

## ESERCIZIO S5L2

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

- Google, per la raccolta delle info.
- Maltego.

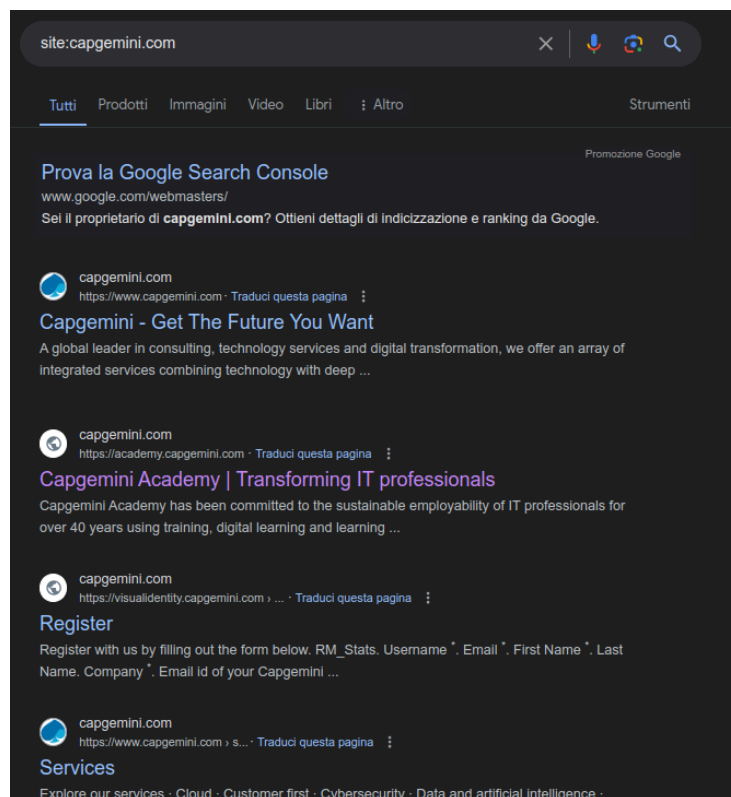
Alla fine dell'analisi, lo studente dovrà produrre un piccolo report dove indicherà per ogni tool utilizzato: il target, le query utilizzate (dove applicabile), i risultati ottenuti.

## SVOLGIMENTO

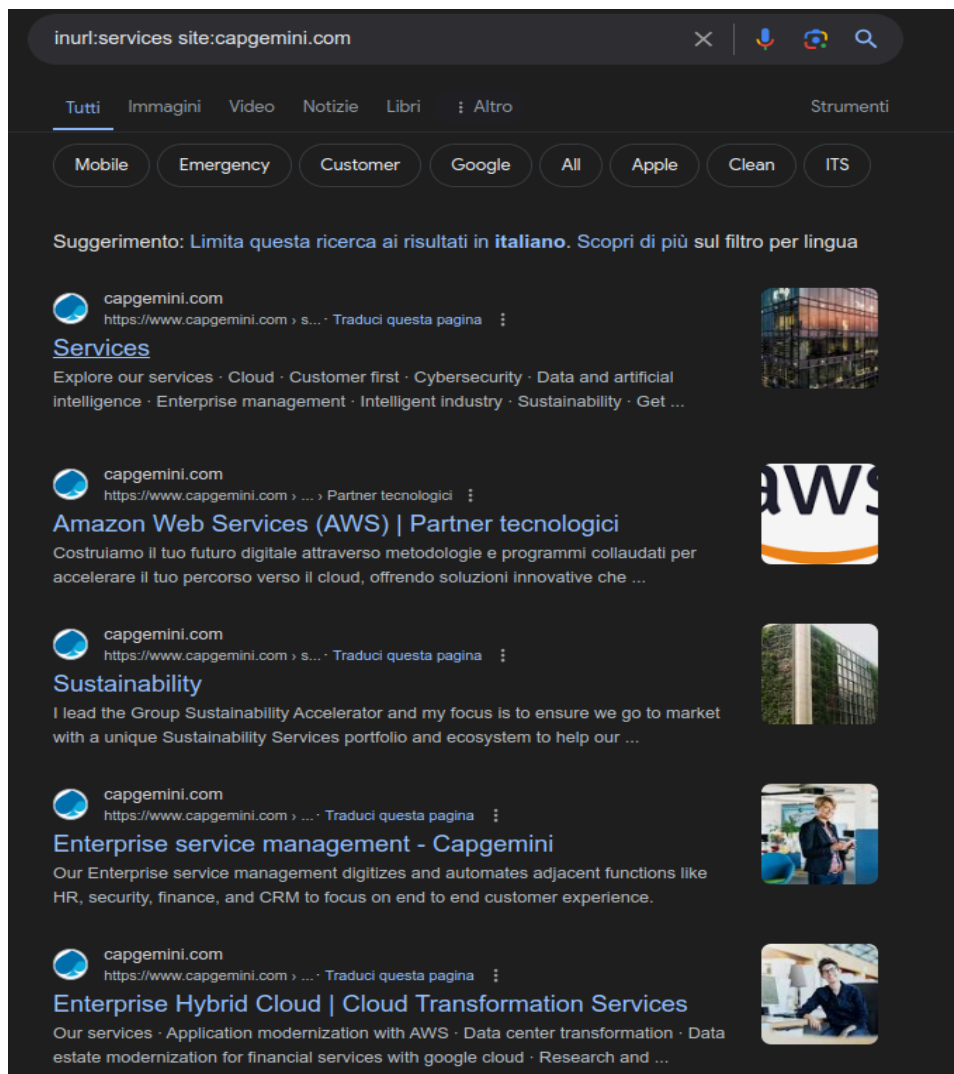
Il target scelto per questa simulazione è una società di consulenza informatica chiamata "Capgemini".

