

# REPORT S5/L1

## Esercizio:

Nell'esercizio di oggi, lo studente effettuerà una simulazione della fase di raccolta informazioni utilizzando dati pubblici su un target a scelta. Lo scopo di questo esercizio è di familiarizzare con i principali strumenti della fase di information gathering.

## Strumenti Principali:

### 1. Google:

- Utilizzato per la raccolta iniziale di informazioni.
- Esempi di utilizzo: ricerca di dati pubblici, articoli, profili social, documenti aziendali.

### 2. Maltego:

- Strumento per l'analisi e la visualizzazione di relazioni tra persone, gruppi, organizzazioni, domini, siti web e altre entità.
- Permette di costruire mappe di connessioni e scoprire informazioni nascoste.

## TARGET

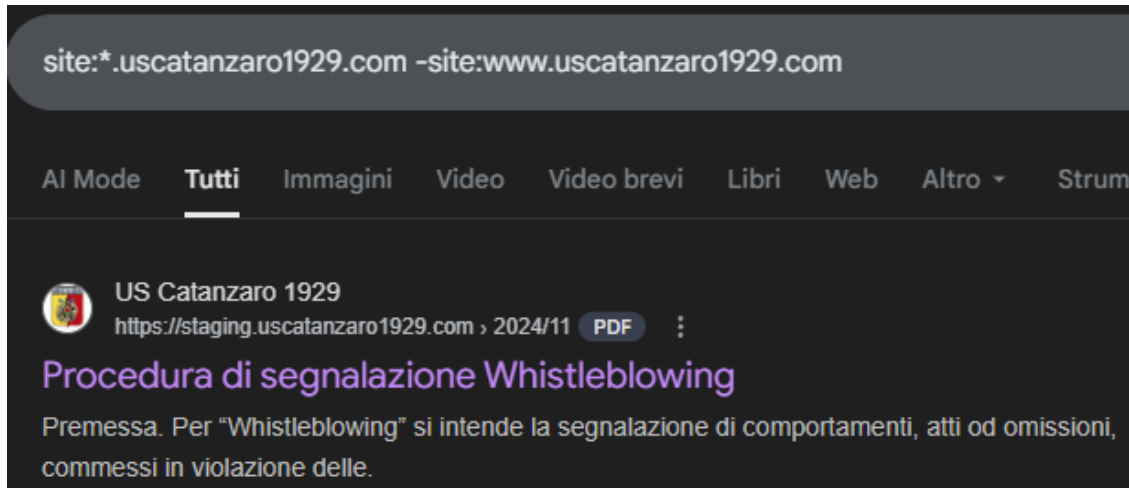
Il target che ho scelto per la simulazione della fase di raccolta informazioni è l'**US Catanzaro 1929**([uscatanzaro1929.com](http://uscatanzaro1929.com)).

## 1. RACCOLTA INFORMAZIONI CON GOOGLE

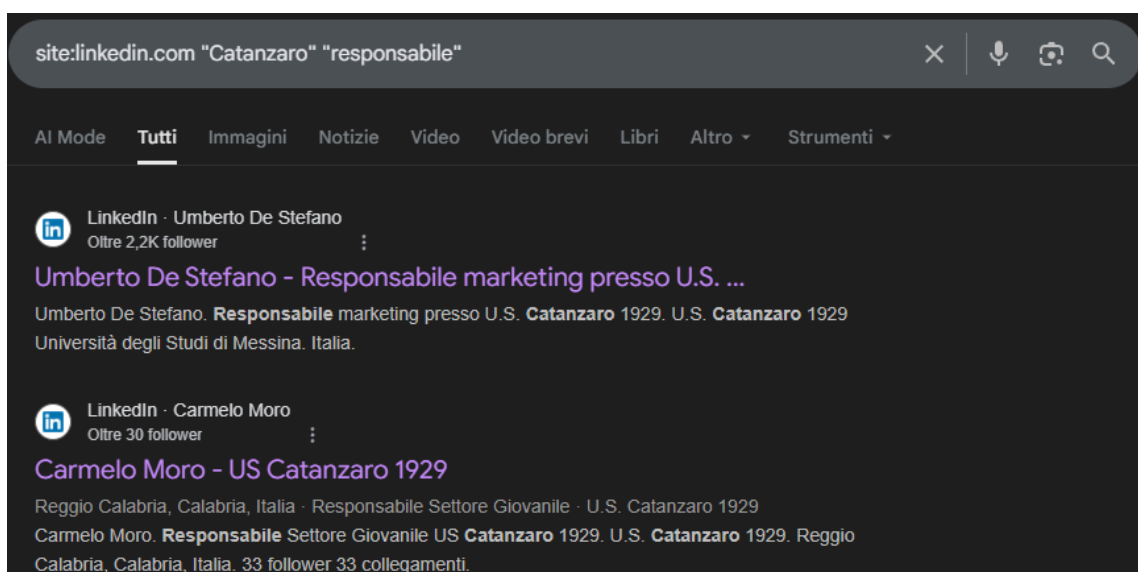
In questa prima fase sono state utilizzate tecniche di **Google Hacking** per **identificare** informazioni pubbliche, contatti e pdf indicizzati appartenenti al target.

