



ILS Perugia



Tecniche OSINT per scoprire le Fake News

Paolo Giardini e Sonia Montegiove

Linux Day 2021, 23 ottobre

Dati a chi?

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"

L'arte di fare OSINT

Esperienza, intuito, istinto sono ciò che separa buoni risultati da risultati scadenti.

Per esempio: trovare un *username* conduce ad altri *profile* (del target, delle sue cerchie) con altri *dati*. Questo può condurre al *nome reale*, che può condurre all'*indirizzo fisico* o ad altre *pagine web*, alla *geolocalizzazione* del target, e via così.

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



Come fare?

Individuate le **informazioni che già conoscete**, ovvero cosa vi è stato dato come “punto di partenza”.

- chi/cosa è il Target;
- a quale domanda dovete rispondere;

Valutando bene le richieste potete **individuare le prime informazioni**, necessarie per indirizzarvi verso un percorso di ricerca e individuare le prime “parole chiave” da inserire in un motore di ricerca.

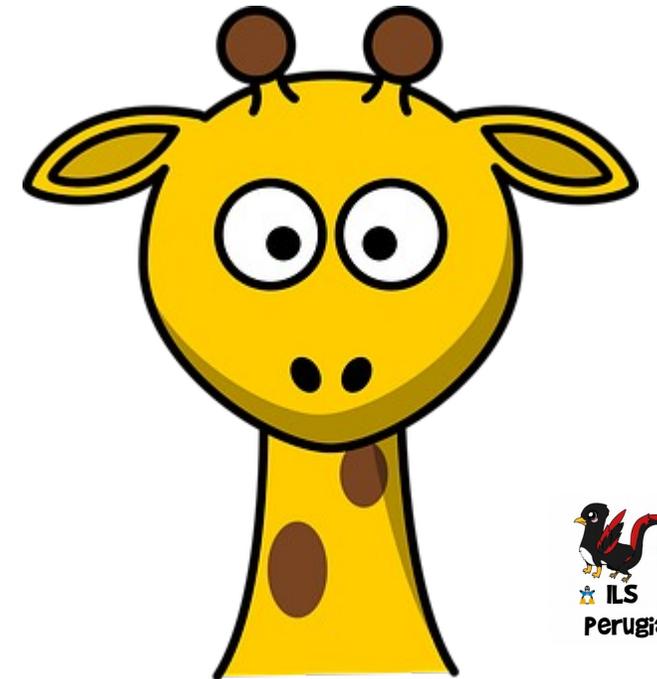
Come fare?

- Ricerca per parole chiave derivate dal contesto
- Analisi delle immagini
- Correlazione delle informazioni disponibili



Cosa serve?

- Fantasia
- Immaginazione
- Capacità logiche
- Qualche conoscenza tecnica



Cominciamo dai motori di ricerca...

- Come funzionano
- Chiavi di ricerca
- Comandi speciali

Come funziona un motore di ricerca?

Ci sono tre parti in un motore di ricerca:

- uno **SPIDER**, che visita ed estrae dati dai siti web
- Un **database** in cui i dati sono indicizzati
- Un motore che, utilizzando un **algoritmo**, analizza la query e restituisce i risultati

Gli operatori di Google per...

Cercare sui social media

Usa il simbolo @ davanti a una parola per cercare sui social media. Ad esempio: @twitter.

Cercare hashtag

Usa il simbolo # davanti a una parola. Ad esempio: #makeup.

Escludere parole dalla ricerca

Usa il simbolo - davanti a una parola da escludere. Ad esempio: paolo rossi - calciatore

Gli operatori di Google per...

Cercare una corrispondenza esatta

Metti una parola o una frase tra virgolette. Ad esempio: "edificio più alto".

Abbinare le ricerche

Inserisci "**OR**" tra ciascuna query di ricerca. Ad esempio: maratona OR gara. OR deve essere scritto in maiuscolo

Cercare in un sito specifico

Scrivi "**site:**" davanti a un sito o un dominio. Ad esempio: site:youtube.com o site:.gov.

Gli operatori di Google per...

Visualizzare la versione di un sito memorizzata nella cache di Google

Scrivi "**cache:**" davanti all'indirizzo del sito.

Ricerca di file

Scrivi: «**filetype:**» davanti al tipo di file cercato (pdf, doc, docx, jpg,...)

Gli operatori di Google per...

Cercare nell'indirizzo della pagina web

Scrivi «**inurl:**» oppure «**allinurl:**» davanti alle parole che devono essere presenti nella URL.

