

OSINT: Information gathering using Maltego

Edoardo Iommi¹
edoardo.iommi@studenti.unicam.it



COMPUTER SCIENCE @ UNICAM

Unicam thesis - OSINT: Information gathering using Maltego

- ▶ Professore e relatore: F. Marcantoni
<https://computerscience.unicam.it/marcantoni/>
- ▶ Studente: Edoardo Iommi
edoardo.iommi@studenti.unicam.it - 105327

INDICE

Introduzione OSINT

Storia

Tipi di informazioni

Metodologie

Metodi

Maltego

Entità

Trasformate

Analisi ed implementazione del progetto

Analisi

Implementazione

CENNI STORICI - 1° GENERAZIONE

La storia
dell'utilizzo delle
informazioni aperte
risale all'emergere
dell'intelligence come
strumento a sostegno
delle decisioni e delle
azioni di un governo.

Tuttavia, non si è mai avuto un approccio metodico fino a quando gli Stati Uniti non hanno aperto la strada all'istituzionalizzazione e alla professionalizzazione di questa attività di intelligence.



CENNI STORICI - 2° GENERAZIONE



Con l'avvento di Internet e l'ascesa dei social media, il contesto dell'OSINT si è fatto più complesso in termini di fonti e metodi.

CASI D'USO

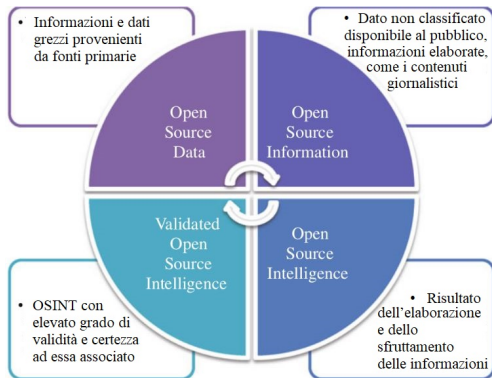
L'OSINT non è più utilizzata esclusivamente dalla comunità dell'intelligence, ma da una serie di altre figure.

Si vuole qui illustrare una serie di casi d'uso:

- ▶ Investigazione
- ▶ Sicurezza informatica
- ▶ Analisi attività criminali
- ▶ Analisi militari
- ▶ Investigazione sui social network
- ▶ Giornalismo
- ▶ Ricerca scientifica
- ▶ Monitoraggio dei governi
- ▶ Antifrode e riciclaggio denaro

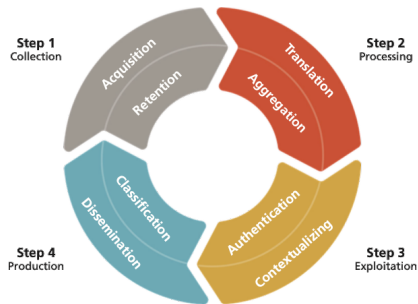
TIPI DI INFORMAZIONI

L'OSINT include tutte le fonti di informazione accessibili al pubblico. Queste informazioni sono disponibili online o offline, possono essere raggruppate nel seguente modo:



METODOLOGIE DI RICERCA

Nel contesto dell'OSINT, ci si concentra su quattro fasi chiave: raccolta, elaborazione, sfruttamento e produzione.



METODI DI ANALISI

Nonostante gli strumenti di raccolta OSINT si evolvano quasi quotidianamente, i vari metodi utilizzati dagli strumenti cambiano meno drasticamente e questi sono:



ANALISI
LESSICALE



ANALISI
GEOSPAZIALE



ANALISI DEI
SOCIAL NETWORK

MALTEGO

Maltego è un software utilizzato per l'intelligence open-source, che offre l'estrazione dei dati in tempo reale e la raccolta di informazioni, attraverso un grafico basato su nodi.

Maltego permette:

1. Estrarre facilmente dati da fonti disperse e nascoste
2. Unire automaticamente le informazioni corrispondenti in un grafico
3. Mapparle visivamente per esplorare il panorama dei dati



va



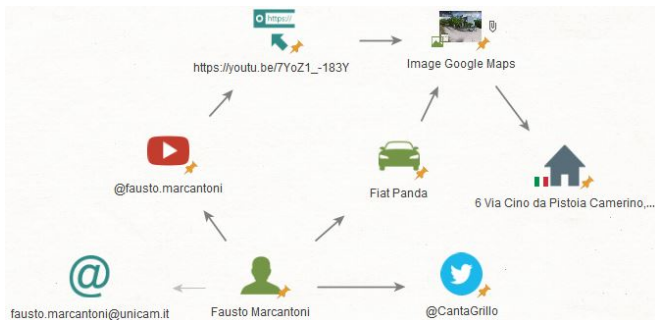
MALTEGO

Maltego è uno strumento completo per l'analisi dei collegamenti grafici ed è in grado di fornire delle ottime mappe "mentali" composte da:

► ENTITÀ

► COLLEGAMENTI

► TRASFORMATE



MALTEGO: ENTITÀ

Un'entità è una rappresentazione grafica di qualsiasi tipo di informazione che si trova nella vita reale, come ad esempio nomi e cognomi, numeri di telefono, e-mail, DNS, account di diversi social network, posizioni geografiche e persino frasi.



