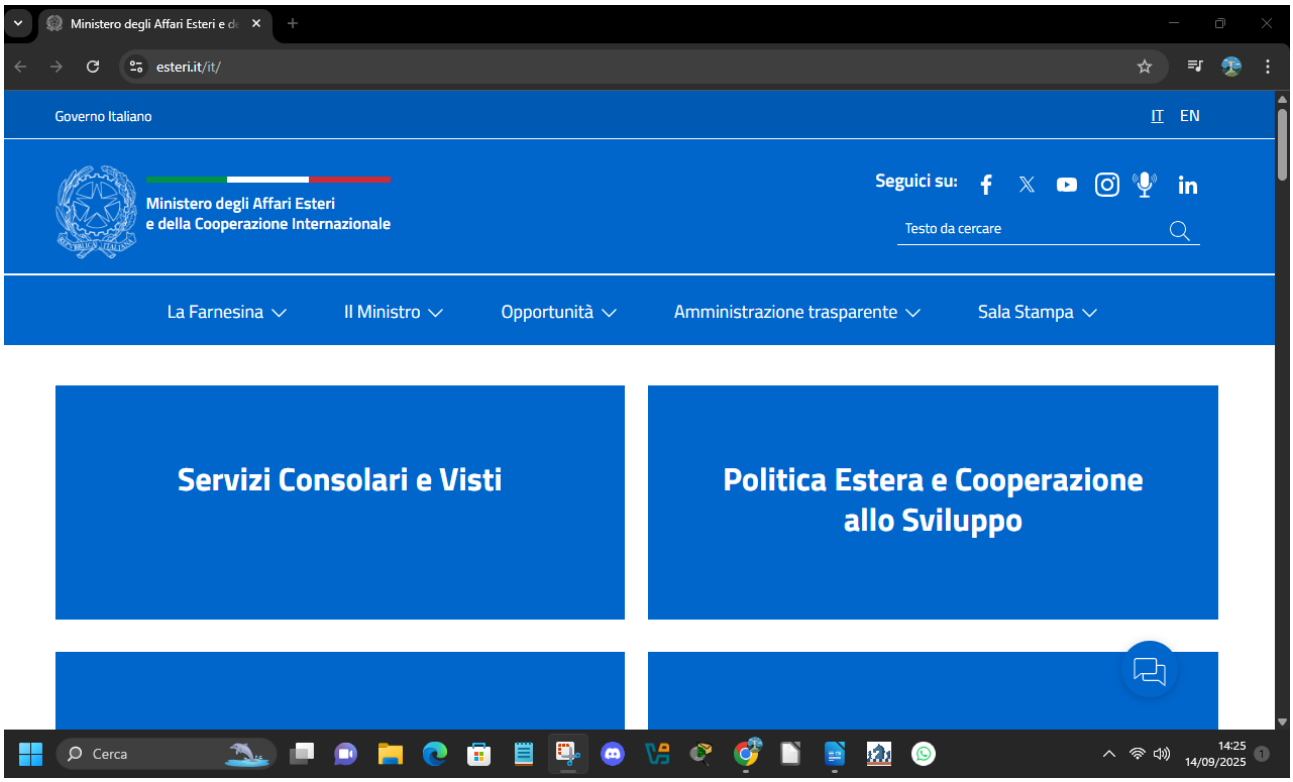
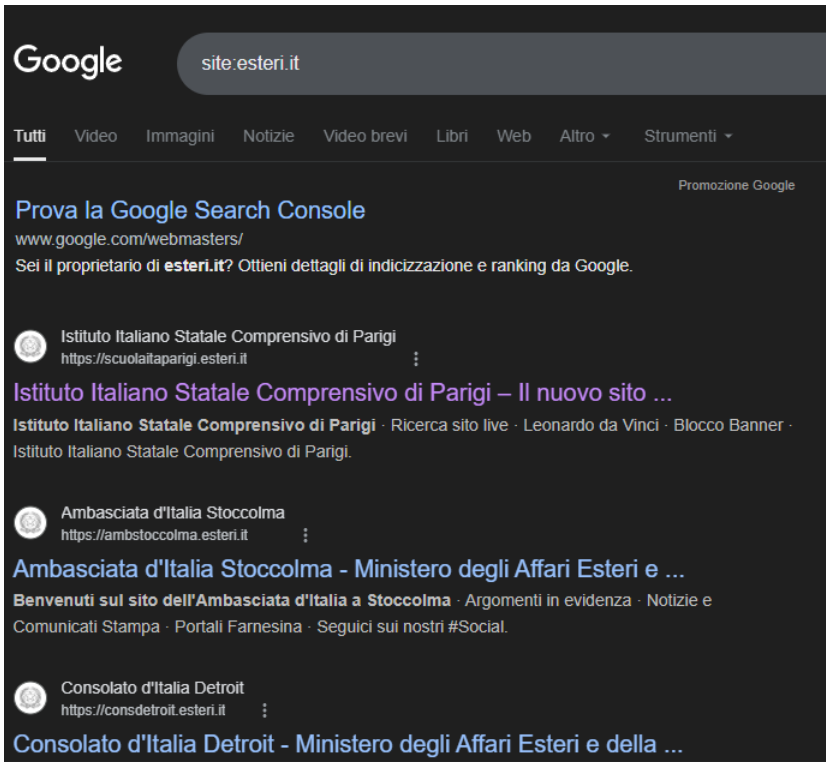
W10D1 – FRANCESCO MONTALTO