### Google

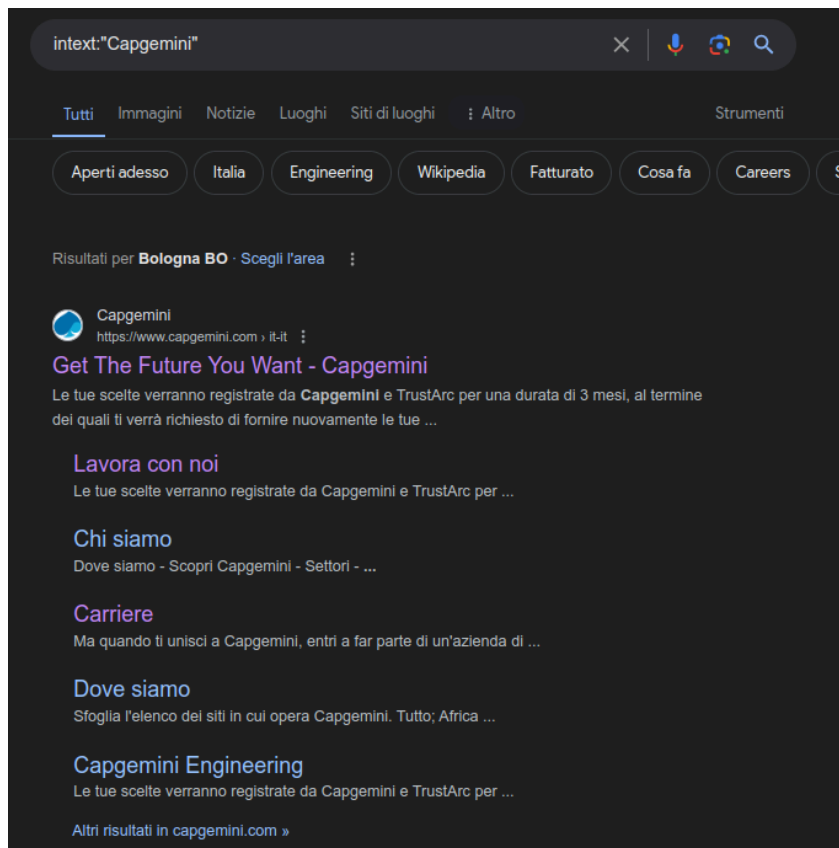
- **site:capgemini.com:** Questa query ha mostrato tutte le pagine indicizzate da Google nel sito ufficiale di "Capgemini". Questo mi ha permesso di esplorare diverse sezioni del sito, come le pagine dei servizi, "Chi siamo", e "Carriere".