MALTEGO: GESTIONE DELLE ENTITÀ

Maltego consente di gestire le entità consentendone la:

- ▶ CREAZIONE
- ▶ MODIFICA
- ▶ IMPORTAZIONE
- ▶ ESPORTAZIONE

Cosa succede se trovo un dato non rappresentabile con Maltego?

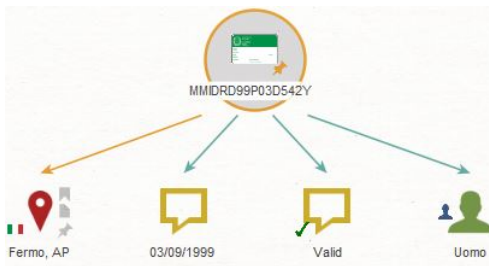
Possiamo creare ad hoc un'entità con le proprietà necessarie e l'icona che meglio la rappresentano.

MALTEGO: CREAZIONE ENTITÀ AD HOC

MALTEGO: TRASFORMATE

Le trasformate sono degli script che prendono in input un'entità e poi restituiscono informazioni correlate sotto forma di altre entità come output.

Le query che generano le trasformate dalle entità sono basate su XML, quindi il codice Python converte le query e le risposte in oggetti Python, generando così nuove entità.



MALTEGO: CREAZIONE TRASFORMATA

Cosa succede ho un entità creata ad hoc e voglio applicarle una trasformata si di essa?

Attraverso uno script Python e la libreria Maltego TRX è possibile creare una trasformata scegliendo:

- ▶ L'**input** su cui dovrà lavorare
- ▶ L'**output** che dovrà generare

Input entity type Codice Fiscale [thesis.CodiceFiscale_1] W1

Command line to be executed (in working directory):

```
C:\Users\eddy1\AppData\Local\Programs\Python\Python310\python.exe python.py local.inform.codicefiscale "Entity Value" "field1=field1 value;field2=field2 value" W2
```

```
# Definizione tipo e contenuto dell'entita
location_entity = response.addEntity(Location, location)

# Aggiunta proprieta' addizionali Overlay
location_entity.addOverlay(
    'IT',
    OverlayPosition.SOUTH_WEST,
    OverlayType.IMAGE
)
```

Figure: Input $\rightarrow$ Maltego

Figure: Output $\rightarrow$ Python

Figure: Definizione input e output trasformata

MALTEGO: AGGIUNTA TRASFORMATATA

ANALISI ED IMPLEMENTAZIONE DEL PROGETTO

L'elaborato di tesi in questione si basa sullo sviluppo di un processo investigativo tramite l'impiego di Maltego.

- Obiettivo: fornire all'utente quante più informazioni possibili circa un target specifico



Figure: Immagine su cui si è incentrata l'attività investigativa

ANALISI DEL PROGETTO

Il flusso di lavoro svolto si è sviluppato seguendo diverse fasi:

1. Ottenimento immagine
2. Raccolta di informazioni mediante l'analisi dell'immagine
 - ▶ Analisi sfondo dell'immagine
 - ▶ Analisi primo piano dell'immagine
 - ▶ Analisi punti di rilievo
3. Analisi dei soggetti presenti
 - ▶ Analisi dei social network dei soggetti
4. Raccolta ed osservazione informazioni estratte

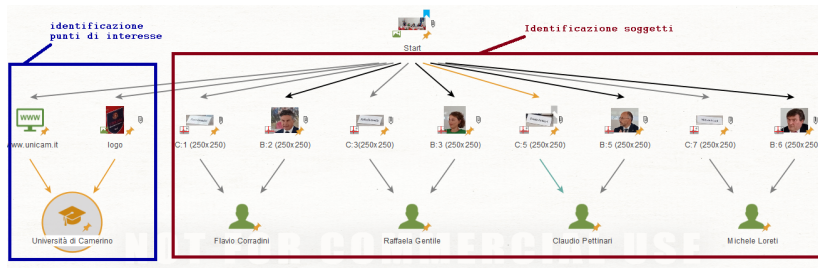
IMPLEMENTAZIONE DEL PROGETTO

INDIVIDUAZIONE SOGGETTI

Nella fase iniziale ci si è avvalsi un Image mapper che ha consentito di sezionare l'immagine sovrapponendo una griglia (250x250).

