Esercizio Unit 2

S1L1

MIRKA FEBBO

Traccia

EPICODE

Esercizio
Info Gathering

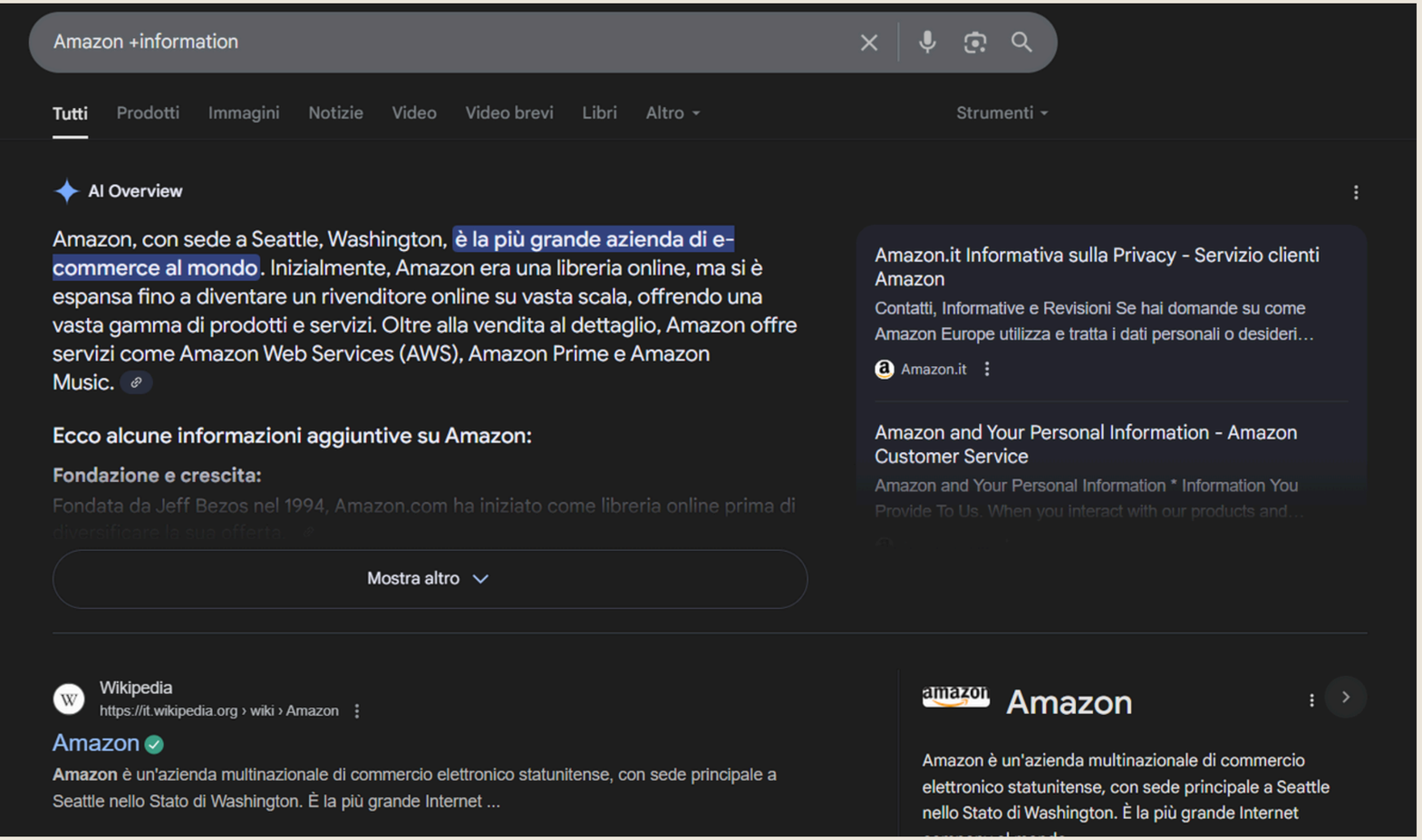
Esercizio:

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.

Oggi abbiamo affrontato la prima fase del penetration test, ovvero la raccolta di informazioni. Abbiamo anche imparato alcuni operatori e tecniche per effettuare ricerche mirate su Google

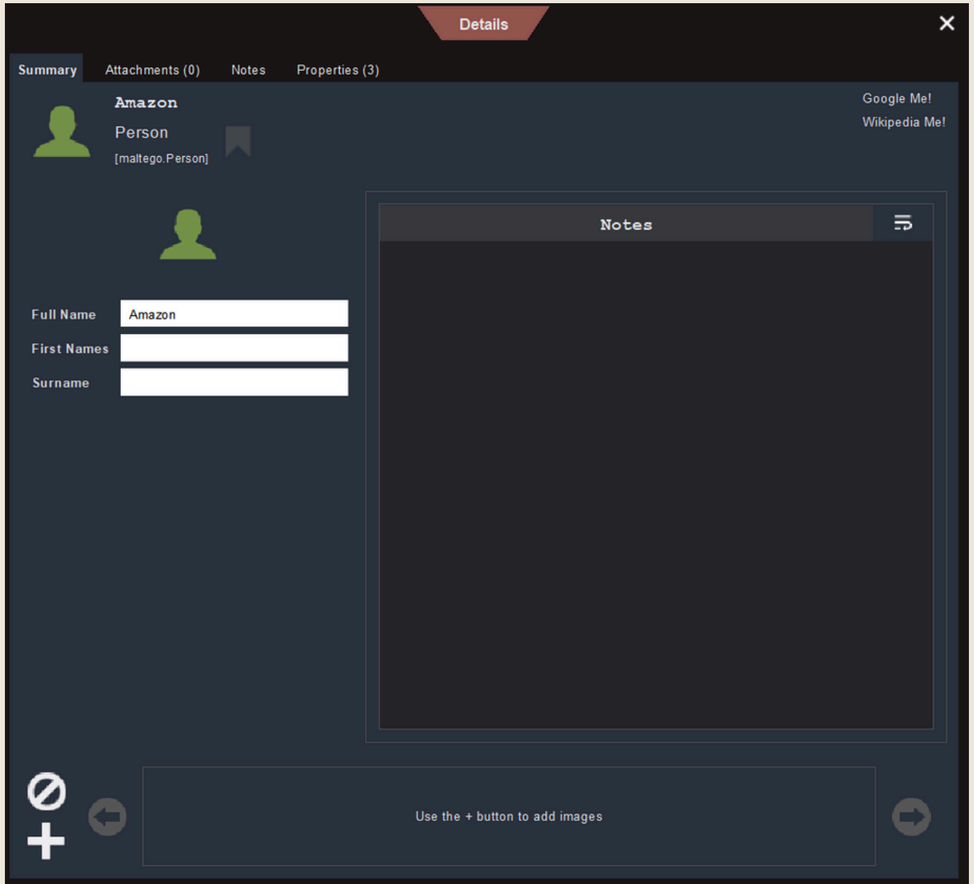


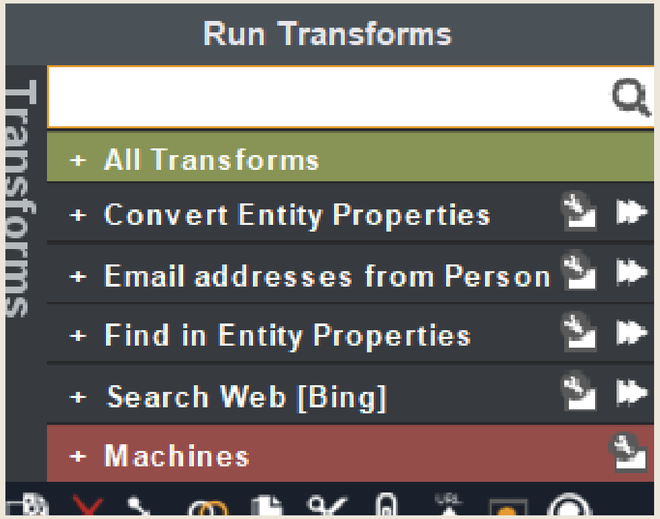
Un esempio è l’operatore booleano '+' che consente di cercare informazioni specifiche, includendo solo i risultati che contengono la parola preceduta dal simbolo e ignorando quelli non rilevanti.

