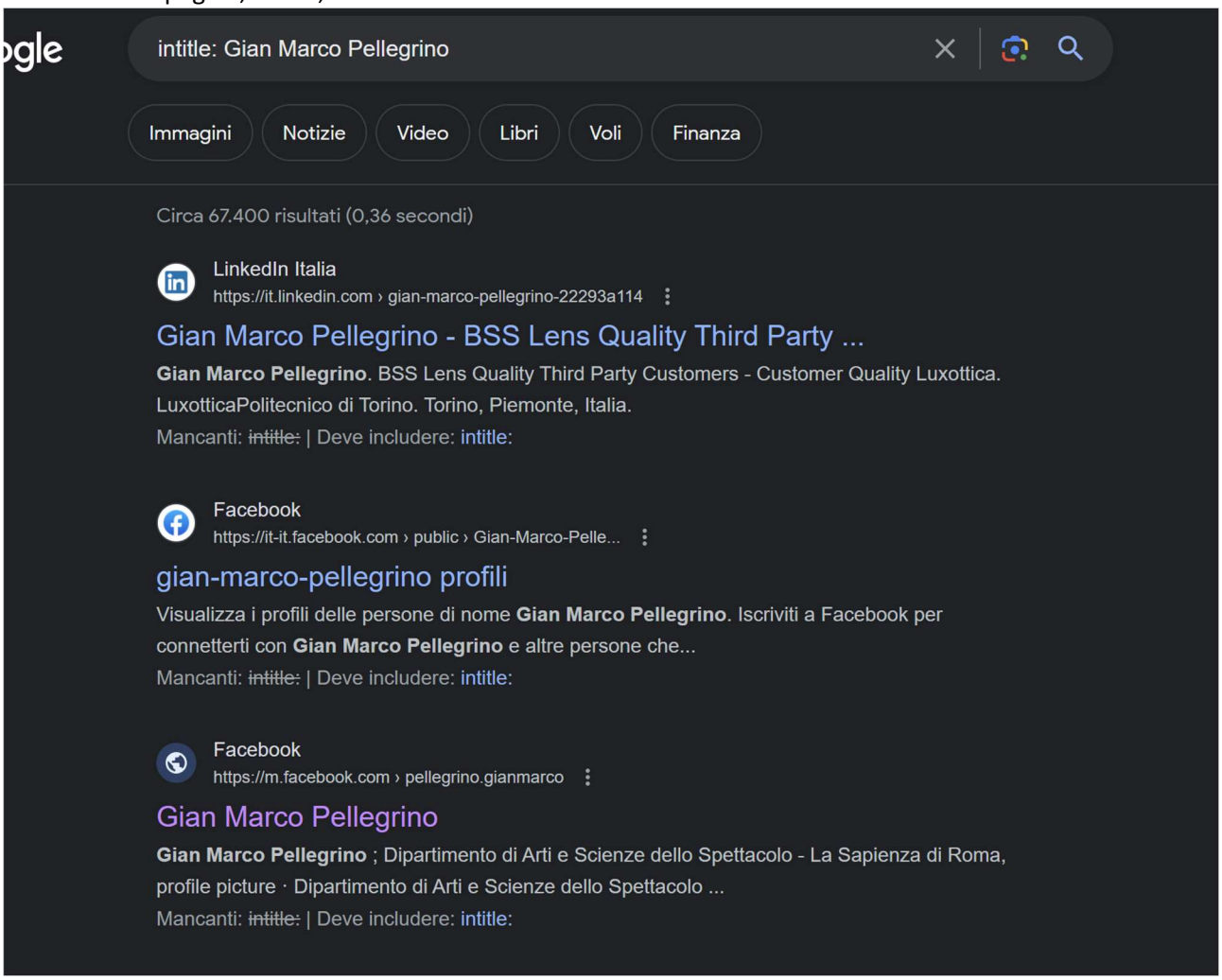
L’esercizio odierno era basato sulla ricerca e raccolta di informazioni riguardo un target.

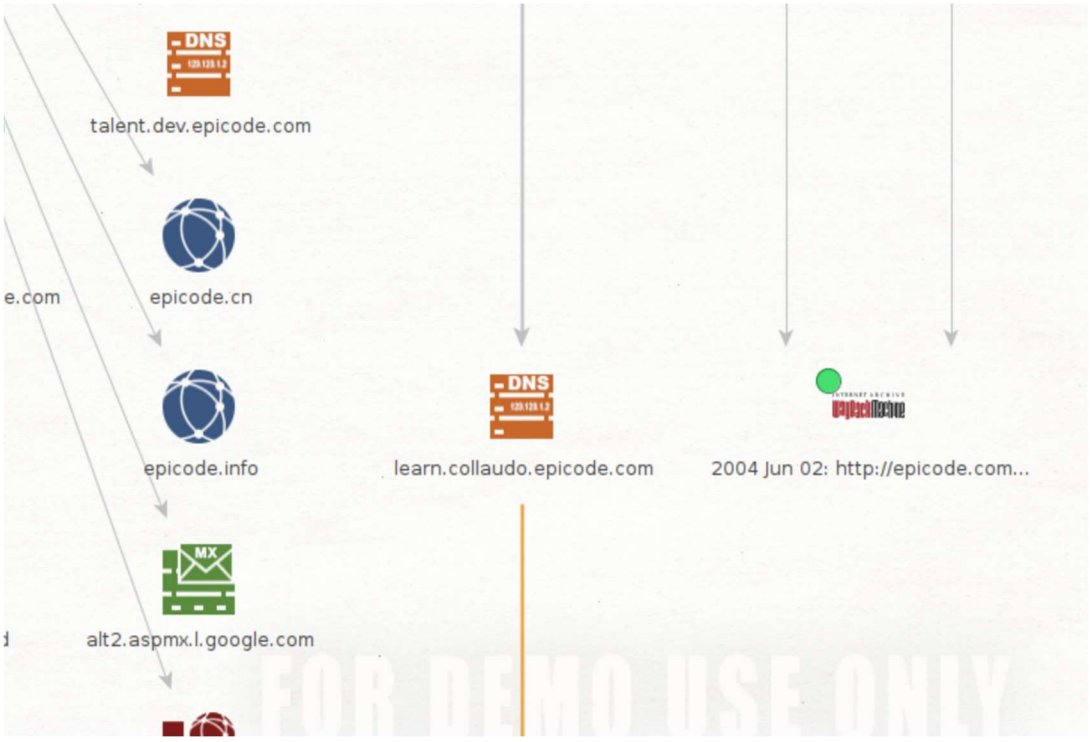
Il principale era il proprio nome e cognome, ma ciò ha prodotto risultati solamente tramite google, il terzo il risultato della pagina, infatti, si riferisce a me.



