Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Information Gathering
Parte 3

Arcangelo Castiglione
arcastiglione@unisa.it

Utilizzo di Crawler

Surface Mapping ed Asset Discovery – Maltego

- Sviluppato originariamente dall'azienda Sudafricana Paterva
  - Successivamente è diventata Maltego Technologies GmbH, un'azienda con sede a Monaco (Germania)

- Permette di estrarre, raccogliere e rappresentare informazioni in modo significativo
  - Si basa fortemente sul concetto di *Open Source Intelligence (OSINT)*

- Consente di
  - Identificare le relazioni chiave tra le informazioni raccolte
  - Visualizzare graficamente le relazioni tra i dati
    - Così che sia più facile individuare aspetti comuni tra le informazioni

MALTEGO

Utilizzo di Crawler

Maltego – Caratteristiche Principali

- Strumento interattivo per il Data Mining
  - Utilizzato nelle investigazioni online per trovare relazioni tra informazioni provenienti da varie fonti di dati sulla rete Internet

- Si basa sul concetto di **Trasformata** (*transform*)

- **Trasformata:** serie di operazioni che permettono di
  - Automatizzare il processo di ricerca e raccolta informazioni su diverse fonti di dati
  - Mostrare i risultati della raccolta in maniera grafica
    - Così da evidenziare le relazioni semantiche tra i dati

MALTEGO

Utilizzo di Crawler

Maltego – Caratteristiche Principali

- Consente di raccogliere molte informazioni su un determinato asset
  - DNS
  - Whois
  - Blocchi di Rete
  - Indirizzi IP
  - Sottodomini
  - Etc

MALTEGO

Utilizzo di Crawler

Maltego – Caratteristiche Principali

- Consente anche di raccogliere informazioni sulla «componente umana» appartenente ad un determinato asset
  - Aziende, enti ed organizzazioni
  - Indirizzi fisici
  - Indirizzi e-mail
  - Siti Web
  - Social Network
  - Numeri di telefono
  - Etc

MALTEGO

Utilizzo di Crawler

Maltego – Caratteristiche Principali

- Consente anche di raccogliere informazioni sulla «componente umana» appartenente ad un determinato asset
  - Aziende, enti ed organizzazioni
  - Indirizzi fisici
  - Indirizzi e-mail
  - Siti Web
  - Social Network
  - Numeri di telefono
  - Etc

E molto altro ancora…

MALTEGO

Utilizzo di Crawler

Maltego – Caratteristiche Principali

- Esistono tre versioni di Maltego
  - **Maltego Community Edition (CE)** [Che utilizzeremo per il corso]
    - Costo: gratis
  - Professional
    - Costo: a partire da 6000 euro all'anno
  - Organization
    - Costo: i dettagli sui costi per questo piano non sono disponibili pubblicamente e possono variare in base alle dimensioni dell'organizzazione, ai requisiti e alle funzionalità desiderate
- Tutte le versioni di Maltego hanno accesso ad una libreria di trasformate standard
  - Per la raccolta di informazioni da una vasta gamma di fonti pubbliche, comunemente utilizzate durante le indagini online e nella Digital Forensics

MALTEGO

Utilizzo di Crawler

Maltego – Community Edition

- Utilizzeremo la «Community Edition» di Maltego

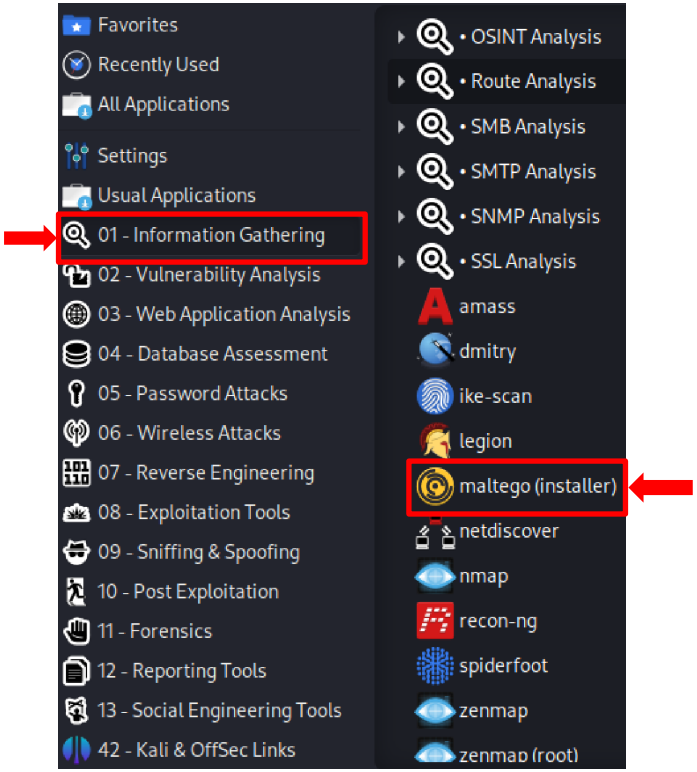
- Fornisce un sottoinsieme limitato delle funzionalità di Maltego
  - Supporta al massimo 200 interrogazioni (*Credits*)
  - Numero ridotto di trasformate rispetto a tutte quelle disponibili
  - Non può essere usata per fini commerciali
  - È eseguita su Server condivisi tra tutti gli utenti della «Community»
    - Talvolta, potrebbe essere non molto efficiente
  - Fornisce supporto limitato all'utente

MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

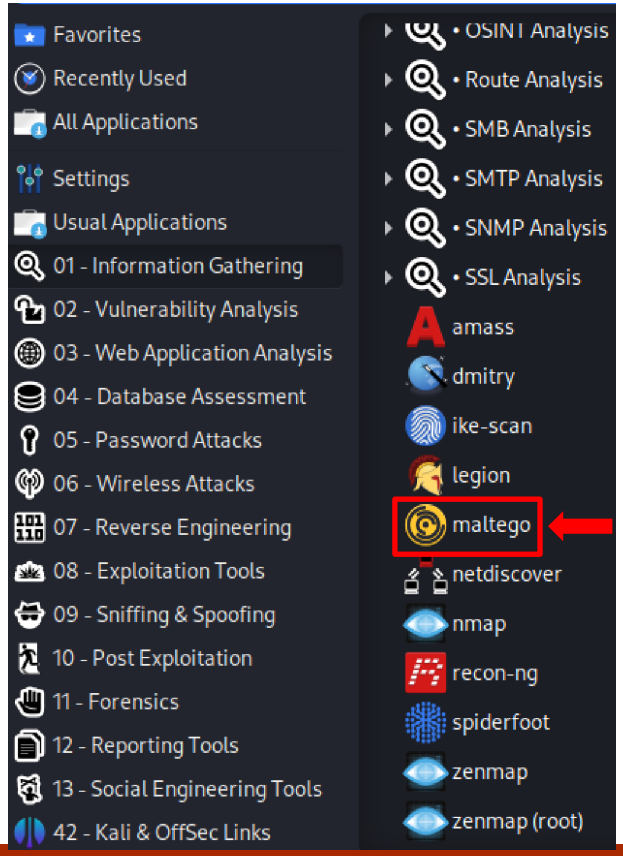
- Maltego va installato in Kali Linux, dove è presente già un installer
  - Selezionare **`maltego (installer)`** dal menu «**`01 – Information Gathering`**»



Utilizzo di Crawler

Maltego – Primo Avvio

- Dopo l'installazione, può essere avviato tramite lo stesso menù

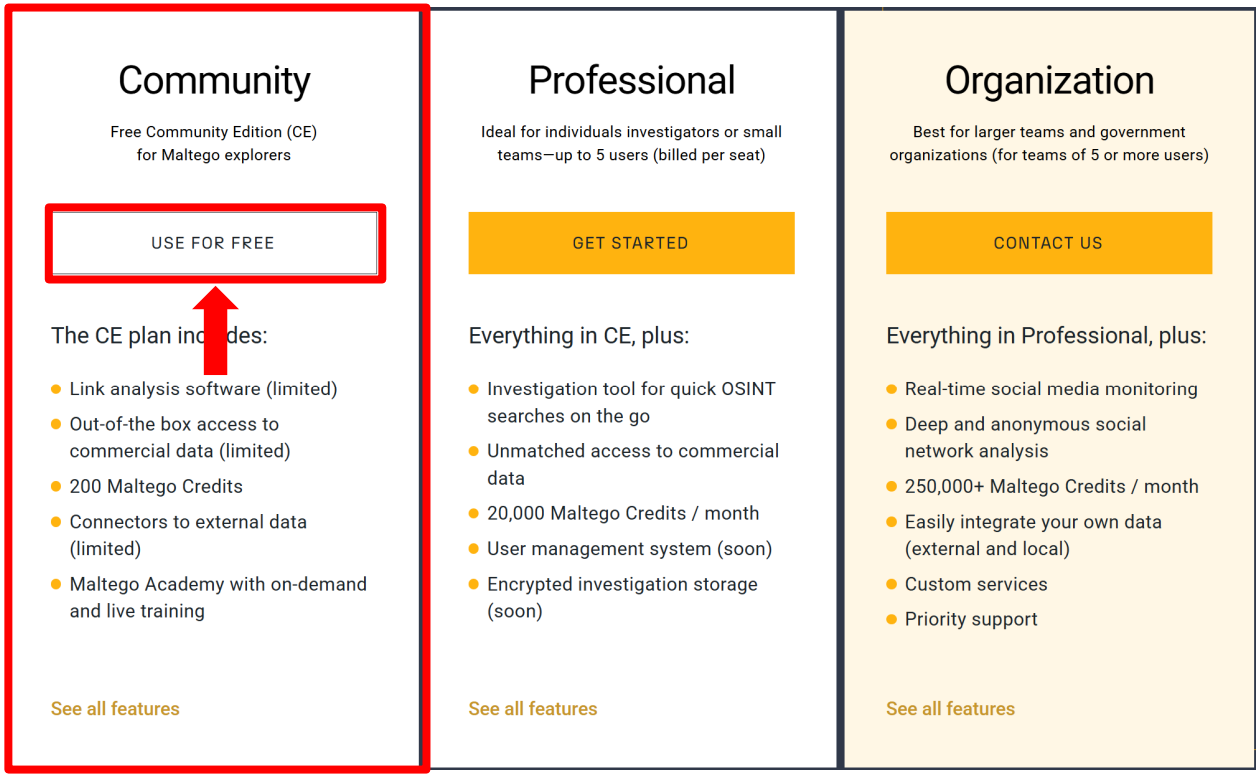


MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

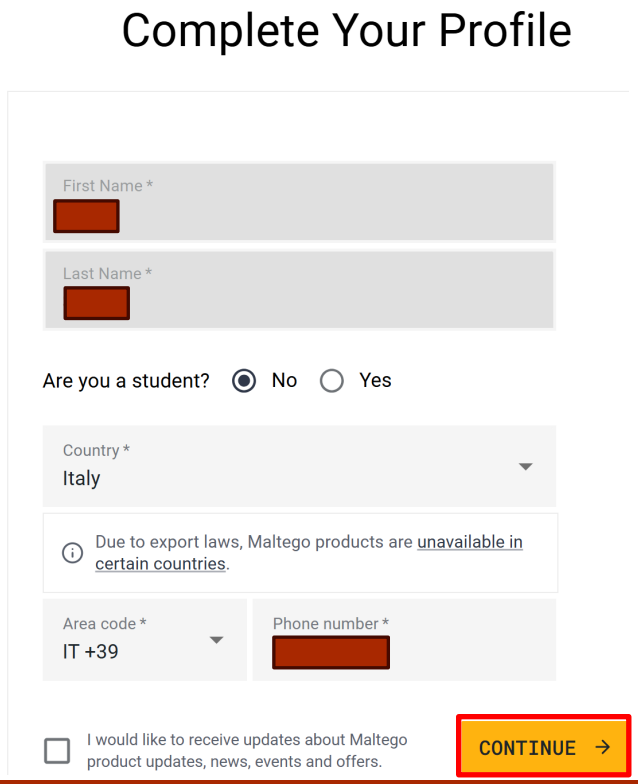
- Successivamente, è necessario effettuare la registrazione del prodotto
  - https://www.maltego.com/pricing/



Utilizzo di Crawler

Maltego – Primo Avvio

- Successivamente, è necessario effettuare la registrazione del prodotto
  - https://www.maltego.com/pricing/

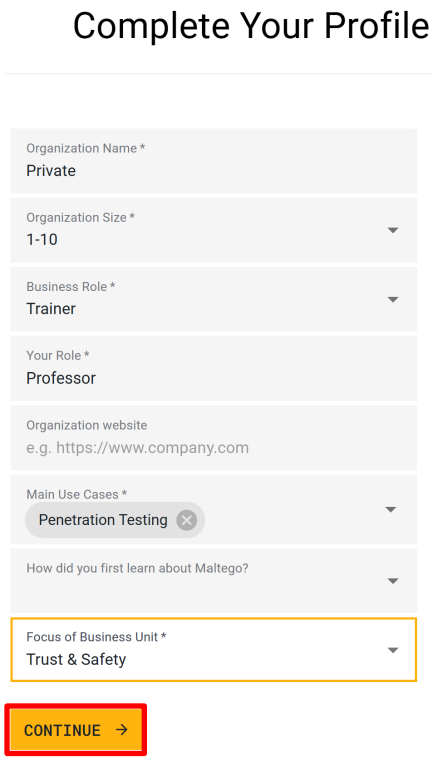


MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

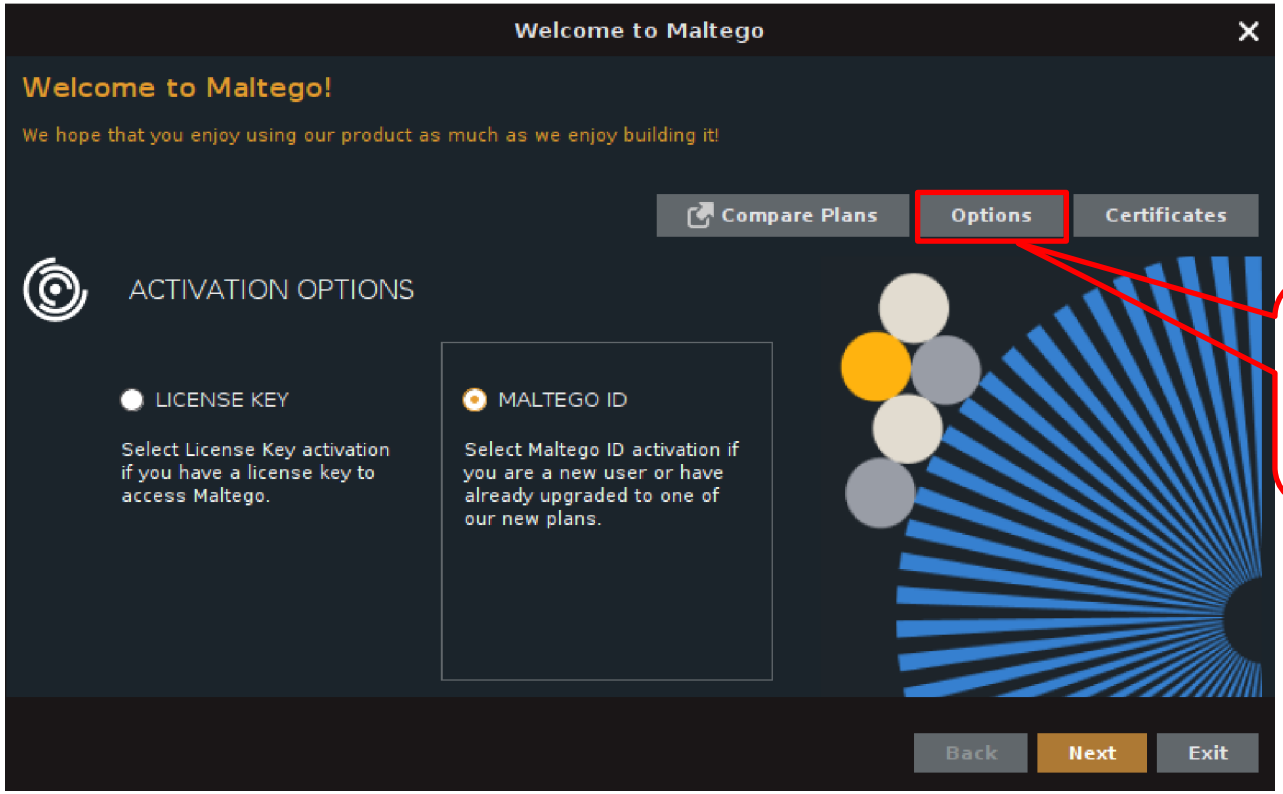
- Successivamente, è necessario effettuare la registrazione del prodotto
  - https://www.maltego.com/pricing/



Utilizzo di Crawler

Maltego – Primo Avvio

- Una volta terminata la registrazione del prodotto, è possibile tornare alla schermata di Maltego, così da poterlo attivare



Assicurarsi che non sia impostato un proxy

MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

- Una volta terminata la registrazione del prodotto, è possibile tornare alla schermata di Maltego, così da poterlo attivare

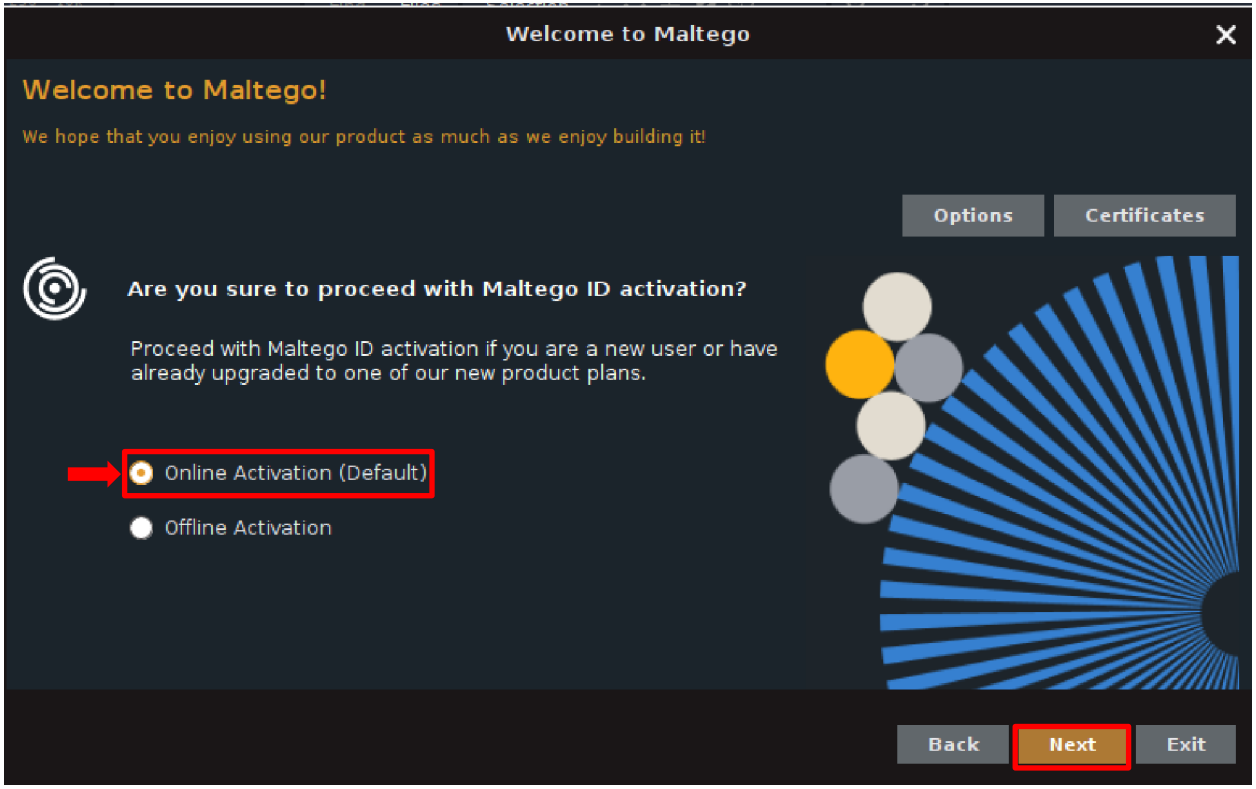
Assicurarsi che non sia impostato un proxy

MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione

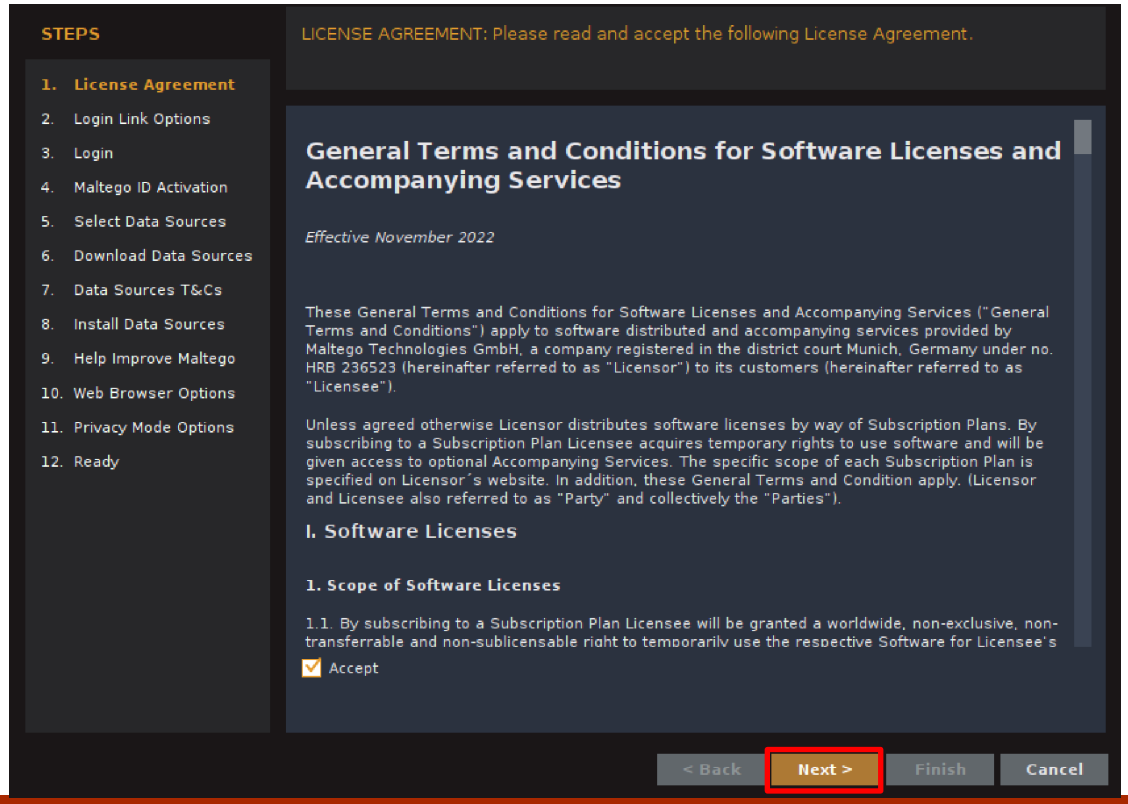


MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

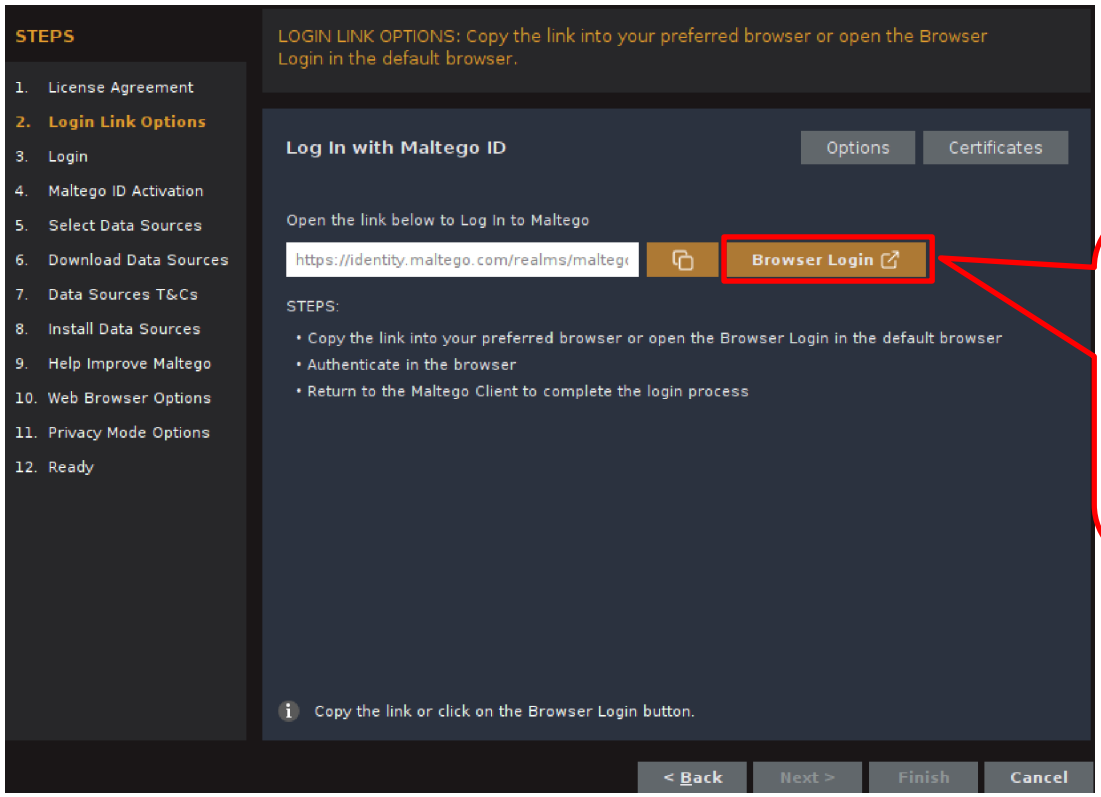
- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione



Utilizzo di Crawler

Maltego – Primo Avvio

- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione



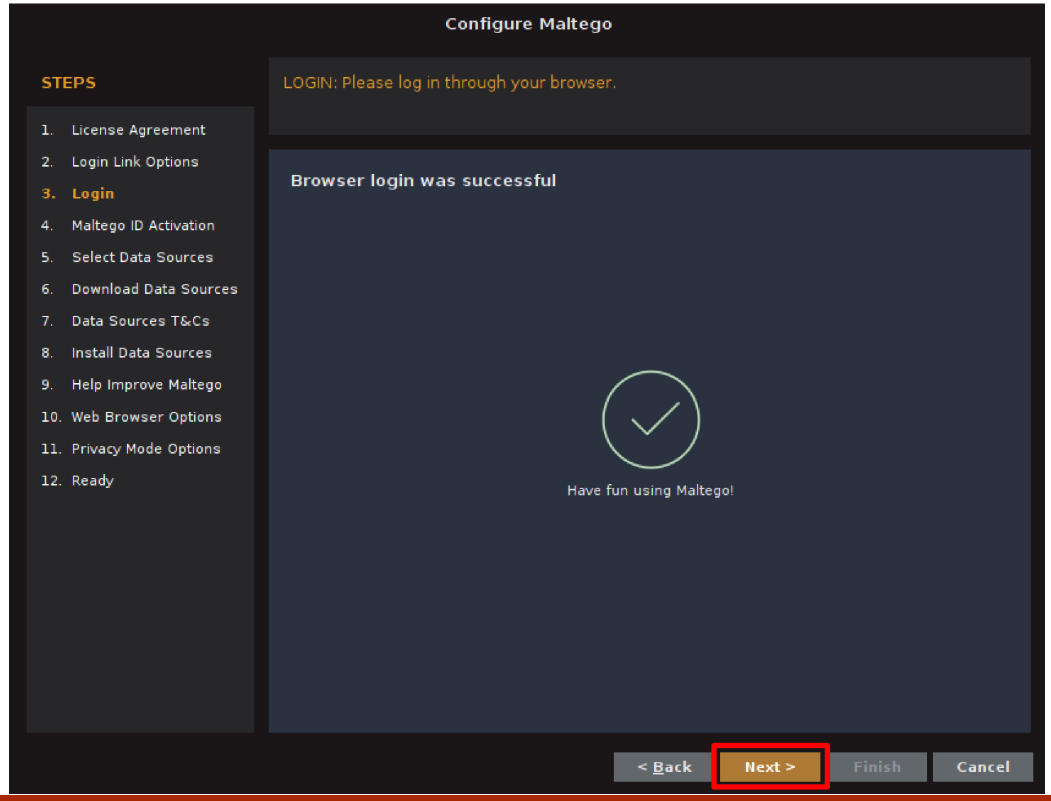
Effettuare il login tramite browser, utilizzando le credenziali inserite durante la registrazione

MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione

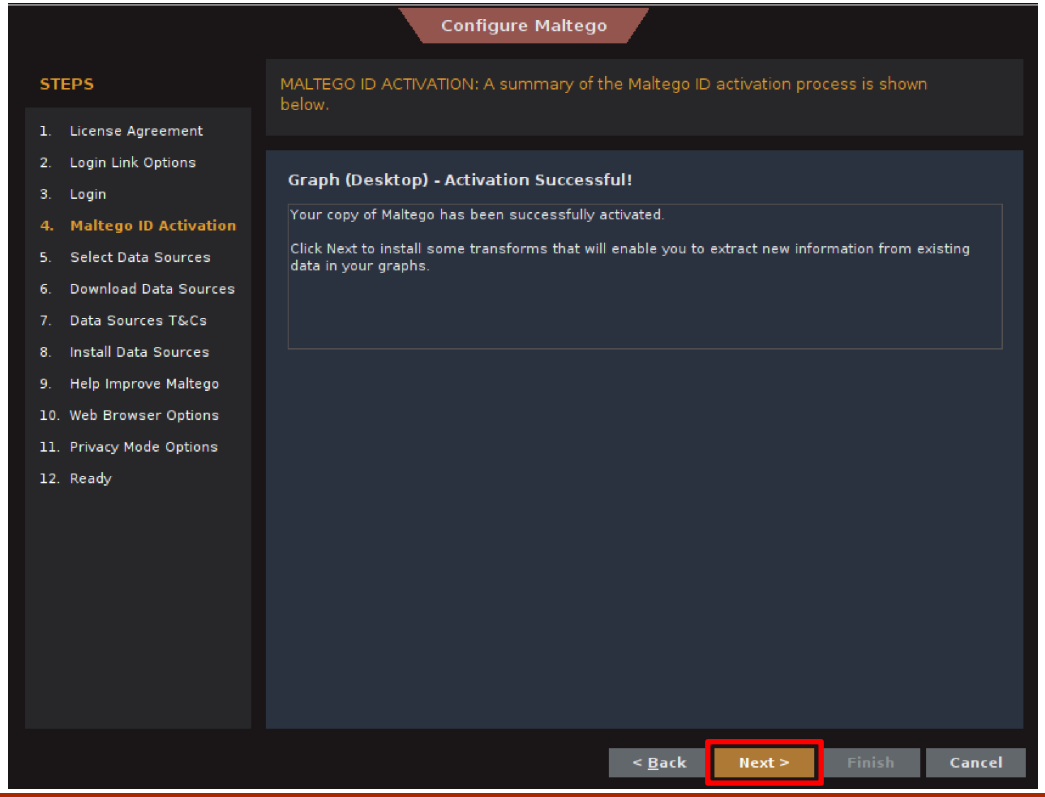


MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

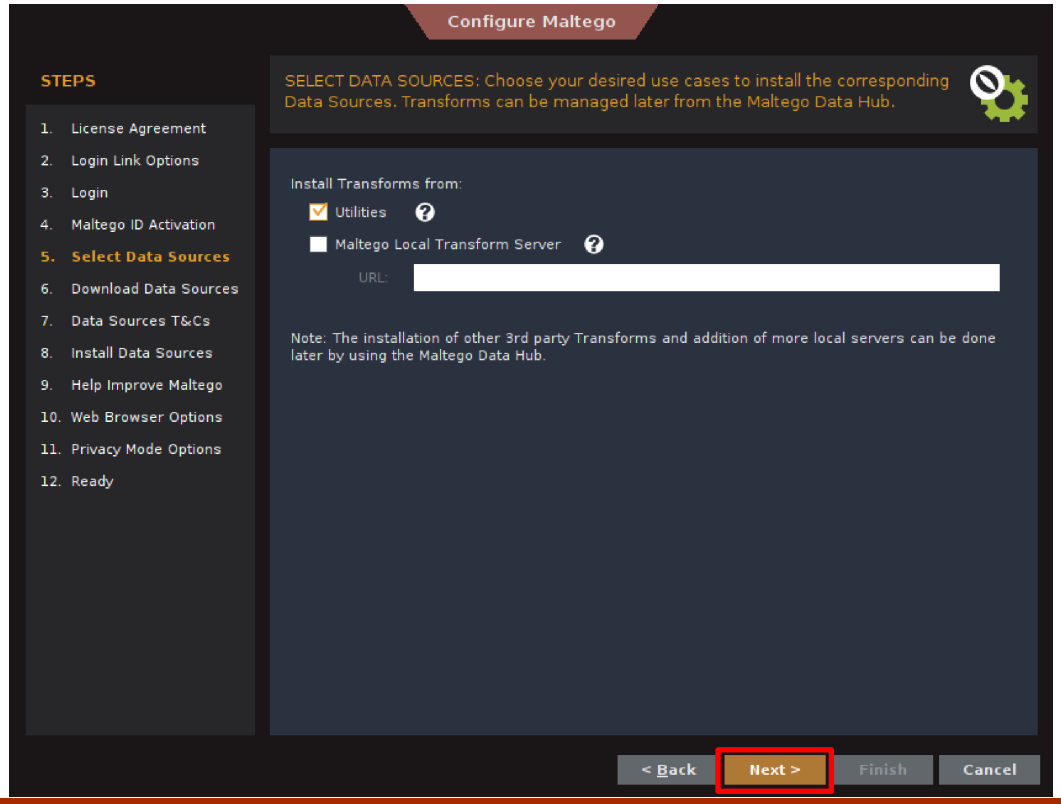
- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione



Utilizzo di Crawler

Maltego – Primo Avvio

- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione

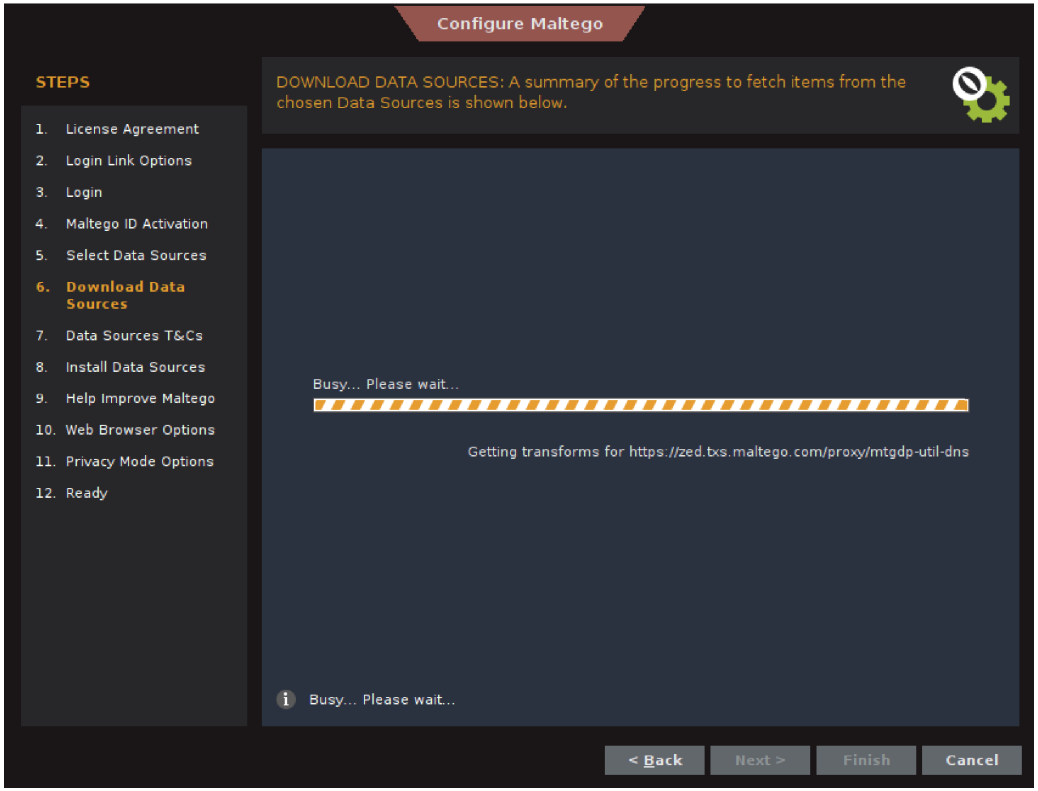


MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

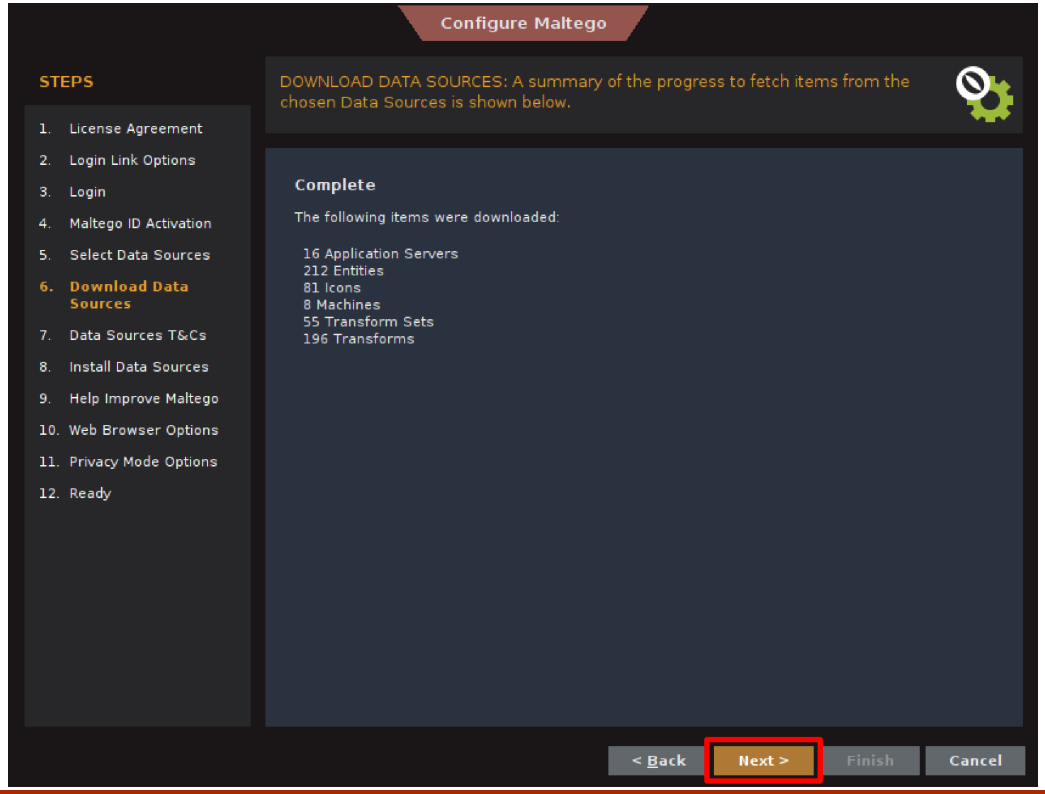
- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione



Utilizzo di Crawler

Maltego – Primo Avvio

- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione

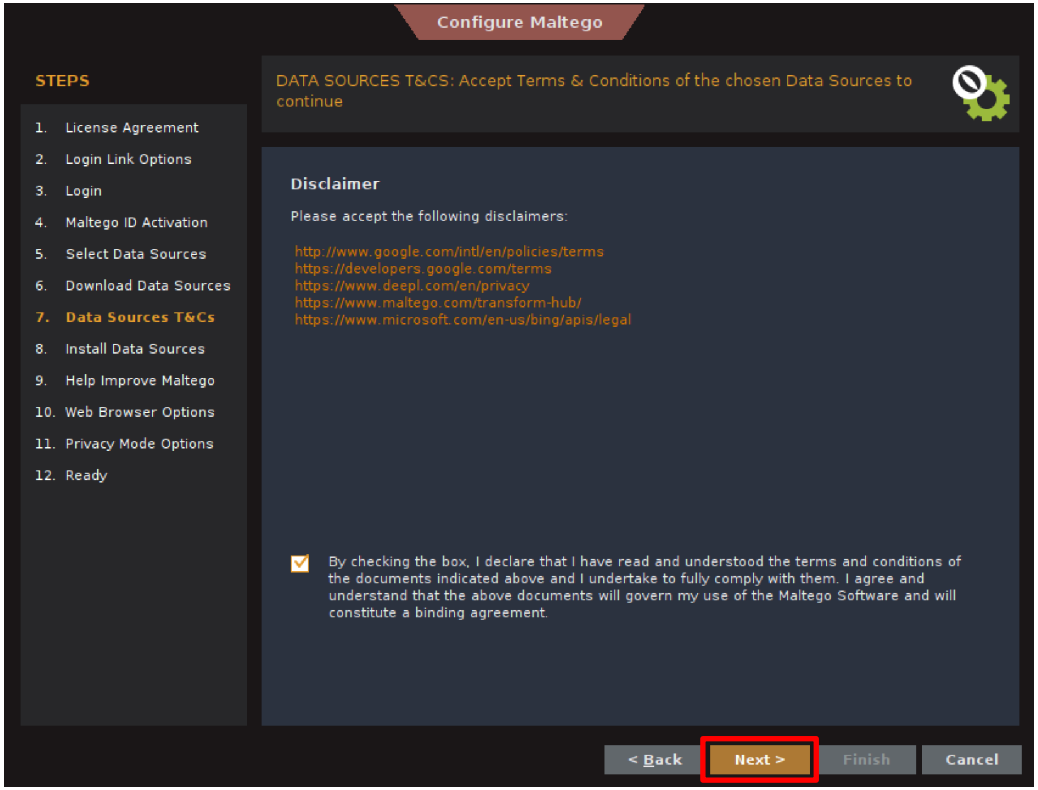


MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione

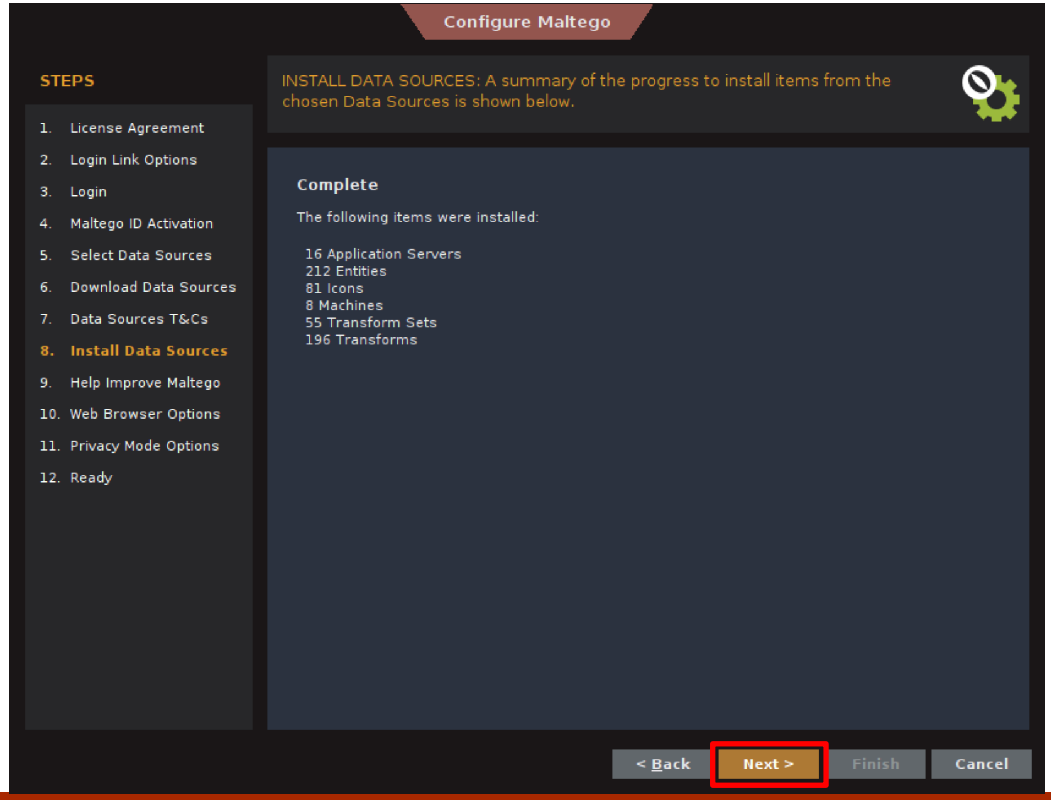


MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

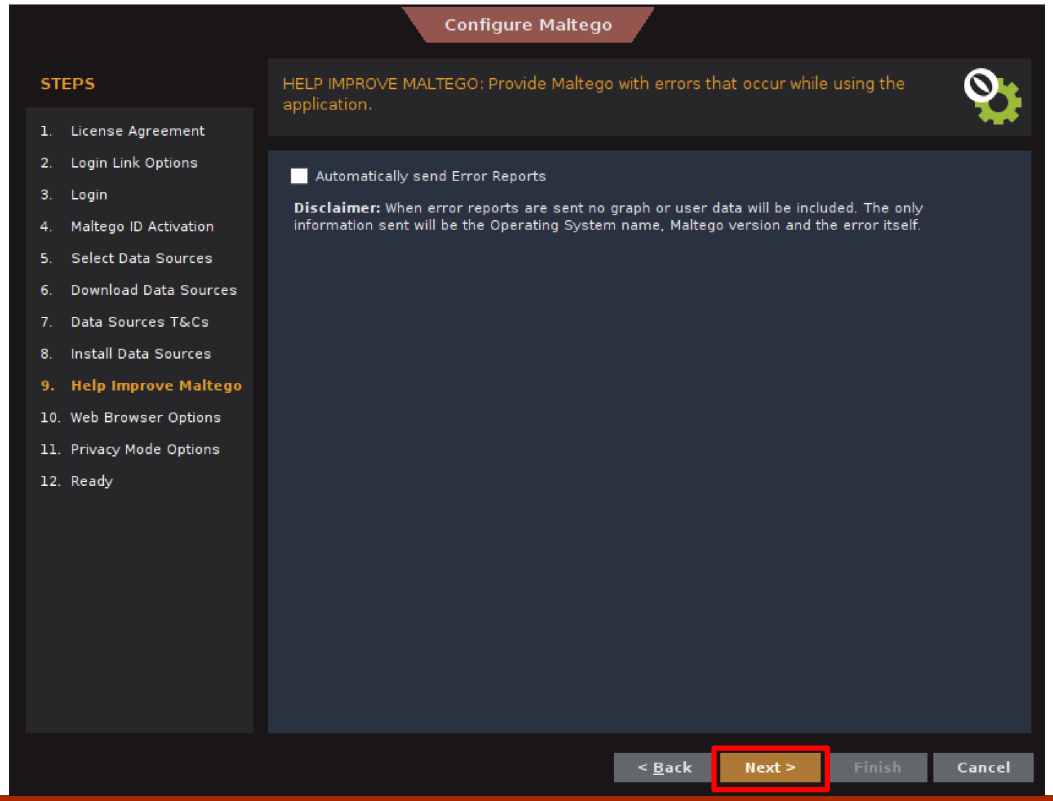
- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione



Utilizzo di Crawler

Maltego – Primo Avvio

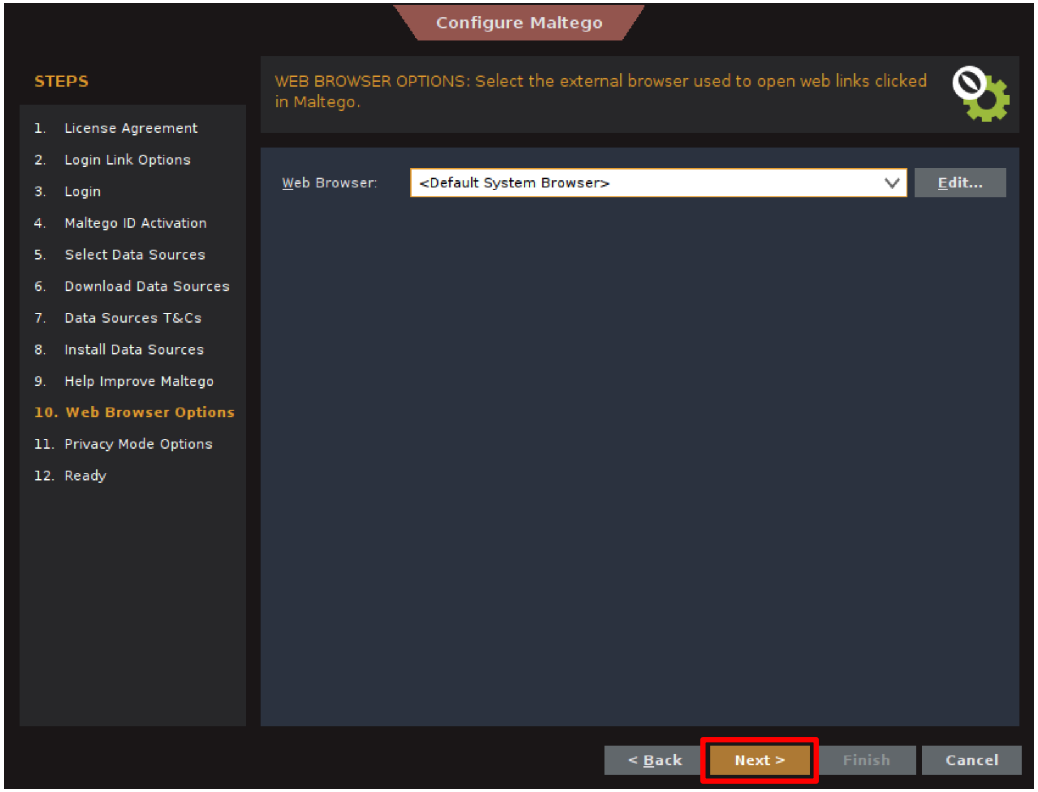
- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione



Utilizzo di Crawler

Maltego – Primo Avvio

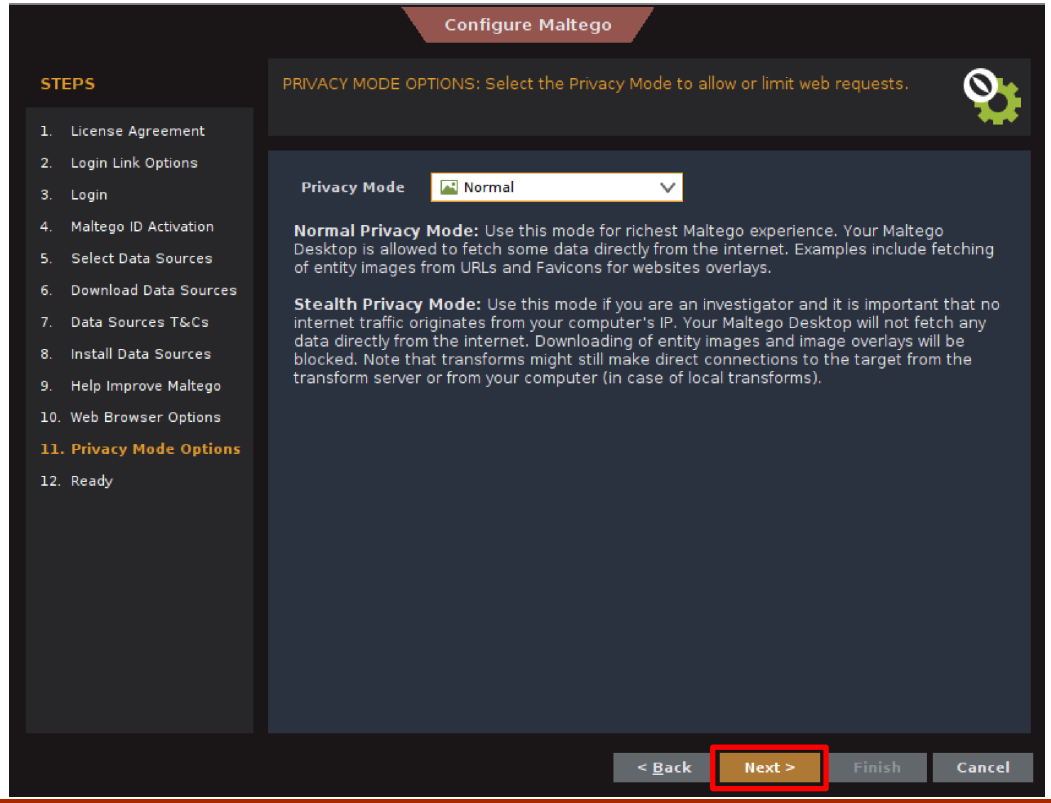
- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione



Utilizzo di Crawler

Maltego – Primo Avvio

- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione

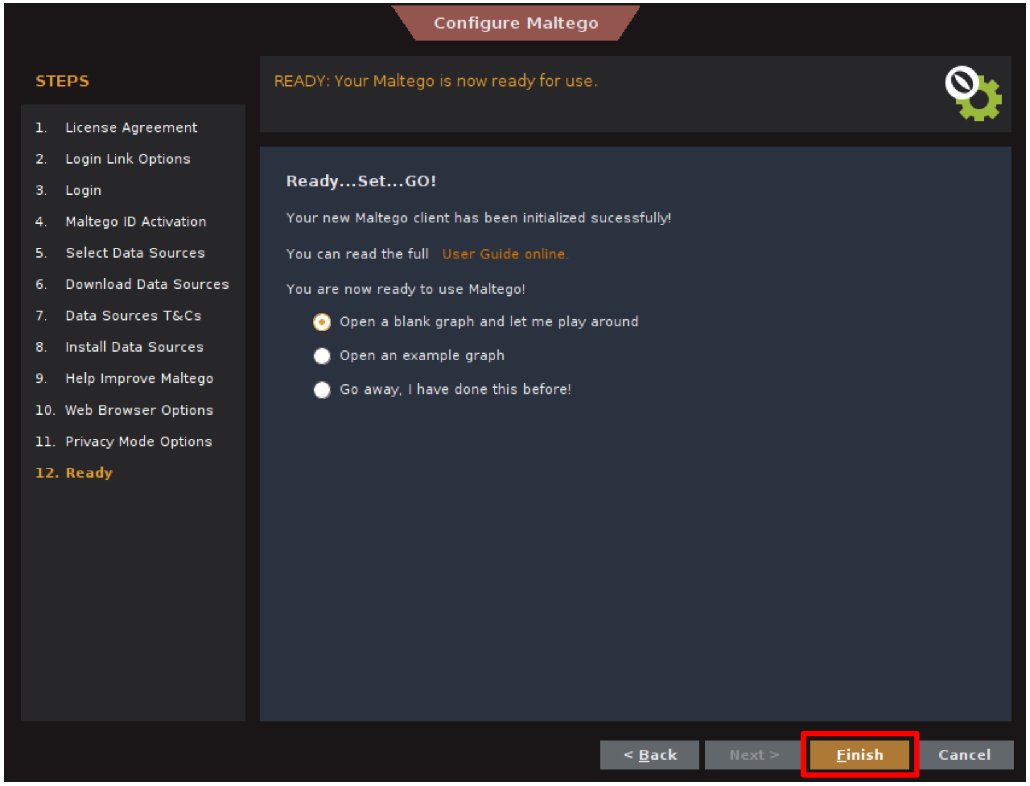


MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione

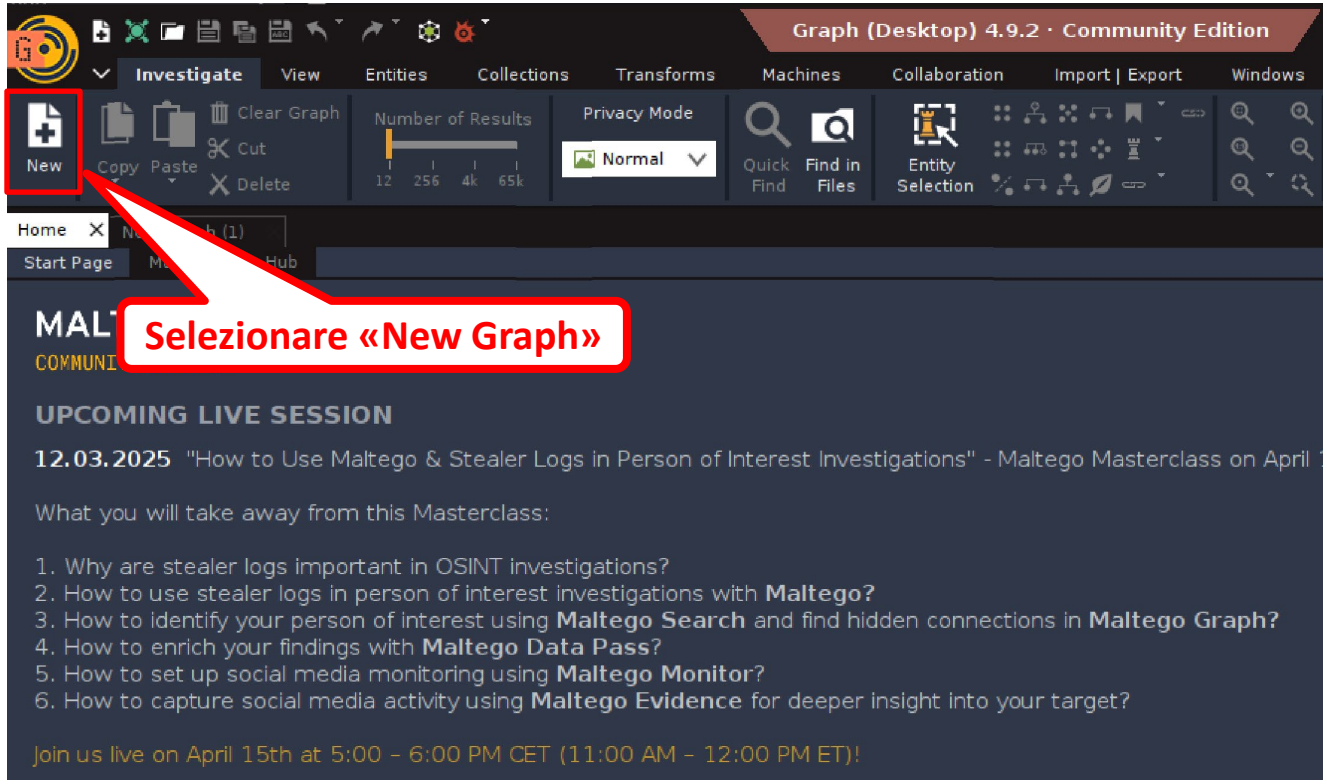


MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

- Una volta terminata la registrazione del prodotto, è possibile tornare alla schermata di Maltego per poterlo utilizzare

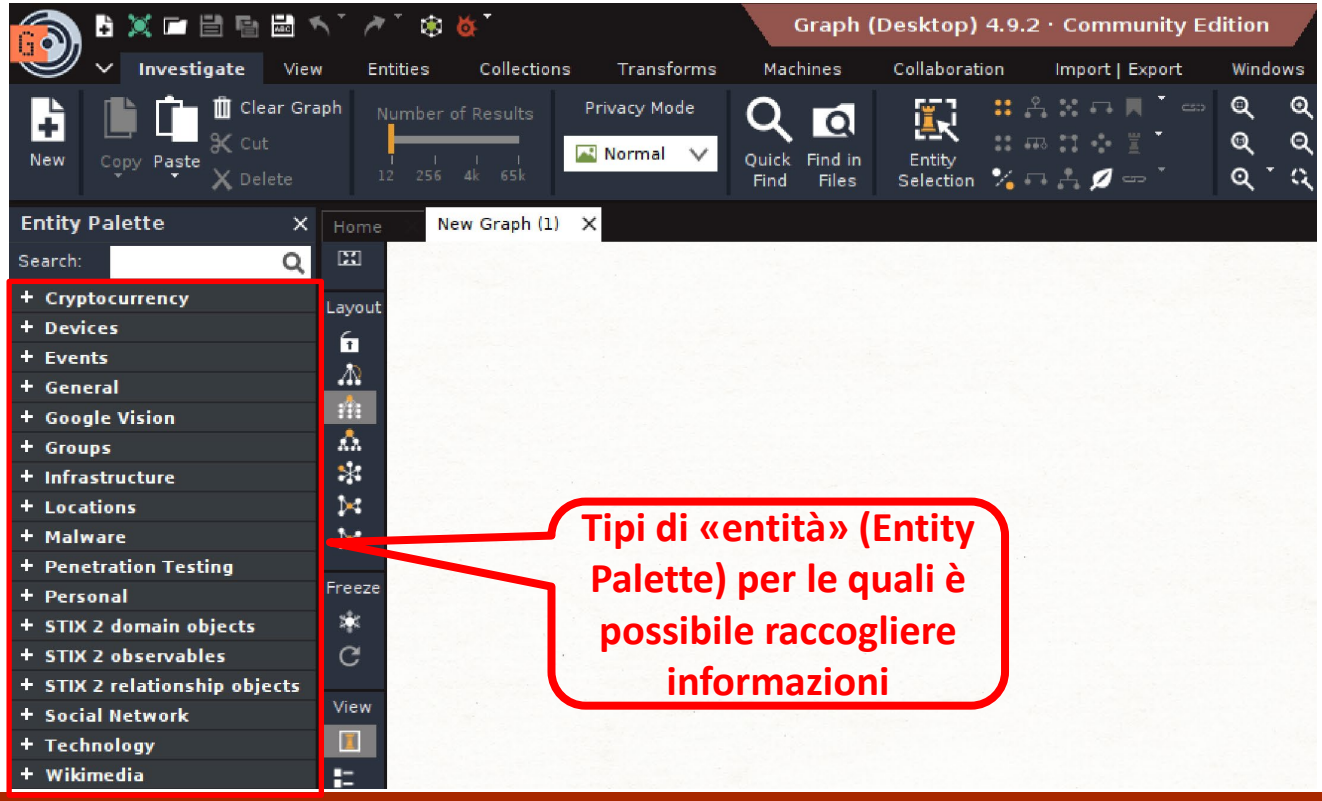


MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

- Una volta terminata la registrazione del prodotto, è possibile tornare alla schermata di Maltego per poterlo utilizzare



MALTEGO

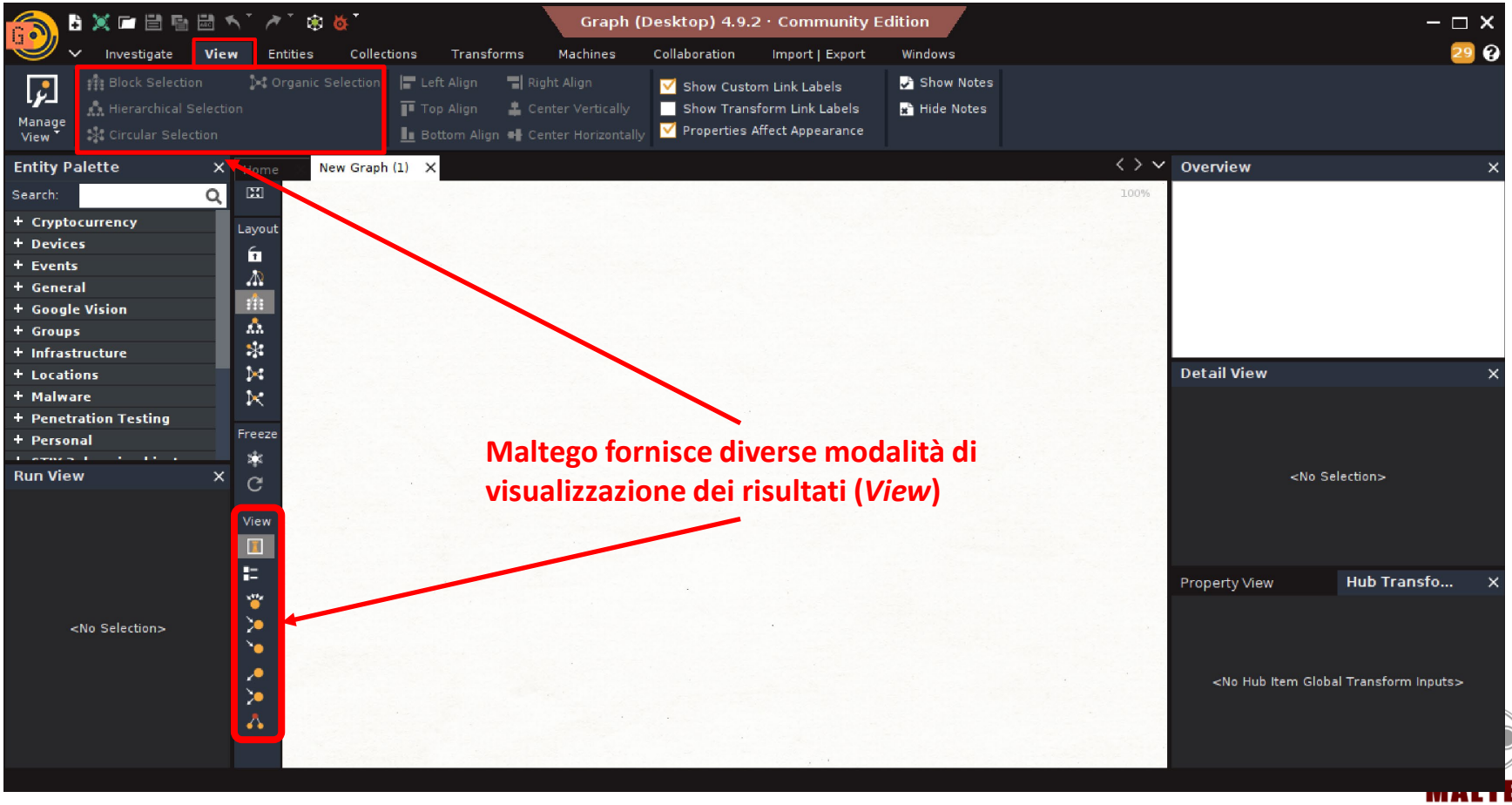
Utilizzo di Crawler

Maltego – Entity Palette

- Le entità (*Entity Palette*) sono suddivise in 17 gruppi
  - **Cryptocurrency**
  - **Devices**
  - **Events**
  - **Groups**
  - **General**
  - **Google Vision**
  - **Infrastructure**
  - **Locations**
  - **Malware**
  - **Penetration Testing**
  - **Personal**
  - **Social Network**
  - **Technology**
  - **Wikimedia**
  - **STIX 2 domain objects**
  - **STIX 2 observables**
  - **STIX 2 relationship objects**

