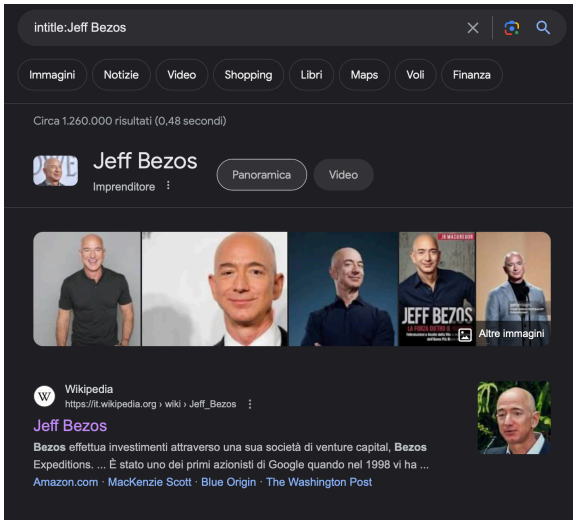
Nell’esercizio di oggi lo studente effettuerà una simulazione di fase di raccolta informazioni utilizzando dati pubblici su un target a scelta. Lo scopo di questo esercizio è di familiarizzare con i tool principali della fase di information gathering, quali:
- Google, per la raccolta delle info
- Maltego

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

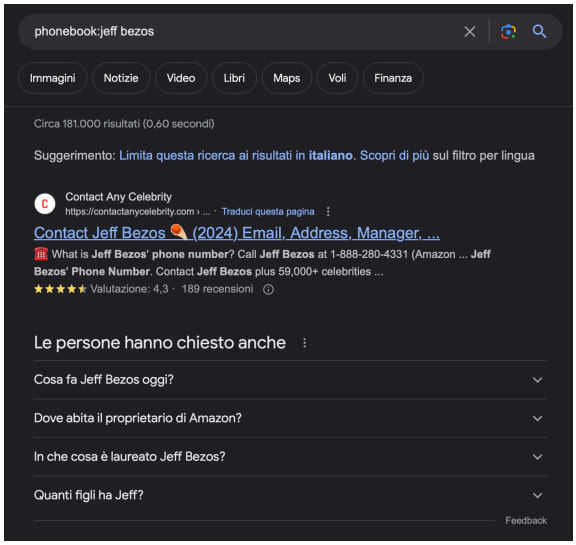
Come target ho individuato **Jeff Bezos**.

Google Hacking

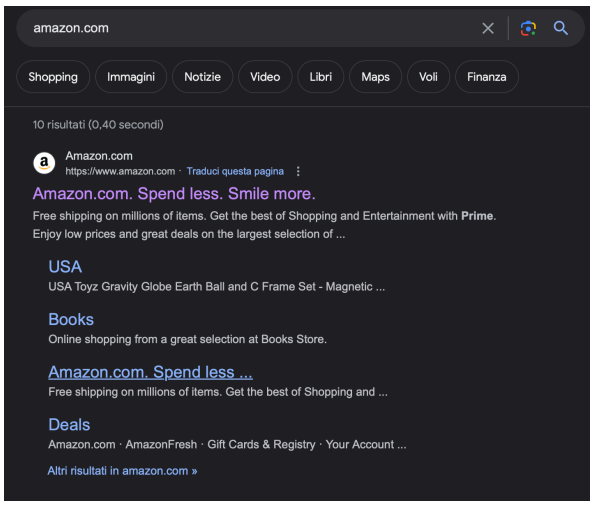


Grazie alla query ***intitle:Jeff Bezos*** su google.com ho cercato le pagine che contenessero nel titolo il nome del target e ne ho trovate diverse che raccontassero la sua vita e di cosa si occupa. Da qui ho evinto che ad oggi ricoprisse la carica di presidente esecutivo della società Amazon Inc..

