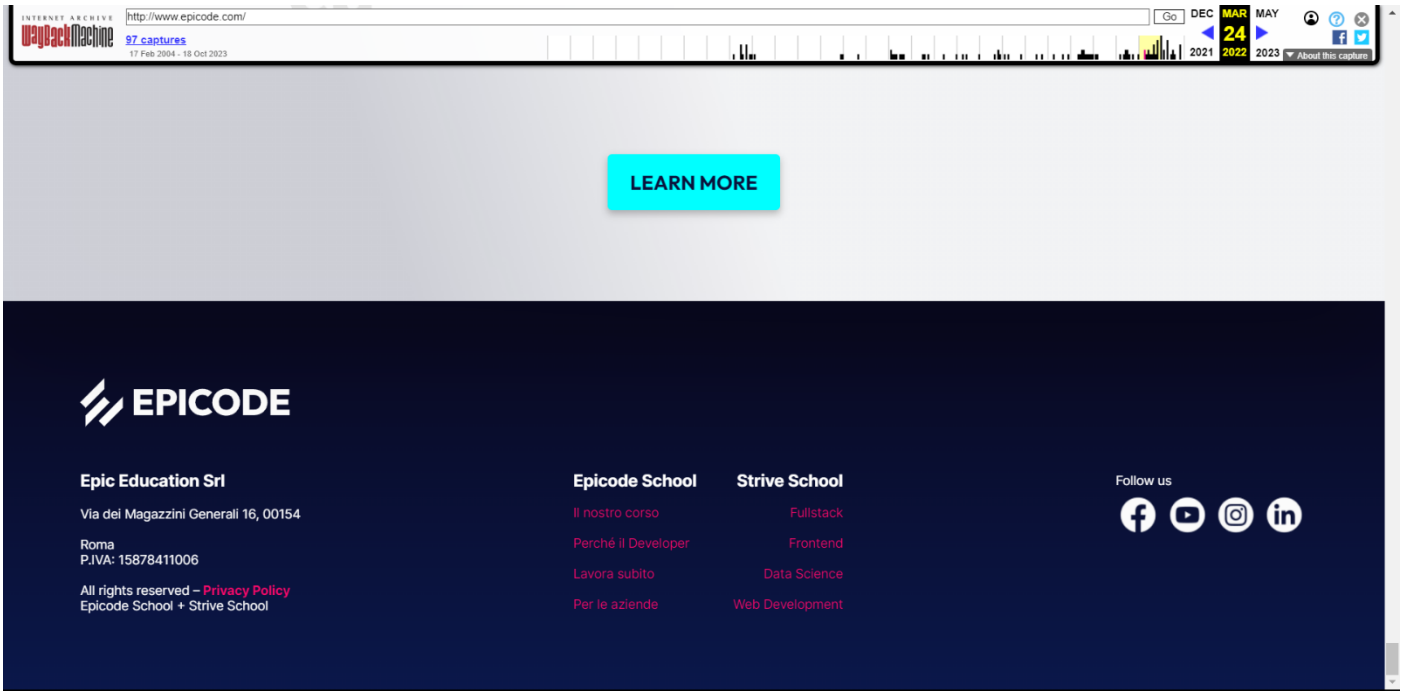
Pen-test fase 2: esercizio di raccolta informazioni

