

## 1. Obiettivo dell'esercitazione

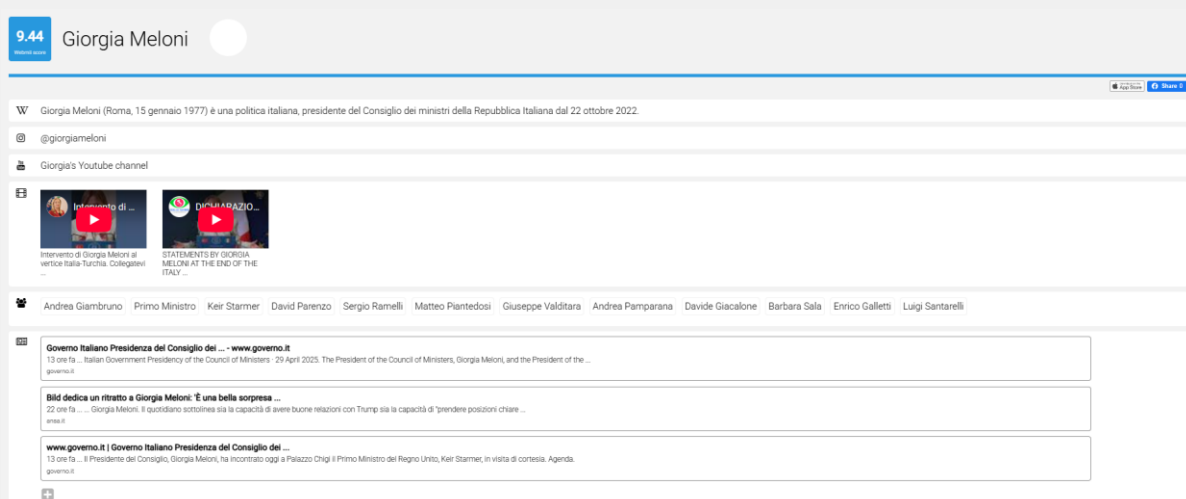
L'obiettivo dell'attività è simulare la fase iniziale di un penetration test, con particolare attenzione alla raccolta di informazioni da fonti aperte (OSINT – Open Source Intelligence). Questa fase è fondamentale all'interno di un processo di analisi della sicurezza, in quanto consente di acquisire dati pubblicamente disponibili sul bersaglio, utili per le successive fasi di attacco mirato.

## 2. Scelta del soggetto

Il soggetto selezionato è Giorgia Meloni, attuale Presidente del Consiglio dei Ministri. La scelta è motivata dall'elevata esposizione mediatica e dalla disponibilità di contenuti pubblici, che permettono un'analisi realistica e articolata. L'approccio seguito è stato incrementale: dalla ricognizione generale si è passati alla mappatura relazionale e tecnica.

## 3. Strumenti

### 3.1 WebMii



Lo strumento è stato impiegato per ottenere un primo indice di visibilità online del soggetto.