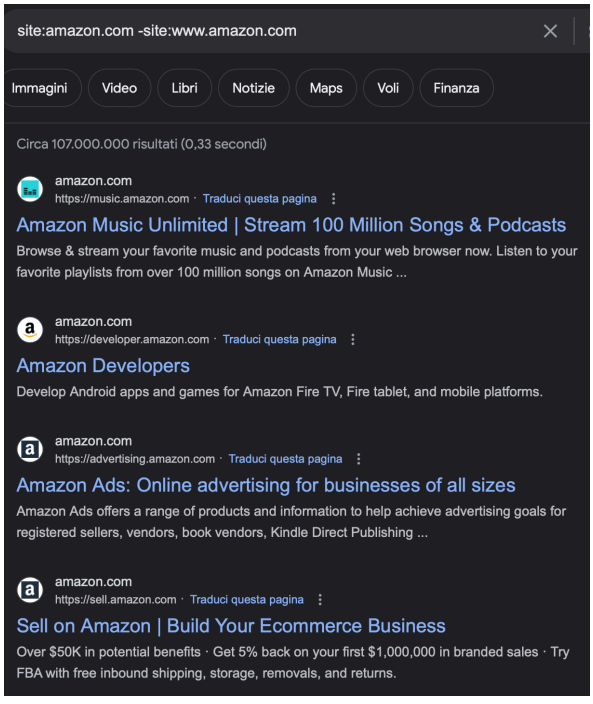
Sempre utilizzando google ho provato a ricercare il contatto di Jeff Bezos con la query ***phonebook:Jeff Bezos*** la quale ha restituito come risultato una pagina, rivelatasi poi non affidabile, che permetteva di contattare persone famose sottoscrivendo un abbonamento.



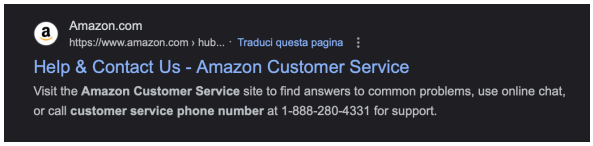
Nella ricerca successiva mi sono concentrato sulla società di Jeff Bezos, Amazon. Usando la ricerca classica per trovare il sito dell'azienda ho dedotto che l'url più a utilizzato, quindi quello che potrebbe essere più esposto ad eventuali attacchi informatici, è proprio quello legato all'e-commerce di Amazon dato che google lo dava al primo posto nei risultati.



Successivamente utilizzando la query ***site:amazon.com -site:www.amazon.com*** sono andato a cercare tutti gli eventuali sottodomini del sito principale per avere una panoramica completa.

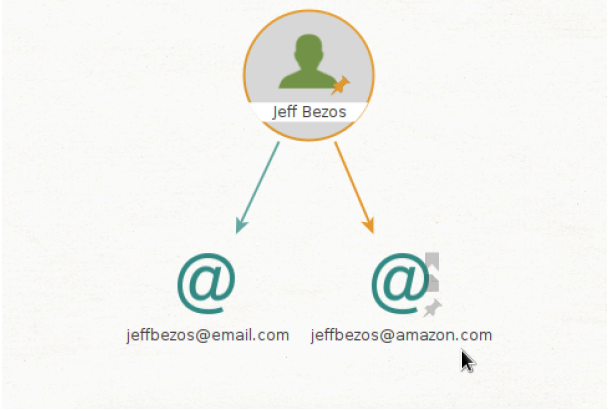


Utilizzando la query ***Phonebook:amazon*** invece di quella precedente, che aveva come oggetto Jeff Bezos, sono riuscito a risalire ad un numero USA appartenente alla società Amazon. Si tratta del numero attivo 24/7 del servizio clienti di Amazon.

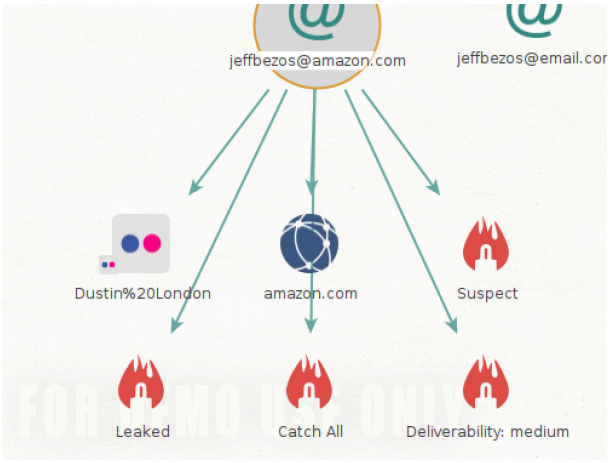


Maltego

Utilizzando sempre Jeff Bezos come target, mi sono spostato sul tool Maltego per effettuare una ricerca inerente a lui. Il risultato è stato il seguente:

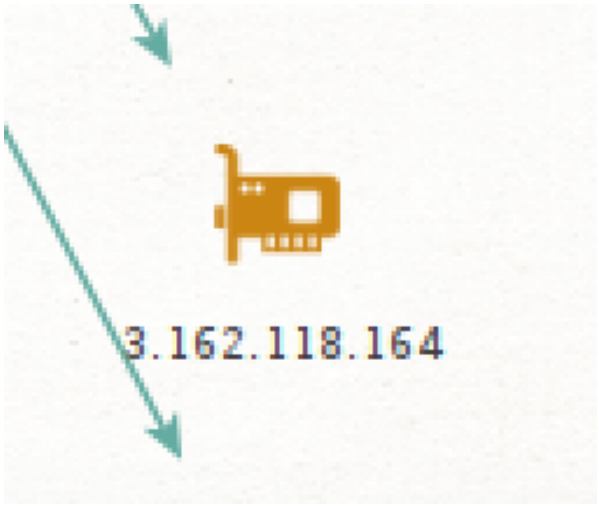


Andando ad analizzare l'indirizzo mail di destra il programma mi ha restituito il seguente risultato

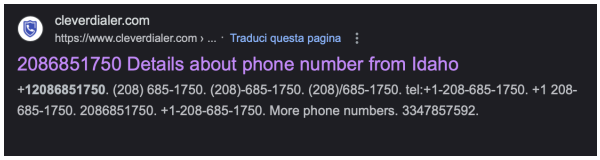


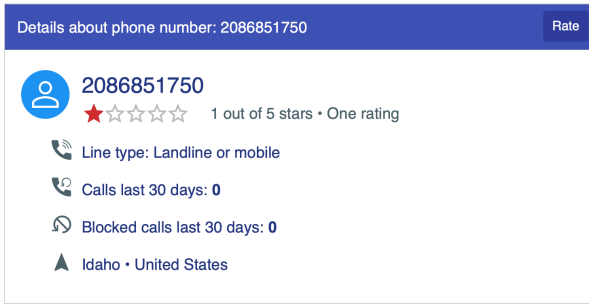
Da qui ho deciso di andare più a fondo sul sito, per vedere se fossi riuscito a trovare altre informazioni utili per un eventuale attacco ad Amazon. All'interno dei risultati ho trovato il sito americano di amazon.com e ho deciso di selezionare questo per cercare dati su di esso.

Ciò che sono riuscito a trovare è l'indirizzo IP che potrebbe essere del sito

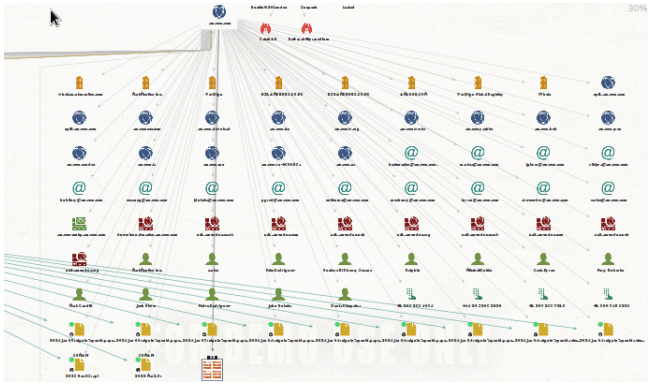


Un numero di telefono, che cercandolo poi con una semplice ricerca su google ho scoperto non essere collegato ad amazon e che è stato segnalato per frode.





Infine ho trovato un elenco di persone che potrebbero avere a che fare con la società o esserne collaboratori.



Tra i vari risultati ho trovato un uomo che si chiama John Duksta, che da una ricerca condotta utilizzando la query ***intitle:john duksta amazon*** su google ho scoperto essere un Security Engineer che ha lavorato per delle grandi società informatiche.