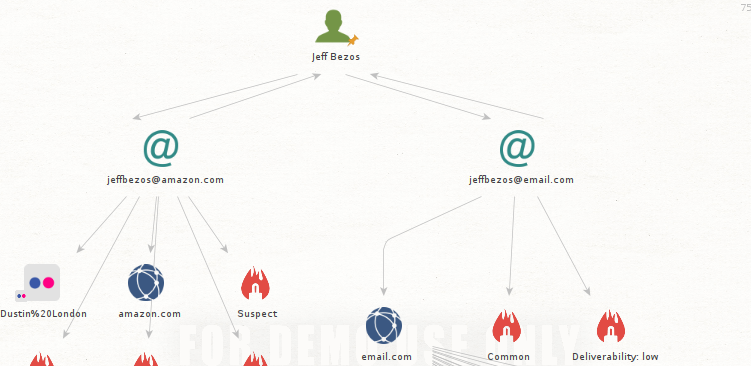
S5/L2

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 e Maltego.

Il nostro target di riferimento è Jeff Bezos è un  imprenditore e informatico statunitense.

È il fondatore, proprietario e presidente del gruppo [Amazon](https://it.wikipedia.org/wiki/Amazon), la più grande società di [commercio elettronico](https://it.wikipedia.org/wiki/Commercio_elettronico) al mondo, nonché il fondatore e amministratore delegato di [Blue Origin](https://it.wikipedia.org/wiki/Blue_Origin), società attiva nei voli spaziali, ed il proprietario del [*Washington Post*](https://it.wikipedia.org/wiki/The_Washington_Post).

Scrivendo il suo nome nel target person di Maltego ci vengono mostrate due email:

* [Jeffbezos@amazon.com](mailto:Jeffbezos@amazon.com)
* [jeffbezos@email.com](mailto:jeffbezos@email.com)

Cliccando su [jeffbezos@email.com](mailto:jeffbezos@email.com) 🡪 e successivamente su email.com 🡪 arriviamo al DNS:



Cliccando a sua volta su DNS ci trova un IPv4 pubblico: 3.33.243.145

Inserendo questo IP su Whois abbiamo questo risultato:



Dalle prime informazioni possiamo vedere il NetRange, un intervallo che copre un ampio spettro di indirizzi IP E indica che tutti gli indirizzi compresi tra 3.0.0.0 e 3.127.255.255 sono assegnati o riservati per l’uso da parte dell’organizzazione. Mentre il CIDR ci indica che il blocco di indirizzi comprende tutte le combinazioni possibili per i primi 9 bit, mentre i rimanenti 23 bit sono riservati agli indirizzi host all’interno della rete. Vediamo poi il nome dell’organizzazione ovvero: Amazon Tecnologies e la città: Seattle (WA).

Poi attraverso la query di google: Phoneback Jeff Bezos, siamo riusciti a trovare queste informazioni:

