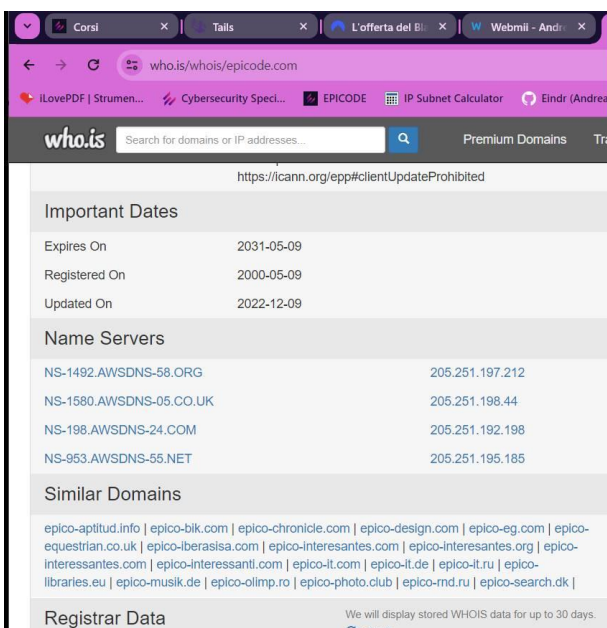


# Settimana 5 Esercizio 2

## Raccolta delle informazioni

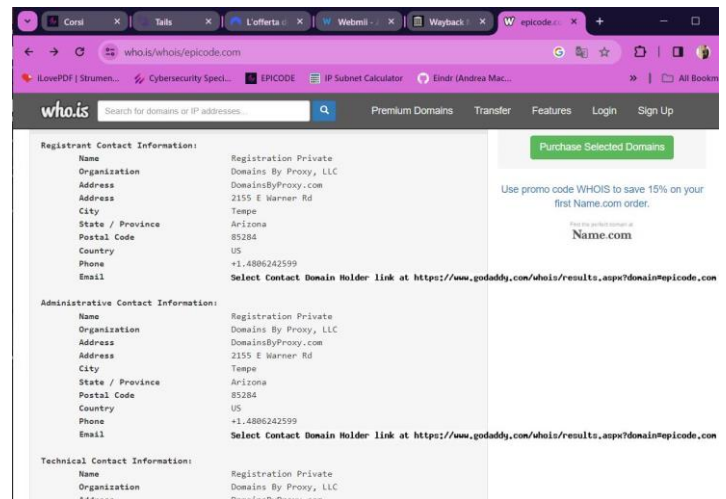
Oggi andremo a familiarizzare con i vari tool disponibili per reperire informazioni per una determinata persona (Andrea Macchi in questo caso) o per una determinata azienda (EPICODE).

Iniziamo a trovare informazioni riguardo la rete di un'azienda. È possibile utilizzare diversi tool quali Shodan, Whols e Wayback Machine. Con essi possiamo andare a vedere aziende e persone associate ad un indirizzo IP o ad un dominio come gli esempi riportati in figura (possiamo notare dei servizi Amazon, si presume DSN):



The screenshot shows the who.is website interface. The search bar contains 'epicode.com'. The results display the following information:

- Important Dates:**
  - Expires On: 2031-05-09
  - Registered On: 2000-05-09
  - Updated On: 2022-12-09
- Name Servers:**
  - NS-1492.AWSDNS-58.ORG 205.251.197.212
  - NS-1580.AWSDNS-05.CO.UK 205.251.198.44
  - NS-198.AWSDNS-24.COM 205.251.192.198
  - NS-953.AWSDNS-55.NET 205.251.195.185
- Similar Domains:**
  - epico-aplitud.info | epico-bik.com | epico-chronicle.com | epico-design.com | epico-eg.com | epico-equestrian.co.uk | epico-iberasisa.com | epico-interesantes.com | epico-interesantes.org | epico-interessantes.com | epico-interessanti.com | epico-it.com | epico-ll.com | epico-ll.ru | epico-libraries.eu | epico-musik.de | epico-olimp.ro | epico-photo.club | epico-rnd.ru | epico-search.dk |
- Registrar Data:** We will display stored WHOIS data for up to 30 days.



The screenshot shows the who.is website interface with the search bar containing 'epicode.com'. The results display the following contact information:

- Registrant Contact Information:**
  - Name: Registration Private
  - Organization: Domains By Proxy, LLC
  - Address: DomainsByProxy.com
  - City: Tempe
  - State / Province: Arizona
  - Postal Code: 85284
  - Country: US
  - Phone: +1.4886242599
  - Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=epicode.com
- Administrative Contact Information:**
  - Name: Registration Private
  - Organization: Domains By Proxy, LLC
  - Address: DomainsByProxy.com
  - City: Tempe
  - State / Province: Arizona
  - Postal Code: 85284
  - Country: US
  - Phone: +1.4886242599
  - Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=epicode.com
- Technical Contact Information:**
  - Name: Registration Private
  - Organization: Domains By Proxy, LLC
  - Address: DomainsByProxy.com

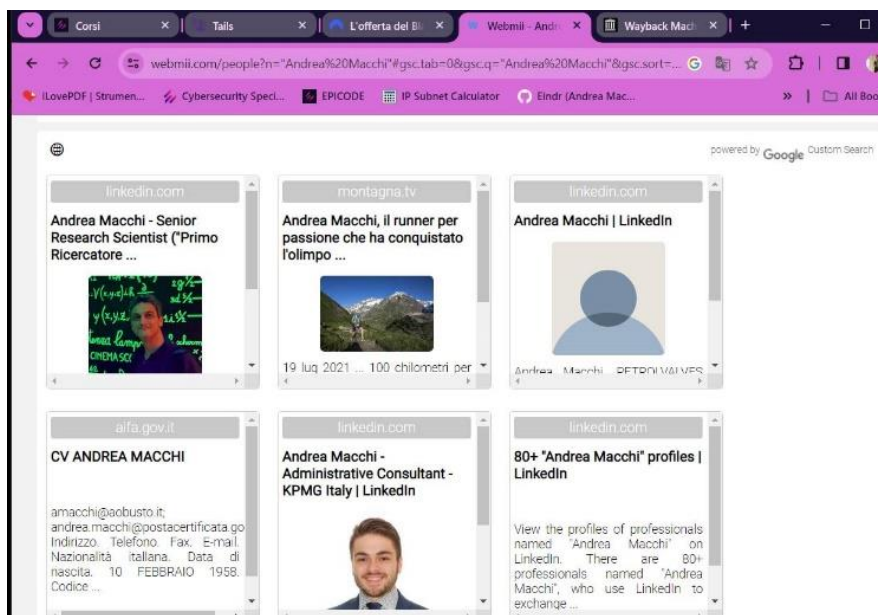
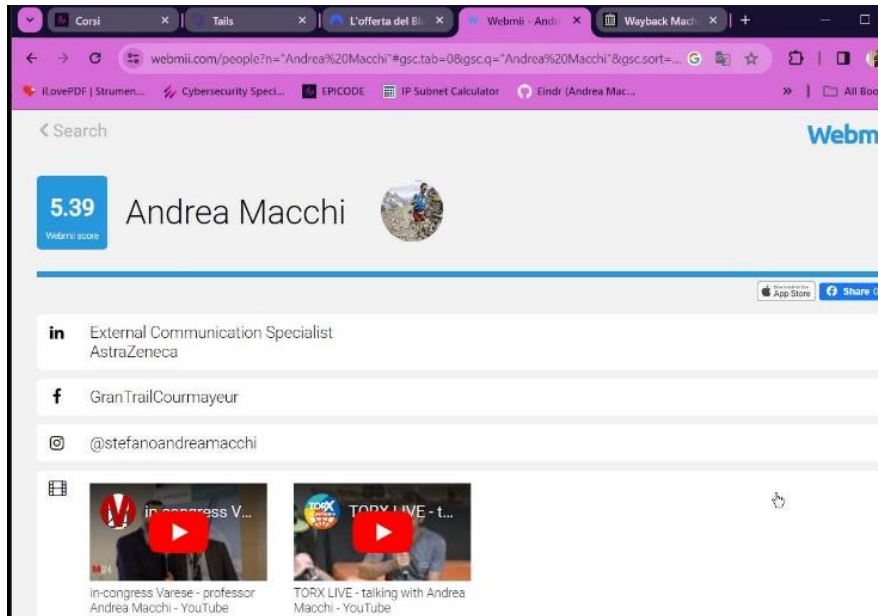
Con Wayback Machine possiamo anche andare a visionare una cronologia delle modifiche apportate al sito così da poter andare a cercare vulnerabilità all'interno del codice che potrebbero essere ancora presenti. Inoltre posso anche andare a trovare file o informazioni ormai cancellate (numeri di telefono, e-mail etc.)



The screenshot shows the Wayback Machine website interface. The search bar contains 'epicode.com'. The results display the following information:

- Calendar:** Saved 97 times between February 17, 2004 and October 18, 2023.
- Timeline:** A bar chart showing the frequency of saves over time, with a peak in 2023.