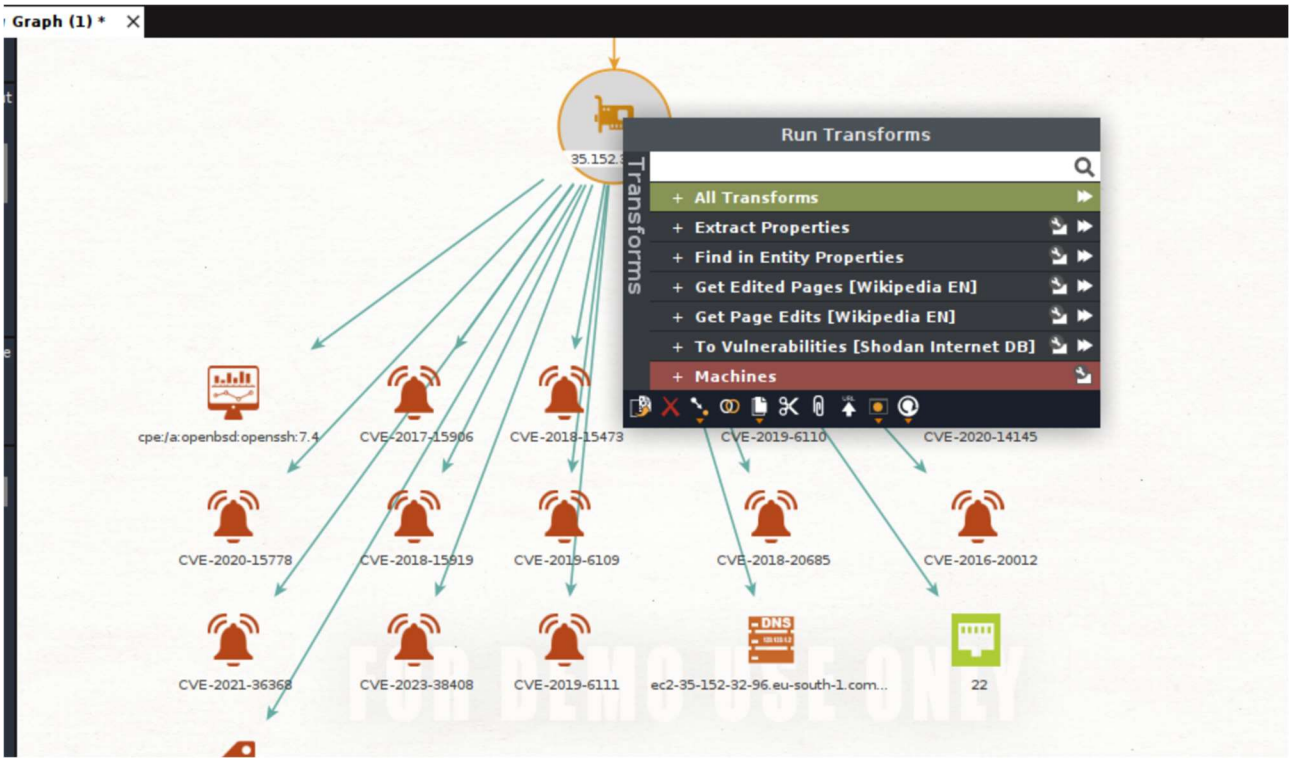
Maltego non ha prodotto risultati.

Il secondo target è stato Epicode. Cercando il dominio Epicode.com su maltego è stato possibile trovare molteplici risultati

Tra cui learn.collaudo.epicode.com, probabilmente il nuovo sito che Epicode sta costruendo in sostituzione del learn attuale:



Da lì, essendo il nome del dominio tradotto dal dns, ho cercato di estrapolare l'ip:



E dopo aver trovare un IP (sempre ipotizzando che non sia un proxy) ho cercato le vulnerabilità che Maltego suugeriva.

Come è possibile vedere, viene segnalata la porta 22, utilizzata per il protocollo SSH, e le vulnerabilità riscontrate relative al protocollo, CVE-2021-36368 per esempio sarebbe vulnerabilità alla public key authentication e CVE-2023-38408 ha un path di ricerca non abbastanza affidabile.