## 1.1 Query utilizzate:

- **site:\*.uscatanzaro1929.com -site:www.uscatanzaro1929.com**  
(per identificare sottodomini)



- **site:linkedin.com "Catanzaro" "responsabile"** (per identificare il personale)



- **"@uscatanzaro1929.com"** (per trovare indirizzi email)

## 1.2 Risultati ottenuti:

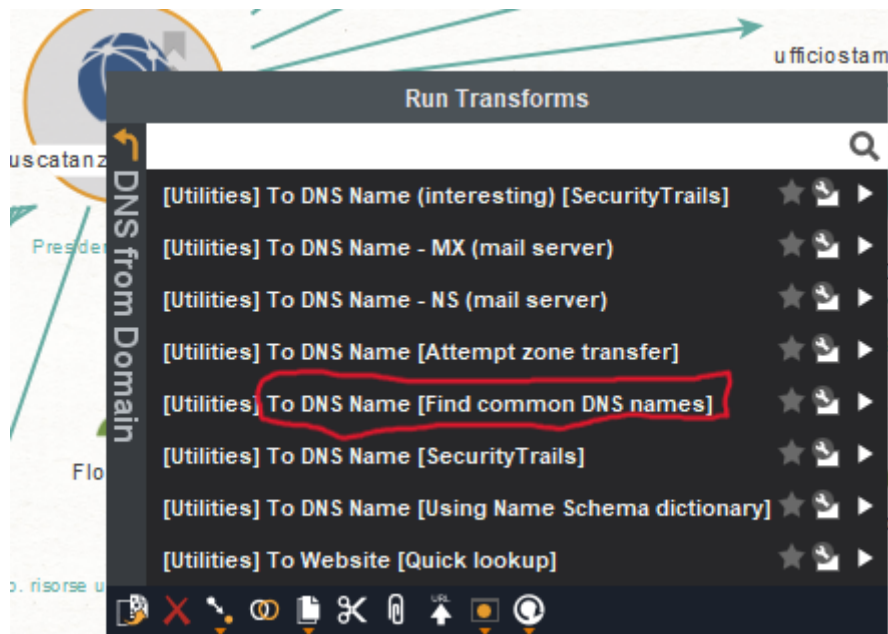
- **Sottodomini:** individuato il sottodominio ***staging.uscatanzaro1929.com***
- **Contatti email:** individuati indirizzi email per: ***Segreteria, Ufficio Stampa, Amministrazione, Marketing, Settore Giovanile*** e ***SLO***
- **Personale:** individuati ruoli chiave tra cui il ***Presidente***, il ***Responsabile Marketing***, le ***Risorse Umane***, l'***Allenatore***
- **Numeri telefonici:** individuato il numero telefonico di ***rete fissa*** della ***segreteria***

## 2. ANALISI CON MALTEGO

Nella seconda fase, i dati raccolti sono stati importati in **Maltego** per visualizzare le relazioni tra le entità umane e l'infrastruttura tecnologica del club

### 2.1. Operazioni effettuate:

- Creazione di nodi per ogni **responsabile, email, numero telefonico e sottodominio** individuato.
- **Mappatura server:** rilevati ulteriori sottodomini attraverso il transforms “**to DNS Name[find common DNS names]**”



- **Risoluzione degli IP** per i **server individuati** attraverso il transforms “**Resolve to IP**”