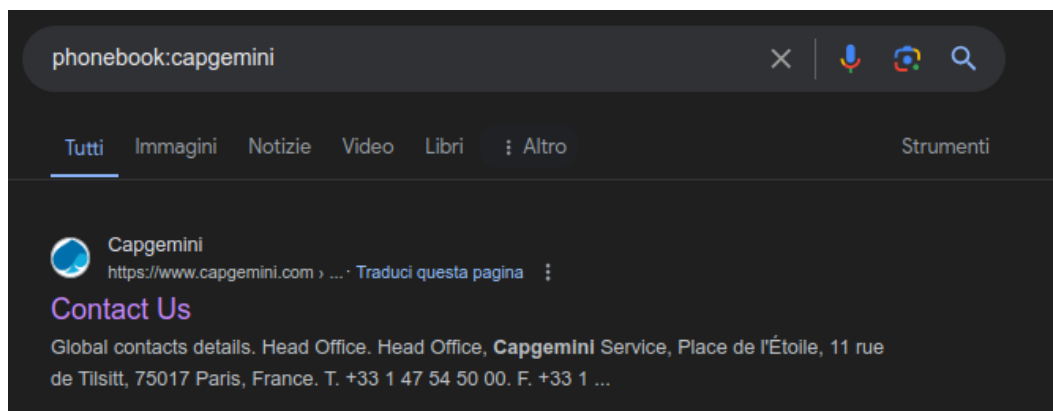
- **inurl:services site:capgemini.com**: Con questa query, ho trovato la pagina dei servizi di "Capgemini", che dettaglia le aree di competenza dell'azienda.



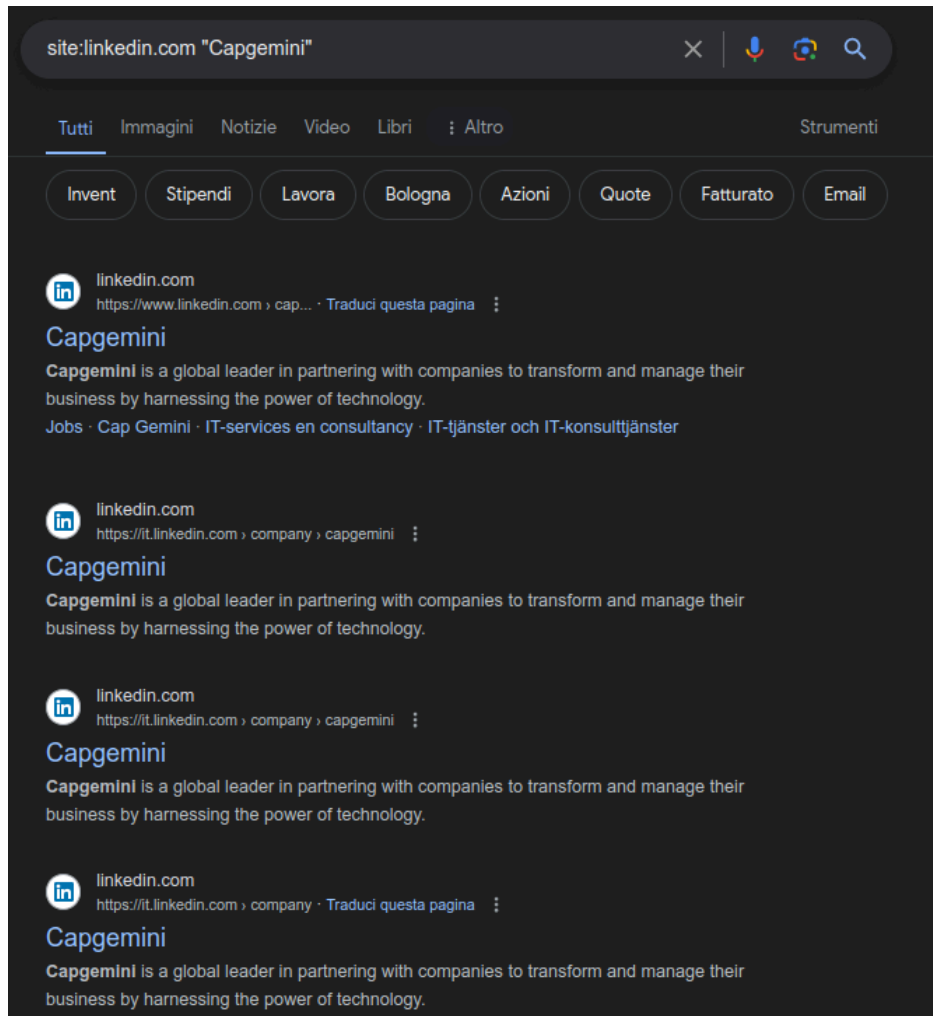
- **intext:"Capgemini"**: Questa query ha mostrato pagine web e documenti che menzionano "Capgemini", consentendomi di scoprire articoli di notizie, blog e comunicati stampa.