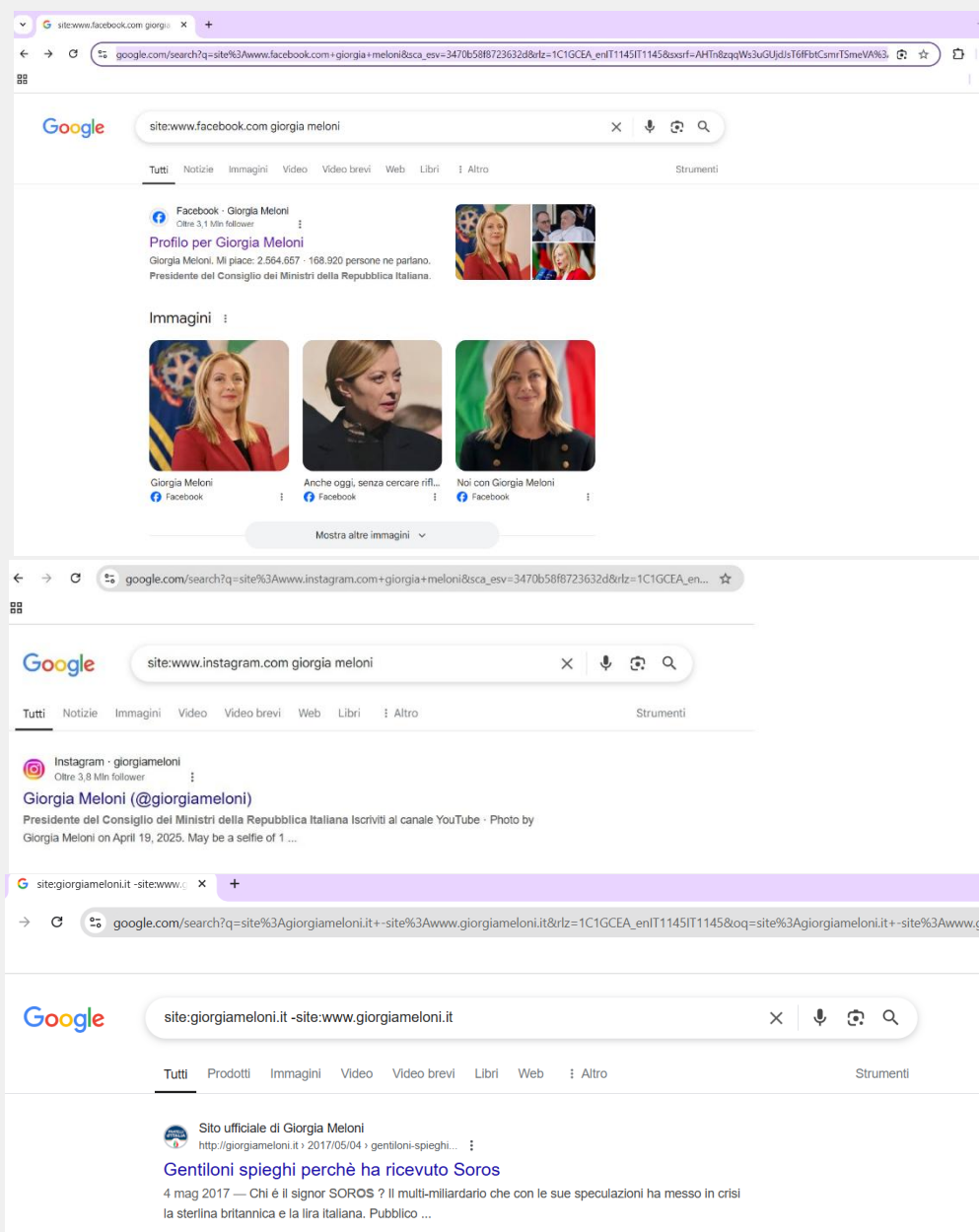
- **Risultato:** punteggio di visibilità molto elevato, con fonti che includono immagini, articoli, profili e menzioni.
- **Utilità:** ha confermato la forte presenza online del target e fornito primi spunti per l'esplorazione con strumenti OSINT più avanzati.

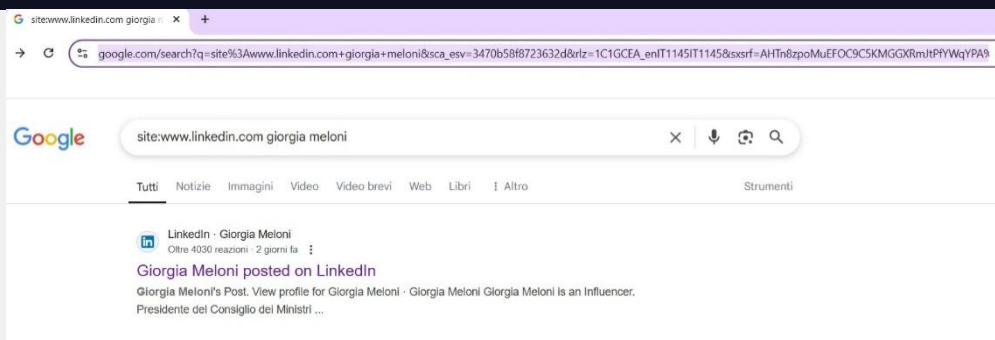
### 3.2 Google e Google Dorking

Sono state condotte ricerche con l'utilizzo di operatori avanzati (es. site:, filetype:, intitle:), per estrarre informazioni più specifiche e difficilmente accessibili tramite ricerche tradizionali.

#### Obiettivi raggiunti:

- Identificazione di profili social associati;
- Recupero di articoli biografici, libri e incarichi istituzionali;
- Informazioni su legami familiari e relazioni politiche.



