free web proxy**
  - hidemyass (<http://www.hidemyass.com/>)
  - o soluzioni alternative...
2. **Fatevi una lista di proxy da paesi diversi e tenetela aggiornata!**
3. **Sistema operativo GNU/Linux live per proteggere la privacy**
  - Tails (<https://tails.boum.org/>)
4. **VPN (trovate un provider serio)**
5. **The Onion Router (TOR): Tor browser**
  - <https://www.torproject.org>

# Proteggere la propria azienda

1. Formare dipendenti e dirigenti per un utilizzo consapevole degli strumenti (computer, mobile, mail, social networks,...)
1. Definire e applicare policy e best practice
1. Verificare periodicamente il grado di consapevolezza degli utenti
1. Utilizzare strumenti di prevenzione (blocco dei servizi/siti, analisi e filtraggio dei contenuti,...)

# Proteggere la propria azienda

1. Verificare quali informazioni rilascia/ha rilasciato la propria organizzazione
1. Valutare / sanitizzare i documenti pubblicati / da pubblicare
1. Valutare quali informazioni sono pubblicamente disponibili da altre fonti sulla propria organizzazione o su di noi

# Mission

1. Ogni team deve scegliere un team Leader (che cambierà per ogni missione) il quale dovrà:
  - assegnare i compiti ai membri del team e verificare l'avanzamento dei lavori
  - Presentare in un report i risultati della missione (-5-10 minuti)
2. Il report dovrà contenere i fatti e le informazioni trovate, le fonti, gli strumenti ed i metodi utilizzati
3. Preparete delle slide per illustrare il report

# Software

1. **XMIND** (<http://www.xmind.net/>) is the most professional and popular mind mapping tool
2. **FOCA** (<https://www.elevenpaths.com/labstools/foca/index.html>) is a tool used mainly to find metadata and hidden information in the documents it scans.
3. **MALTEGO** (<https://www.paterva.com/web6/products/maltego.php>) is a unique platform developed to deliver a clear threat picture to the environment that an organization owns and operates. Recommended third-party transform **SOCIAL LINKS** (<https://mtg-bi.com>)
4. **CREEPY** (<http://github.com/ilektrojohn/creepy/>) is a Geolocation OSINT Tool. Offers geolocation information gathering through social networking platforms
5. **EXIF VIEWER** (<https://addons.mozilla.org/it/firefox/addon/exif-viewer/>) is an add-on for Firefox. Displays the Exif and IPTC data in local and remote JPEG images
6. **TOR BROWSER** (<https://www.torproject.org/projects/torbrowser.html.en>) lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software
7. **PALISCOPE** (<https://www.paliscopes.com>) is an investigation and collection tool for OSINT
8. **HUNCHLY** (<https://www.hunch.ly>) is an investigation and collection tool for OSINT



# Link: strumenti e documentazione

1. <http://www.phibetaiota.net/wp-content/uploads/2014/01/Ben-Benavides-Social-Web-Sites-A-Guide.pdf>
2. <http://www.phibetaiota.net/2014/01/ben-benavides-exploring-social-media-web-sites-a-guide-for-the-open-source-analyst/>
3. <http://www.onstrat.com/osint/>
4. [site://www.css.ethz.ch osint](http://www.css.ethz.ch/osint/)
5. <http://demosthenes.info/blog/670/The-Face-Of-Lorem-Ipsum-Profile-Generators-And-Random-User-Images>
6. <http://it.fakenamegenerator.com/gen-male-it-it.php>
7. <http://www.datafakegenerator.com/generator.php>
8. <http://simitator.com/generator/facebook>
9. <http://www.phibetaiota.net/wp-content/uploads/2013/07/2013-07-11-OSINT-Zool-Kit-On-The-Go-Bag-O-Tradecraft.pdf>
10. <http://www.wikihow.com/Reveal-a-Fake-Facebook-Account>
11. <http://www.difesaonline.it/index.php/it/15-notizie/approfondimenti/280-la-demodologia-l-osint-open-source-intelligence-italiana>
12. <http://rr.reuser.biz/>
13. <https://twitter.com/OSINTCenter>
14. <http://www.inteltechniques.com/links.html>
15. <http://actualfacebookgraphsearches.tumblr.com/>

# Links: staying under the radar

1. <http://bugmenot.com/>
2. <https://www.guerrillamail.com/>
3. <http://mailinator.com/>
4. <http://10minutemail.com/>
5. <http://getairmail.com/>
6. <http://receive-sms-online.com/>
7. <http://www.receivesmsonline.net/>
8. <http://www.pinger.com/tfw/>

# Links: pubblicazioni

1. <http://www.opensourceintelligence.eu/ric/doc/INSCOM%20OSINT%20HB.pdf>
2. <http://www.opensourceintelligence.eu/ric/doc/The%20Extreme%20Searcher%27s%20Internet%20Handbook.pdf>
3. <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/docs/EBB-005.pdf>
4. <http://www.phibetaiota.net/wp-content/uploads/2009/07/OSINT-2ool-Kit-OnThe-Go-Bag-O-Tradecraft.pdf>
5. [http://www.oss.net/dynamaster/file\\_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf](http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf)
6. <http://verificationhandbook.com/>

# Links: fonti

1. <https://krebsonsecurity.com/2017/09/who-is-marcus-hutchins/>
2. <https://twitter.com/AntDeRosa/status/430108306573500417/photo/1>
3. <http://deepweblinks.org/>
4. <http://thehiddenwiki.org/>
5. <http://tordeepweb.com/>
6. <http://dirnxxdraygbifgc.onion/>
7. <http://mashable.com/2009/08/21/gorgeous-facebook-visualizations/>
8. <http://www.internationalanalysiscenter.com/research-tools.html>
9. <http://fas.org/>
10. <https://sites.google.com/site/audaces2006fortunaiuvat2010/osint-strategic-news>

# Analisi delle Fonti Aperte OSINT

Raoul Chiesa e Ing. Selene Giupponi