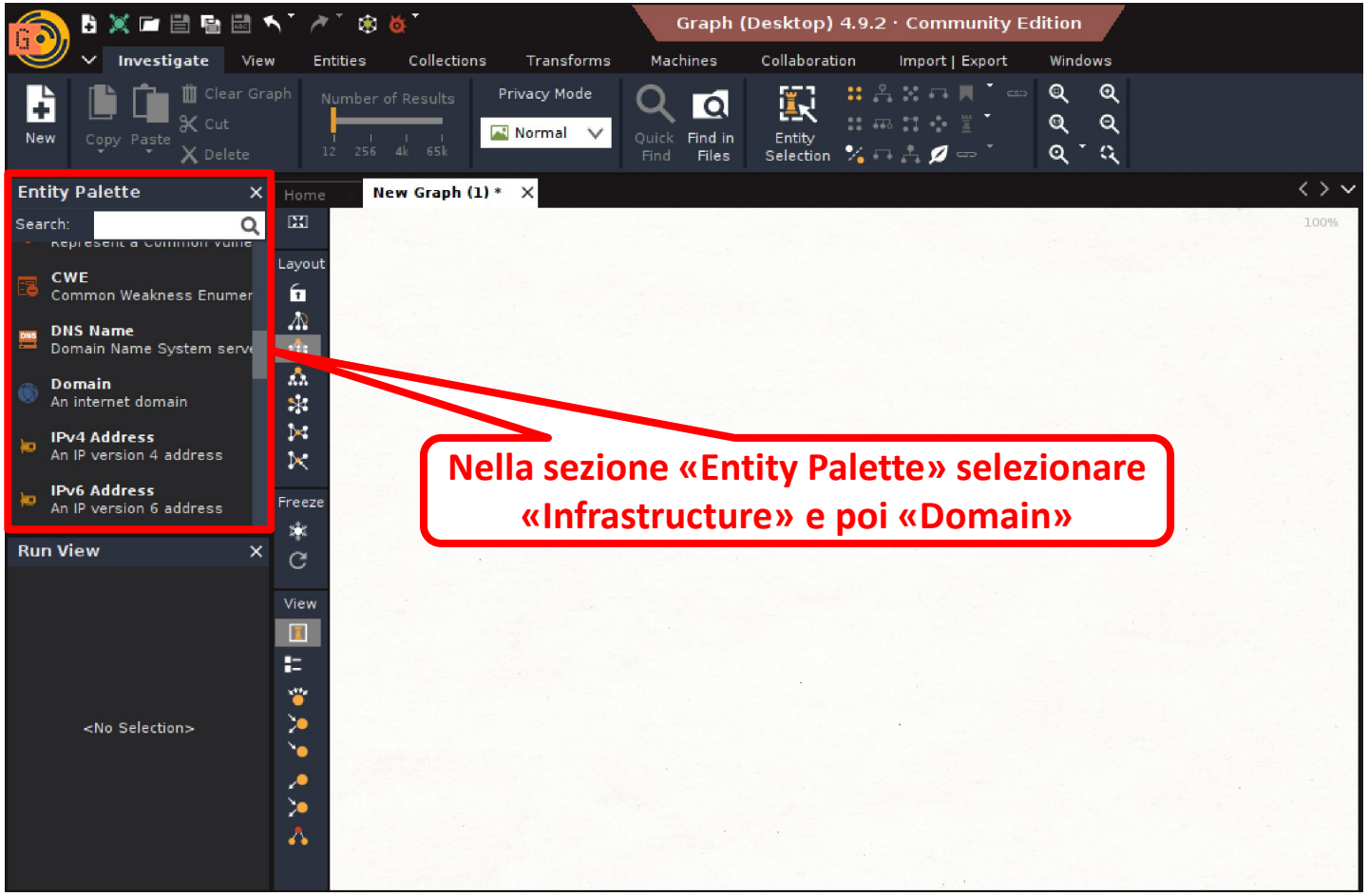
Utilizzo di Crawler

Maltego – View



Utilizzo di Crawler

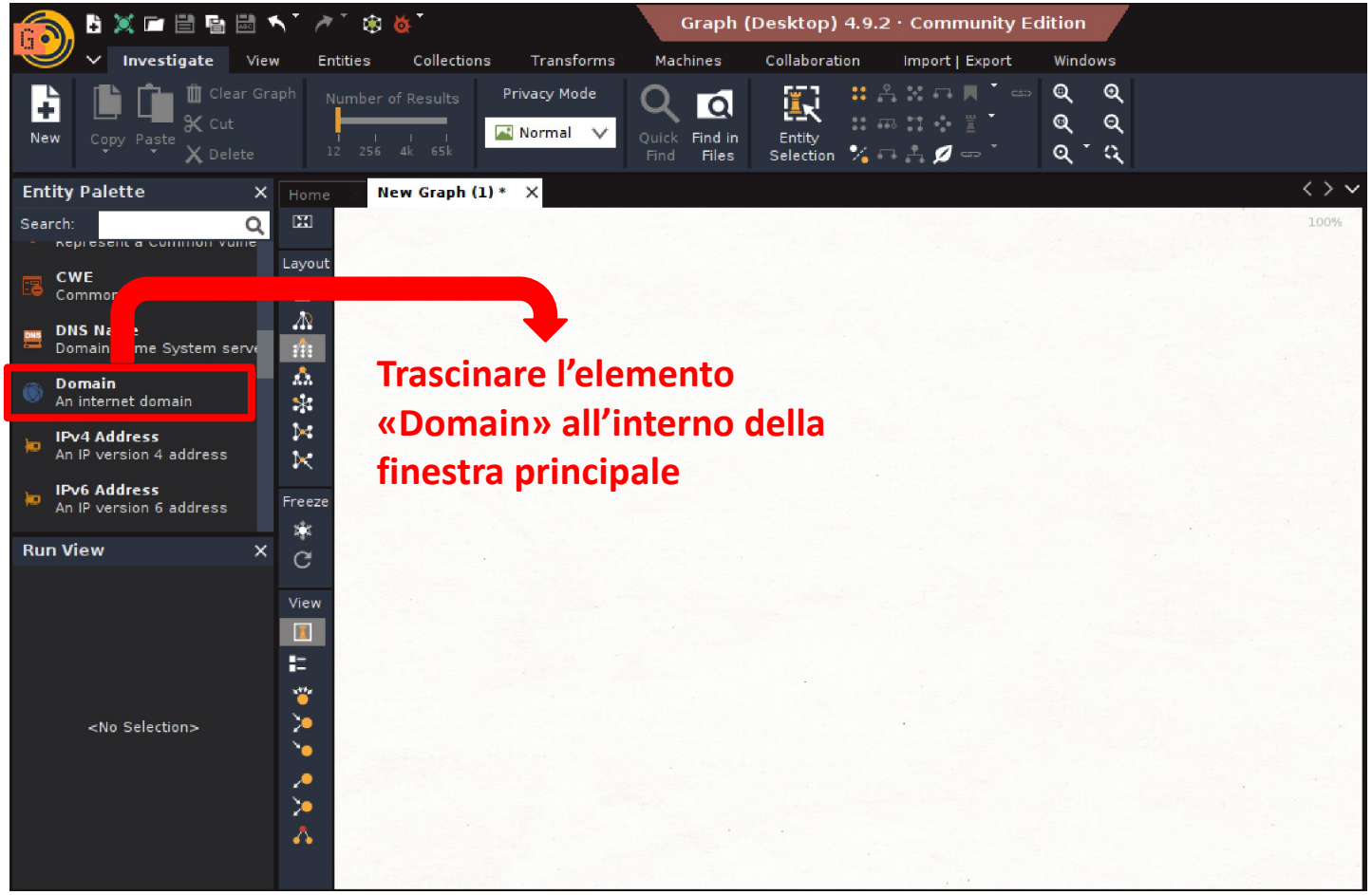
Maltego – Esempio 1



MALTEGO

Utilizzo di Crawler

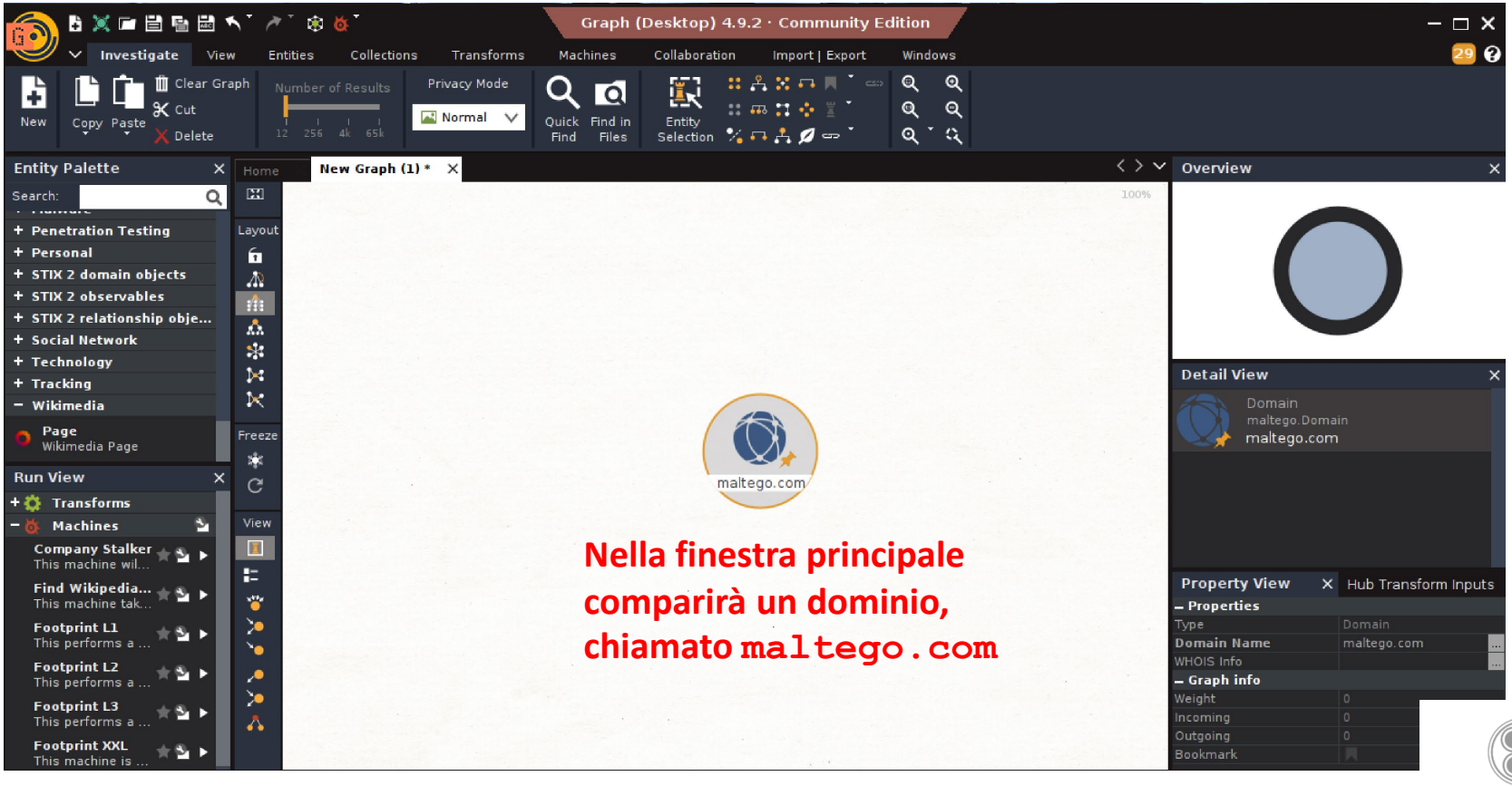
Maltego – Esempio 1



MALTEGO

Utilizzo di Crawler

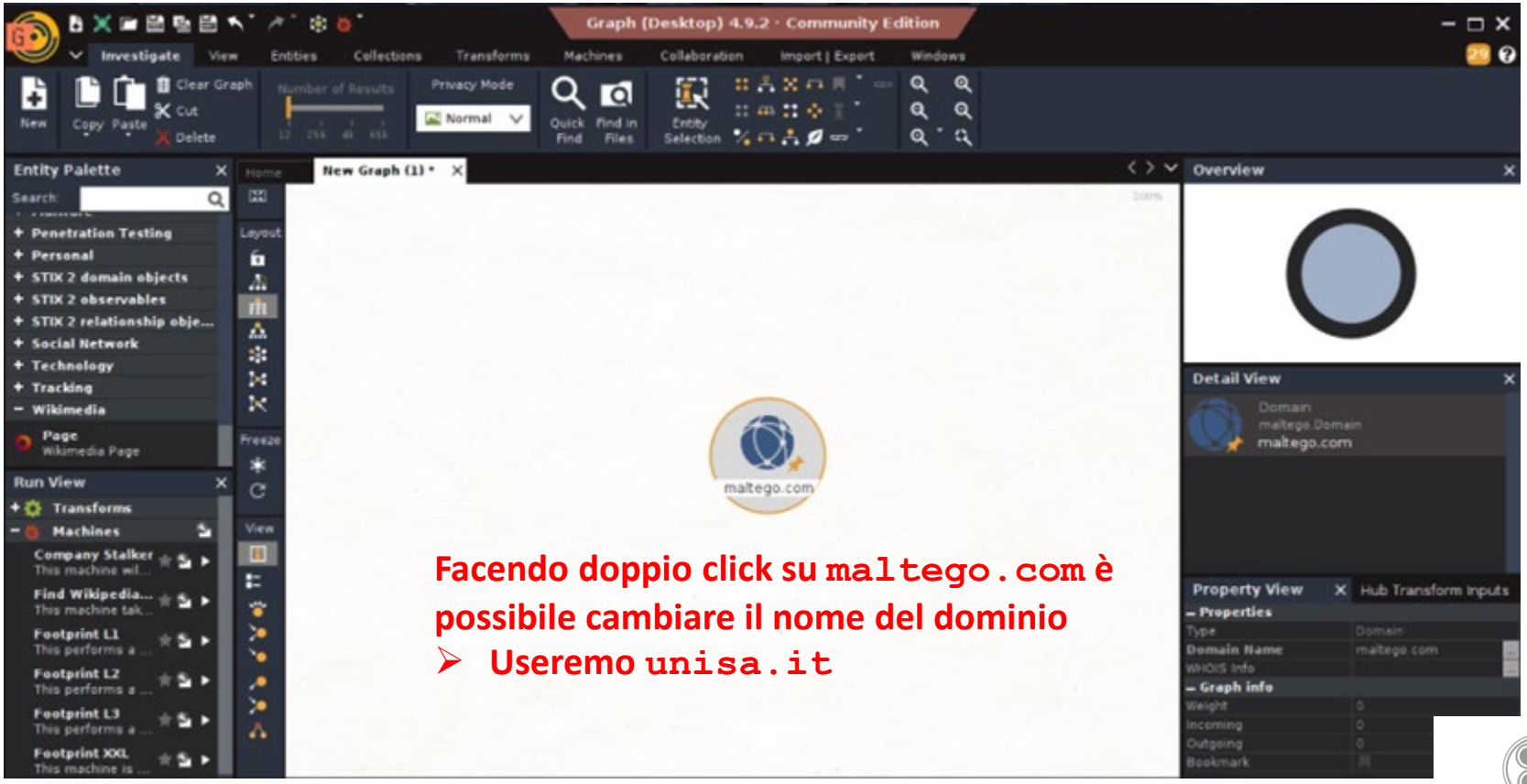
Maltego – Esempio 1



MALTEGO

Utilizzo di Crawler

Maltego – Esempio 1



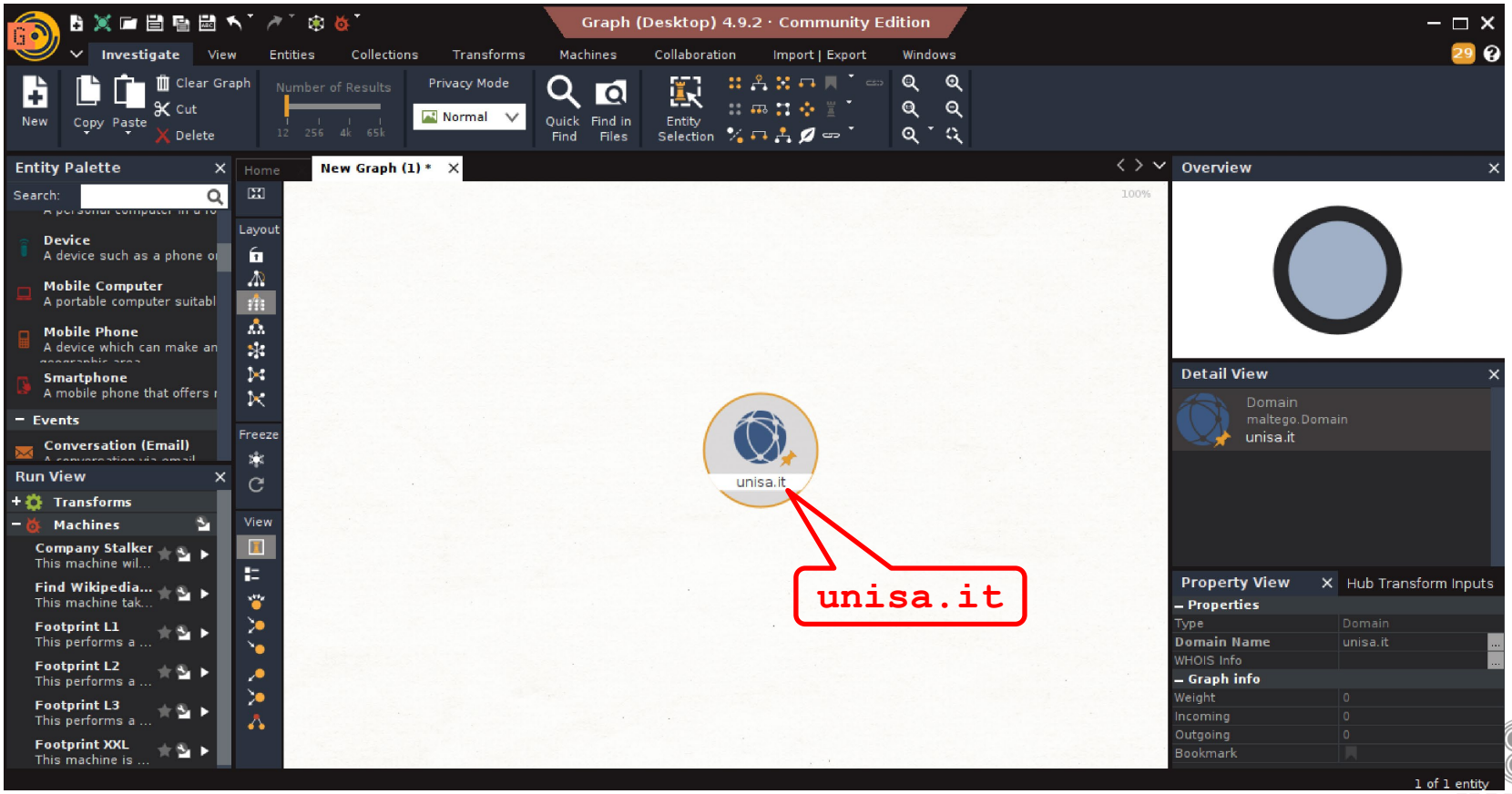
Facendo doppio click su `maltego.com` è possibile cambiare il nome del dominio

- **Useremo `unisa.it`**

MALTEGO

Utilizzo di Crawler

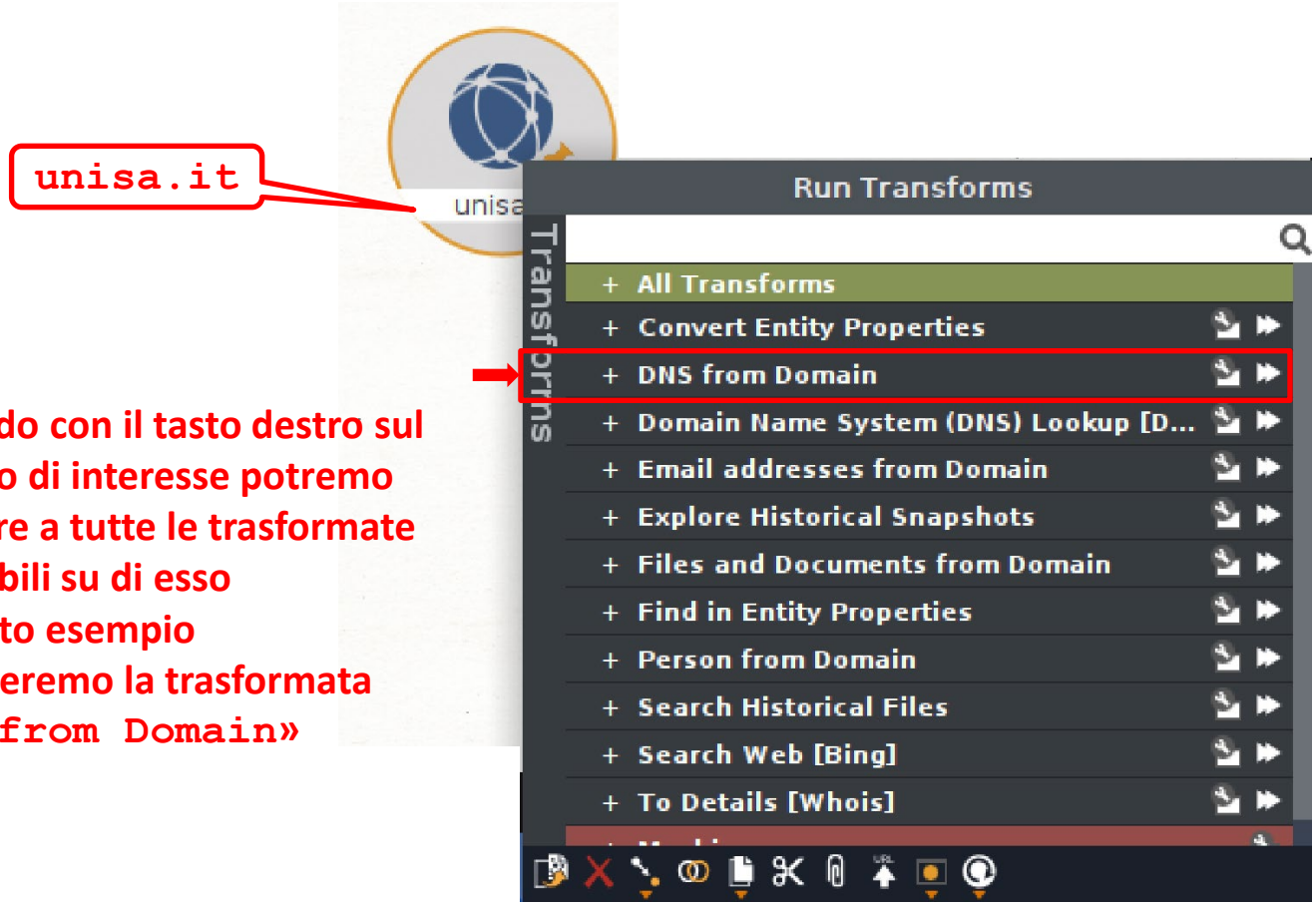
Maltego – Esempio 1



MALTEGO

Utilizzo di Crawler

Maltego – Esempio 1

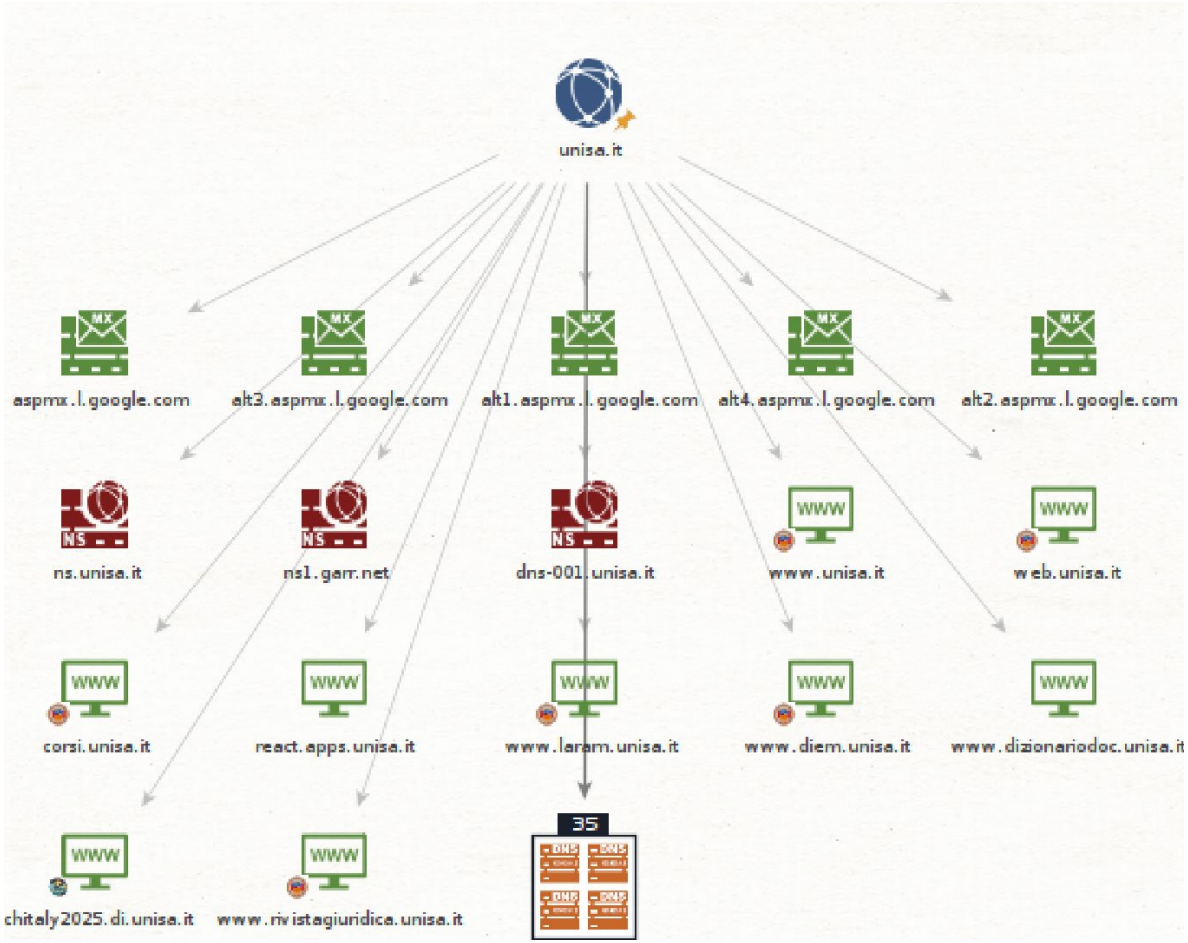


- **Cliccando con il tasto destro sul dominio di interesse potremo accedere a tutte le trasformate applicabili su di esso**
- **In questo esempio applicheremo la trasformata «`DNS from Domain`»**

MALTEGO

Utilizzo di Crawler

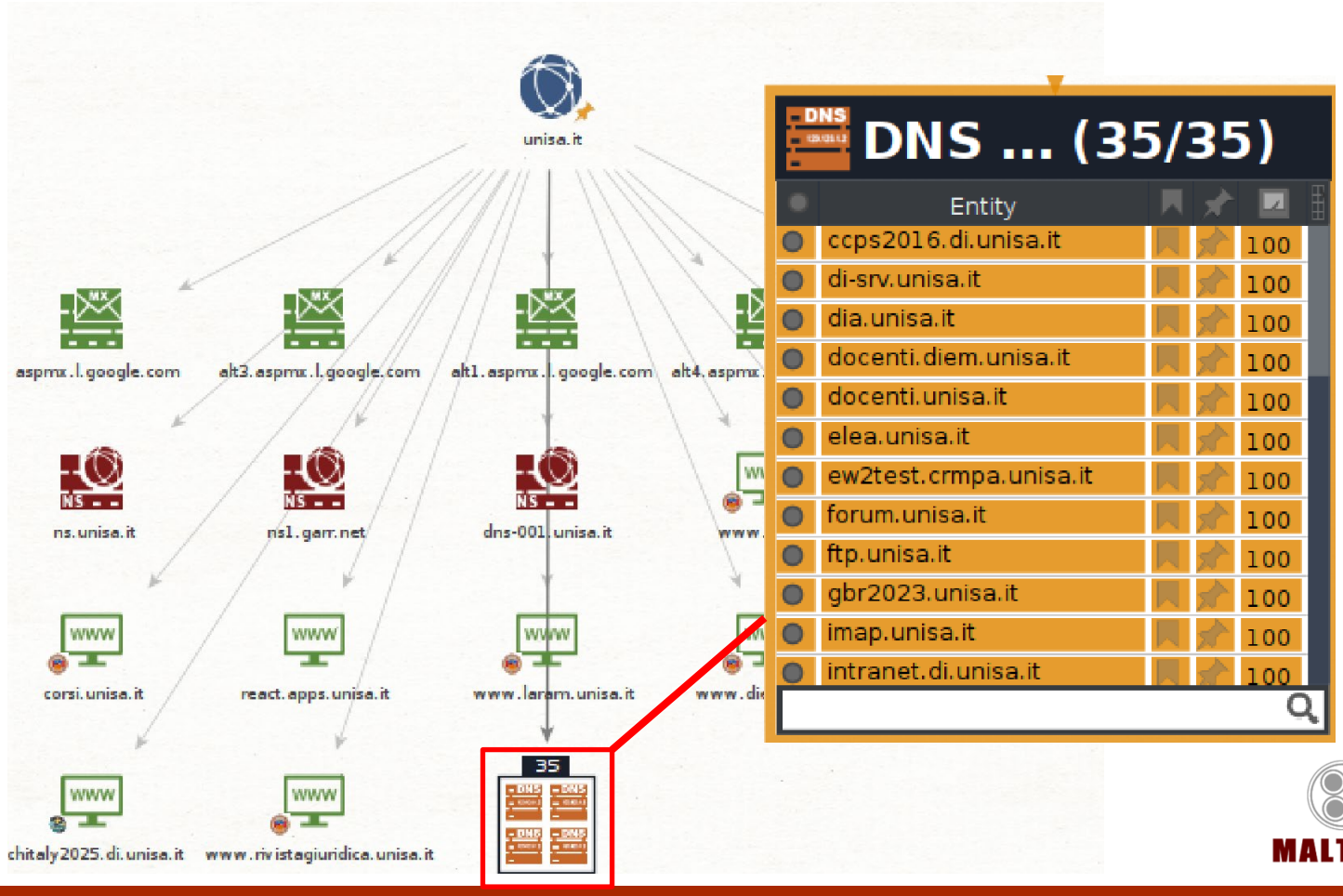
Maltego – Esempio 1



MALTEGO

Utilizzo di Crawler

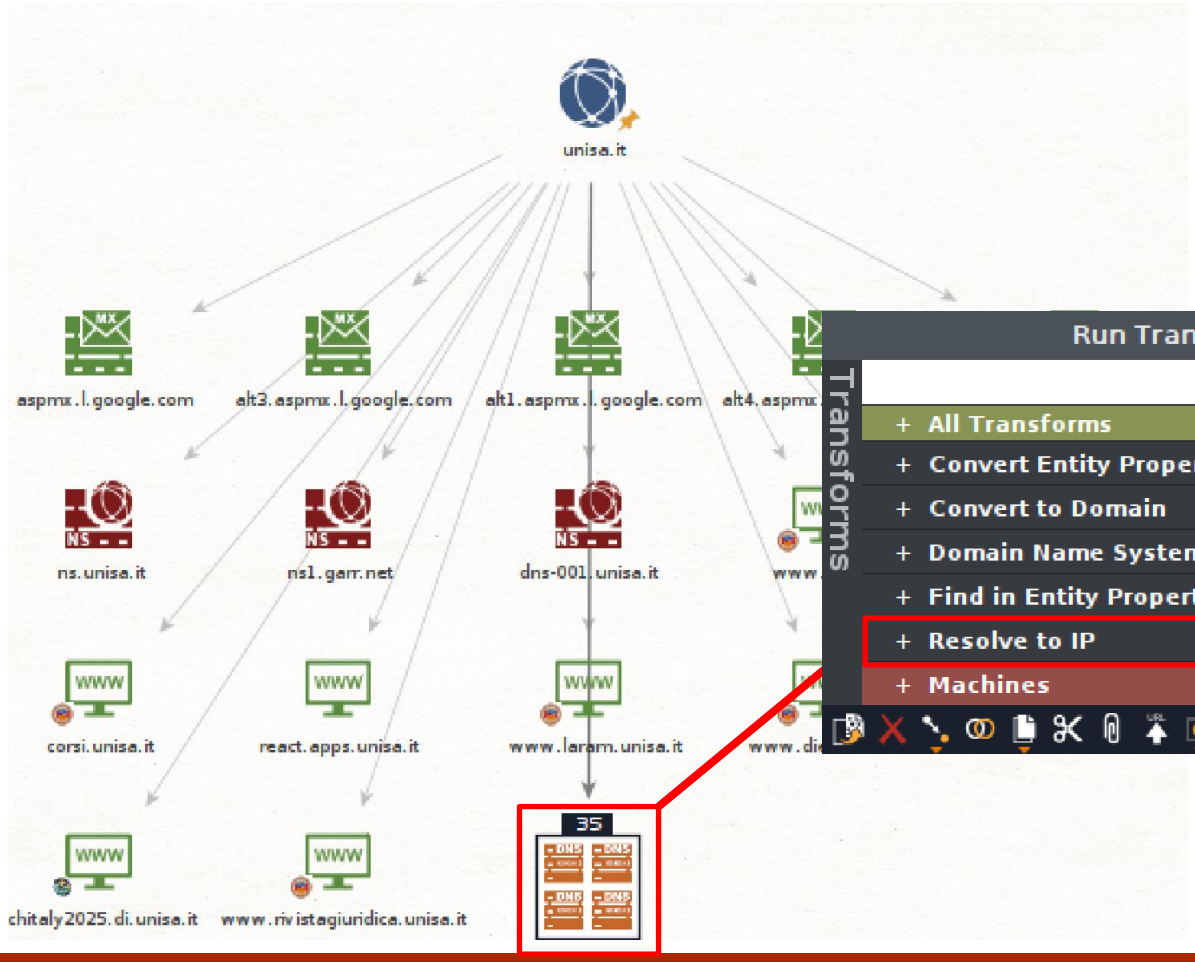
Maltego – Esempio 1



MALTEGO

Utilizzo di Crawler

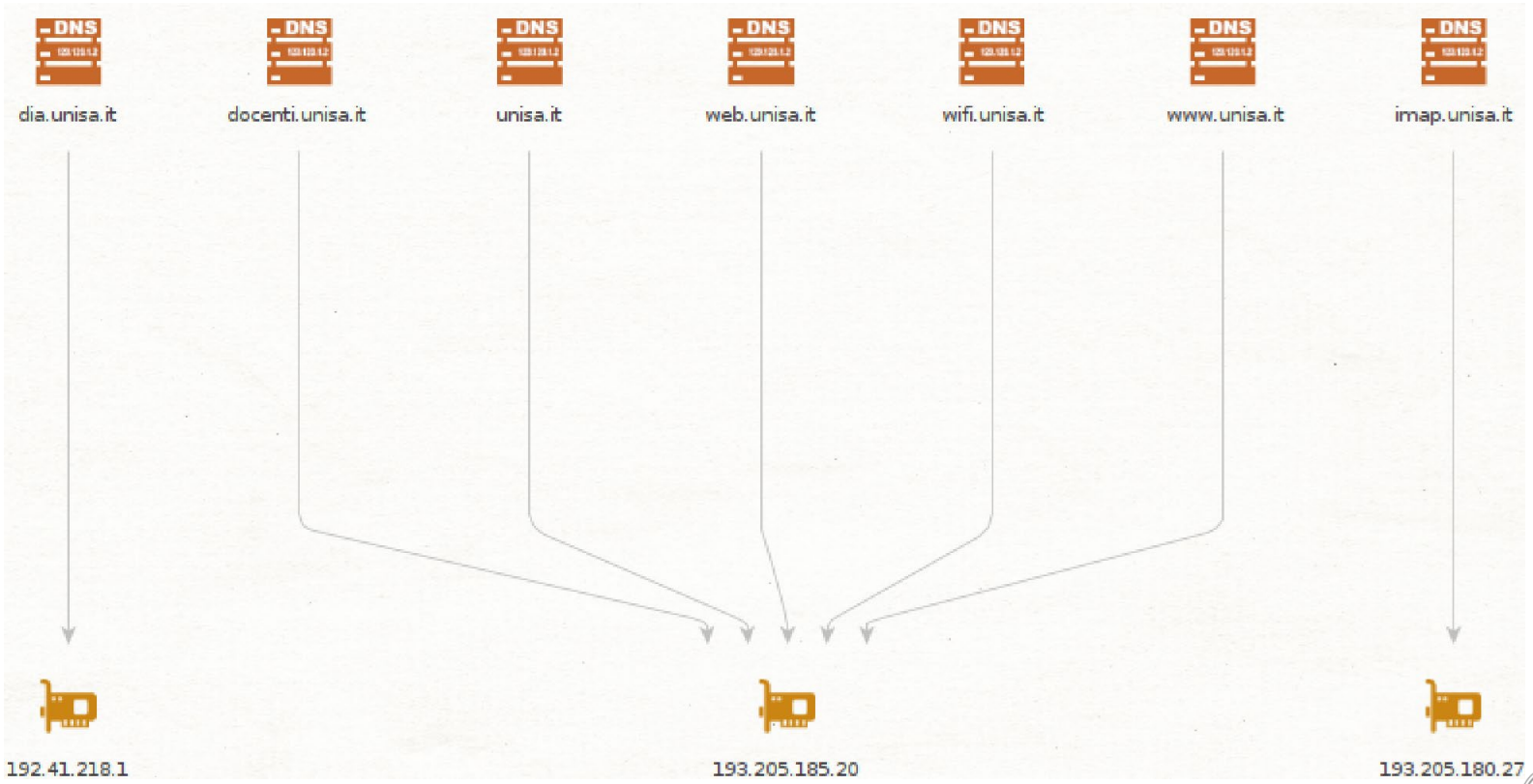
Maltego – Esempio 2



MALTEGO

Utilizzo di Crawler

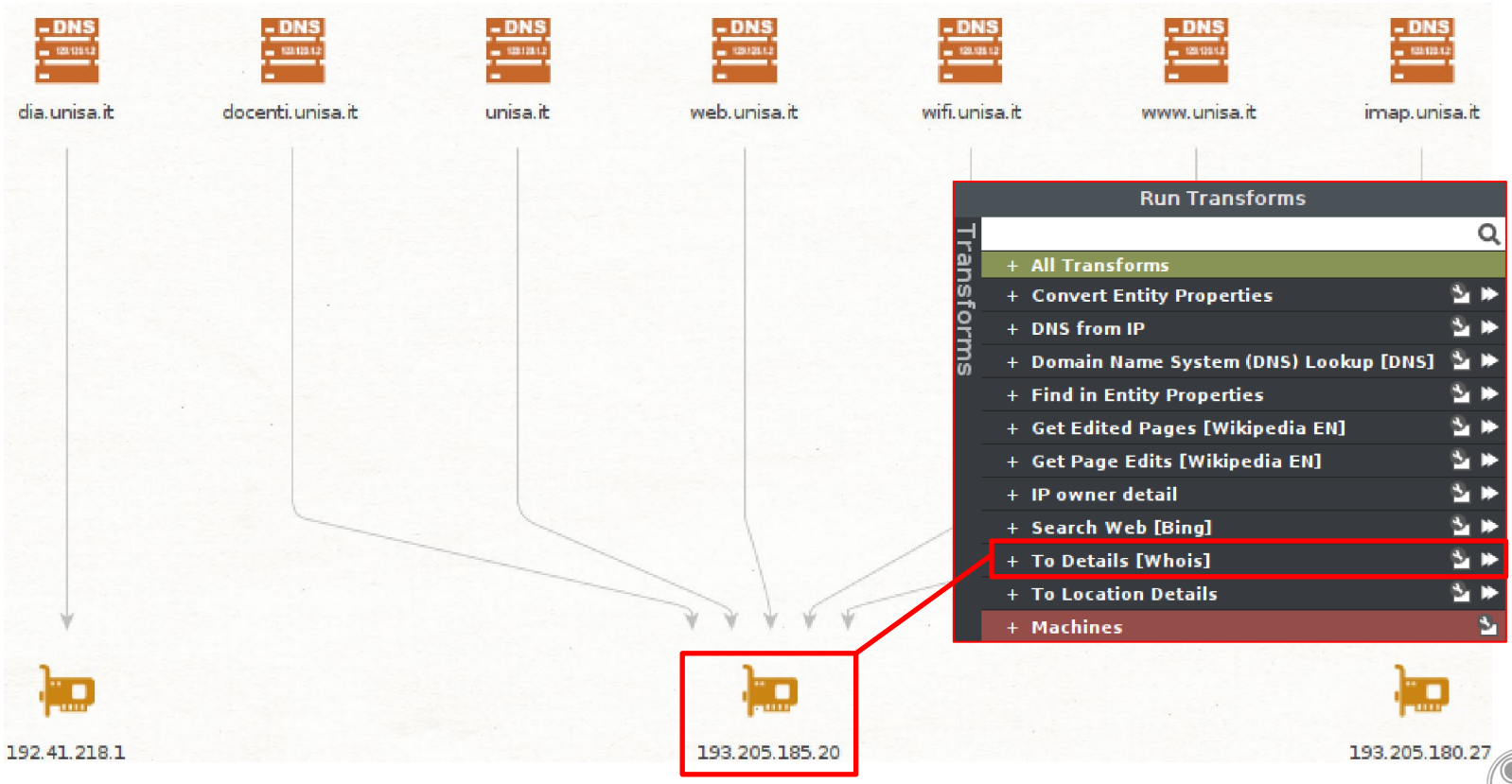
Maltego – Esempio 2



MALTEGO

Utilizzo di Crawler

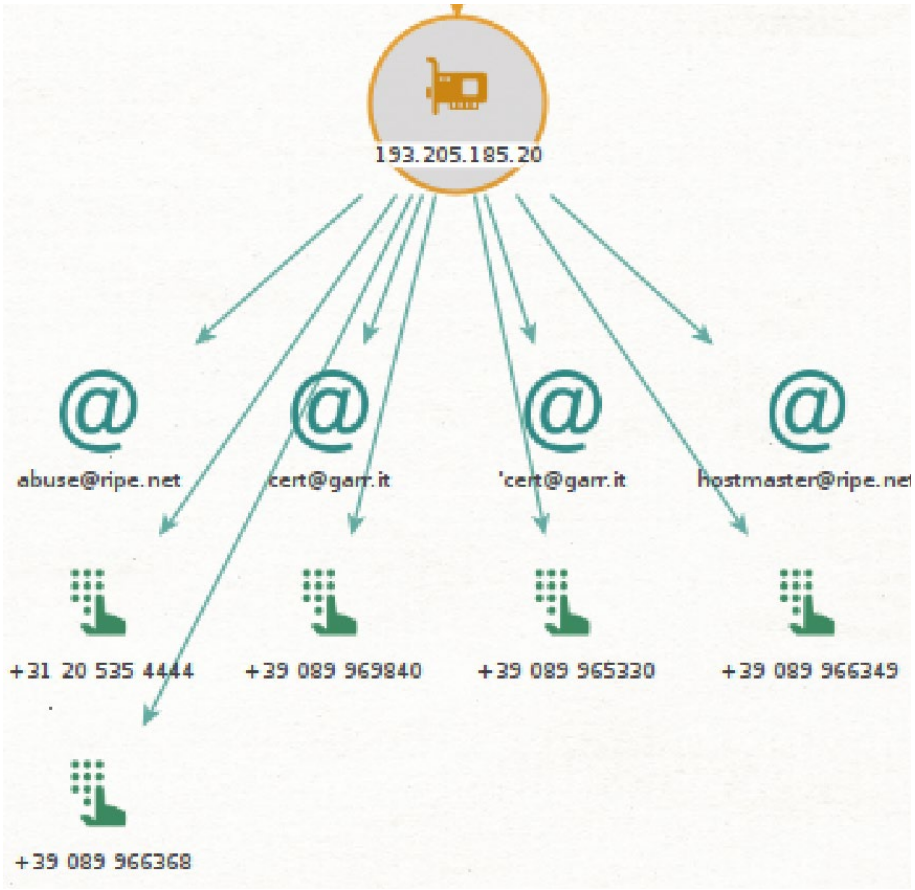
Maltego – Esempio 3



MALTEGO

Utilizzo di Crawler

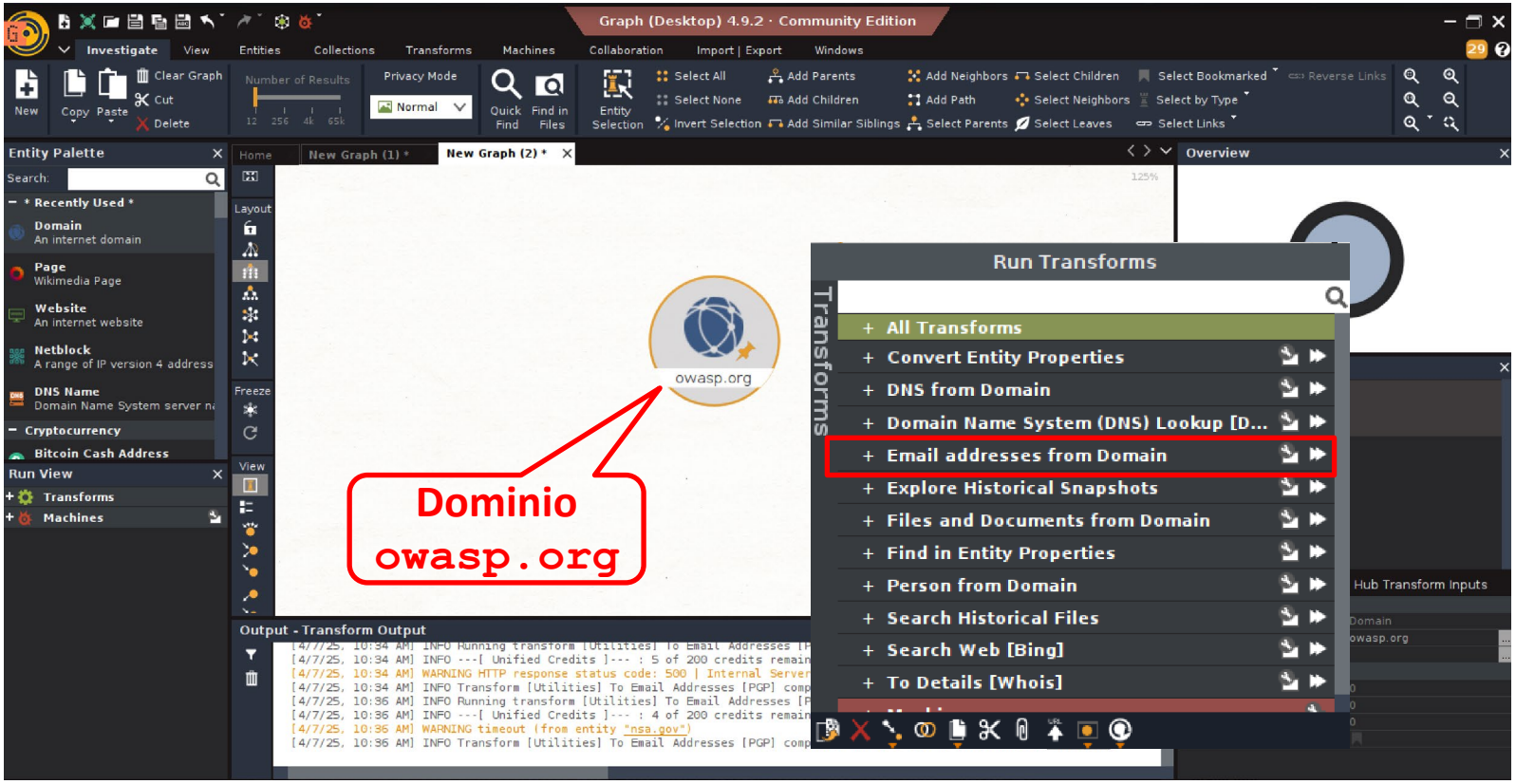
Maltego – Esempio 3



MALTEGO

Utilizzo di Crawler

Maltego – Esempio 4



MALTEGO

Utilizzo di Crawler

Maltego – Esempio 4

MALTEGO

Utilizzo di Crawler

Surface Mapping ed Asset Discovery – SpiderFoot

- Strumento di *ricognizione*, basato su OSINT, per la raccolta e l'analisi automatica di dati
  - Interroga oltre 100 fonti di dati per raccogliere informazioni su indirizzi IP, nomi di dominio, indirizzi e-mail e molto altro ancora
- Si integra con numerose fonti di informazioni ed utilizza una vasta gamma di metodi per l'analisi dei dati, rendendoli di facile consultazione
- Grazie ad un Web server integrato può essere utilizzato mediante un'interfaccia Web-based semplice e intuitiva
  - Ma può anche essere anche usato interamente da riga di comando
- È scritto in Python e rilasciato sotto licenza MIT

spiderfoot

Utilizzo di Crawler

SpiderFoot

- Per utilizzare lo strumento SpiderFoot è sufficiente specificare l'asset di interesse e scegliere i moduli da abilitare per tale strumento
  - SpiderFoot si occupa automaticamente di raccogliere i dati, per comprendere le caratteristiche dell'asset e come esse sono in relazione

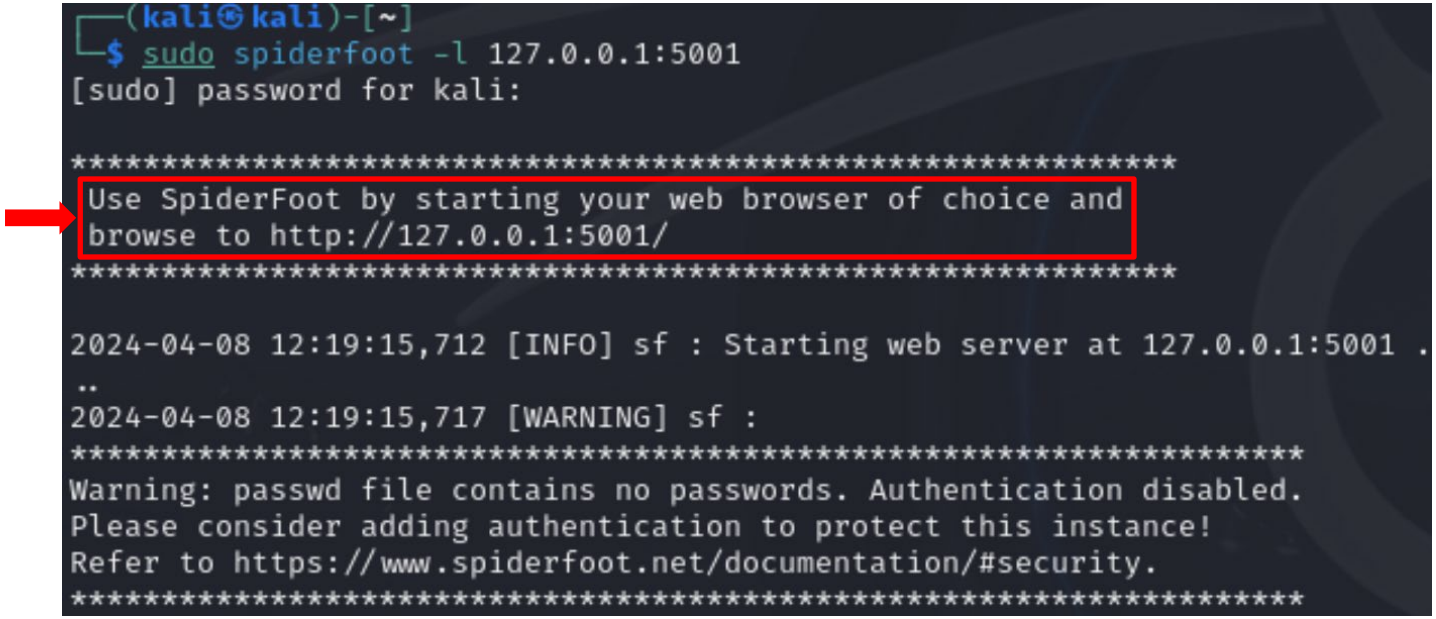
- I risultati restituiti da una scansione tramite SpiderFoot possono rivelare molte informazioni sull'asset
  - Anche eventuali data leak, vulnerabilità o altre informazioni sensibili che potrebbero essere sfruttate durante un processo di penetration testing

spiderfoot

Utilizzo di Crawler

SpiderFoot – Esempio

- Spiderfoot può essere avviato da terminale nel modo seguente
  - **`sudo spiderfoot -l 127.0.0.1:5001`**

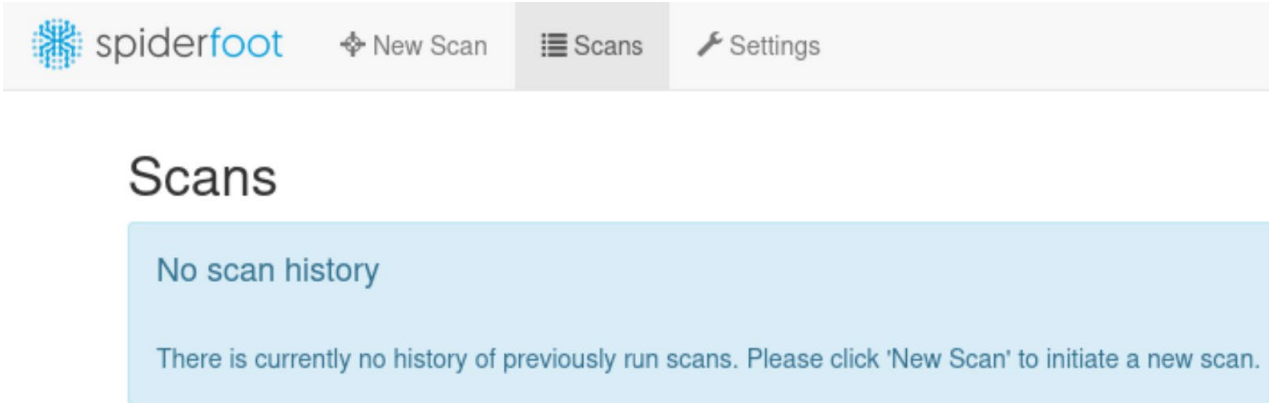


spiderfoot

Utilizzo di Crawler

SpiderFoot – Esempio

- Spiderfoot può essere utilizzato tramite Web browser, accedendo all'URL seguente
  - `http://127.0.0.1:5001/`

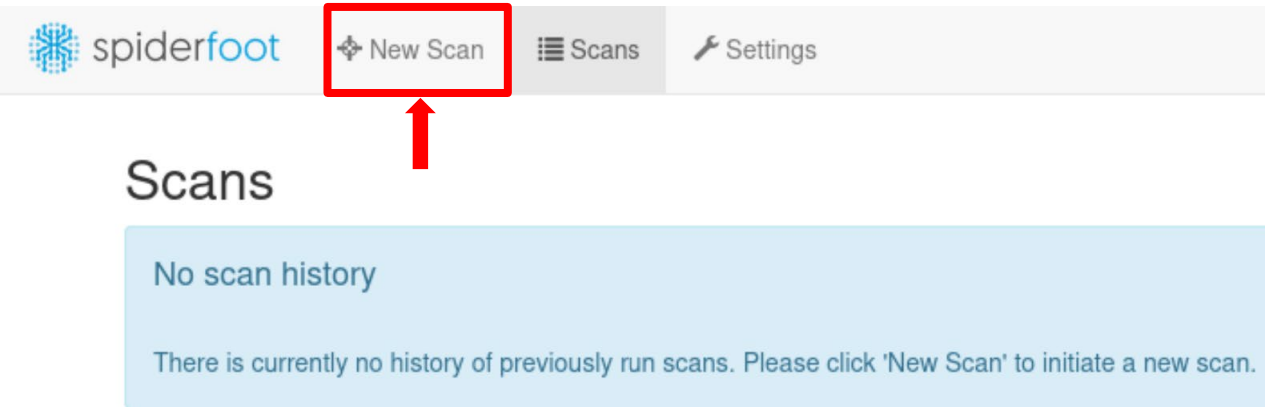


spiderfoot

Utilizzo di Crawler

SpiderFoot – Esempio

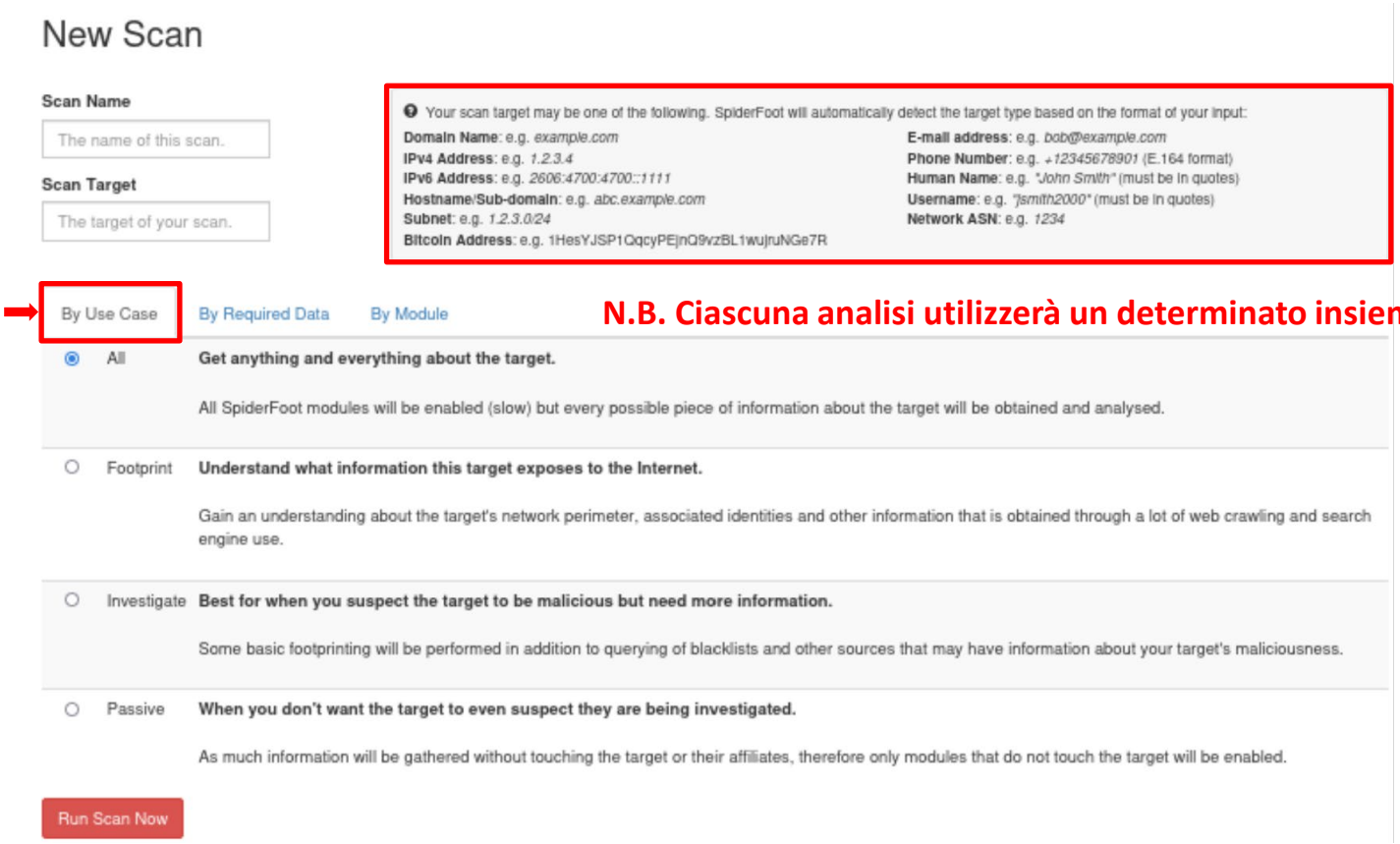
- Configurazione di una nuova scansione



Utilizzo di Crawler

SpiderFoot – Esempio

- Scelta del tipo di analisi da effettuare («**`By Use Case`**»)



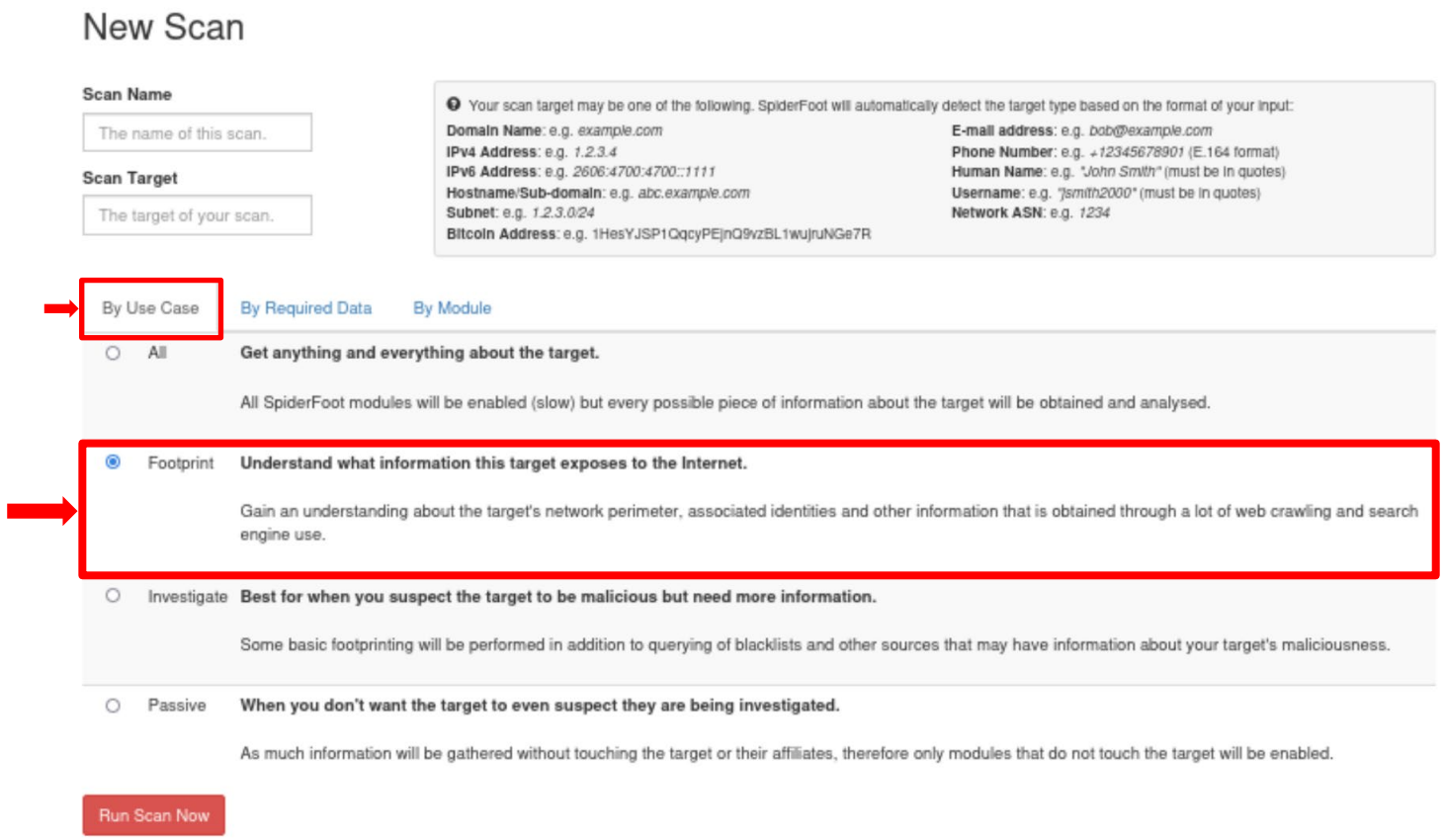
N.B. Ciascuna analisi utilizzerà un determinato insieme di moduli

spiderfoot

Utilizzo di Crawler

SpiderFoot – Esempio

- Scelta del tipo di analisi da effettuare («**`Footprint`**»)

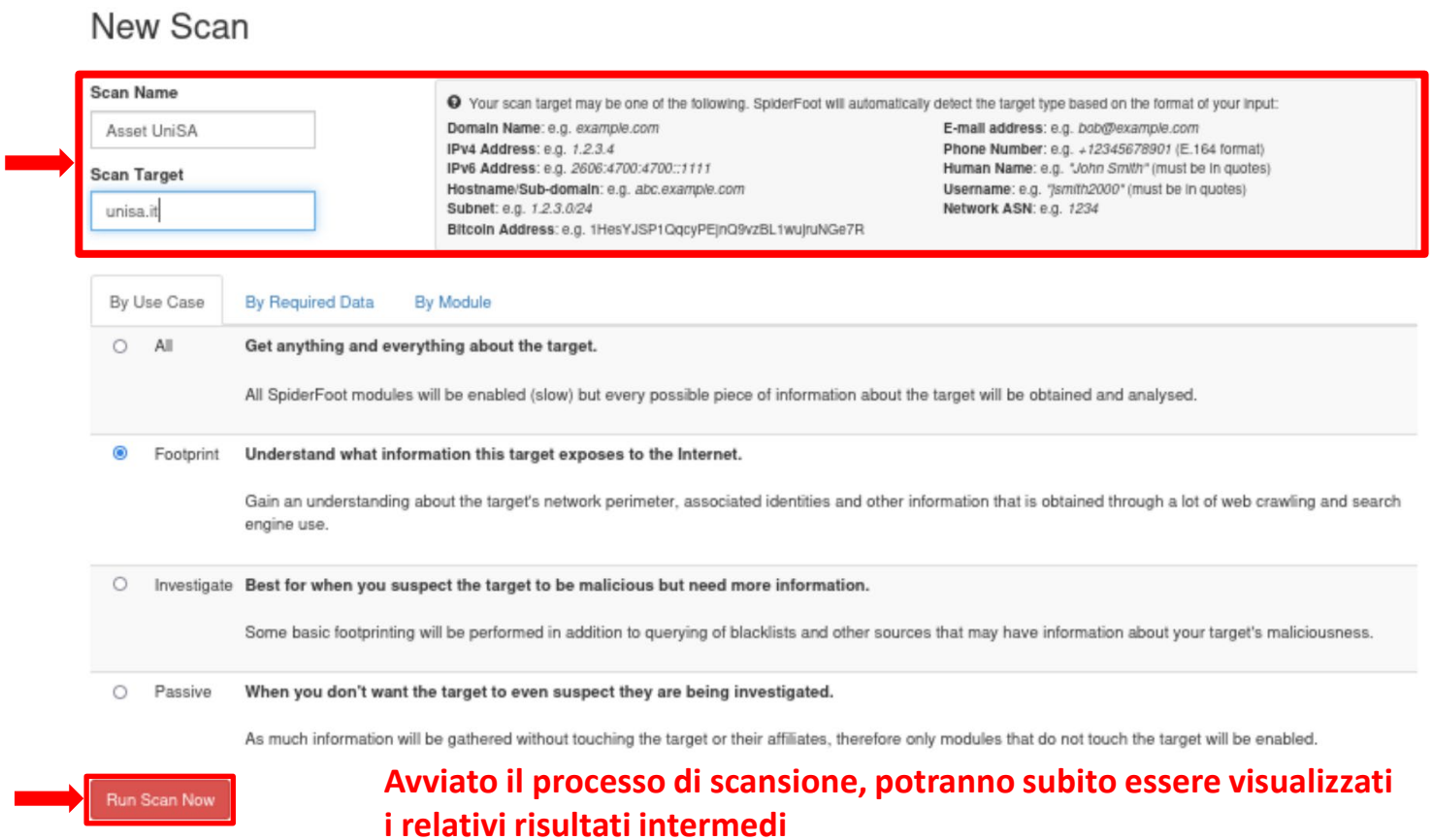


spiderfoot

Utilizzo di Crawler

SpiderFoot – Esempio

- Definizione dell'asset («**`unisa.it`**»)



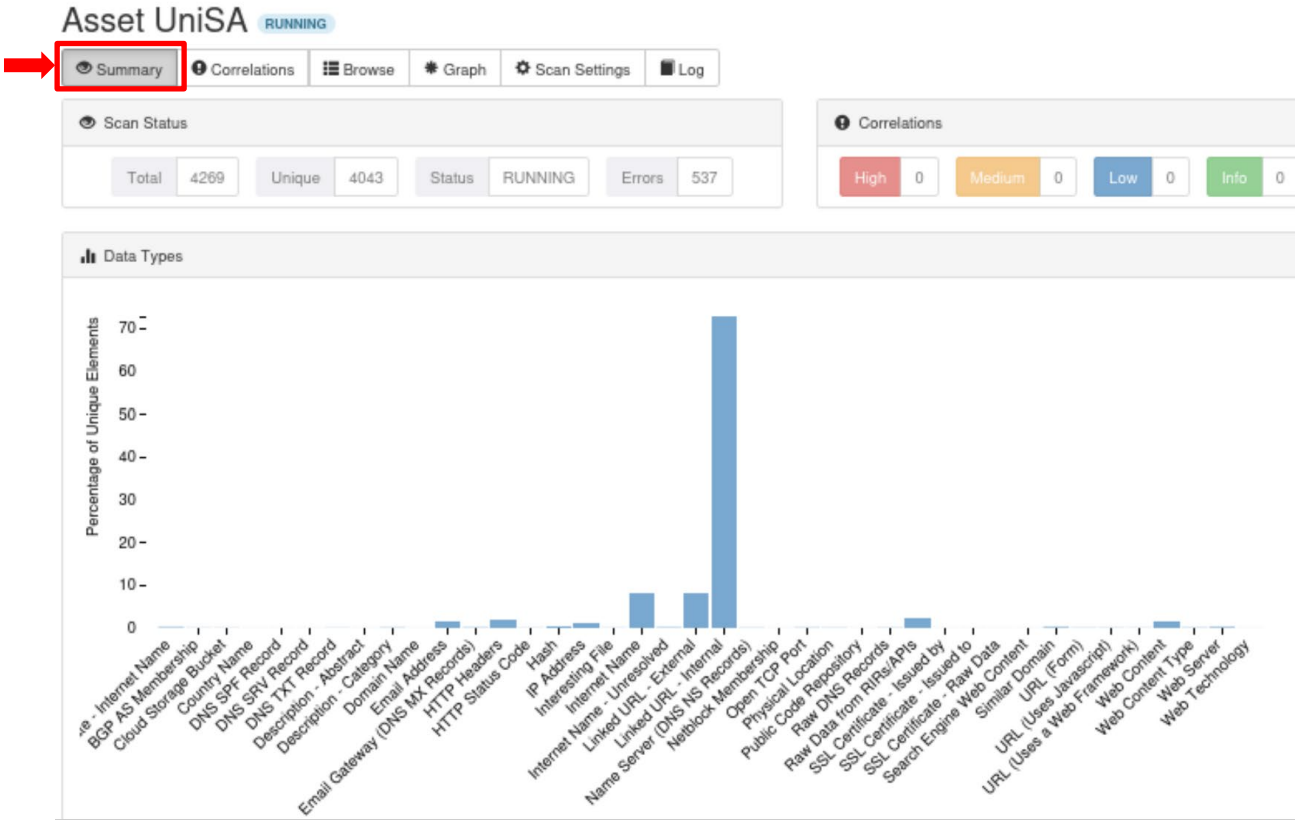
Avviato il processo di scansione, potranno subito essere visualizzati i relativi risultati intermedi

spiderfoot

Utilizzo di Crawler

SpiderFoot – Esempio

- Riepilogo dei risultati ottenuti dalla scansione

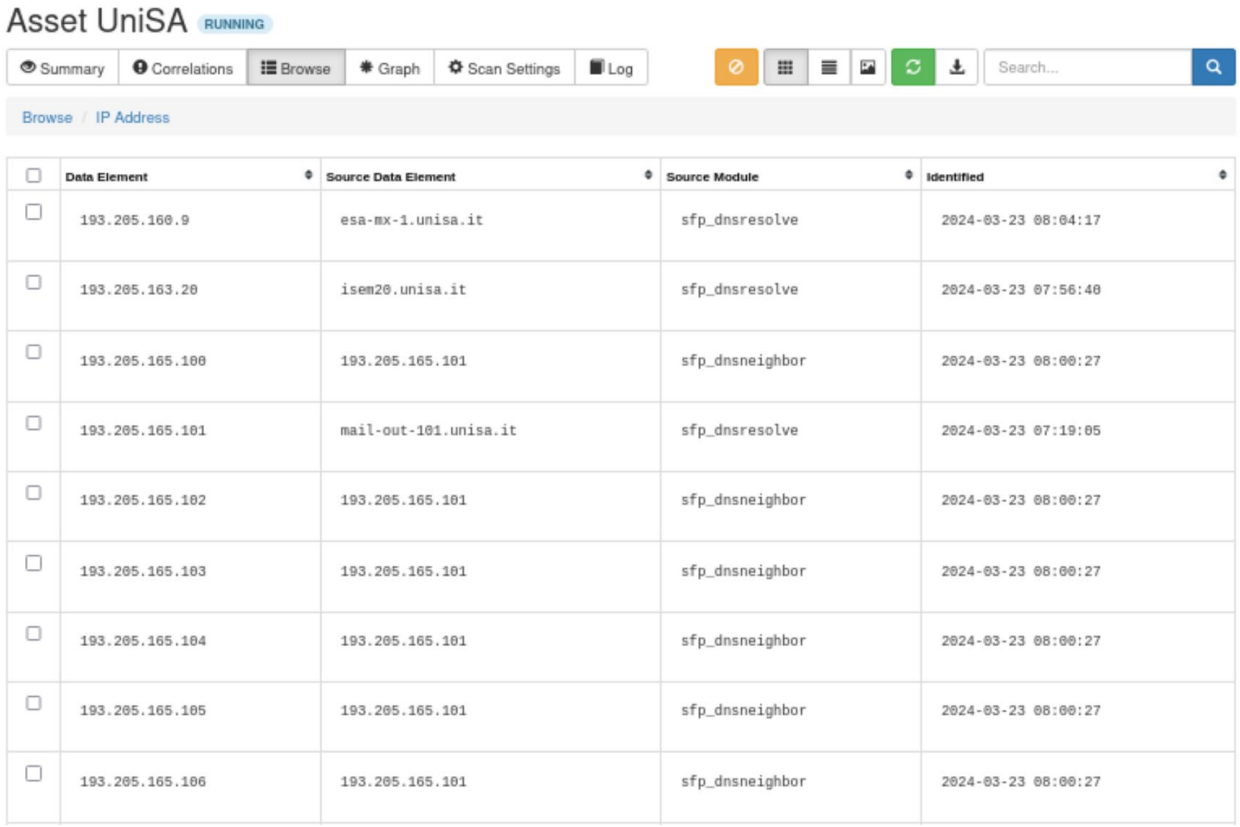


spiderfoot

Utilizzo di Crawler

SpiderFoot – Esempio

- Risultati ottenuti dalla scansione (*Indirizzi IP*)



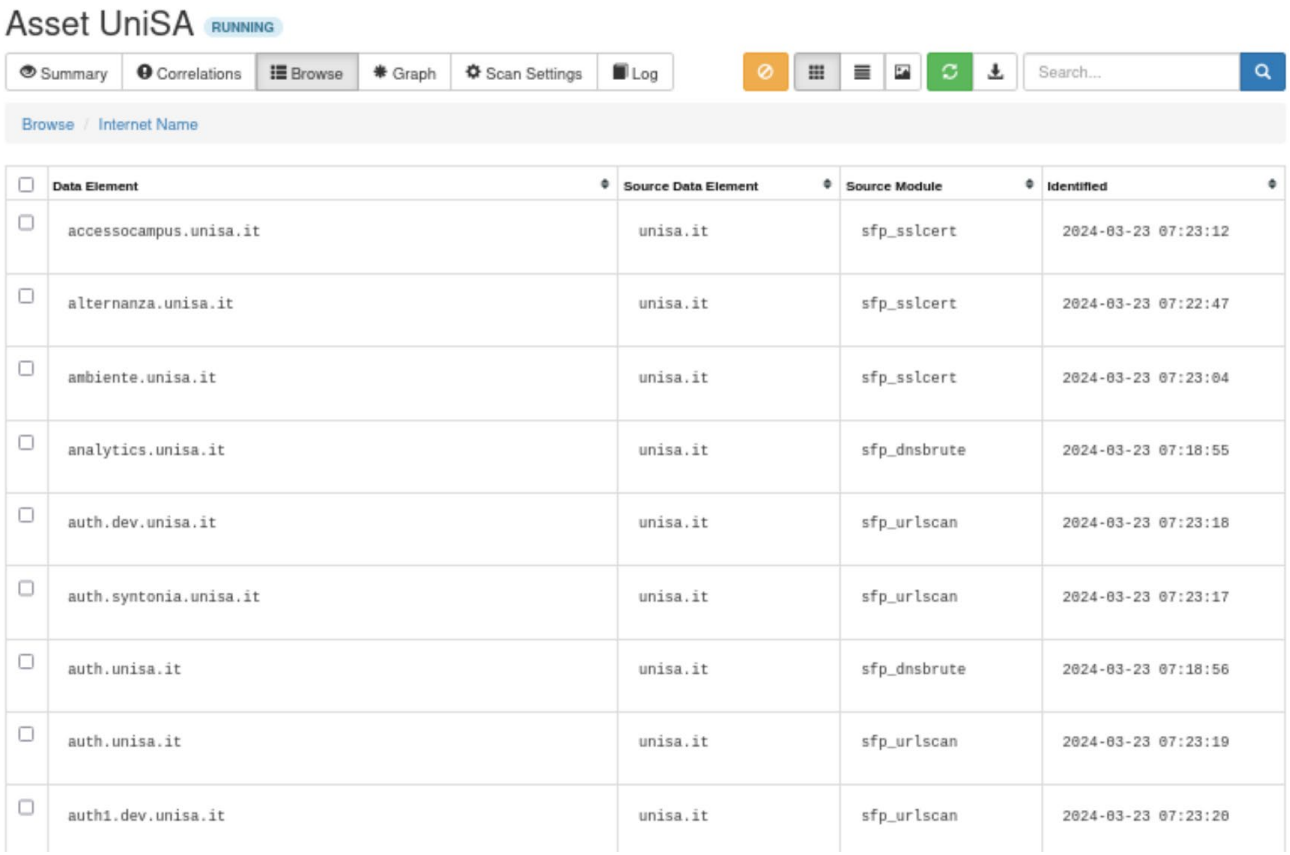
Data Element	Source Data Element	Source Module	Identified
193.205.160.9	esa-mx-1.unisa.it	sfp_dnsresolve	2024-03-23 08:04:17
193.205.163.20	isem20.unisa.it	sfp_dnsresolve	2024-03-23 07:56:40
193.205.165.100	193.205.165.101	sfp_dnsneighbor	2024-03-23 08:00:27
193.205.165.101	mail-out-101.unisa.it	sfp_dnsresolve	2024-03-23 07:19:05
193.205.165.102	193.205.165.101	sfp_dnsneighbor	2024-03-23 08:00:27
193.205.165.103	193.205.165.101	sfp_dnsneighbor	2024-03-23 08:00:27
193.205.165.104	193.205.165.101	sfp_dnsneighbor	2024-03-23 08:00:27
193.205.165.105	193.205.165.101	sfp_dnsneighbor	2024-03-23 08:00:27
193.205.165.106	193.205.165.101	sfp_dnsneighbor	2024-03-23 08:00:27

spiderfoot

Utilizzo di Crawler

SpiderFoot – Esempio

- Risultati ottenuti dalla scansione (*Sottodomini*)



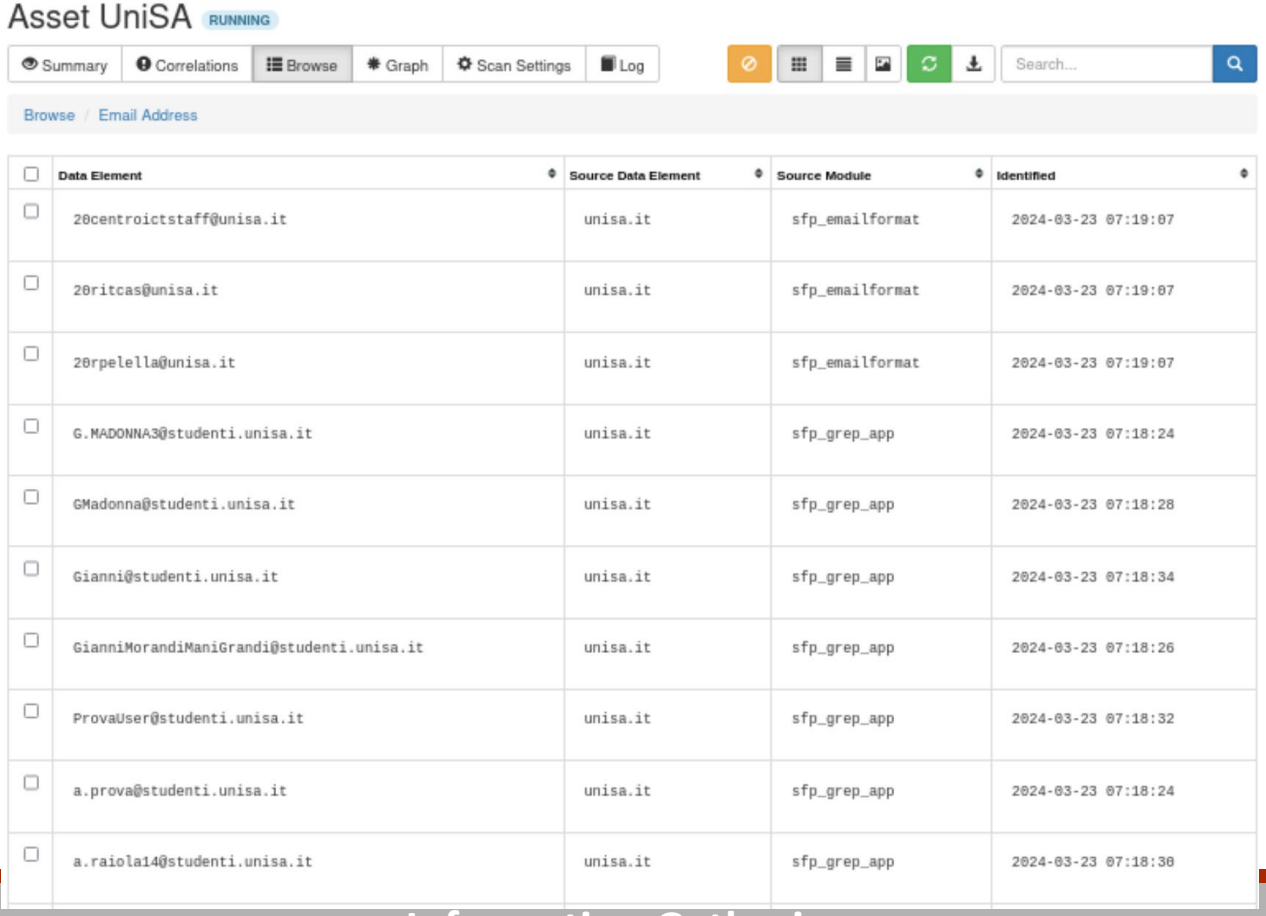
Data Element	Source Data Element	Source Module	Identified
accessocampus.unisa.it	unisa.it	sfp_sslcert	2024-03-23 07:23:12
alternanza.unisa.it	unisa.it	sfp_sslcert	2024-03-23 07:22:47
ambiente.unisa.it	unisa.it	sfp_sslcert	2024-03-23 07:23:04
analytics.unisa.it	unisa.it	sfp_dnsbrute	2024-03-23 07:18:55
auth.dev.unisa.it	unisa.it	sfp_urlscan	2024-03-23 07:23:18
auth.syntonia.unisa.it	unisa.it	sfp_urlscan	2024-03-23 07:23:17
auth.unisa.it	unisa.it	sfp_dnsbrute	2024-03-23 07:18:56
auth.unisa.it	unisa.it	sfp_urlscan	2024-03-23 07:23:19
auth1.dev.unisa.it	unisa.it	sfp_urlscan	2024-03-23 07:23:20

spiderfoot

Utilizzo di Crawler

SpiderFoot – Esempio

- Risultati ottenuti dalla scansione (*Indirizzi e-mail*)



Data Element	Source Data Element	Source Module	Identified
20centroictstaff@unisa.it	unisa.it	sfp_emailformat	2024-03-23 07:19:07
20ritcas@unisa.it	unisa.it	sfp_emailformat	2024-03-23 07:19:07
20rpelella@unisa.it	unisa.it	sfp_emailformat	2024-03-23 07:19:07
G.MADONNA3@studenti.unisa.it	unisa.it	sfp_grep_app	2024-03-23 07:18:24
GMadonna@studenti.unisa.it	unisa.it	sfp_grep_app	2024-03-23 07:18:28
Gianni@studenti.unisa.it	unisa.it	sfp_grep_app	2024-03-23 07:18:34
GianniMorandiManiGrandi@studenti.unisa.it	unisa.it	sfp_grep_app	2024-03-23 07:18:26
ProvaUser@studenti.unisa.it	unisa.it	sfp_grep_app	2024-03-23 07:18:32
a.prova@studenti.unisa.it	unisa.it	sfp_grep_app	2024-03-23 07:18:24
a.raiola14@studenti.unisa.it	unisa.it	sfp_grep_app	2024-03-23 07:18:30

spiderfoot

Utilizzo di Crawler

Surface Mapping ed Asset Discovery – OWASP Amass

- Framework che consente di effettuare operazioni di Surface Mapping ed Asset Discovery mediante
  - Information gathering passiva, basata su OSINT
  - Information gathering attiva, basata su *bruteforcing*

- Fornisce
  - Vari strumenti per l'asset discovery
  - Un database integrato per la memorizzazione dei risultati
  - Modelli per la formalizzazione dell'asset

Amass
OWASP

Utilizzo di Crawler

OWASP Amass – Caratteristiche Principali

- **Raccolta delle informazioni:** automatizza la raccolta di informazioni sull'asset
  - Nomi di dominio, sottodomini, indirizzi IP, certificati SSL/TLS, server e-mail, etc
- **Integrazione delle informazioni:** integra dati provenienti da varie fonti di informazioni
  - Motori di ricerca, database di record DNS, servizi di cloud hosting, social network, etc
- **Analisi della superficie di attacco:** consente di identificare potenziali punti di ingresso e vulnerabilità
  - Rilevando host «non autorizzati» o servizi esposti che potrebbero essere «presi di mira da attacchi»
- **Esportazione dei dati:** permette di esportare in diversi formati i risultati della raccolta di informazioni
  - Facilitandone l'analisi e l'utilizzo da parte di altri strumenti e processi di sicurezza

Amass OWASP

Utilizzo di Crawler

OWASP Amass – Comandi

- Composto da due comandi
  - **`amass intel`** – Si occupa di raccogliere informazioni di varia tipologia riguardanti l'asset
  - **`amass enum`** – Si occupa dell'enumerazione, attiva e passiva, dei sottodomini relati all'asset

Utilizzo di Crawler

OWASP Amass – Comando `intel`

- **`amass intel -h`**

```
Usage: amass intel [options] [-whois -d DOMAIN] [-addr ADDR -asn ASN -cidr CI
DR]

  -active
        Attempt certificate name grabs
  -addr value
        IPs and ranges (192.168.1.1-254) separated by commas
  -asn value
        ASNs separated by commas (can be used multiple times)
  -cidr value
        CIDRs separated by commas (can be used multiple times)
  -config string
        Path to the YAML configuration file. Additional details below
  -d value
        Domain names separated by commas (can be used multiple times)
  -demo
        Censor output to make it suitable for demonstrations
  -df value
        Path to a file providing root domain names
  -dir string
        Path to the directory containing the output files
```

Output parziale

Utilizzo di Crawler

OWASP Amass – Comando `enum`

- **`amass enum -h`**

```
Usage: amass enum [options] -d DOMAIN

  -active
        Attempt zone transfers and certificate name grabs
  -addr value
        IPs and ranges (192.168.1.1-254) separated by commas
  -alts
        Enable generation of altered names
  -asn value
        ASNs separated by commas (can be used multiple times)
  -aw value
        Path to a different wordlist file for alterations
  -awm value
        "hashcat-style" wordlist masks for name alterations
  -bl value
        Blacklist of subdomain names that will not be investigated
  -blf string
        Path to a file providing blacklisted subdomains
  -brute
        Execute brute forcing after searches
  -cidr value
        CIDRs separated by commas (can be used multiple times)
```

Output parziale

Utilizzo di Crawler

OWASP Amass – enum – Esempio

- **`amass enum -d unisa.it`**

```
┌──(kali㉿kali)-[~]
└─$ amass enum -d unisa.it
unisa.it (FQDN) --> ns_record --> ns1.garr.net (FQDN)
unisa.it (FQDN) --> ns_record --> dns-001.unisa.it (FQDN)
unisa.it (FQDN) --> ns_record --> ns.unisa.it (FQDN)
unisa.it (FQDN) --> mx_record --> alt3.aspmx.l.google.com (FQDN)
unisa.it (FQDN) --> mx_record --> aspmx.l.google.com (FQDN)
unisa.it (FQDN) --> mx_record --> alt4.aspmx.l.google.com (FQDN)
unisa.it (FQDN) --> mx_record --> alt1.aspmx.l.google.com (FQDN)
unisa.it (FQDN) --> mx_record --> alt2.aspmx.l.google.com (FQDN)
corsi.unisa.it (FQDN) --> cname_record --> www.unisa.it (FQDN)
biblioteche.unisa.it (FQDN) --> cname_record --> www4.unisa.it (FQDN)
jobincampus.unisa.it (FQDN) --> cname_record --> www.unisa.it (FQDN)
tfia.diem.unisa.it (FQDN) --> cname_record --> docenti.diem.unisa.it (FQDN)
h40.cla.unisa.it (FQDN) --> a_record --> 193.205.173.90 (IPAddress)
digitalstories.ictateneo.unisa.it (FQDN) --> cname_record --> ict219.ictateneo.unisa.it (FQDN)
linuxas.seda.unisa.it (FQDN) --> a_record --> 193.205.167.86 (IPAddress)
placement.unisa.it (FQDN) --> cname_record --> webgroup01-debzgtdscyfrc9ff.z01.azurefd.net (FQDN)
6000r.unisa.it (FQDN) --> a_record --> 193.205.160.190 (IPAddress)
archeo5.dbc.unisa.it (FQDN) --> a_record --> 193.205.170.90 (IPAddress)
allievo32.cla.unisa.it (FQDN) --> a_record --> 193.205.173.232 (IPAddress)
provola.cbs.unisa.it (FQDN) --> a_record --> 193.205.187.129 (IPAddress)
```

Amass OWASP

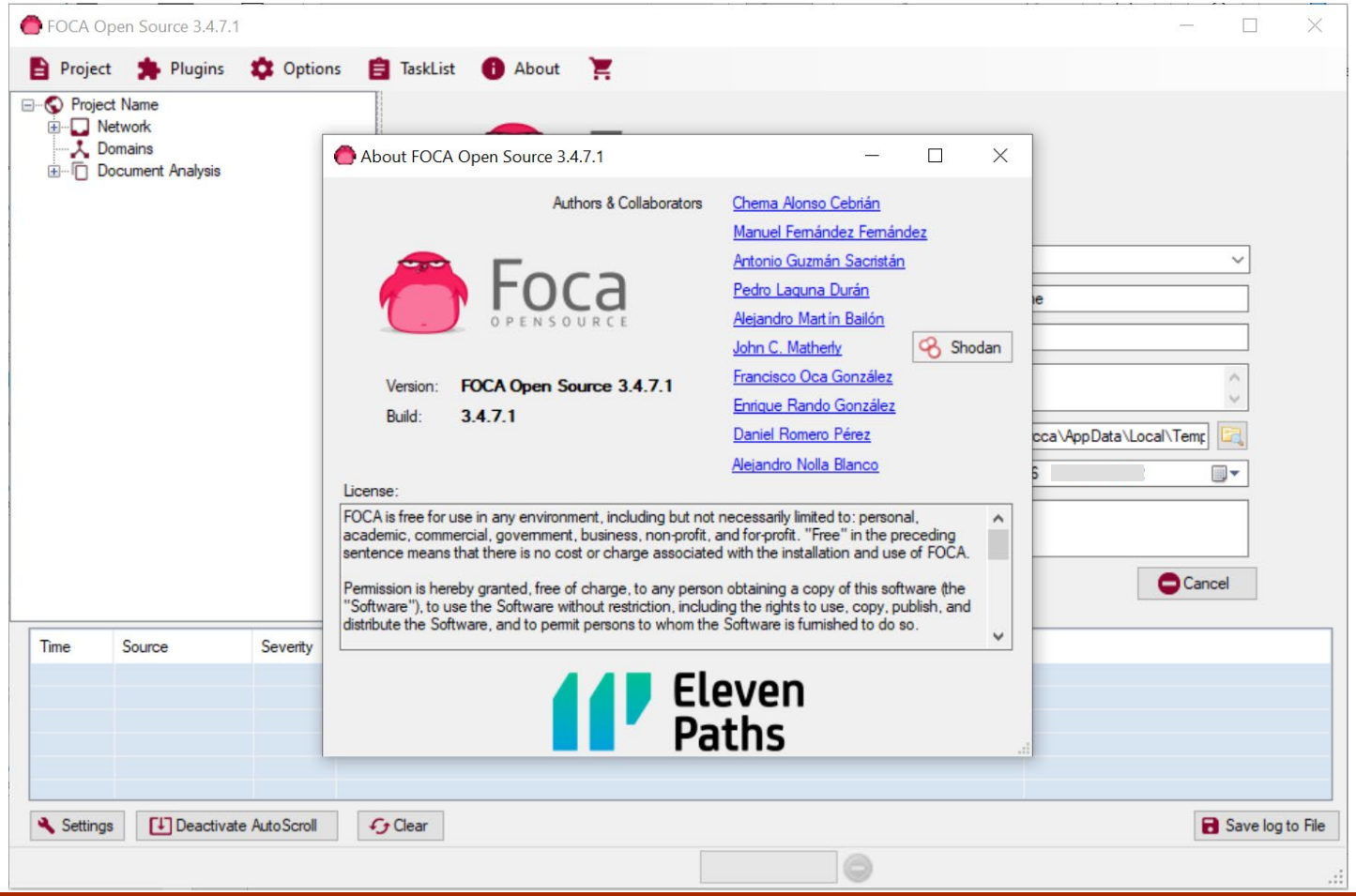
Utilizzo di Crawler

Ricerca di Metadati – FOCA

- ***FOCA** (**F**ingerprinting **O**rganizations with **C**ollected **A**rchives)*
  - Permette di trovare metadati ed informazioni nascoste nei file
    - I file vengono scaricati ed analizzati automaticamente
  - Scaricabile gratuitamente
    - https://github.com/ElevenPaths/FOCA/releases
  - Richiede l'installazione di un database SQL per poter funzionare
    - https://github.com/ElevenPaths/FOCA/wiki/How-to-set-up-a-SQL-database-connection

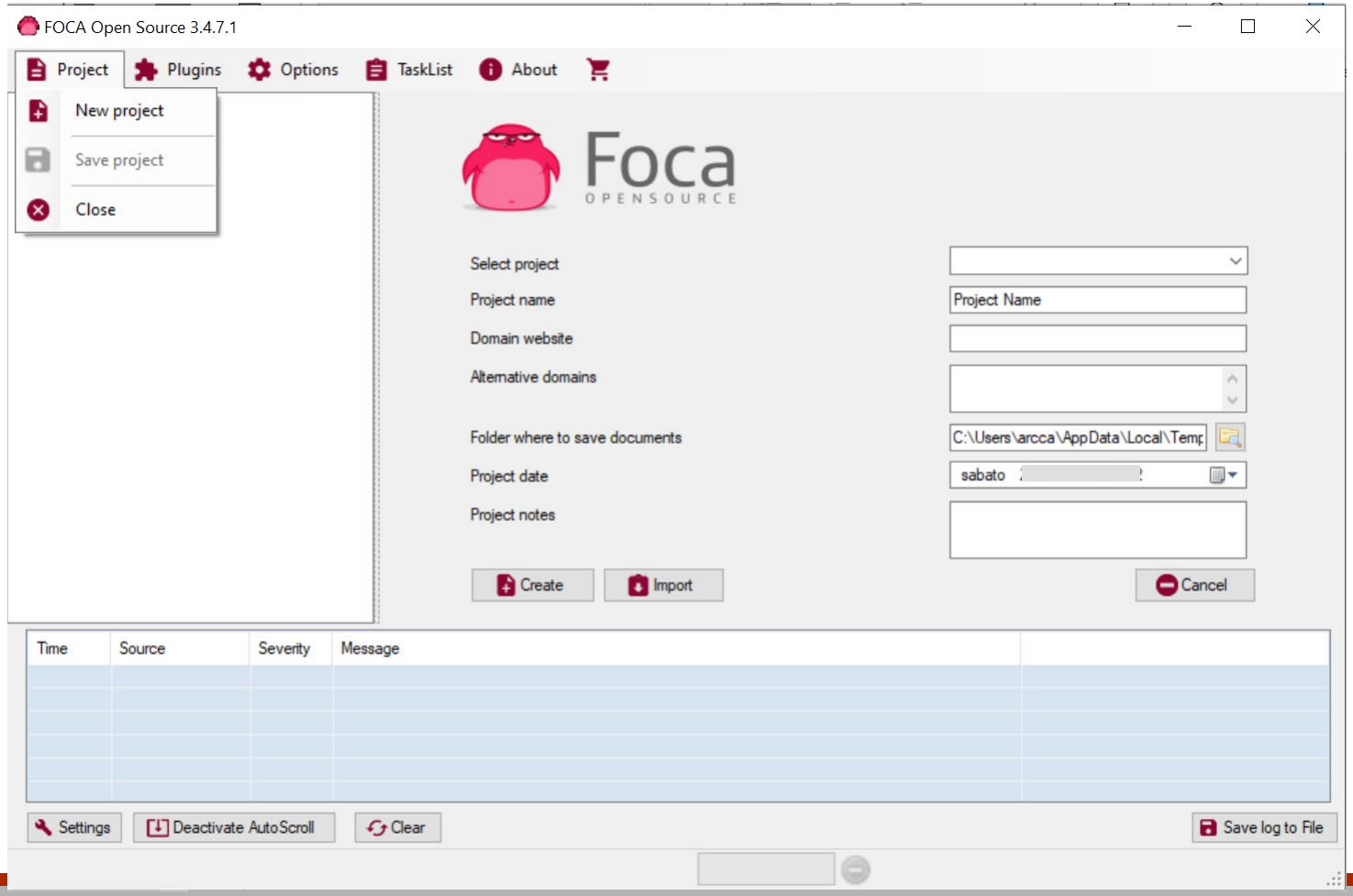
Utilizzo di Crawler

Ricerca di Metadati – FOCA



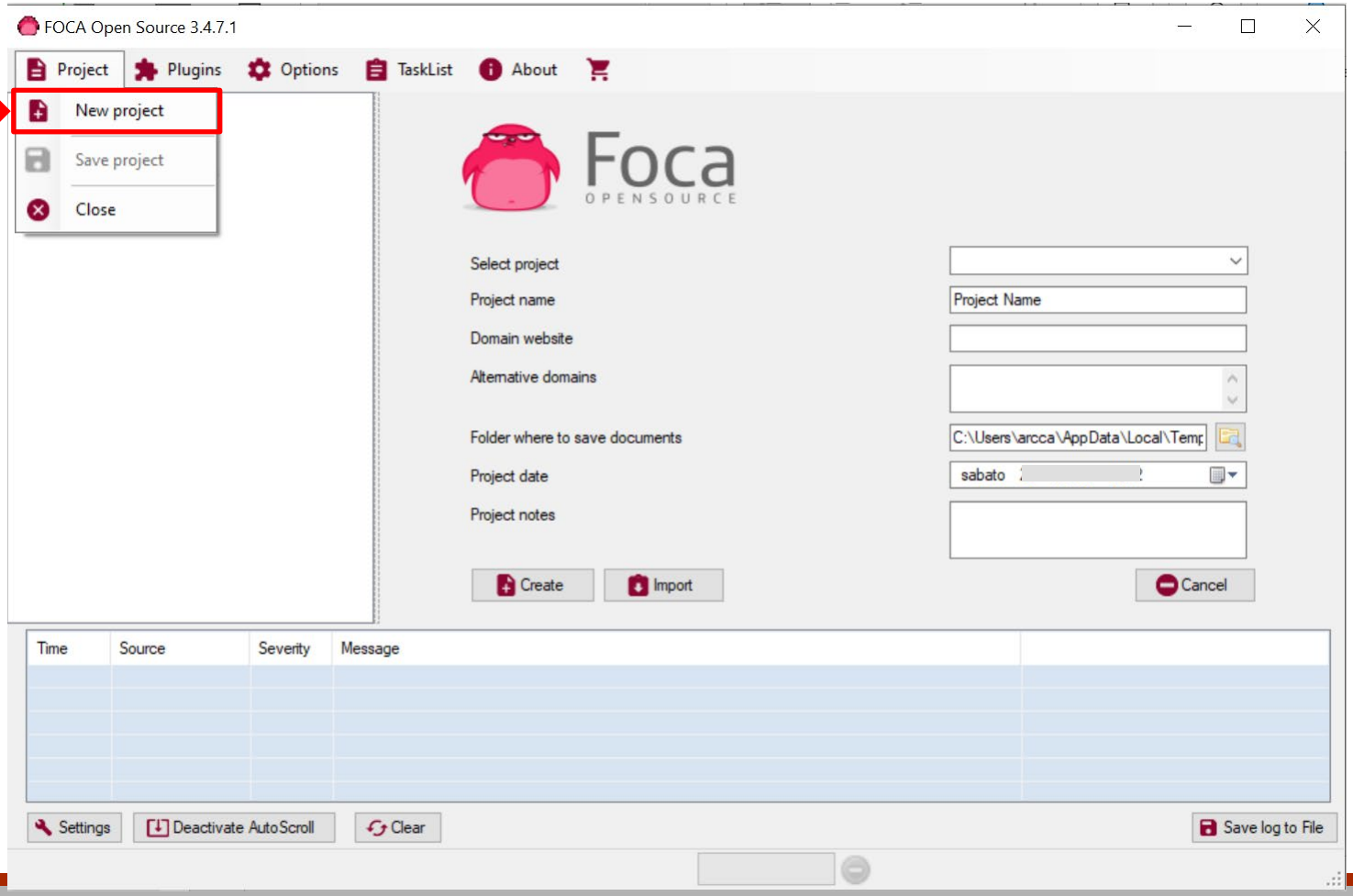
Utilizzo di Crawler

Ricerca di Metadati – FOCA



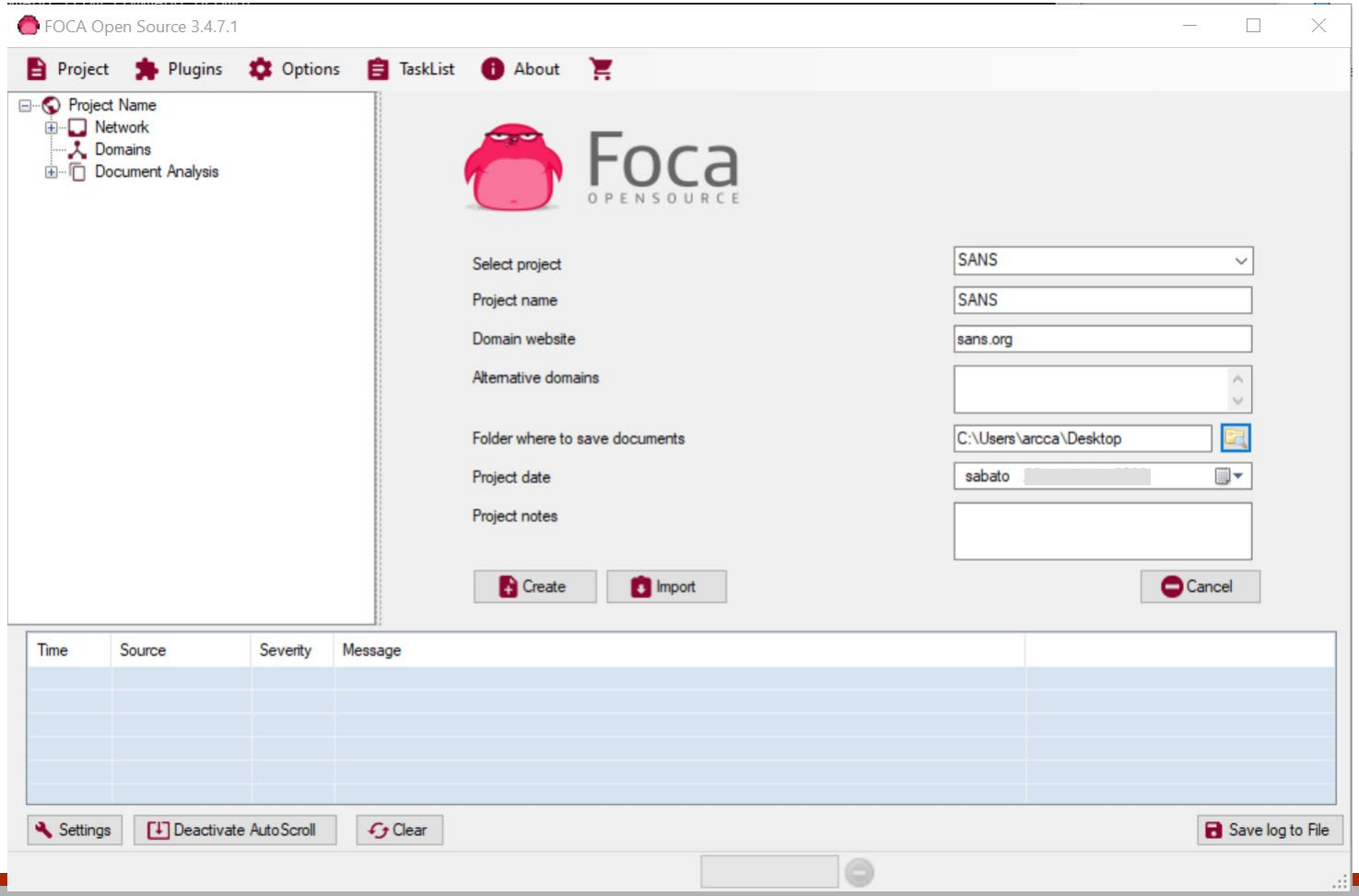
Utilizzo di Crawler

Ricerca di Metadati – FOCA



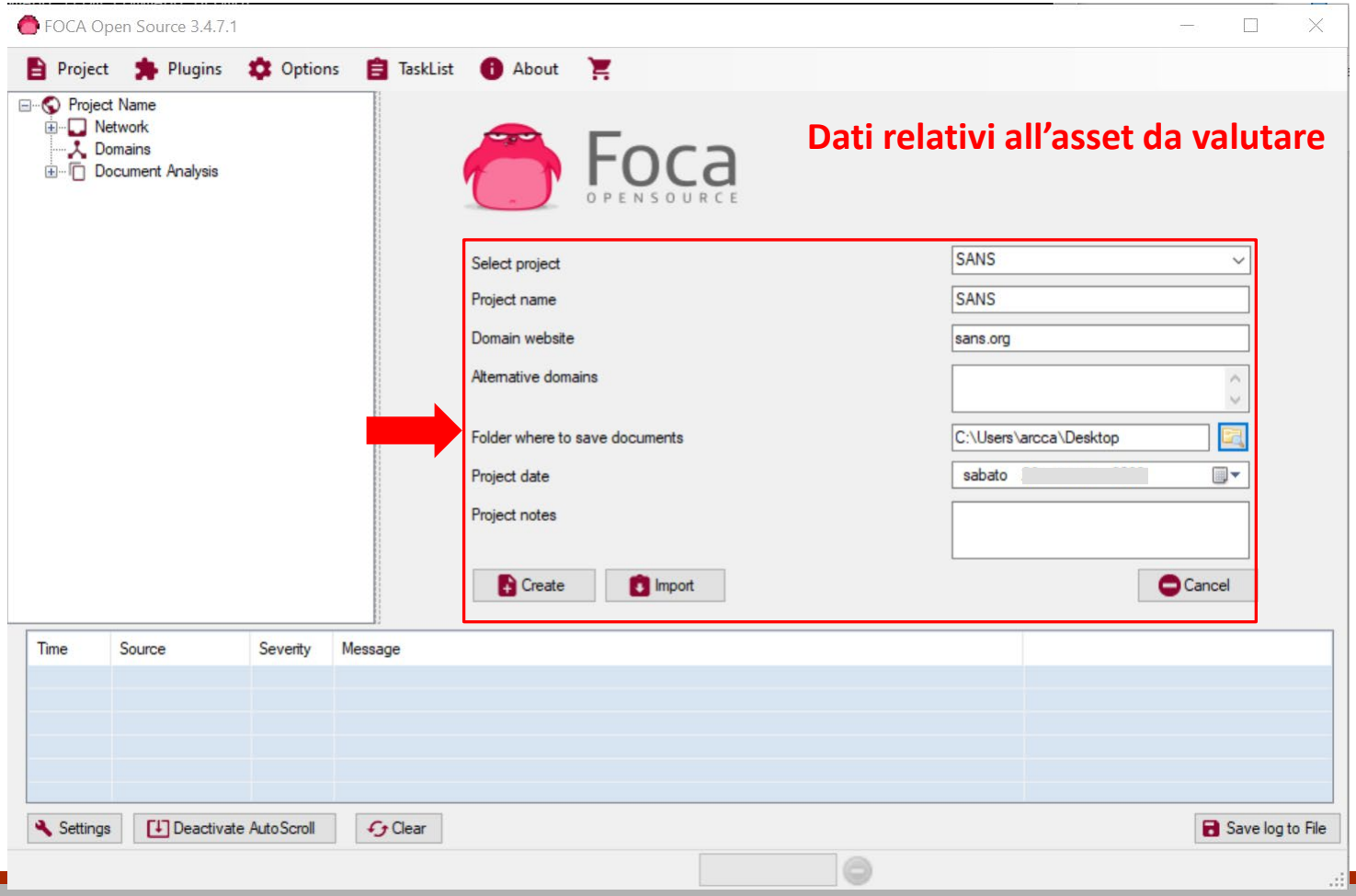
Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