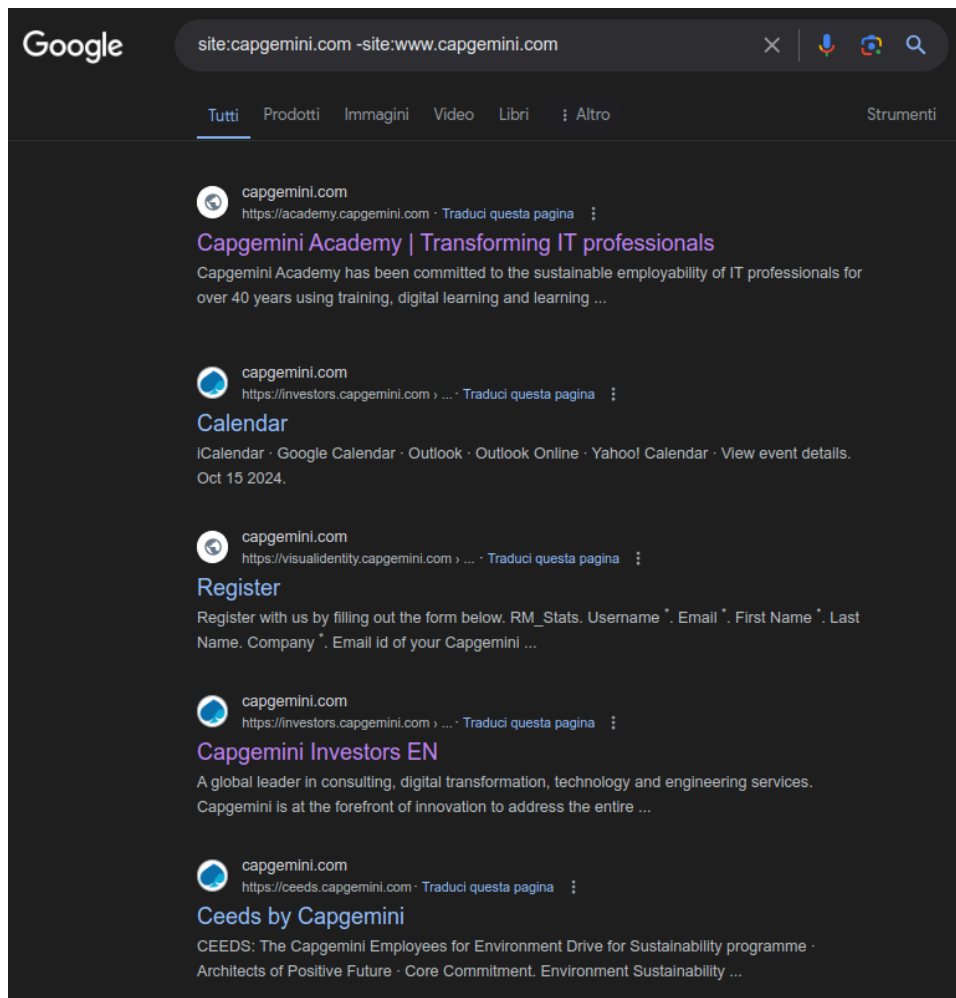
- **phonebook:capgemini**: Utilizzando questa query, ho cercato elenchi telefonici e contatti associati a "Capgemini", trovando numeri di telefono e indirizzi email di diversi dipartimenti.



- **site:linkedin.com "Capgemini"**: Questa query mi ha portato ai profili LinkedIn legati a "Capgemini", dove ho trovato informazioni sui dipendenti, dirigenti e aggiornamenti aziendali.



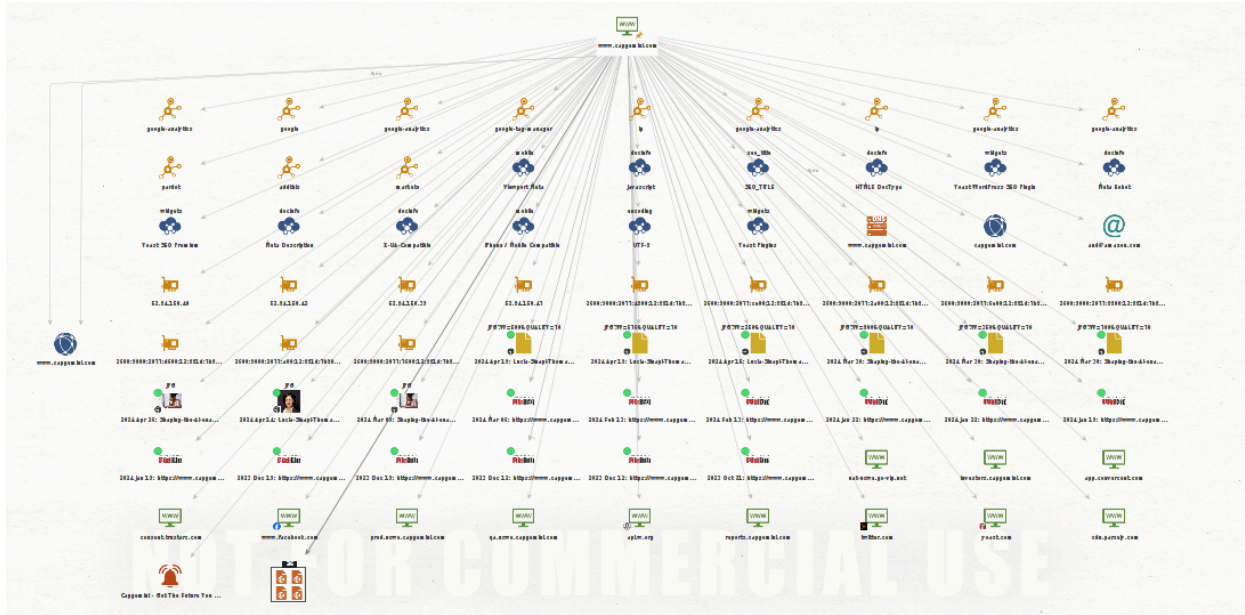
- **site:capgemini.com -site:www.capgemini.com:** Questa query ha escluso la root capgemini del sito principale, permettendomi di concentrarmi su altre pagine come quelle del calendario, della registrazione e degli investitori.