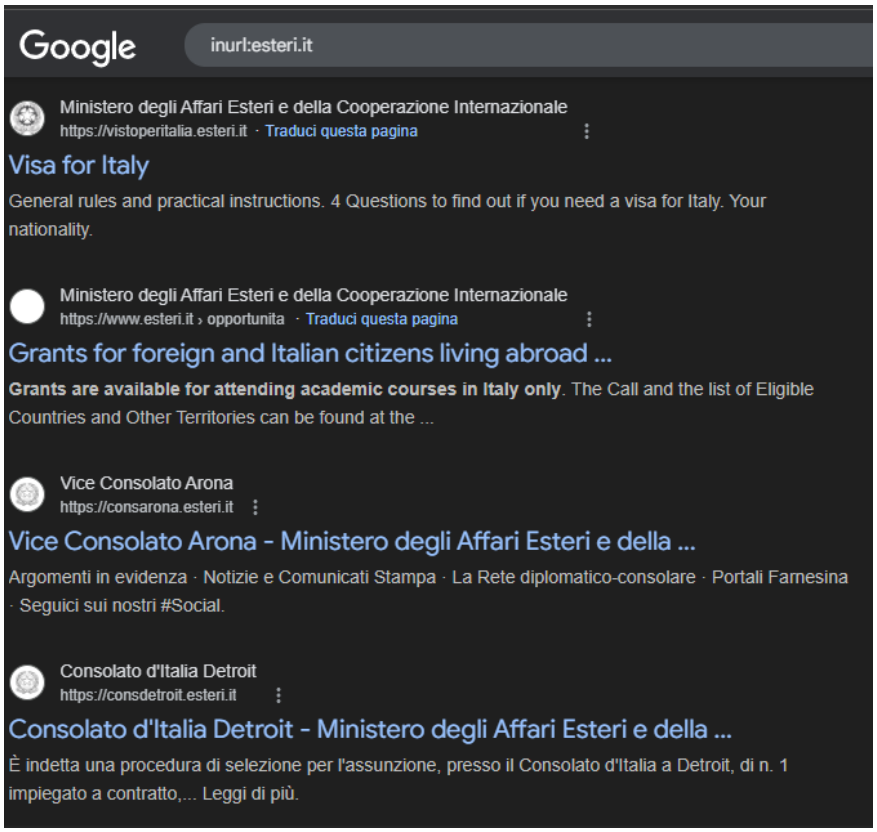
PER QUESTO ESERCIZIO HO SCELTO COME SITO WEB IL SITO DEL MINISTERO DEGLI AFFARI ESTERI E DELLA COOPERAZIONE INTERNAZIONALE, “ESTERI.IT” RAGGIUNGIBILE DA “https://www.esteri.it/it/”. A SEGUIRE, TUTTI I COMANDI DI GOOGLE HACKING.

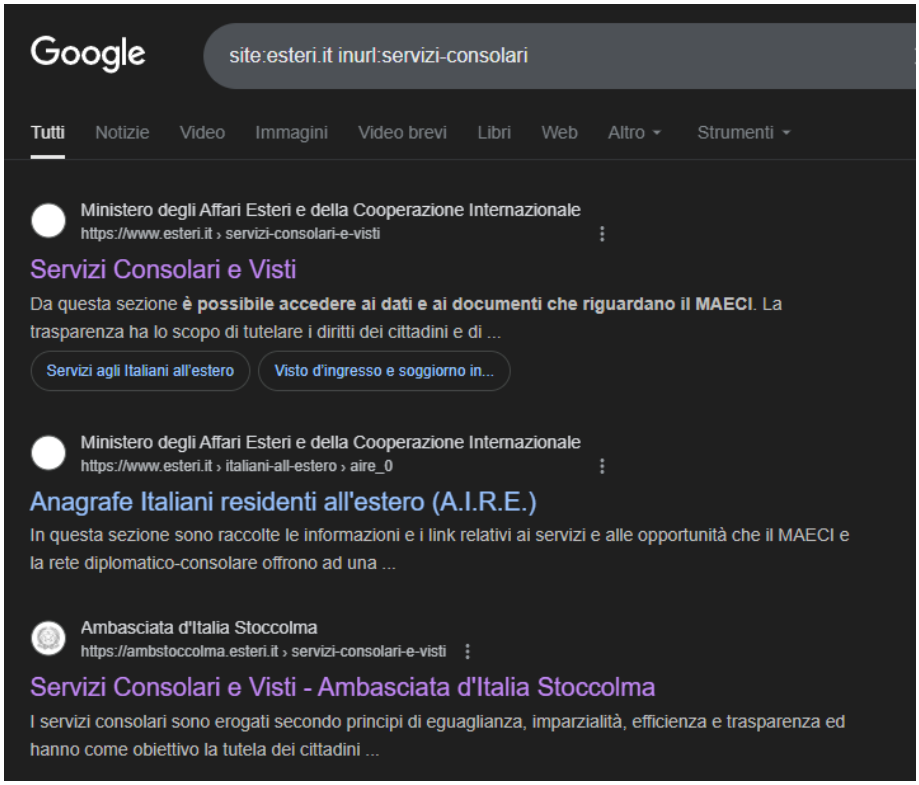


1. **SITE:** Lo scopo di questo comando è vedere l’insieme delle pagine indicizzate (anche sottodomini). Nell’esempio in questione possiamo vedere le varie pagine istituzionali indicizzate, e pagine di Ambasciate, Consolati (sottodomini tipo “amb...”, “cons…”, ecc…); un dominio abbastanza ramificato.