Cercare nel titolo della pagina

Scrivi «**intitle:**» oppure «**allintitle:**» davanti alle parole che devono essere presenti nel titolo della pagina.

Cercare nel testo della pagina

Scrivi: «**intext:**» oppure «**allintext:**» davanti alle parole che devono essere presenti nel testo della pagina.

Oppure?

Se non volete faticare o non ricordate tutti gli operatori, è possibile utilizzare **Google Advanced Search**, l'interfaccia web di Google che mostra tutte le opzioni di ricerca disponibili.

https://www.google.it/advanced_search

E per le immagini?

Una immagine, se analizzata correttamente, può rivelare molte informazioni oltre a quelle «visive» in primo piano.

- **Esaminare il soggetto**, l'ambiente, le persone, la situazione, il contesto; valutate tutti i particolari presenti nell'immagine
- **Esaminare dove è stata reperita** (sito web, social, ...)
- Effettuare una **ricerca "per immagine"** per trovare altre informazioni disponibili in rete



Per fare una ricerca su immagini è possibile **acquisire direttamente dallo schermo l'immagine da cercare** con lo «strumento di cattura» di Windows od altri strumenti di cattura dello schermo.

Ma lo storico di Internet?

Un aspetto interessante da notare di Internet è che è molto **facile individuare informazioni su vecchi siti web mai dismessi**. Questo ovviamente, fino a quando non vengano eliminati, aggiornati, modificati, venduti.

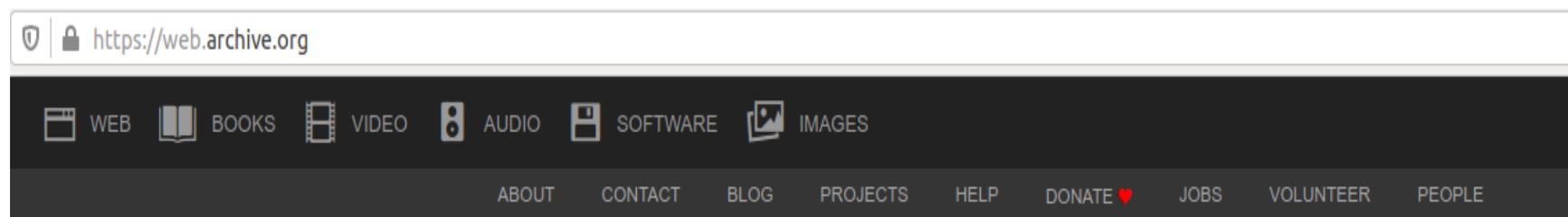
Spesso però è ancora possibile rintracciare le informazioni un tempo presenti su questi siti tramite speciali servizi online.

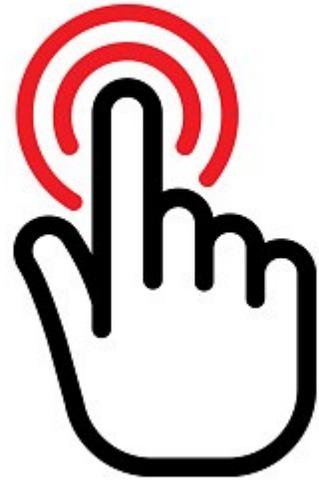
Alcuni di questi sono **“Wayback Machine”**, un progetto con lo scopo di archiviare e rendere disponibili pagine web e le loro modifiche nel tempo e «archive.is».

<https://archive.org/web/>

Consultando Wayback Machine è possibile (a volte) recuperare interessanti informazioni quali vecchie informazioni pubblicate, articoli, foto, rubriche telefoniche, vecchi dati che possono essere comparati con i dati attuali.

Esistono altri servizi simili, basta cercare...





Pronti?

Comincia la challenge!

In chat trovate il link dove scaricare un documento con l'elenco delle sfide da risolvere.

Vi proporremo una lista di dieci notizie o fatti, alcuni veri altri falsi.

Sta a voi scoprire se si tratta di **realtà o fake news!**

Comincia la challenge!

Avrete 1 punto per ogni sfida correttamente risolta.

Dividetevi i compiti, avete solo 45 minuti di tempo!

Vince il team che avrà dato il maggior numero di risposte esatte.

Ma non solo!

Dovrete anche avere le prove che dimostrano la correttezza della vostra risposta, scrivendo la soluzione in un documento che dovrete caricare su una cartella a challenge conclusa.



Buon lavoro (e viva il lupo!)