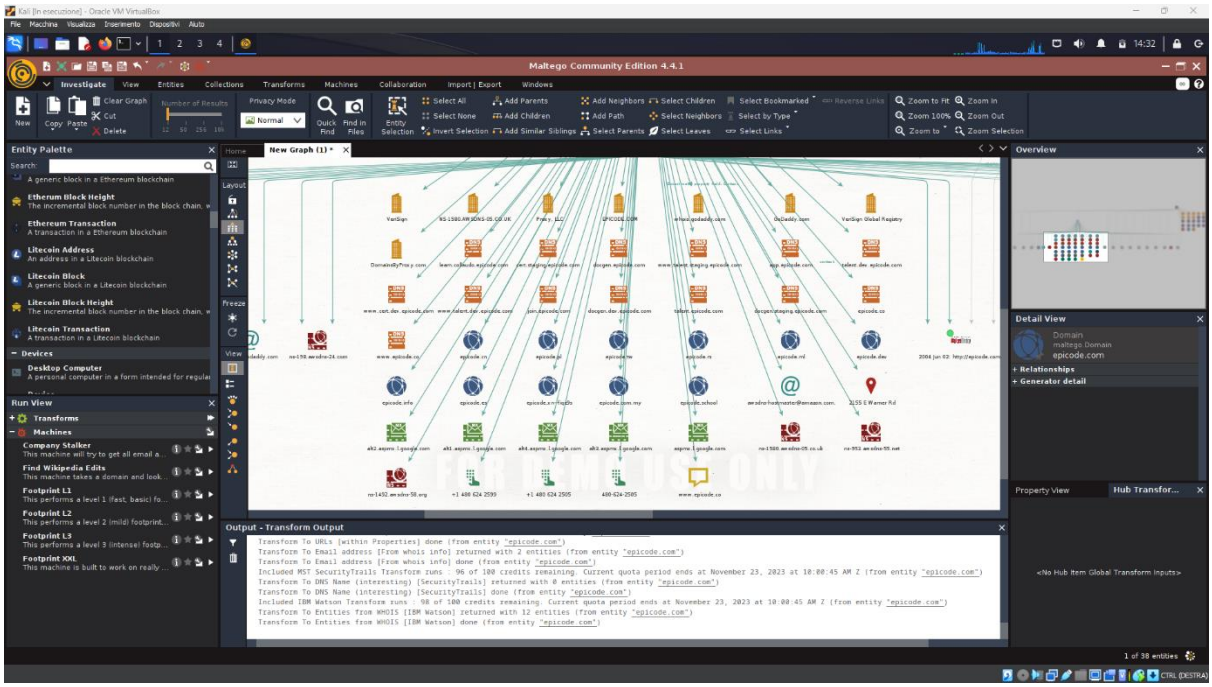
L'esercizio di oggi verteva sull'utilizzo di alcuni tool per la raccolta di informazioni relative a un determinato bersaglio. A scopi accademici, abbiamo usato "Epicode" come possibile bersaglio e una combinazione di Maltego e altri software online (Google, NSlookup, Wayback Machine per citarne alcuni).

Innanzitutto, iniziamo la nostra indagine con una ricerca Google, utilizzando qualche tecnica avanzata. Cerchiamo "intitle:epicode" per far si che tra le ricerche avremo solo risultati aventi "epicode" nel titolo: da qui abbiamo a disposizione i social di Epicode tra i quali Instagram, LinkedIn e Facebook per fare alcuni esempi.

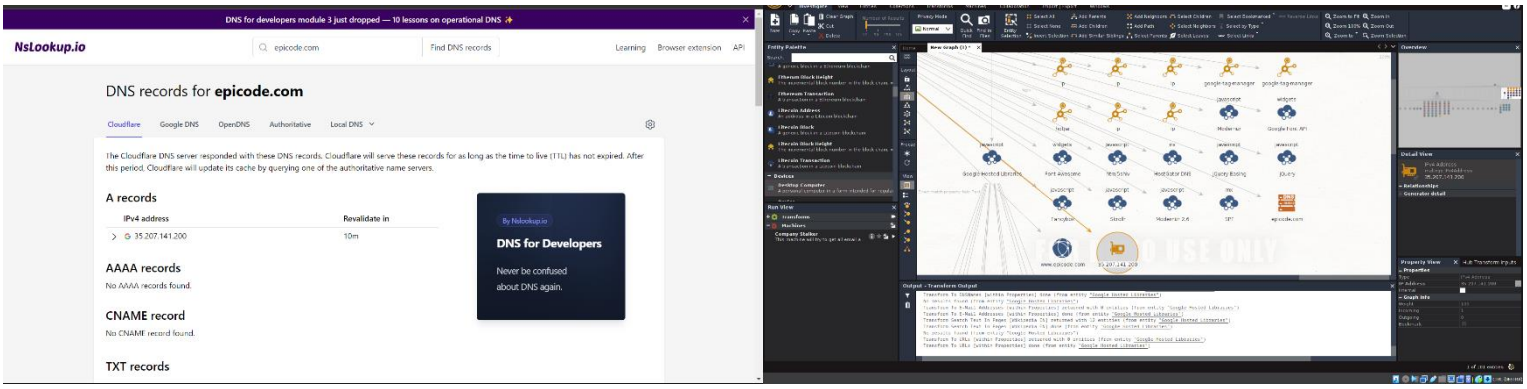
Successivamente proviamo a cercare l'indirizzo tramite Wayback Machine per verificare se nelle vecchie versioni del sito web possiamo trovare qualche informazione non più presente nella versione aggiornata: come mostra l'immagine seguente, abbiamo trovato in una vecchia release l'indirizzo della sede di Epicode a Roma; una ulteriore ricerca tramite Google ci conferma la sede non è cambiata negli anni.