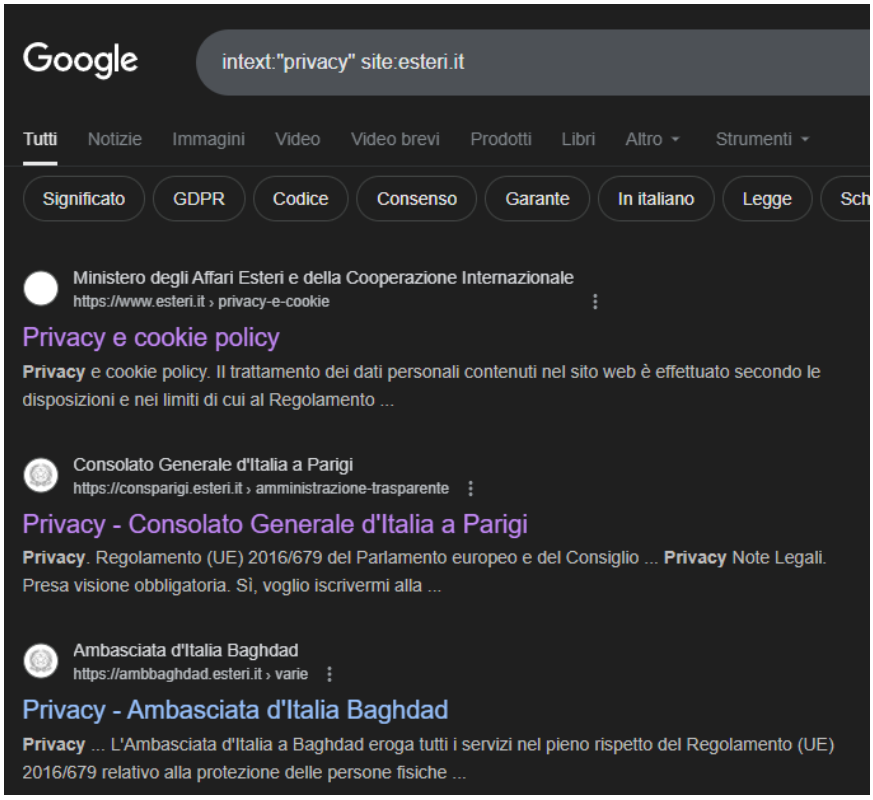


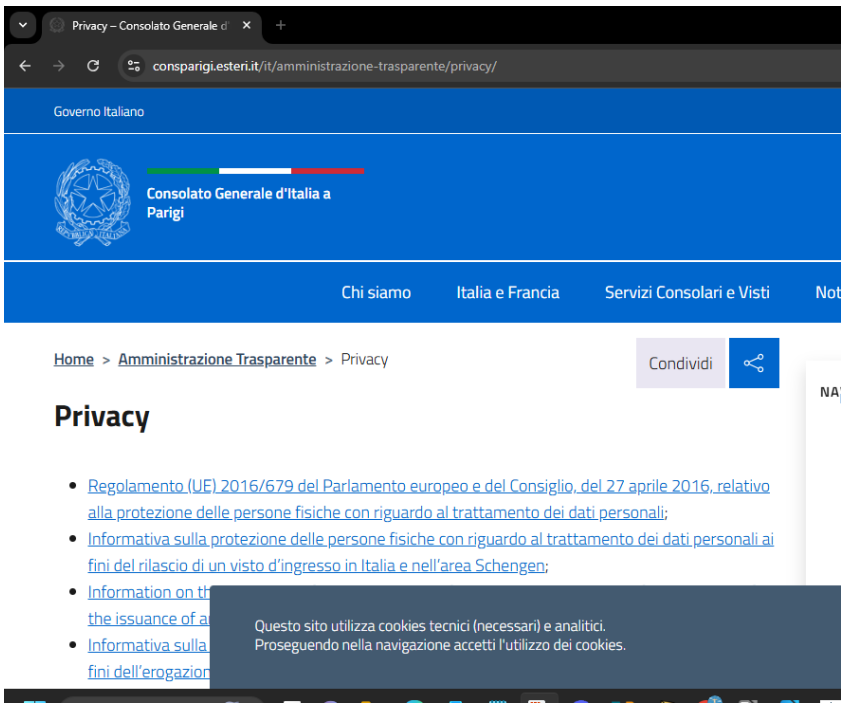
2. **INURL:** Lo scopo di “inurl” è elencare URL che contengono il testo, nel nostro caso, “esteri.it” . Come visibile dalla seconda immagine, INURL è particolarmente utile quanto usato con i segmenti di percorso: in quest’ultimo caso ci vengono mostrate tutte le pagine del dominio “esteri.it” che hanno nell’URL la stringa “servizi- consolari”.