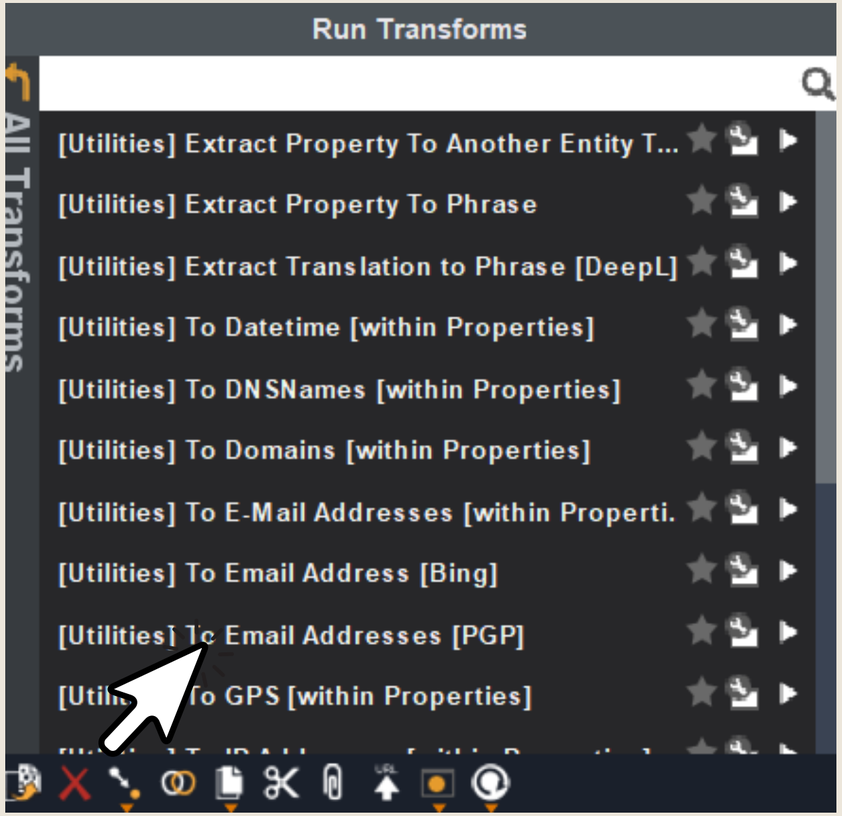
Un altro operatore utile è inurl:Amazon, che permette di trovare pagine web il cui URL contiene la parola 'Amazon'. Questo è particolarmente utile per restringere la ricerca a siti o contenuti specifici legati a un determinato termine presente nell’indirizzo web.