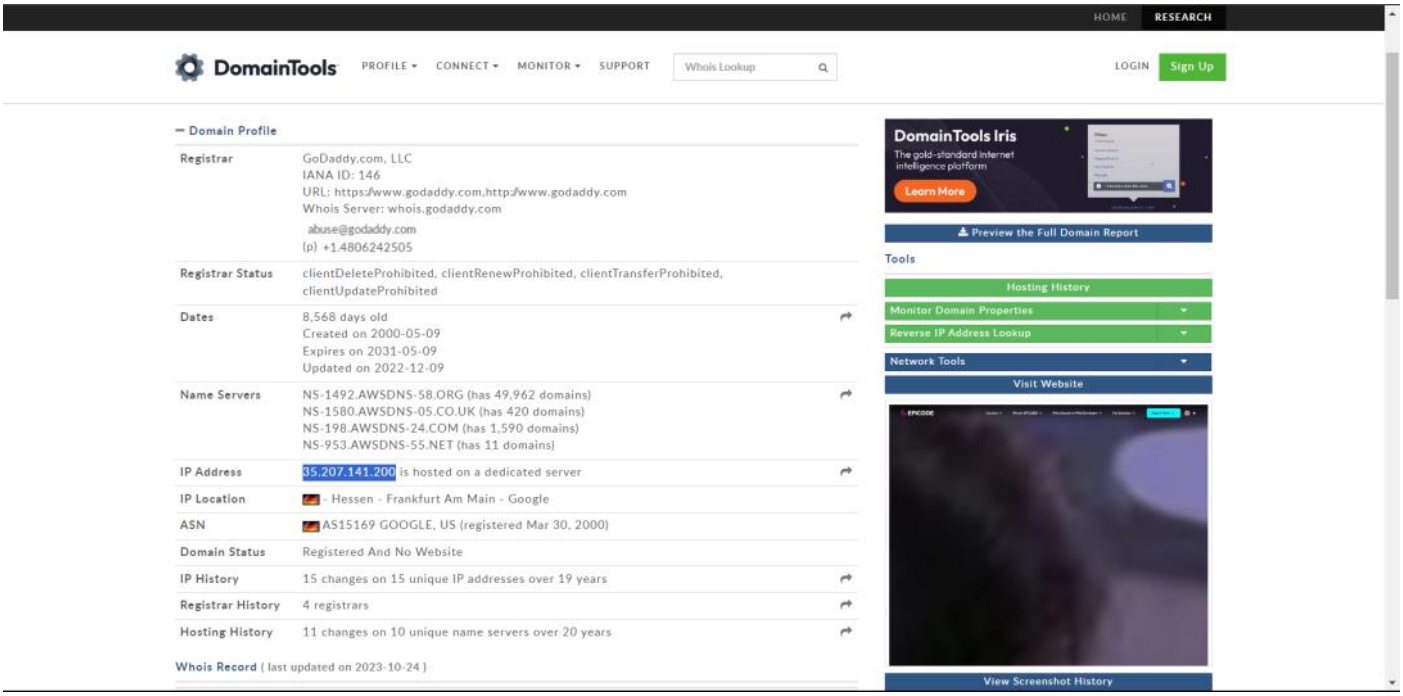
Passiamo quindi al software Maltego, il quale dopo aver messo in input ciò che cerchiamo è in grado di scandagliare il web alla ricerca di più informazioni possibili al riguardo e di metterle in correlazione tra loro. Abbiamo effettuato la prima ricerca con questo software inserendo "epicode.com" come target e specificando che si trattava di un website.



Tra i vari risultati forniteci, possiamo notare goDaddy; facendo qualche ulteriore ricerca, scopriamo che questo è probabilmente il servizio a cui Epicode ha comprato il dominio. In particolare, usando un geolocalizzatore di indirizzi IP, scopriamo che il server principale su cui gira Epicode (all'indirizzo IP 35.207.141.207, come vedremo in seguito) sembra trovarsi a Francoforte, in Germania. Da qui infine ricaviamo anche l'indirizzo IP pubblico di Epicode, a cui diamo una conferma confrontando i risultati con NSlookup.



Cerchiamo tale indirizzo su WhoIs e confermiamo quanto precedentemente detto su goDaddy e Francoforte.