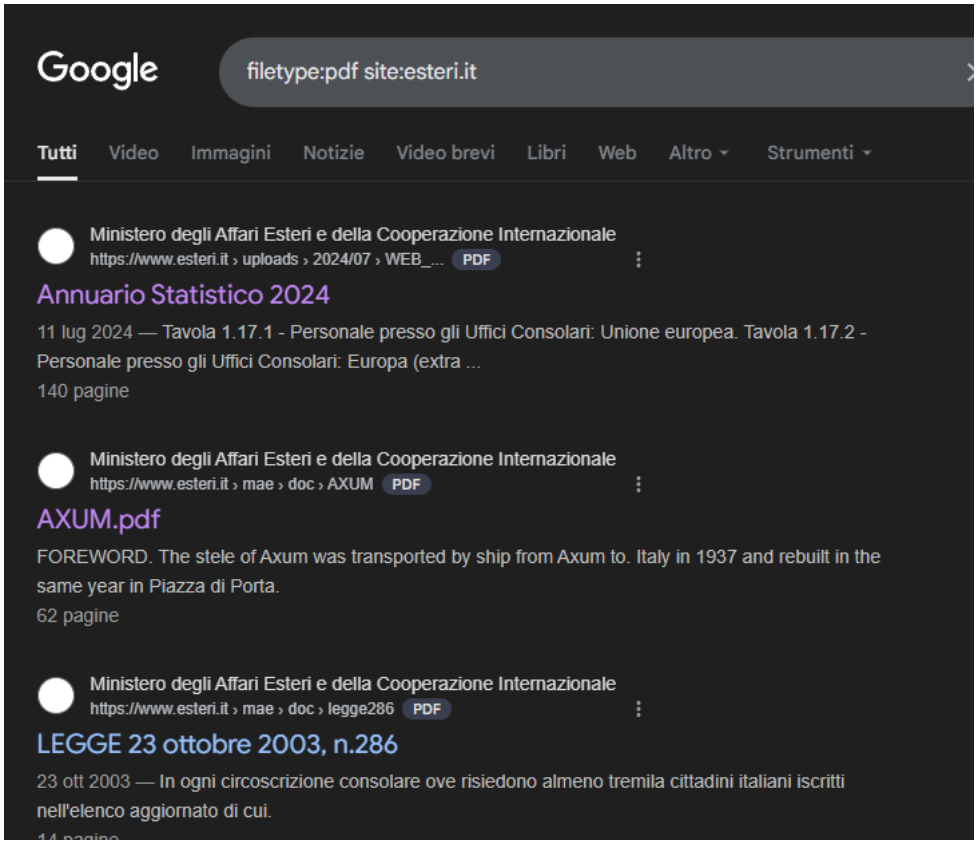


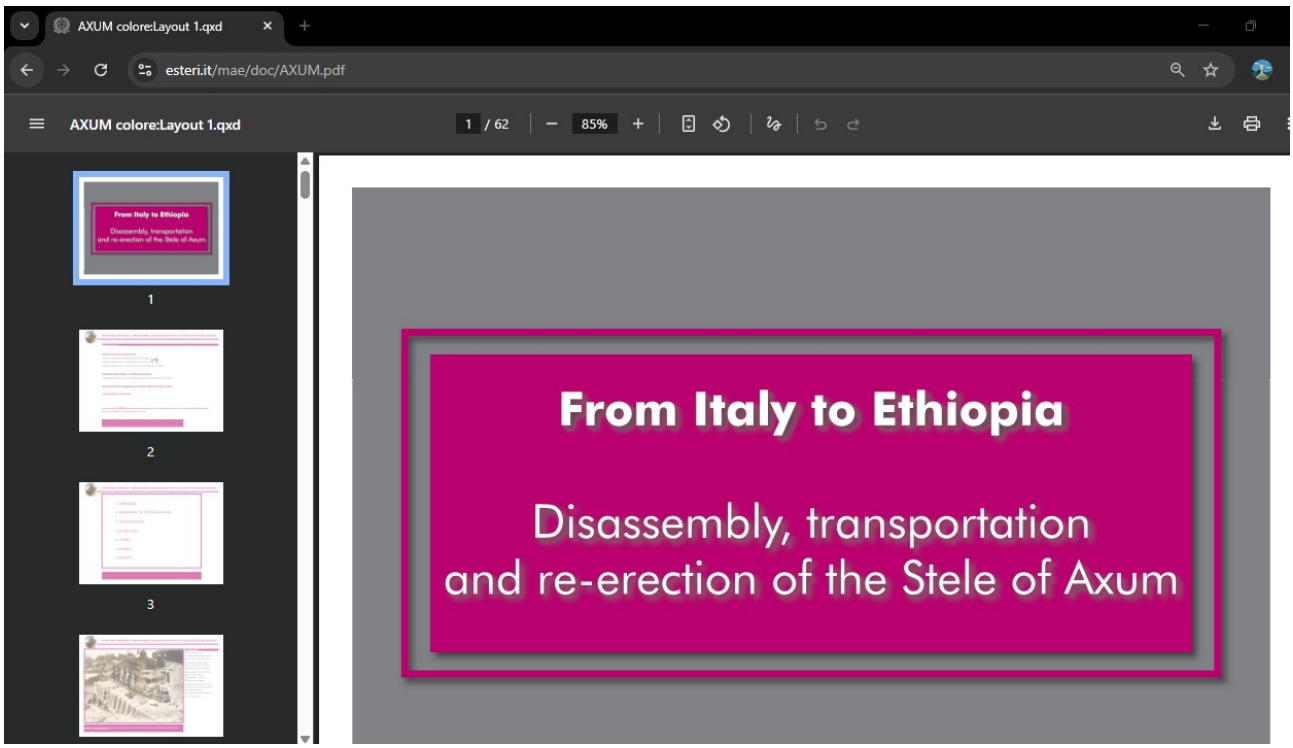
3. **INTEXT:** Lo scopo di “intext” è trovare pagine che menzionano la successiva parola nei loro contenuti. Nel nostro caso, la parola che abbiamo cercato è “privacy”, quindi ho strutturato il comando di ricerca come “intext:"privacy" site:esteri.it”.





4. **FILETYPE:** Lo scopo di “filetype” è elencare documenti PDF pubblici (che nel nostro caso vanno dai rapporti, moduli, leggi, ai bandi, ecc...). Il comando di ricerca si costruisce così: “filetipe:(pdf,doc,txt,xls,ppt…) site:esteri.it”