*Solito gius*

A screenshot of the "scrivi.camera.it" website. The page title is "Scrivi a MELONI Giorgia (MELONI\_G@CAMERA.IT)". The form includes fields for "Oggetto\*", "Email mittente\*", and "Messaggio\*". There is also a section for "Allegato - dimensione massima 10 MB" with a "Scegli file" button and the text "Nessun file selezionato". A blue "INVIA" button is at the bottom right.


### 3.3 ChatGPT

L'intelligenza artificiale è stata utilizzata per colmare alcune lacune informative, ad esempio per ottenere il cognome della figlia del soggetto, non immediatamente reperibile tramite le fonti web. L'IA ha facilitato l'aggregazione e la sintesi di dati frammentati, controllati successivamente tramite le fonti riportate.

cognome della figlia della meloni

Errore durante la ricerca

Errore durante la ricerca

La figlia di Giorgia Meloni si chiama **Ginevra**. È nata il 16 settembre 2016 a Roma, frutto della relazione con il giornalista Andrea Giambruno, conclusasi nel 2023 . 


ilGiornale.it   Wikipedia, l'enciclopedia libera

Ginevra è spesso al centro dell'attenzione mediatica, soprattutto quando accompagna la madre in eventi ufficiali o durante viaggi all'estero. Ad esempio, è stata fotografata con Giorgia Meloni durante il G20 e in altre occasioni pubbliche . Wikipedia, l'enciclopedia libera


La leader di Fratelli d'Italia ha più volte espresso il suo amore per la figlia, condividendo anche momenti privati sui social media. In un'occasione, ha scritto: "Ovunque insieme, topolina mia", accompagnando una foto che la ritraeva con Ginevra . ilGiornale.it

↓

Nonostante la giovane età, Ginevra è già una figura di interesse pubblico, spesso al fianco della madre in eventi ufficiali.

 Fonti

quindi non sai il cognome di Ginevra



Il cognome della figlia di Giorgia Meloni è **Giambruno**. Il suo nome completo è **Ginevra Giambruno**. È nata il 16 settembre 2016 a Roma, frutto della relazione con il giornalista Andrea Giambruno . Donnapop

Giorgia Meloni ha annunciato la separazione da Andrea Giambruno il 20 ottobre 2023, dopo quasi un decennio insieme . AP News

### 3.4 Whois

È stata effettuata un'analisi tecnica del dominio *giorgiameloni.it* per:

- Verificare i dati di registrazione;
- Rintracciare eventuali soggetti coinvolti nella gestione del sito;
- Valutare l'affidabilità e la struttura dell'infrastruttura digitale.

```
(kali@kali)-[~]
$ whois giorgiameloni.it

*****
* Please note that the following result could be a subgroup of
* the data contained in the database.
*
* Additional information can be visualized at:
* http://web-whois.nic.it
*****

Domain:                giorgiameloni.it
Status:                ok
Signed:                no
Created:                2006-03-31 00:00:00
Last Update:           2025-04-16 00:56:22
Expire Date:           2026-03-31

Registrant
  Organization:         Ass. fratelli D'Italia - Centrodestra Nazionale
  Address:              Via Giambattista Vico 1
                       ROMA
                       00196
                       RM
                       IT
  Created:              2014-04-08 12:08:36
  Last Update:          2014-04-08 12:08:36

Admin Contact
  Name:                 Marco Marsilio
  Organization:         Ass. fratelli D'Italia - Centrodestra Nazionale
  Address:              Via Giambattista Vico 1
                       ROMA
                       00196
                       RM
                       IT
  Created:              2014-04-08 12:08:37
  Last Update:          2014-04-08 12:08:37

Technical Contacts
  Name:                 Marco Marsilio
  Organization:         Ass. fratelli D'Italia - Centrodestra Nazionale
  Address:              Via Giambattista Vico 1
                       ROMA
                       00196
                       RM
                       IT
  Created:              2014-04-08 12:08:37
  Last Update:          2014-04-08 12:08:37

Registrar
  Organization:         Aruba s.p.a.
  Name:                 ARUBA-REG
  Web:                  http://www.aruba.it
  DNSSEC:               yes

Nameservers
  dns.technorail.com
  dns2.technorail.com
  dns3.arubadns.net
  dns4.arubadns.cz
```