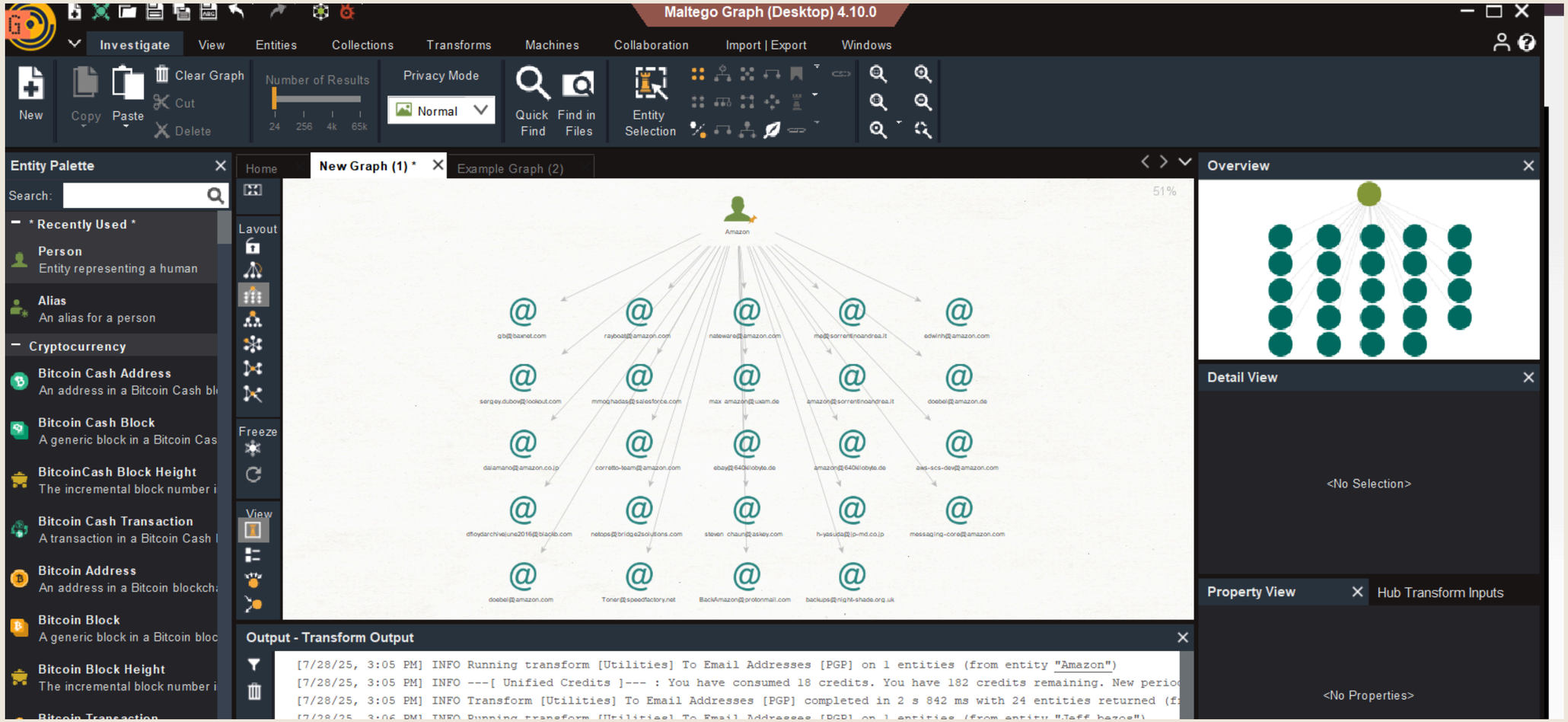
Infine, l’operatore intitle:Amazon consente di visualizzare solo i risultati che hanno la parola 'Amazon' nel titolo della pagina, facilitando l’individuazione di contenuti specifici e rilevanti

Successivamente, abbiamo iniziato a utilizzare Maltego, uno strumento OSINT per la raccolta e la visualizzazione di informazioni.
Ho eseguito una ricerca inserendo 'Amazon' come entità di tipo Person (persona). Poi, cliccando con il tasto destro sull'entità, ho selezionato l’opzione Run All Transforms per eseguire tutte le trasformazioni disponibili. Questo mi ha permesso di cercare e individuare eventuali indirizzi email collegati ad 'Amazon









In conclusione, l’attività è stata molto interessante e utile per comprendere come avviene la fase di information gathering.
L’unica pecca è il costo elevato dello strumento, che limita l’esplorazione più approfondita. Inoltre, ho notato che Maltego è poco efficace nel cercare persone: ad esempio, provando con nomi noti come 'Jeff Bezos', non ho ottenuto risultati.
Nonostante queste limitazioni, è stata comunque un’esperienza molto stimolante.