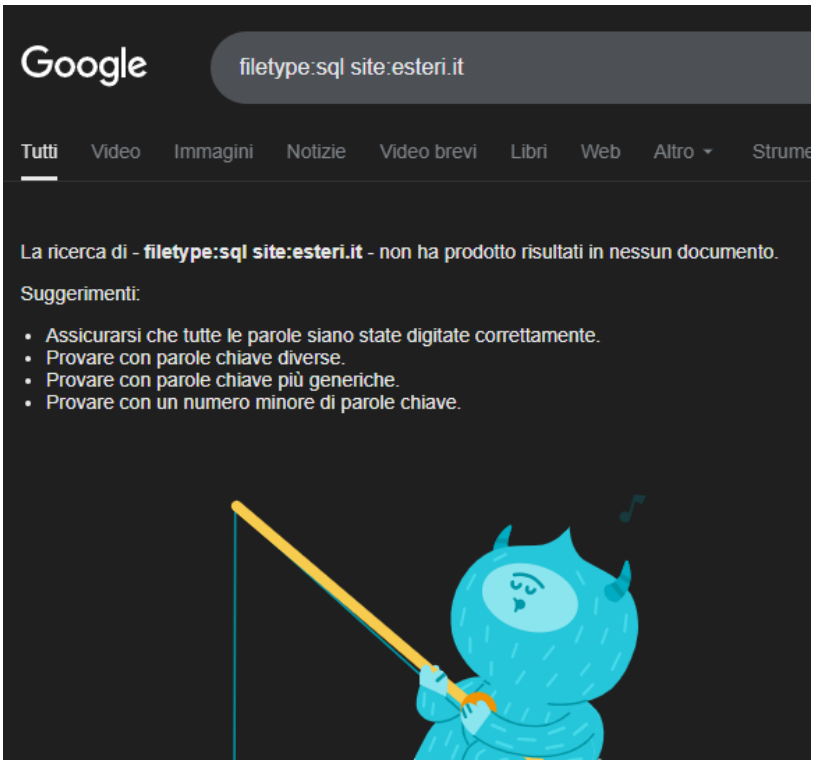




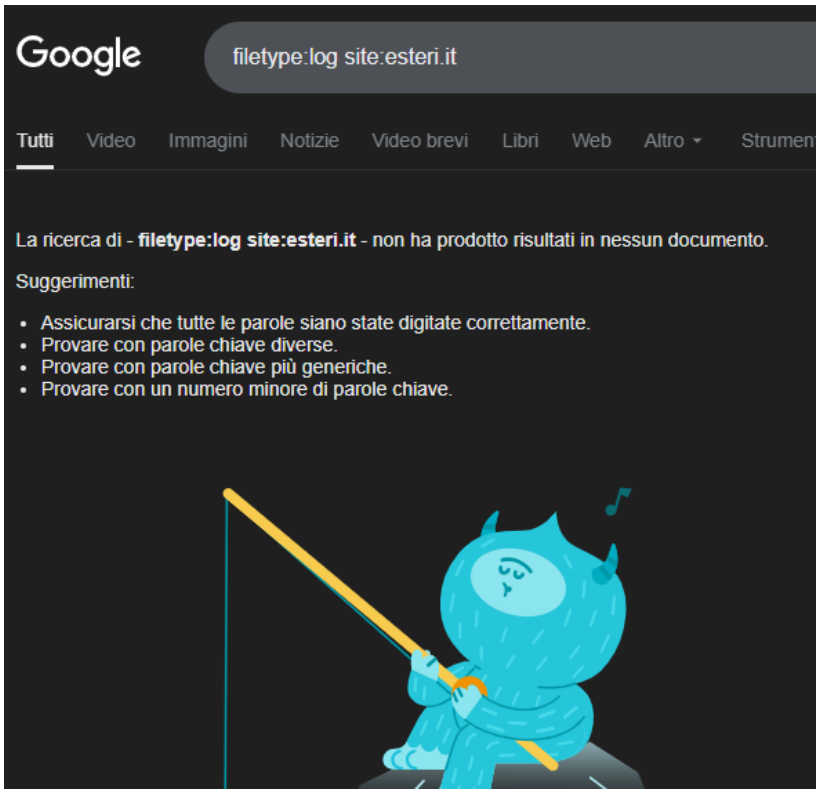
CONSIDERAZIONI FINALI IN BASE AI RISULTATI OTTENUTI:

La valutazione in overall del livello di sicurezza è alta, in quanto non ho personalmente trovato nessun elenco dati esposto e nessun'altra anomalia. Ho comunque eseguito qualche verifica reale sul dominio "esteri.it" tramite **"filetype"**, un po' per farci pratica, ma anche per scovare eventuali punti deboli.

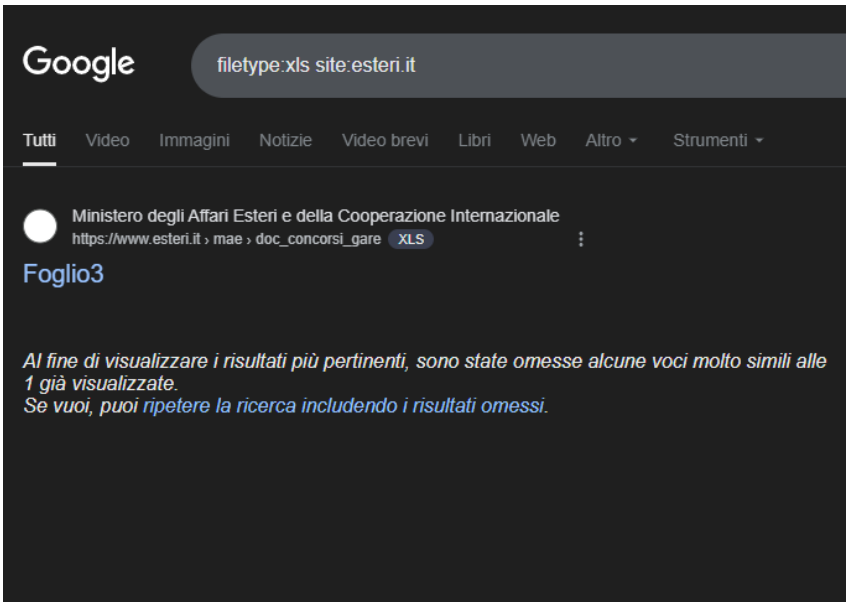
1. **FILETYPE:SQL**
Non sembra che dump DB .sql siano pubblicamente indicizzati.



2. **FILETYPE:LOG**
I file di log divulgati sono un rischio, ma qui non ne ho visti.

