

REPORT ESERCIZIO DI MELTIGO:

Istruzioni:

1. Selezione del Target:
 - Scegli un target per la tua simulazione (può essere un'azienda, una persona pubblica, un sito web, ecc.).
2. Raccolta delle Informazioni con Google:
 - Effettua ricerche utilizzando parole chiave pertinenti al target scelto.
 - Prendi nota delle informazioni rilevanti trovate (es. nomi, indirizzi, contatti, notizie, ecc.).
3. Analisi con Maltego:
 - Importa i dati raccolti in Maltego.
 - Usa Maltego per creare una mappa delle connessioni e delle relazioni tra le informazioni trovate.

Identifica eventuali collegamenti o informazioni aggiuntive non immediatamente visibili.

Alla fine dell'analisi, lo studente dovrà produrre un piccolo report dove indicherà per ogni tool utilizzato:

- Il target.
 - Le query utilizzate (dove applicabile).
 - I risultati ottenuti.
-

Introduzione

L'obiettivo di questo esercizio era simulare la fase di **raccolta informazioni (OSINT)** su un target pubblico, utilizzando strumenti disponibili online.

Il target selezionato è stato **Johnny Depp**, noto attore cinematografico.

Metodologia di Raccolta Dati

Durante la raccolta delle informazioni sono stati utilizzati diversi strumenti e tecniche, tra cui:

- **Google:** per individuare dati pubblici (interviste, documenti, articoli).
- **Social Engineering:** utilizzato per dedurre collegamenti logici tra le informazioni (ad esempio relazioni familiari, ex partner, email riconducibili).
- **Social Media:** ricerca di profili pubblici su piattaforme come Instagram e Twitter.
- **Wikipedia:** per raccogliere informazioni biografiche e famigliari.
- **Articoli di Giornale:** per confermare relazioni personali, numeri pubblici, eventuali email rese pubbliche.

[illegible]

La mappa generata evidenzia le seguenti connessioni:

- **Johnny Depp** è collegato ai genitori **Christopher Mora Depp** e **Betty Sue Palmer**.

Trovati tramite una ricerca approfondita, anche su vari articoli di giornale, sono risaliti ai genitori che non erano presenti né in Wikipedia né in altre fonti “ufficiali”, i genitori di Jhonny Depp lo hanno abbandonato da piccolo, motivo per cui non vengono mai menzionati. Ho trovato un articolo di giornale in cui Jhonny Depp stesso ha rilasciato un’intervista in cui ne parlava. Da lì sono risaliti ai loro nomi – ma non ci sono molte altre informazioni su di loro.

- Relazioni sentimentali note:
 - Ex-compagna: **Vanessa Paradis** da cui hanno avuto una figlia – Lily-Rose Depp.
 - Ex-moglie: **Amber Heard**.
- È stato possibile trovare:
 - Indirizzi email pubblici associati: Depp@aol.com, Johnny@Spankerstein.com.
 - Numeri di telefono e contatti potenzialmente collegati.
 - Profili social verificati: ad esempio @johnnydepp, @vanessa.paradis.
- Figlia: **Lily-Rose Depp**, connessa sia tramite profili social che dati pubblici (inclusi numeri di telefono).

L'uso di **Maltego** ha permesso di rappresentare graficamente queste connessioni, rendendo visibile la rete di relazioni e contatti.

Considerazioni

La raccolta delle informazioni è stata facilitata dalla grande notorietà pubblica del soggetto.

- **Facilità:** alta, molte informazioni erano già disponibili pubblicamente.
- **Criticità:** necessità di verificare l'attendibilità delle fonti, specialmente per dati sensibili (es. numeri di telefono o email).

L'utilizzo combinato di **social engineering** e **ricerca tramite Google** si è dimostrato particolarmente efficace per arricchire il profilo informativo del target

- **Livello di esposizione:** Johnny Depp è altamente “tracciabile” tramite fonti aperte: email, numeri di telefono, social media.
- **Punti di debolezza:** la presenza di decine di fan-site che pubblicano contatti; account presunti di fan che possono confondere chi cerca informazioni ufficiali.

Importazione dati

- Ho creato entità di tipo **Person**, **Email Address**, **Phone Number**, **Social Media Account** e **Image** in Maltego.
- Ho incollato le email e i numeri nel tab "Import Entities".

Trasform usati

- **To Domain** e **To Website** su ogni email per risalire al dominio legato.
- **To Phone Owner** su ogni numero per verificare l'operatore e la località.
- **Person → Social Media Profiles** per trovare eventuali account Instagram/Twitter.
- **Person → Photograph** per recuperare immagini pubbliche associate.

Mappatura delle connessioni

- Il grafico principale ruota attorno a **Johnny Depp**, da cui partono link verso:
 - **Amber Heard** (ex-moglie)
 - **Vanessa Paradis** (ex-partner)
 - **Lily-Rose Depp** (figlia)
 - Email, telefoni e account social identificati
- Ho scoperto nodi secondari, per esempio la mail di Amber Heard e il suo numero, e ho verificato se compariva in altre liste pubbliche.
- Ho inoltre scoperto anche il nome, l'email, e l'Instagram di Camille Vasquez Avvocato di Johnny Depp, che non ho riportato sul diagramma di Maltego e anche la Psicologa (Terapista) di Johnny Depp.

Risultati aggiuntivi

- a. Collegamento tra l'account Instagram di Johnny e quello di Lily-Rose, confermando tag reciproci
 - b. Identificati almeno tre domini web (fan-site) che citano costantemente il suo numero di telefono
 - c. Trovati due profili Twitter con handle simili (possibile tentativo di impersonation)
-

Conclusioni

- **Livello di esposizione:** Johnny Depp è altamente "tracciabile" tramite fonti aperte: email, numeri di telefono, social media.
- **Punti di debolezza:** la presenza di decine di fan-site che pubblicano contatti; account presunti di fan che possono confondere chi cerca informazioni ufficiali.
- **Passi successivi** (opzionali):
 1. Verificare con un trasform "To SSL Certificate" se i domini sono registrati sotto nomi reali.
 2. Estendere la ricerca ai registri WHOIS dei domini trovati.
 3. Analizzare più a fondo eventuali account fake per misurare la portata delle impersonificazioni.