### 3.5 theHarvester

```
[*] Interesting Urls found: 3
https://www.giorgiameloni.it/
https://www.giorgiameloni.it/?s=
https://www.giorgiameloni.it/scrivici/

[*] LinkedIn Links found: 0

[*] IPs found: 19
104.26.8.202
104.26.9.202
172.67.68.246
31.11.36.21
62.149.128.151
62.149.128.154
62.149.128.157
62.149.128.160
62.149.128.163
62.149.128.166
62.149.128.72
62.149.128.74
89.46.105.19
89.46.106.35
89.46.109.60
89.46.110.54
89.46.110.82
89.46.110.84

[*] No emails found.

[*] Hosts found: 11
*.giorgiameloni.it
giorgiameloni.it:mx.giorgiameloni.it
giorgiameloni.it:mx.giorgiameloni.it.
mx.giorgiameloni.it:62.149.128.151
mx.giorgiameloni.it:62.149.128.154
mx.giorgiameloni.it:62.149.128.157
mx.giorgiameloni.it:62.149.128.160
mx.giorgiameloni.it:62.149.128.163
mx.giorgiameloni.it:62.149.128.166
mx.giorgiameloni.it:62.149.128.72
mx.giorgiameloni.it:62.149.128.74
```

Impiegato per raccogliere indirizzi email, domini e sottodomini associati a fonti pubbliche.

#### Esito:

- Sono stati identificati alcuni URL di interesse, tra cui la homepage, una pagina di ricerca e una sezione di contatto (/scrivici/), potenzialmente utile per analisi future su moduli e interazioni web.
- Sono stati rilevati 19 indirizzi IP e diversi record MX legati al dominio, relativi ai server di posta. Questi potrebbero essere soggetti a ulteriori verifiche tecniche nelle fasi successive del penetration test.

Tuttavia, non sono stati trovati indirizzi email né collegamenti a profili professionali (es. LinkedIn), e molti degli IP risultano appartenere a servizi di hosting condiviso (es. Aruba), rendendo complessa l'attribuzione diretta al target.