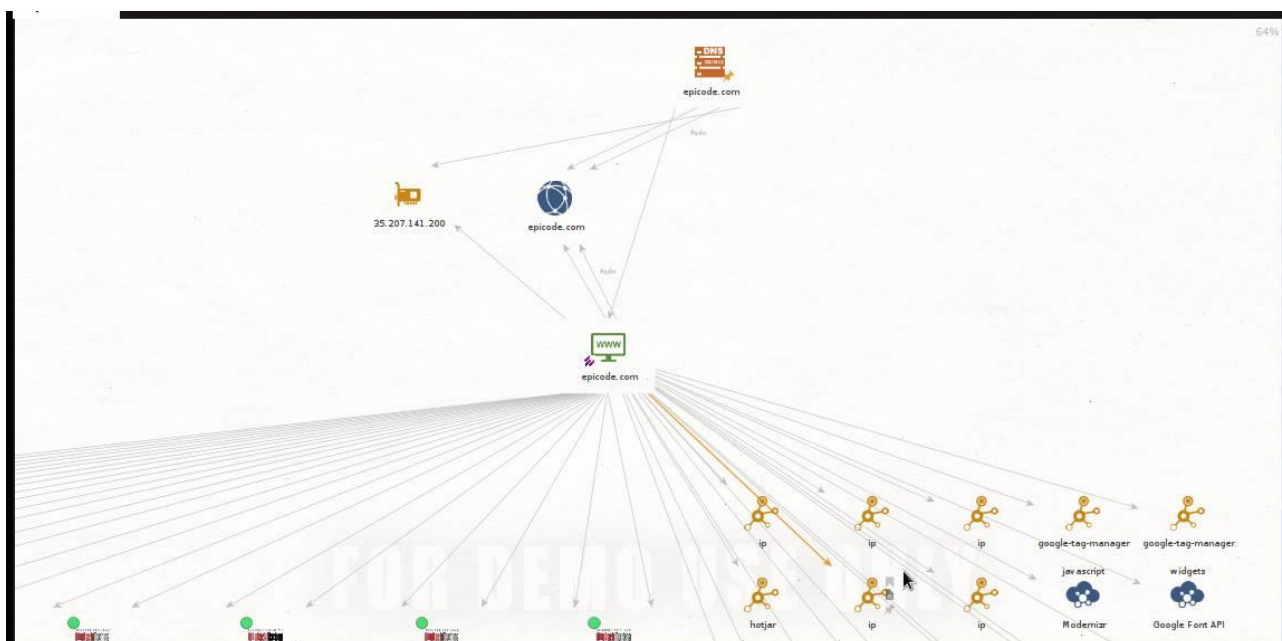
Oltre ai domini, posso anche usare motori di ricerca per trovare il profilo interessato. Usiamo WebMii in questo caso e ci restituirà tutto ciò che trova di correlato al nome (profili social, documenti caricati e pubblici etc.):



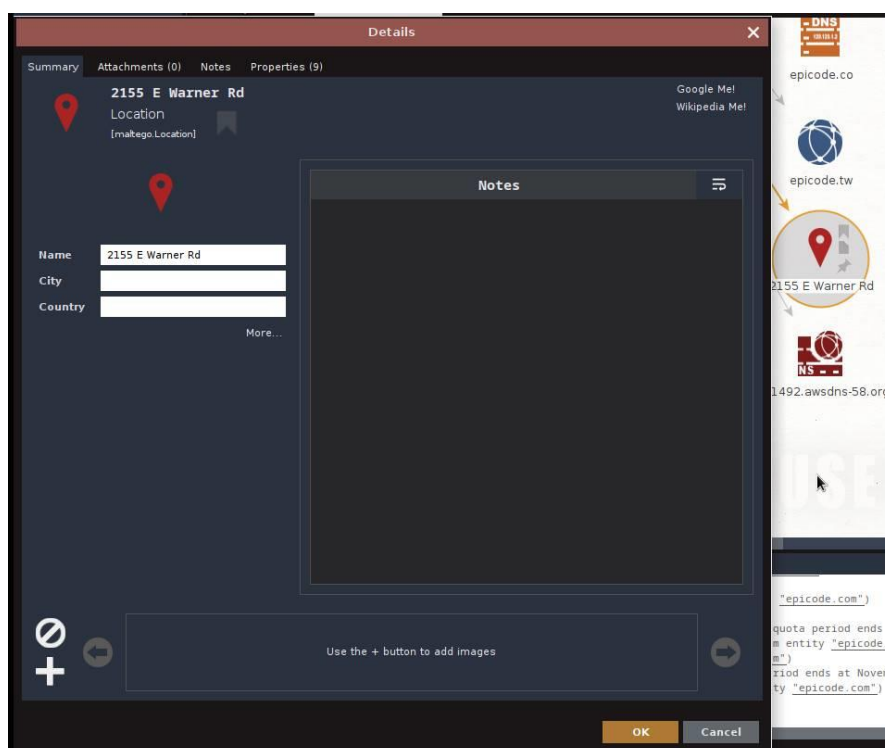
## MALTEGO

Maltego rappresenta una delle risorse più importanti della fase di ricerca: esso permette di avere uno storico delle proprie ricerche tramite una vera e propria “lavagna investigativa” e di trovare velocemente informazioni riguardo un determinato nome o dominio.