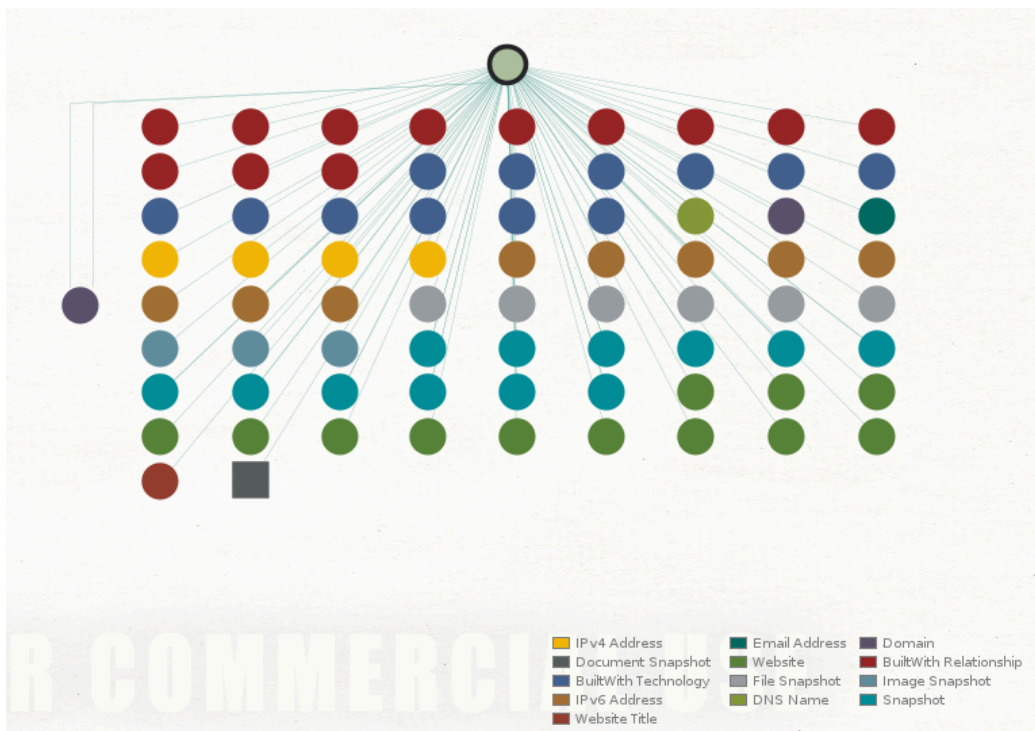
## Maltego

Maltego è stato utilizzato per visualizzare e analizzare le relazioni tra le entità connesse a "Capgemini". Ho impiegato le transform "Standard Transforms CE" e "Social Link CE" per esplorare le informazioni di base e le connessioni sui social media.

- Standard Transforms CE: Con questa transform ho scoperto il dominio principale di "Capgemini" e ho identificato indirizzi email associati, tra cui quelli del servizio clienti e delle risorse umane.



Di seguito è mostrata una mappa generale che divide in categorie, secondo la leggenda in basso, i risultati ottenuti.



- Social Link CE: Queste transform hanno permesso di individuare collegamenti a profili social di "Capgemini", o documenti che si trovano all'interno dei loro social.