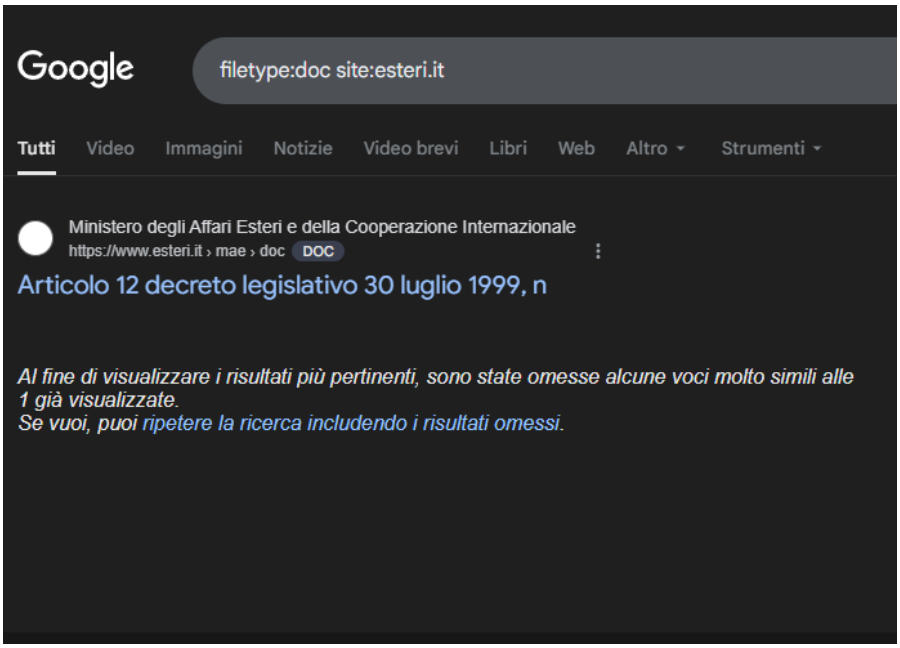


3. **FILETYPE:XLS**
Qui ho effettivamente trovato alcuni file Excel. Non necessariamente problema, ma ho comunque verificato se i file Excel contessero dati personali o interni. Qui c’è effettivamente un file Excel contentente una lista di dati personali (nomi, cognomi e date di nascita) di candidati di ammissione a un bando. Nulla di troppo sensibile o compromettente, per fortuna, anche se non né metterò uno screen per fattori etico/legali.



4. **FILETYPE:DOC / FILETYPE:DOCX**

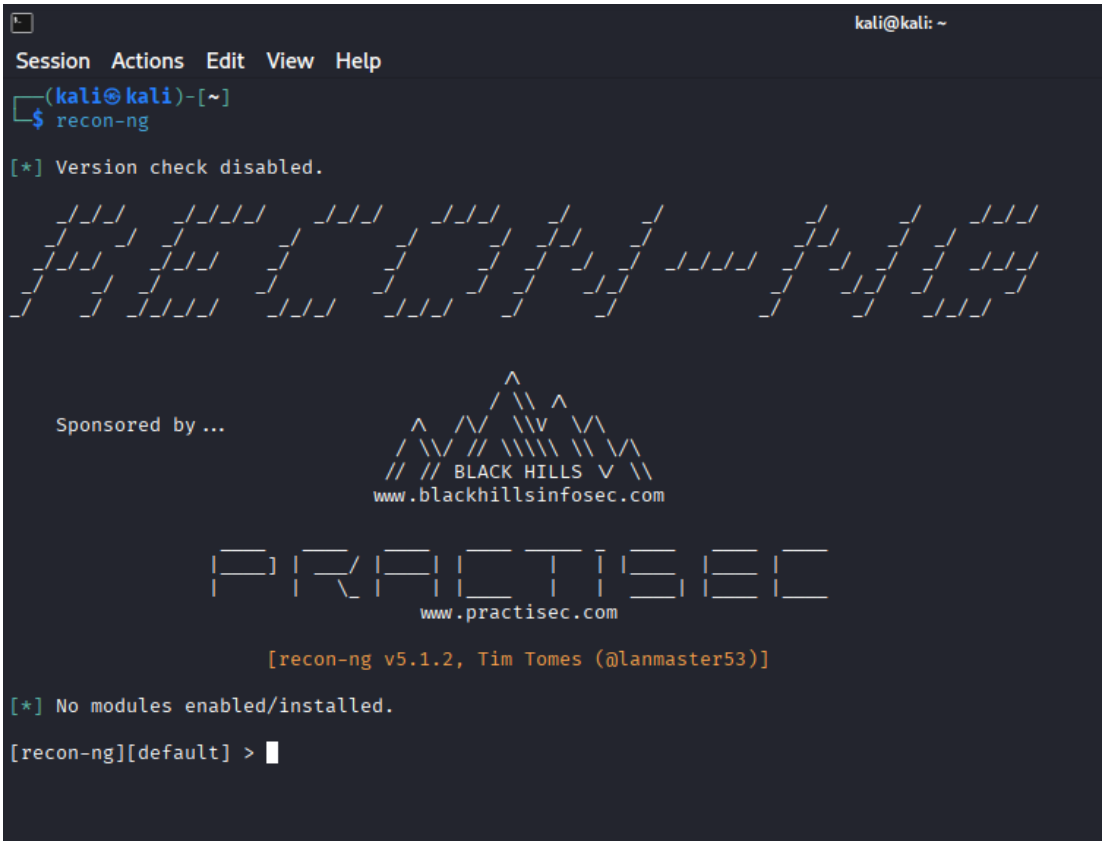
E’ normalmente accettabile se sono documenti ufficiali; è un problema se ci sono bozze, versioni interne, o dati sensibili, che fortunatamente non ho trovato.