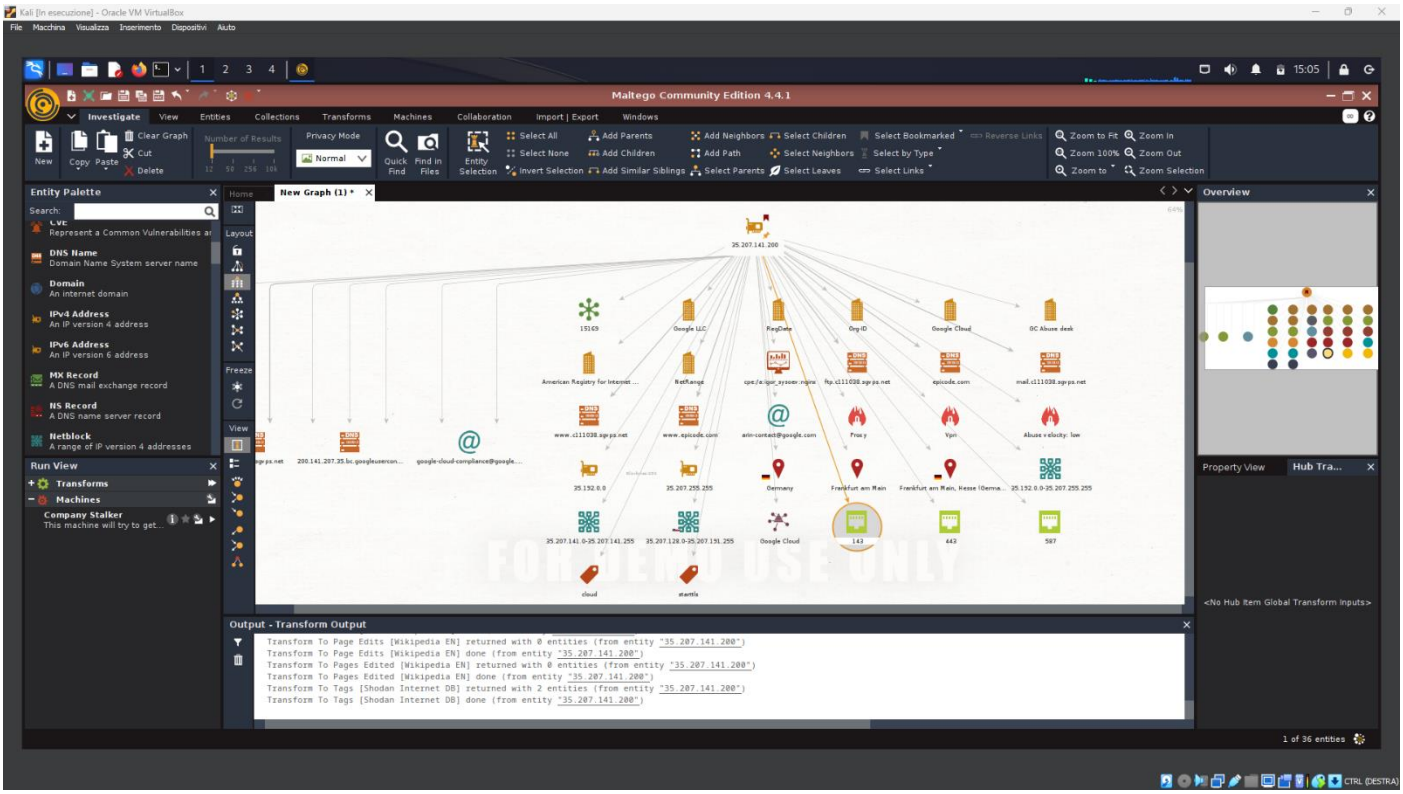


Utilizziamo infine l'IP di Epicode come input per una ricerca tramite Maltengo.

La cosa più interessante che possiamo notare nell'immagine sottostante è la presenza di tre porte:

- 143: IMAP, usata per la ricezione di mail;
- 443 : utilizzata per il protocollo HTTPS;
- 587: usata per SMTP, ossia per inviare mail, invece che la "tipica" porta 25.

Possiamo quindi dedurre che il sito Epicode avrà, almeno in parte, la possibilità di ricevere e inviare e-mail, aprendo quindi la strada a possibili campagne di pishing.


Kali [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Maltego Community Edition 4.4.1
Investigate View Entities Collections Transforms Machines Collaboration Import | Export Windows
Entity Palette
Run View
Transforms
Machines
Company Stalker
This machine will try to get...
New Graph (1) *
Overview
Property View
Hub Tra...
<No Hub Item Global Transform Inputs>
Output - Transform Output
Transform To Page Edits [Wikipedia EN] returned with 0 entities (from entity "35.207.141.200")
Transform To Page Edits [Wikipedia EN] done (from entity "35.207.141.200")
Transform To Pages Edited [Wikipedia EN] returned with 0 entities (from entity "35.207.141.200")
Transform To Pages Edited [Wikipedia EN] done (from entity "35.207.141.200")
Transform To Tags [Shodan Internet DB] returned with 2 entities (from entity "35.207.141.200")
Transform To Tags [Shodan Internet DB] done (from entity "35.207.141.200")
1 of 36 entities