Pro:

1. Miglioramento della selezione degli punti di interesse
2. Capacità di rappresentare i PoI con un'entità ad hoc



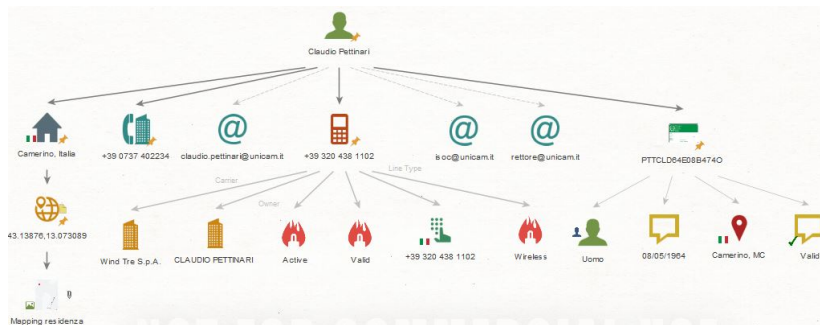
IMPLEMENTAZIONE DEL PROGETTO

RICERCA INFORMAZIONI GENERALI

Ricerca delle informazioni generali riguardo ad un target, cercando di scoprire quante più informazioni.

▶ TARGET: Claudio Pettinari (Person)

▶ # ENTITÀ: 19



IMPLEMENTAZIONE DEL PROGETTO

VERIFICA INFORMAZIONI TRAMITE TRASFORMATATA

Utilizzo della trasformata IPQS per scoprire informazioni legate al numero telefonico di uno dei soggetti identificati.

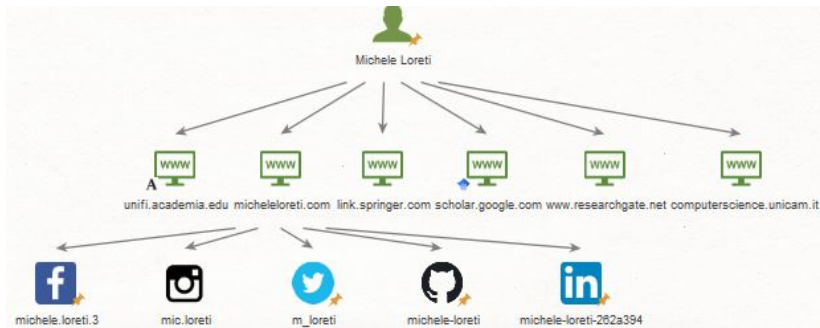
- ▶ Nome trasformata: "Get tags and indicators for phone number [IPQS]"



IMPLEMENTAZIONE DEL PROGETTO

RICERCA PROFILI SOCIAL E FILTRAGGIO DATI

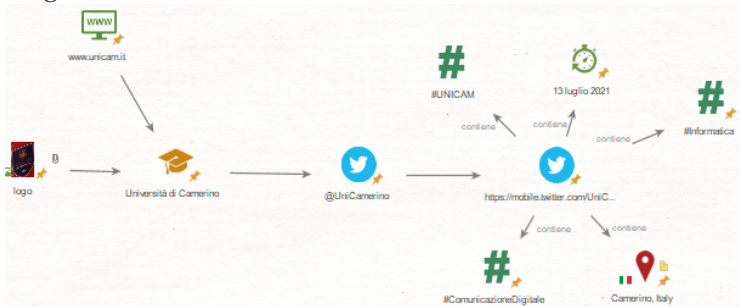
1. Impiego della trasformata, tramite Dorking e ottenimento dei siti web del target
 - ▶ Nome trasformata: toWebSite (Microsoft Bing Search)
2. Filtraggio siti web e ottenimento profili social



IMPLEMENTAZIONE DEL PROGETTO

ANALISI TEMPORALE

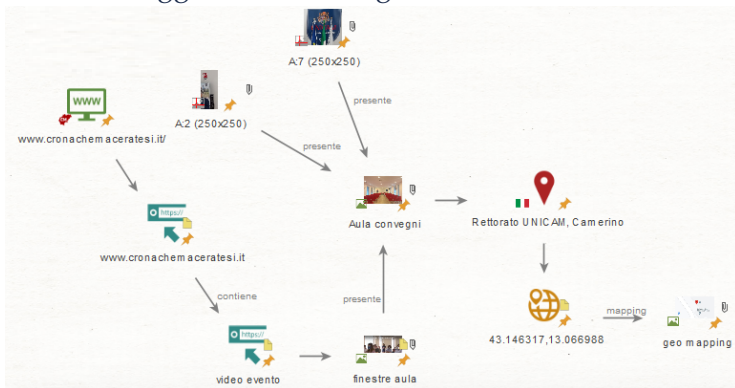
Analisi temporale dell'evento, cercando di individuare quando si è svolto l'evento, tramite la data di pubblicazione delle immagini sui social network (Twitter).



IMPLEMENTAZIONE DEL PROGETTO

ANALISI GEOSPAZIALE

Analisi geospaziale dell'evento, cercando di individuare la posizione esatta dell'evento tracciando le coordinate e informazioni aggiuntive sul luogo.



IMPLEMENTAZIONE DEL PROGETTO

VISUALIZZAZIONE INTEGRALE DEL GRAFICO GENERATO

Grafico finale con tutte le entità raccolte durante il processo di ricerca.

- Per ottenere una migliore visualizzazione del numerose entità, è stato sfruttato il **layout a blocchi**.