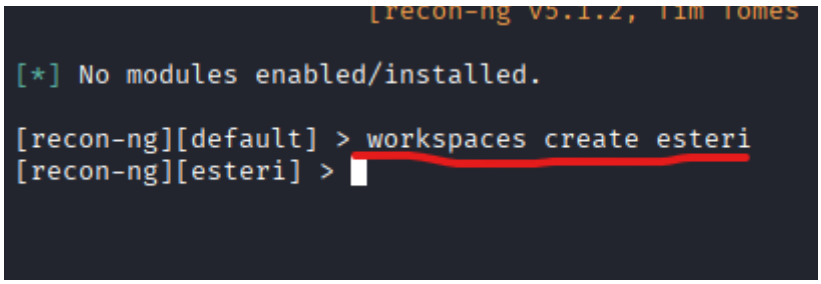
ESERCIZIO FACOLTATIVO

Questo esercizio facoltativo richiede di estendere l'Info Gathering con due tool specifici che troviamo già in Kali Linux: Recon-ng e Maltego. Qui l'ho eseguito con Recon-ng.

1. Recon-ng è un framework OSINT da terminale, organizzato in workspaces e moduli. Ho aperto il comando su Kali ed ho visionato l'apertura di una console di lavoro simile a quella di Metasploitable.



2. Ho poi creato un workspace per tenere separata l'analisi del dominio scelto (nel nostro caso "esteri.it").



3. Ho successivamente inserito il dominio nel database con il comando “insert db domains”, ed ho ovviamente inserito il dominio interessato alla relativa richiesta.

```
[recon-ng][esteri] > db insert domains
domain (TEXT): esteri.it
notes (TEXT): esercitazione
[*] 1 rows affected.
[recon-ng][esteri] >
```

4. Ho potuto verificare con “show domain”.

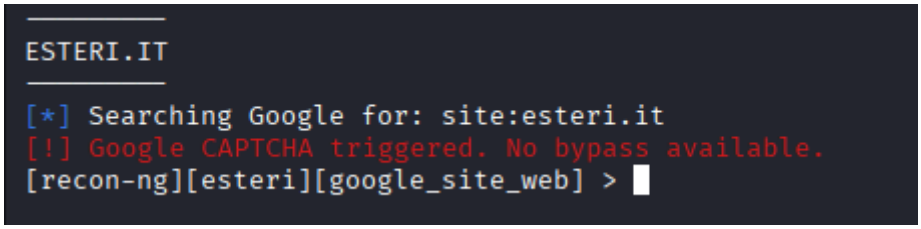
```
[recon-ng][esteri] > show domain
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng][esteri] >
```

5. Ho installato quanti più moduli utili, come suggerito dall’Hint.

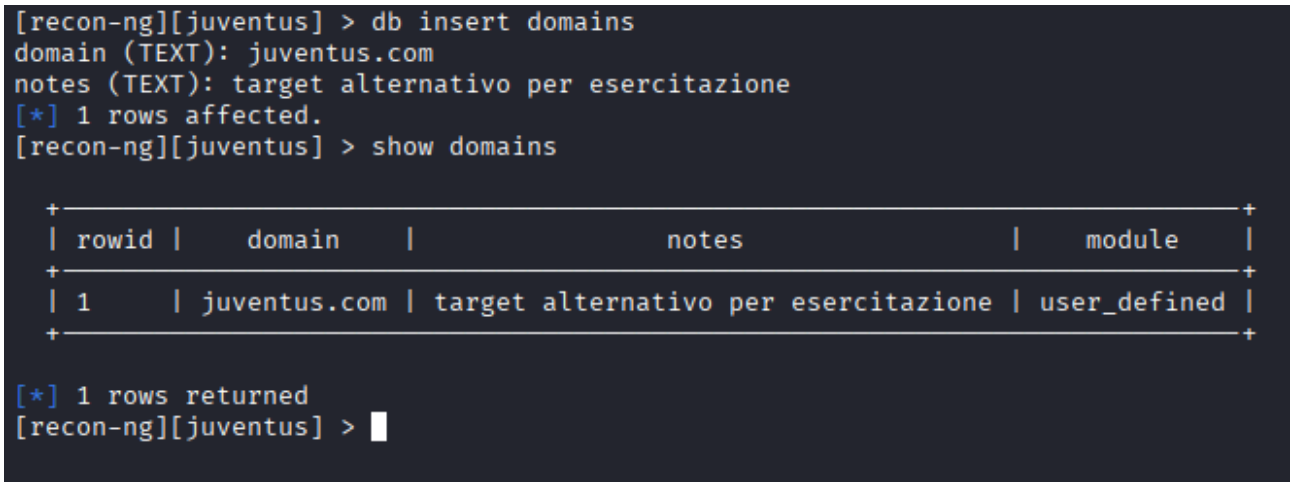
```
[recon-ng][esteri] > marketplace search google
[*] Searching module index for 'google' ...

  +-----------------------------------------------------------------------------+
  |                Path                | Version |     Status    | Updated    | D | K |
  +-----------------------------------------------------------------------------+
  | recon/domains-hosts/google_site_web | 1.0     | not installed | 2019-06-24 |   |   |
  +-----------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][esteri] > marketplace install recon/domains-hosts/google_site_web
[*] Module installed: recon/domains-hosts/google_site_web
[*] Reloading modules ...
[recon-ng][esteri] >
```

```
[recon-ng][esteri] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cach
[*] Module installed: recon/companies-contacts/censys_email_addre
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_who
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-multi/censys_org
[*] Module installed: recon/companies-multi/censys_tls_subjects
[*] Module installed: recon/companies-multi/github_miner
[*] Module installed: recon/companies-multi/shodan_org
[*] Module installed: recon/companies-multi/whois_miner
[*] Module installed: recon/contacts-contacts/abc
[*] Module installed: recon/contacts-contacts/mailtester
[*] Module installed: recon/contacts-contacts/mangle
[*] Module installed: recon/contacts-contacts/unmangle
```