In figura possiamo vedere come possiamo, ad esempio, inserire un server DNS come ricerca di partenza, inserire il dominio di EPICODE e andare ad esplorare i vari rami (dominio, indirizzi IP, e-mail etc..)

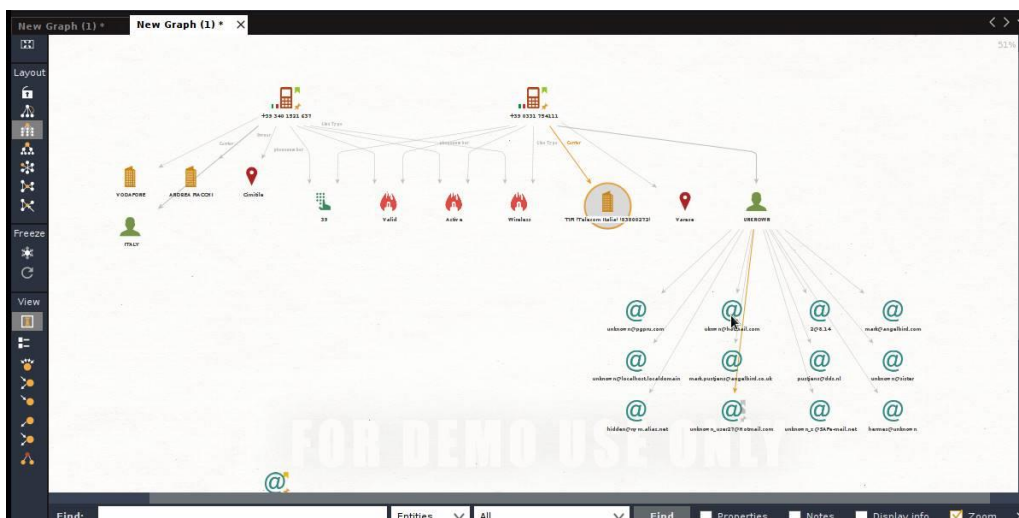
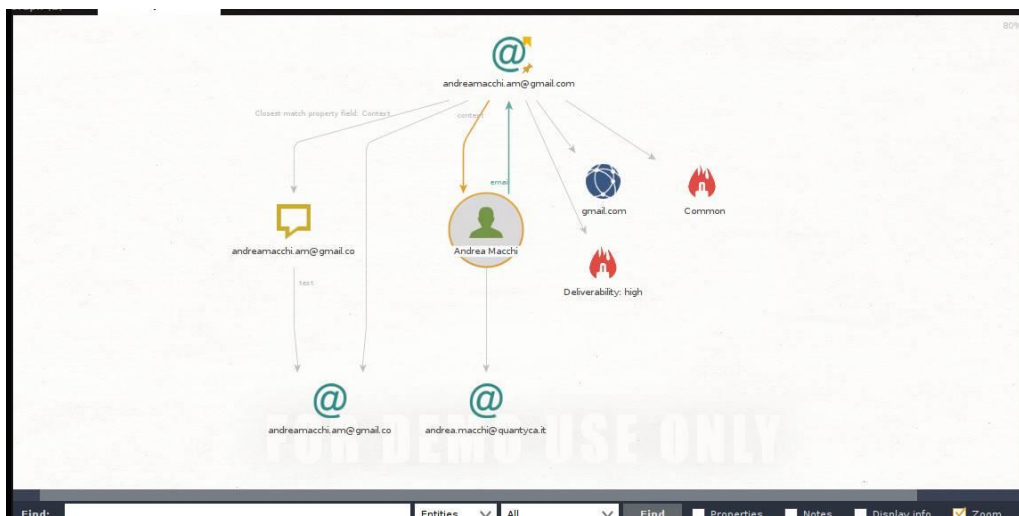


Andando a scavare e integrando una ricerca internet tramite Google, possiamo risalire anche ad informazioni più specifiche come il tipo di servizio hosting, la posizione di questo e molto altro (anche le eventuali porte aperte).





Stessa cosa possiamo fare con un'indirizzo e-mail o un numero di cellulare. Se inseriamo quello personale andrà a trovare le informazioni pubbliche correlate:



Questi sono solo alcuni dei potenti strumenti che abbiamo a disposizione per questa delicata fase di ricerca, ma i tempi di esecuzione possono variare molto e più si approfondisce, più saremo preparati.