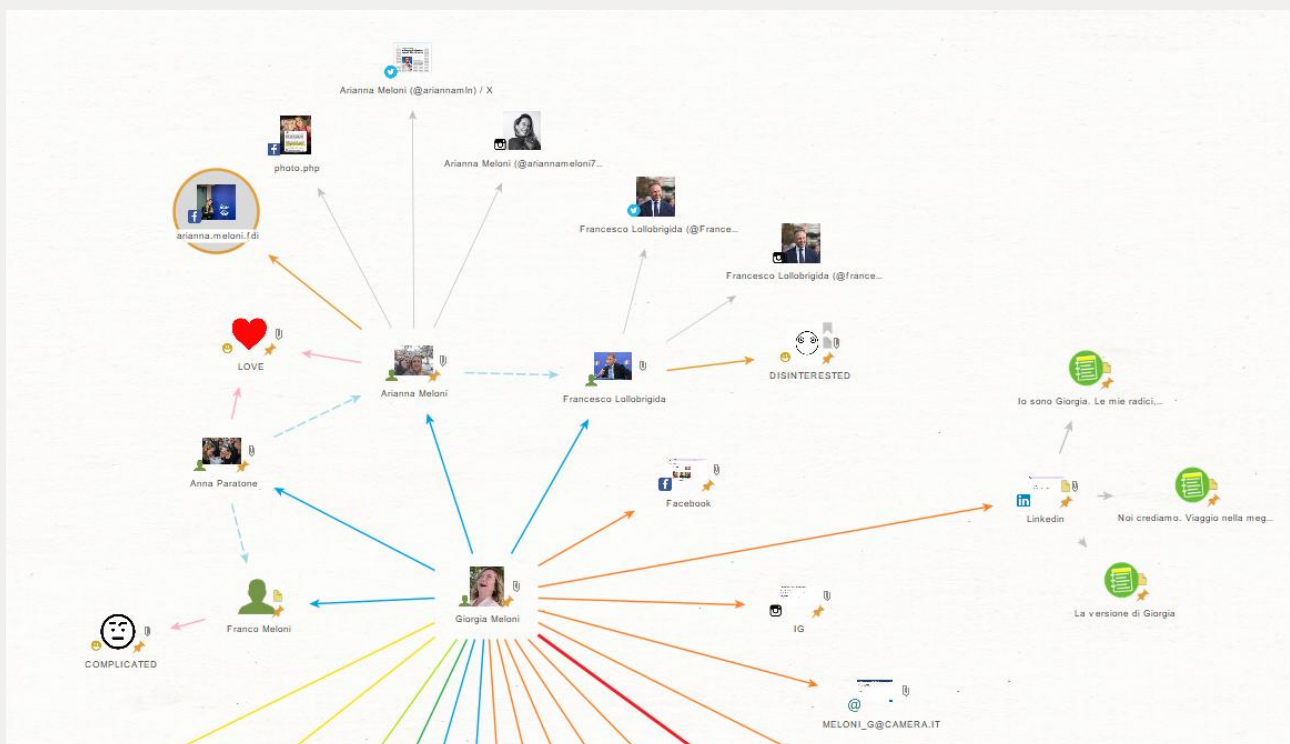
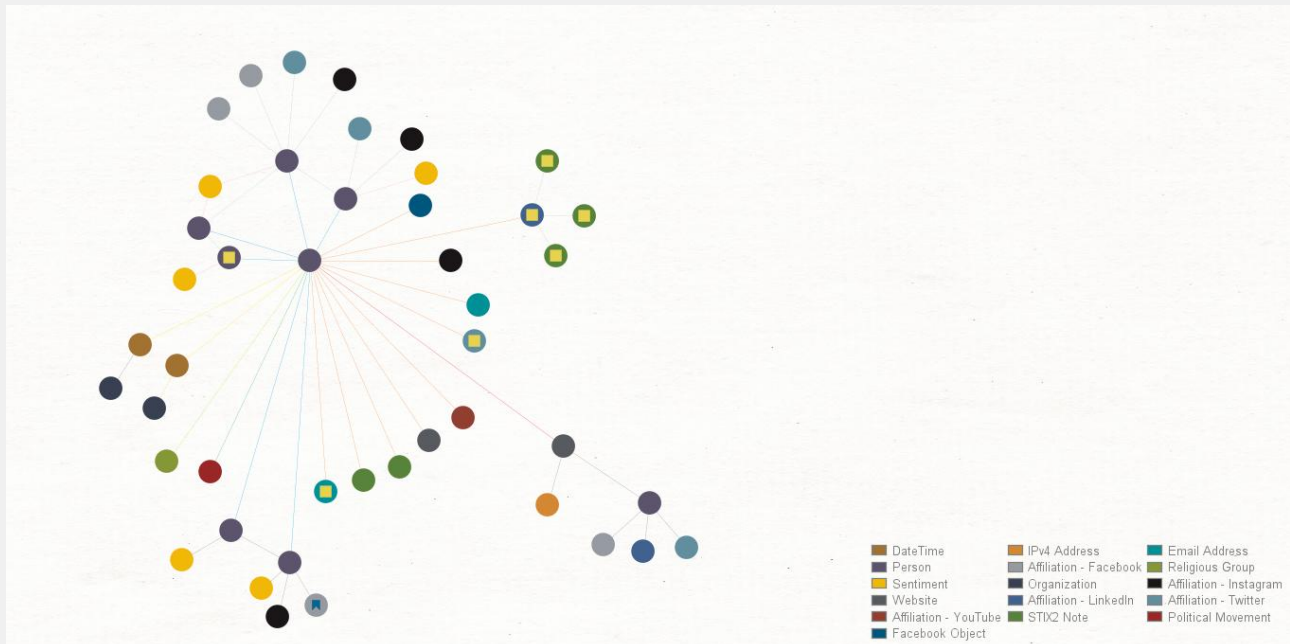
- **Risultato:** lo strumento ha fornito una visione preliminare dell'infrastruttura, ma l'efficacia è risultata limitata, probabilmente a causa della natura istituzionale del sito e della buona gestione della superficie esposta.