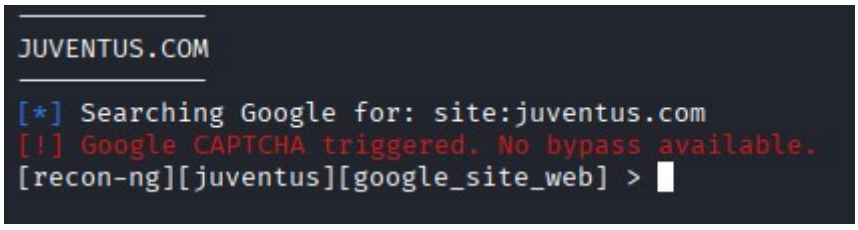
5. Purtroppo, con “esteri.it”, sembrerebbe che Google abbia rilevato un traffico “automatico” e ha bloccato la ricerca con un CAPTCHA .Recon-ng non può superarlo. Per avere dei risultati più concreti, ho quindi provato un modulo alternativo.



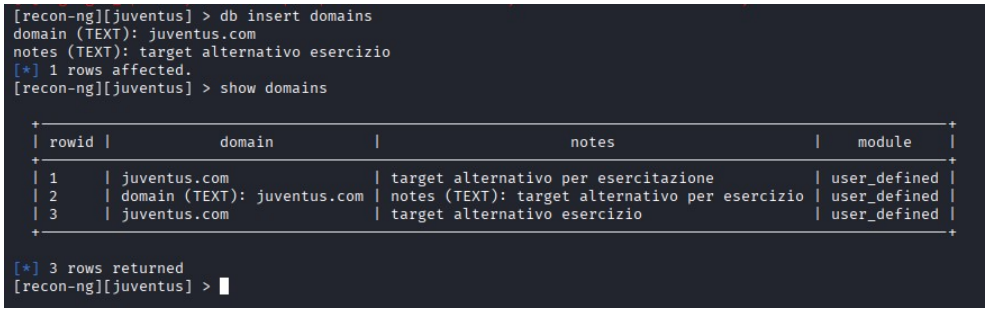
6. Ho quindi creato un nuovo workspace per il dominio “Juventus.com”.



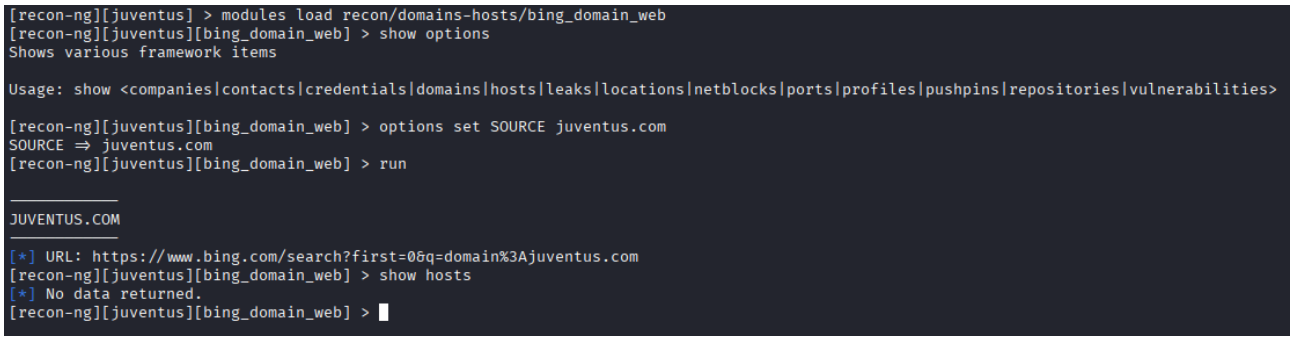
7. Ho installato i moduli principali, anche qui (domini, ,sottodomini…), utilizzando sempre Google. Dopo l’ennesimo blocco, ho provato ad utilizzare Bing, perché sembrerebbe essere meno soggetto a blocchi e Captcha, seppur avente un database più limitato.



8. Ecco la procedura ripetuta con Bing.



9. Ho installato ed eseguito i moduli.
Il primo modulo “marketplace install recon/domains-hosts/bing_domain_web”.carica e installa il modulo bing_domain_web dal marketplace di Recon-ng. Questo modulo usa Bing per cercare sottodomini del dominio target.
Il secondo modulo lo attiva, portandomi dentro al suo “ambiente” di lavoro, dove ho potuto configurare le opzioni.
“Show option” per visualizzare i parametri.
E l’ultimo inserisce come valore del parametro SOURCE il dominio juventus.com, cioè il sito che stiamo analizzando.



10. Tramite il modulo WHOIS ho potuto interrogare i registri WHOIS nel dominio, in modo da ottenere i dati del registrante e contatti pubblici associati al dominio (email tecniche, contatti amministrativi). E’ utile per capire chi gestisce il dominio e raccogli eventuali email o referenti. I comandi sono stati pressappoco i medesimi.

11. Ed infine, tramite il modulo SSL, ho potuto analizzare i certificati SSL/TLS del dominio. A volte emergono sottodomini non facilmente visibili con i motori di ricerca, ma comunque validi e attivi.

12. TABELLA FINALE

Nome Modulo	**Versione**	**Scopo**	**Note**
bing_domain_web	1.0	Ricerca di sottodomini del dominio target usando Bing.	Eseguito su juventus.com, nessun host trovato (No data returned).
whois_pocs	1.0	Recupero contatti WHOIS del dominio target.	Tentata ricerca su juventus.com, errore di parsing API, nessun contatto estratto.
ssl_san	1.0	Estrazione host alternativi dai certificati SSL.	Avviato su juventus.com, nessun dato restituito.