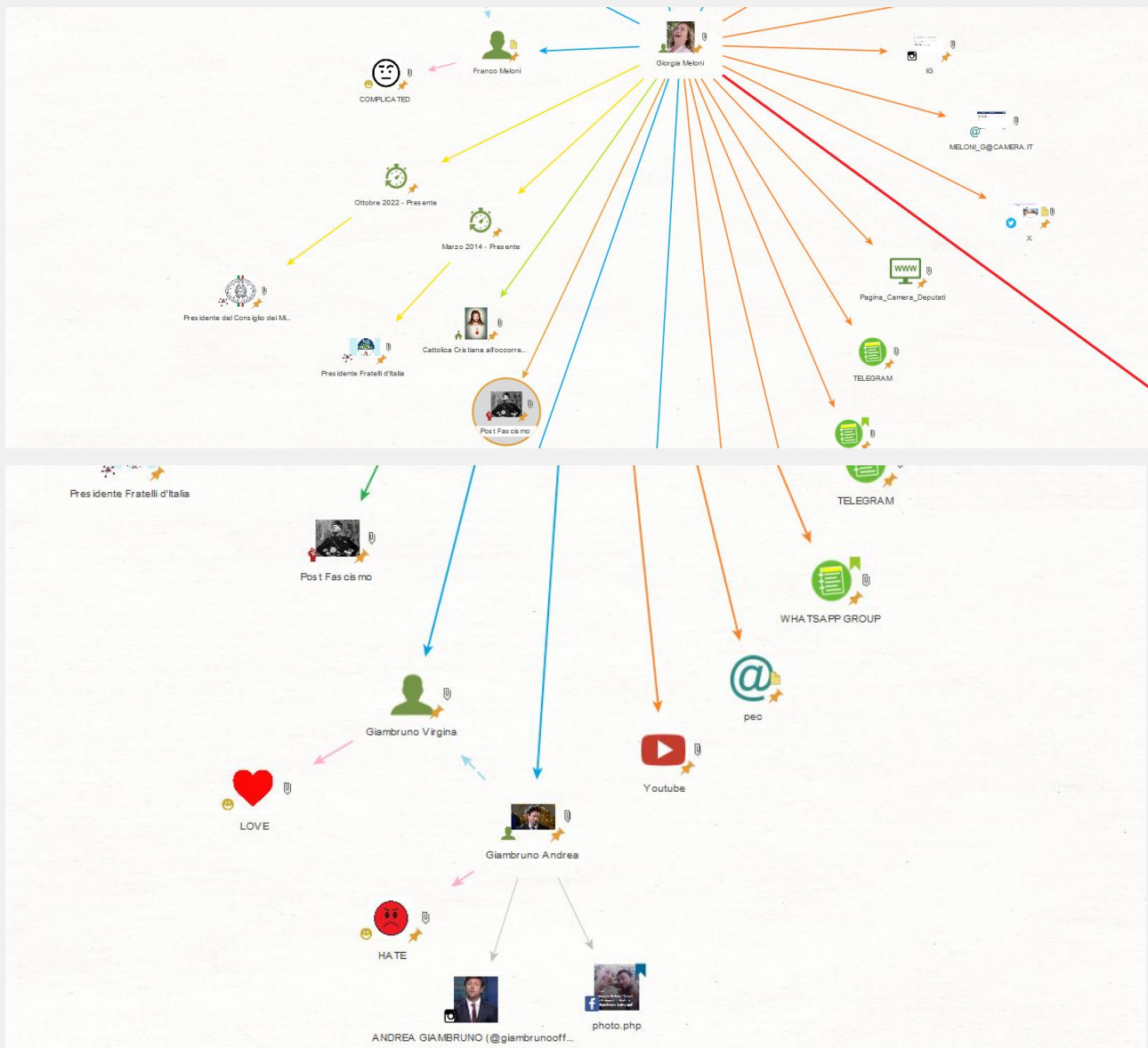


### 3.6 Maltego

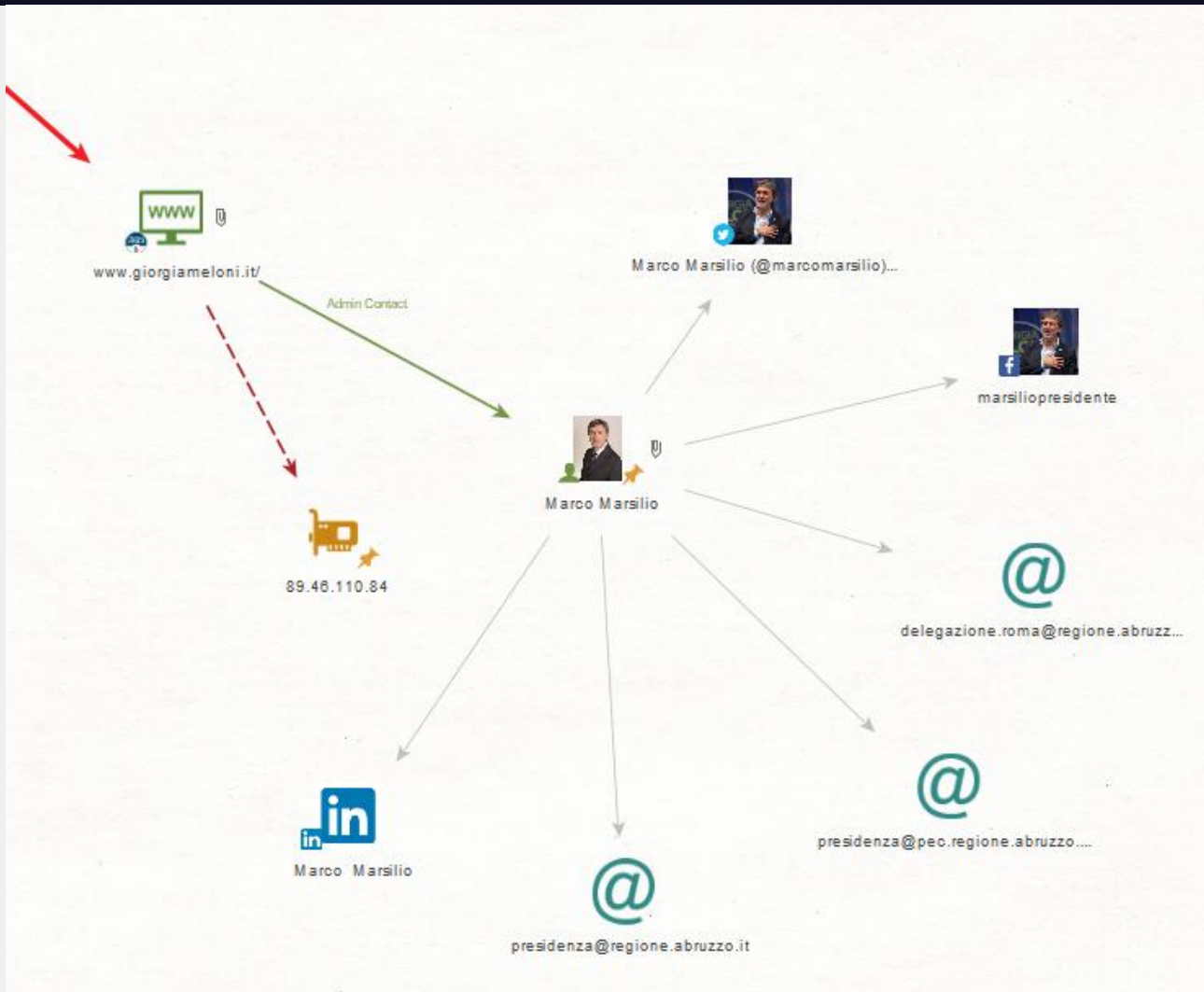
I dati raccolti sono stati importati in Maltego per costruire una rappresentazione grafica delle connessioni del soggetto.

- **Transformer utilizzati:** standard su domini, profili social e relazioni familiari (es. “Person – Email Address”, “To Social Profiles”).
- **Risultato:** generazione di una mappa visiva delle connessioni con individui, entità politiche, domini e canali di comunicazione.









#### 4. Risultati principali

- Conferma dell'elevata esposizione online del soggetto;
- Reperimento di dati personali e professionali pubblicamente accessibili;
- Identificazione di collegamenti familiari e relazioni istituzionali;
- Mappatura tecnica parziale della presenza digitale del soggetto (domini, siti, account pubblici).

## 5. Considerazioni e fasi successive del penetration test

Le informazioni raccolte costituiscono una solida base per le fasi successive di un penetration test, tra cui:

- **Social Engineering:** i dati su familiari e profili social possono essere impiegati per simulare attacchi di phishing mirati.
- **Attack Surface Mapping:** l'analisi dei domini e delle infrastrutture digitali può rivelare vulnerabilità tecniche (es. porte aperte, servizi esposti).
- **Profilazione delle abitudini digitali:** la raccolta di contenuti pubblicati può suggerire pattern di comportamento, orari di attività e preferenze, utili per attacchi personalizzati.

## 6. Conclusione

Questa simulazione ha evidenziato il ruolo cruciale della fase di information gathering all'interno di un penetration test. Le tecniche OSINT, pur non invasive, consentono di raccogliere una quantità significativa di dati pubblici, che, se correttamente elaborati e integrati con strumenti automatici e tecniche successive (come il vulnerability assessment), possono contribuire in modo determinante all'individuazione di punti deboli nella sicurezza informatica di individui o organizzazioni.