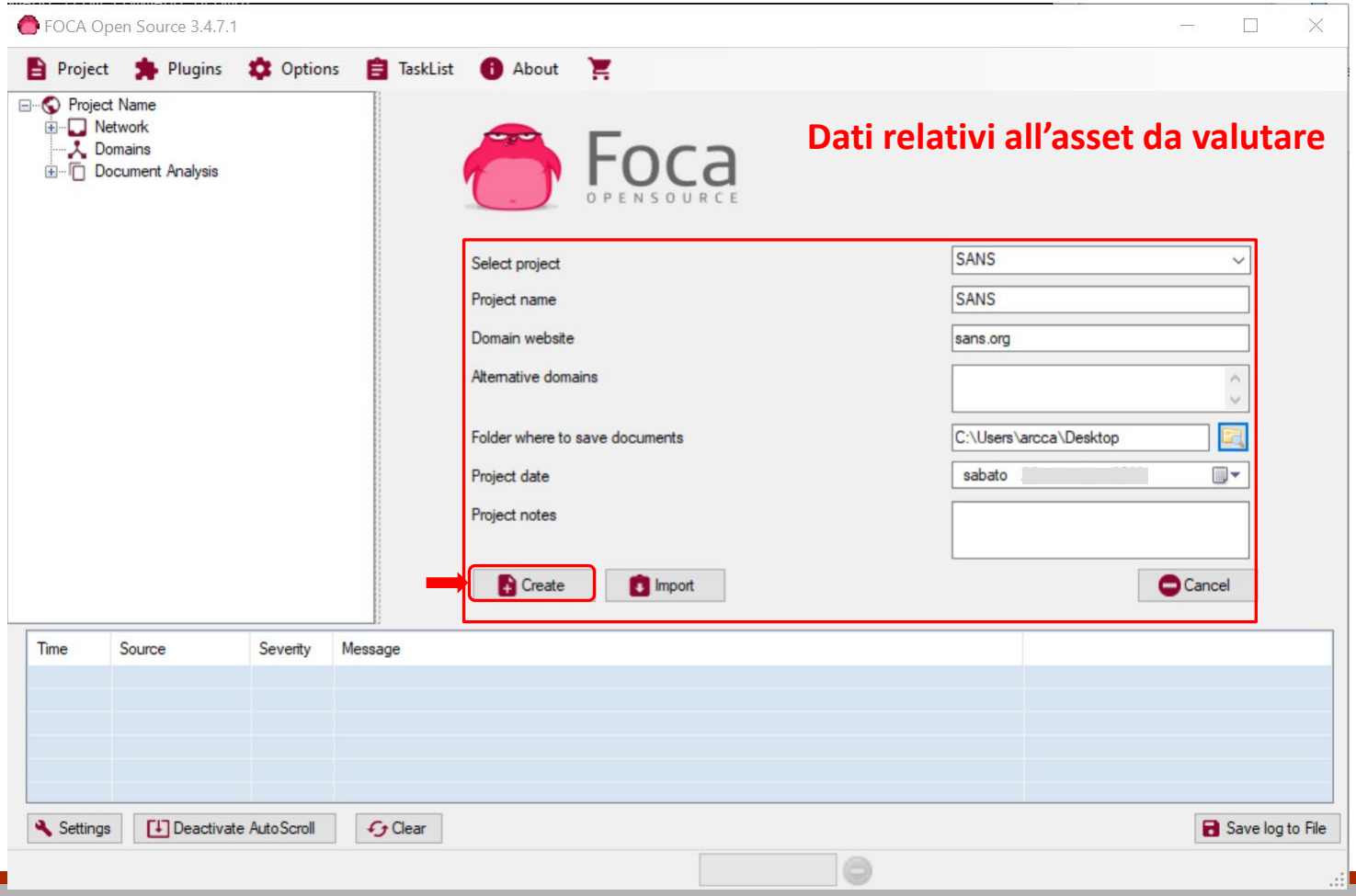
Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



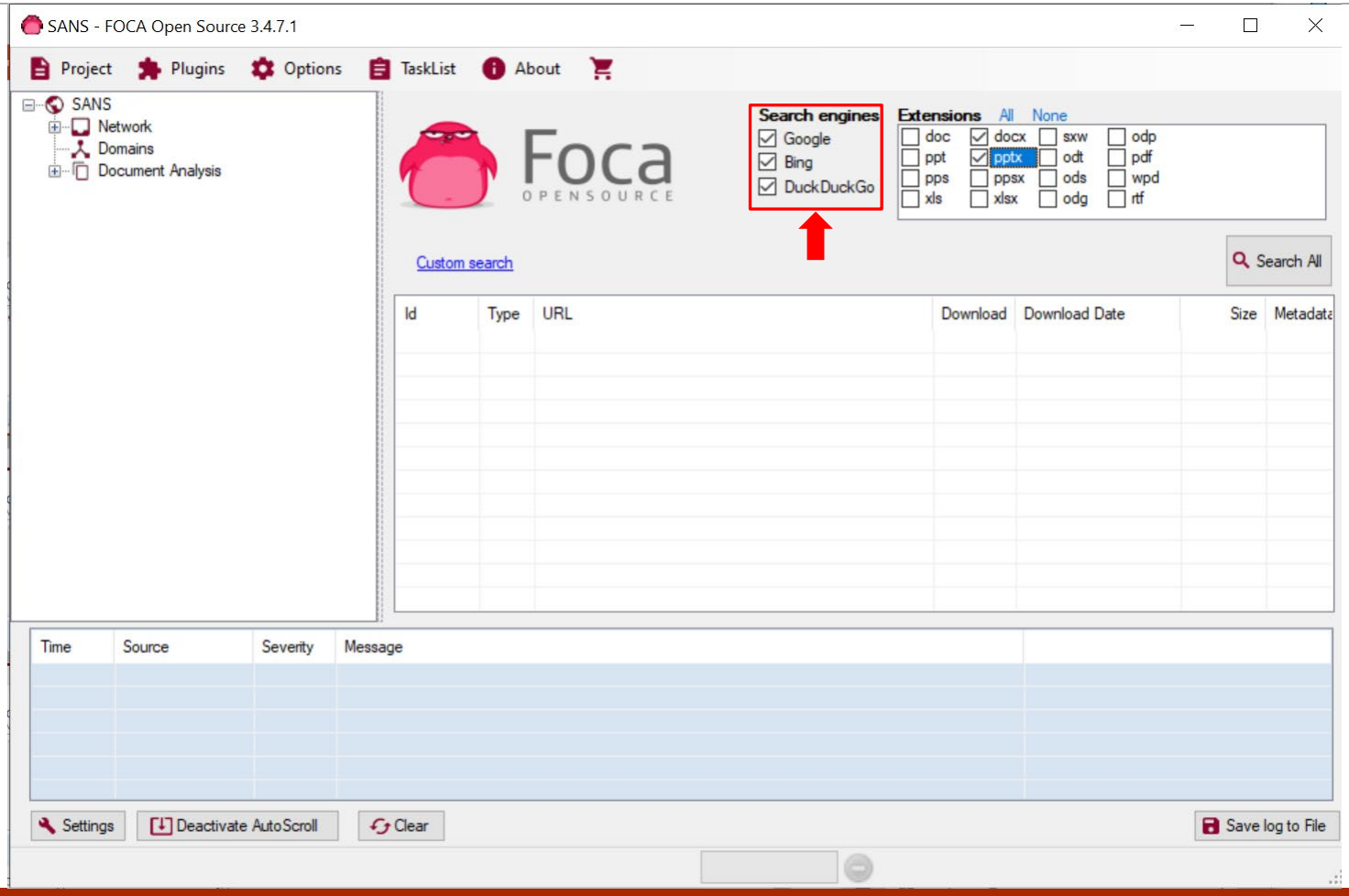
Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



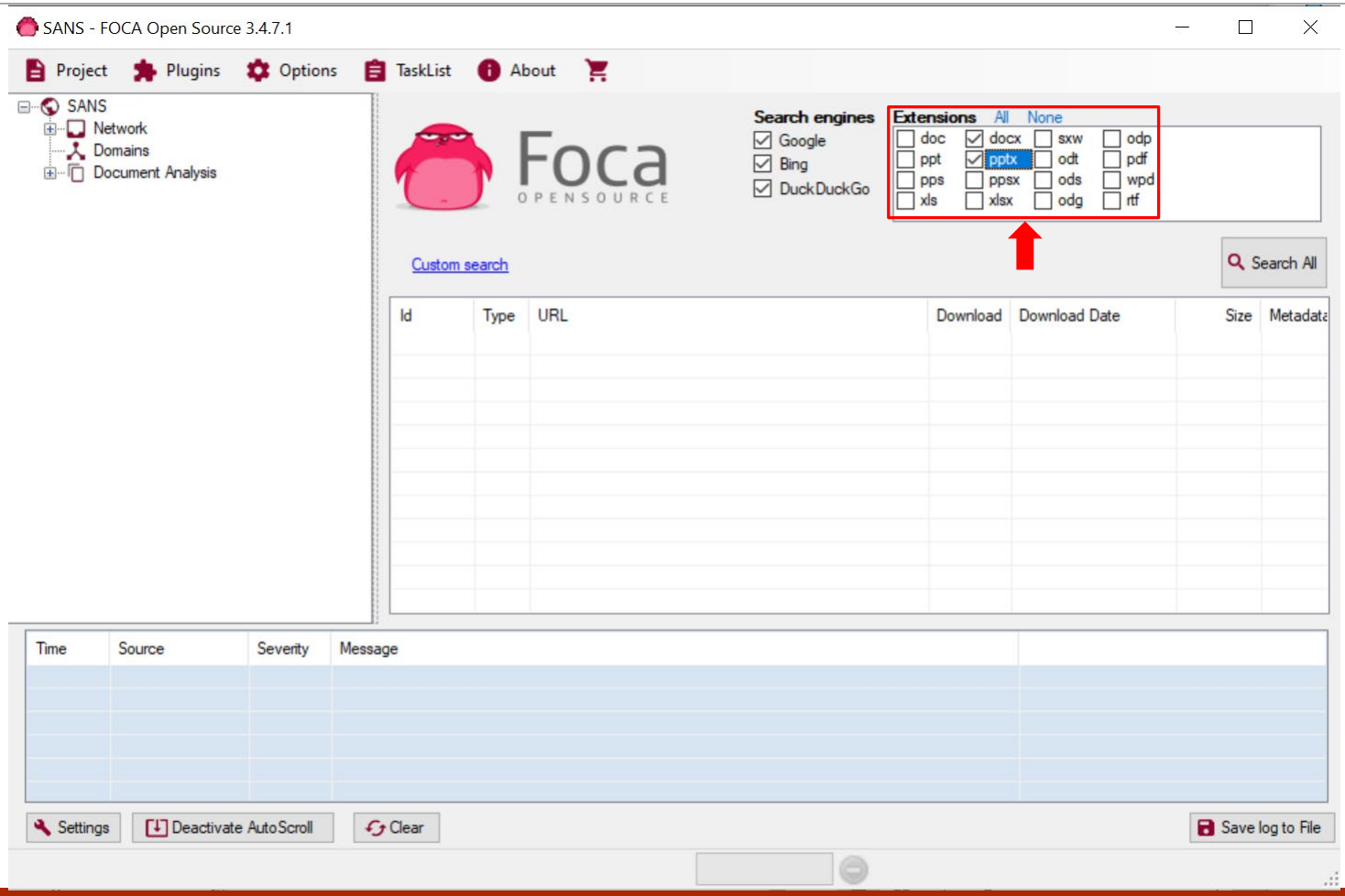
Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



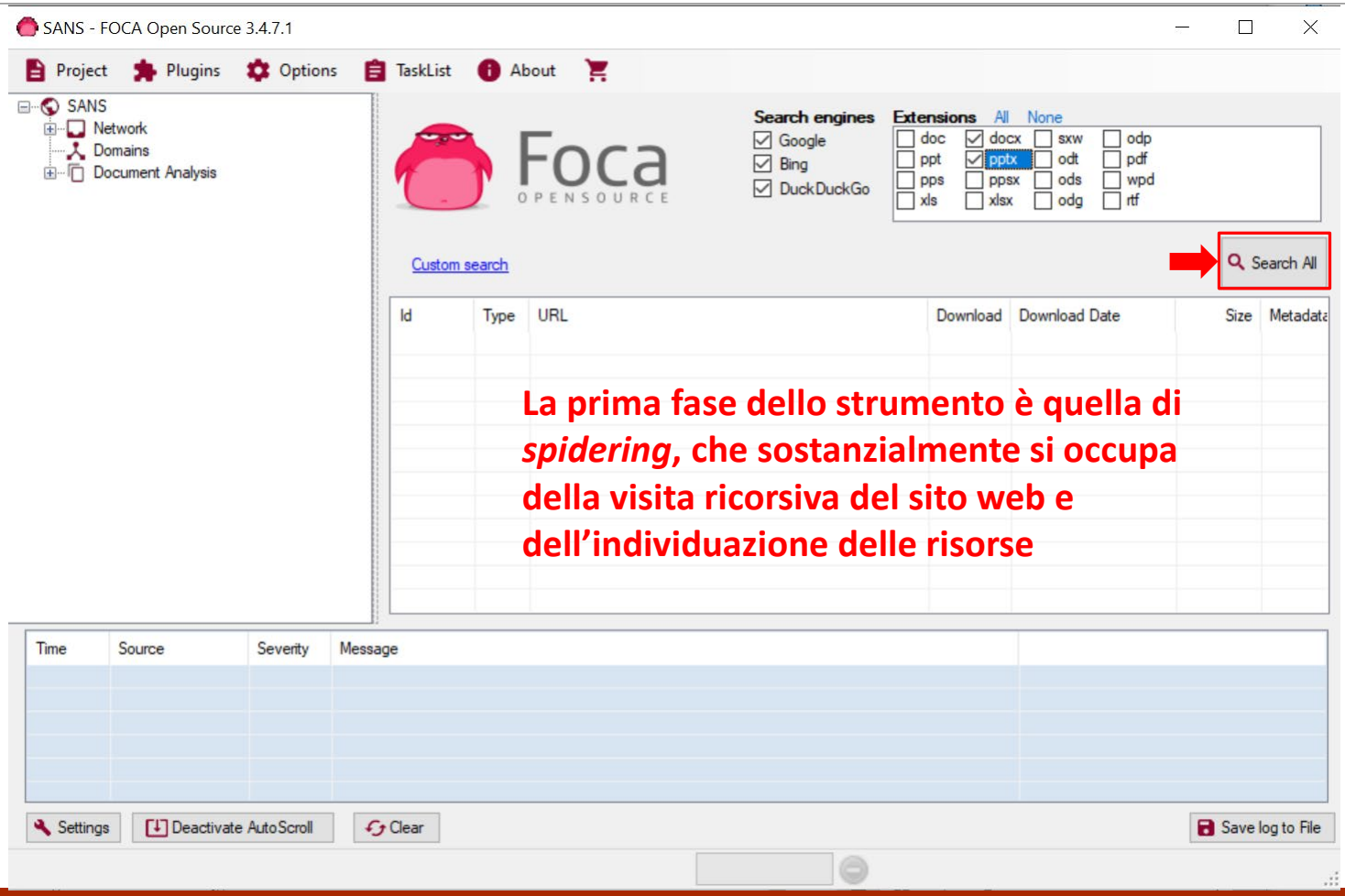
Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



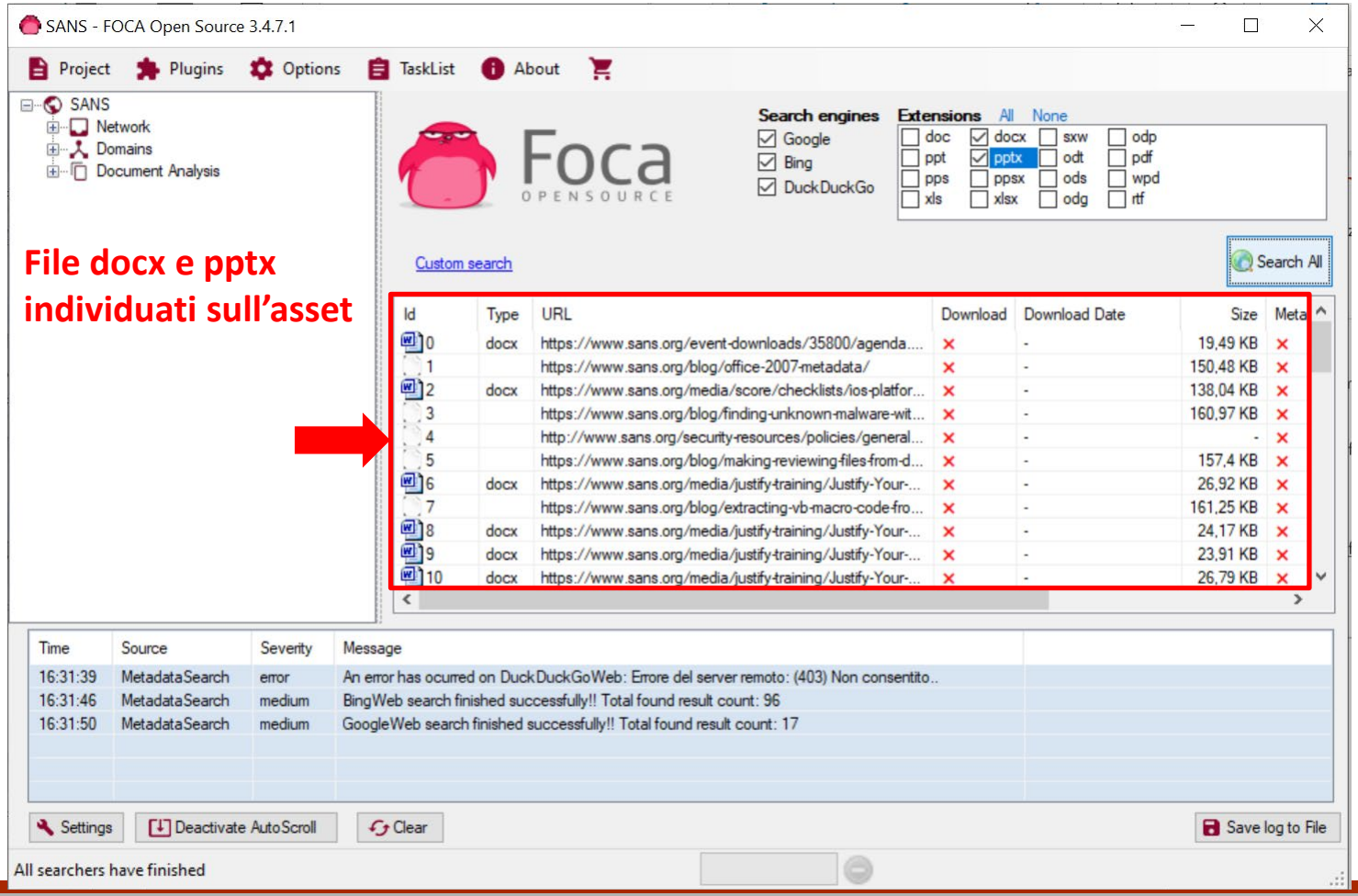
Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



Utilizzo di Crawler

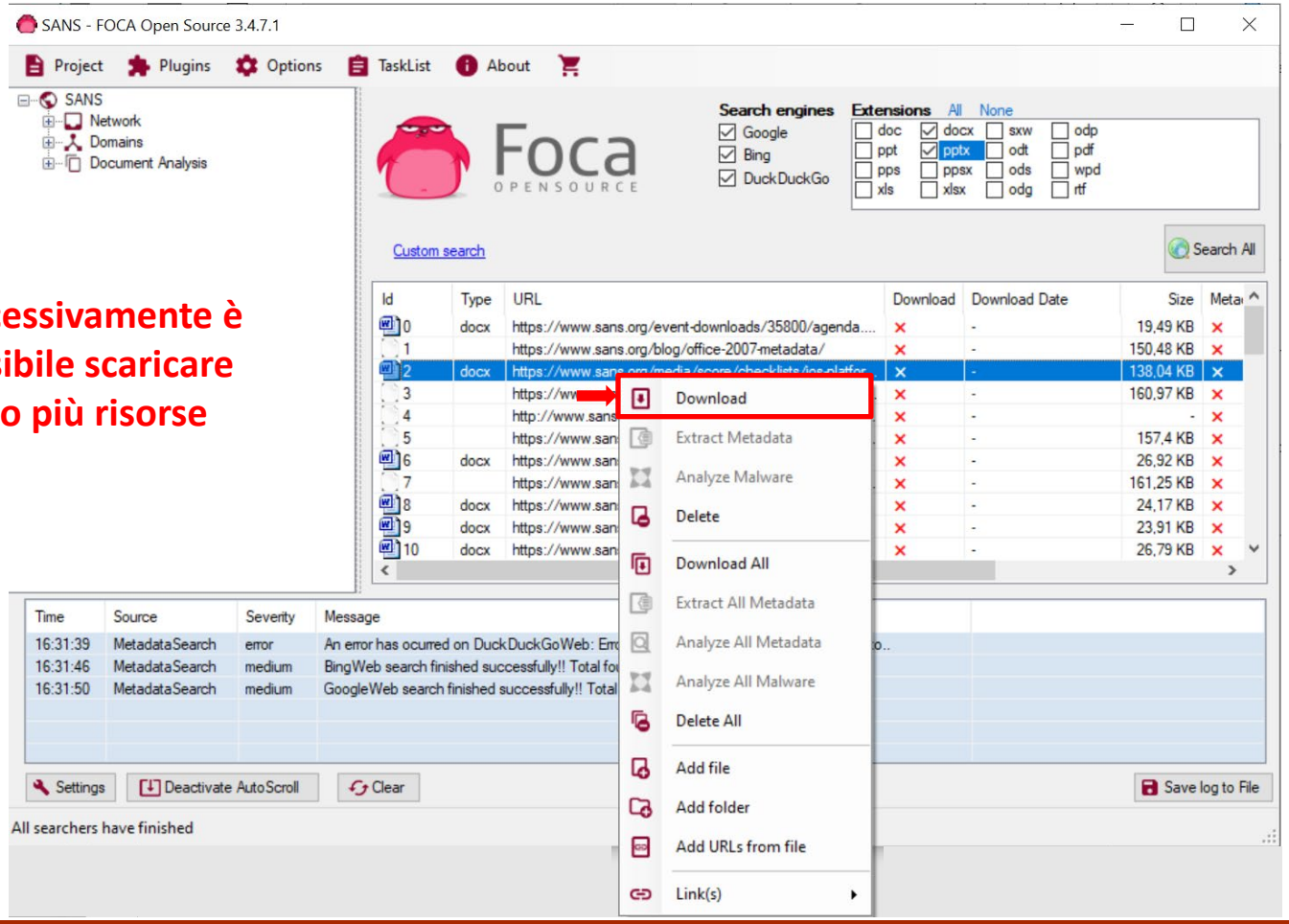
Ricerca di Metadati – FOCA – Esempio



Utilizzo di Crawler

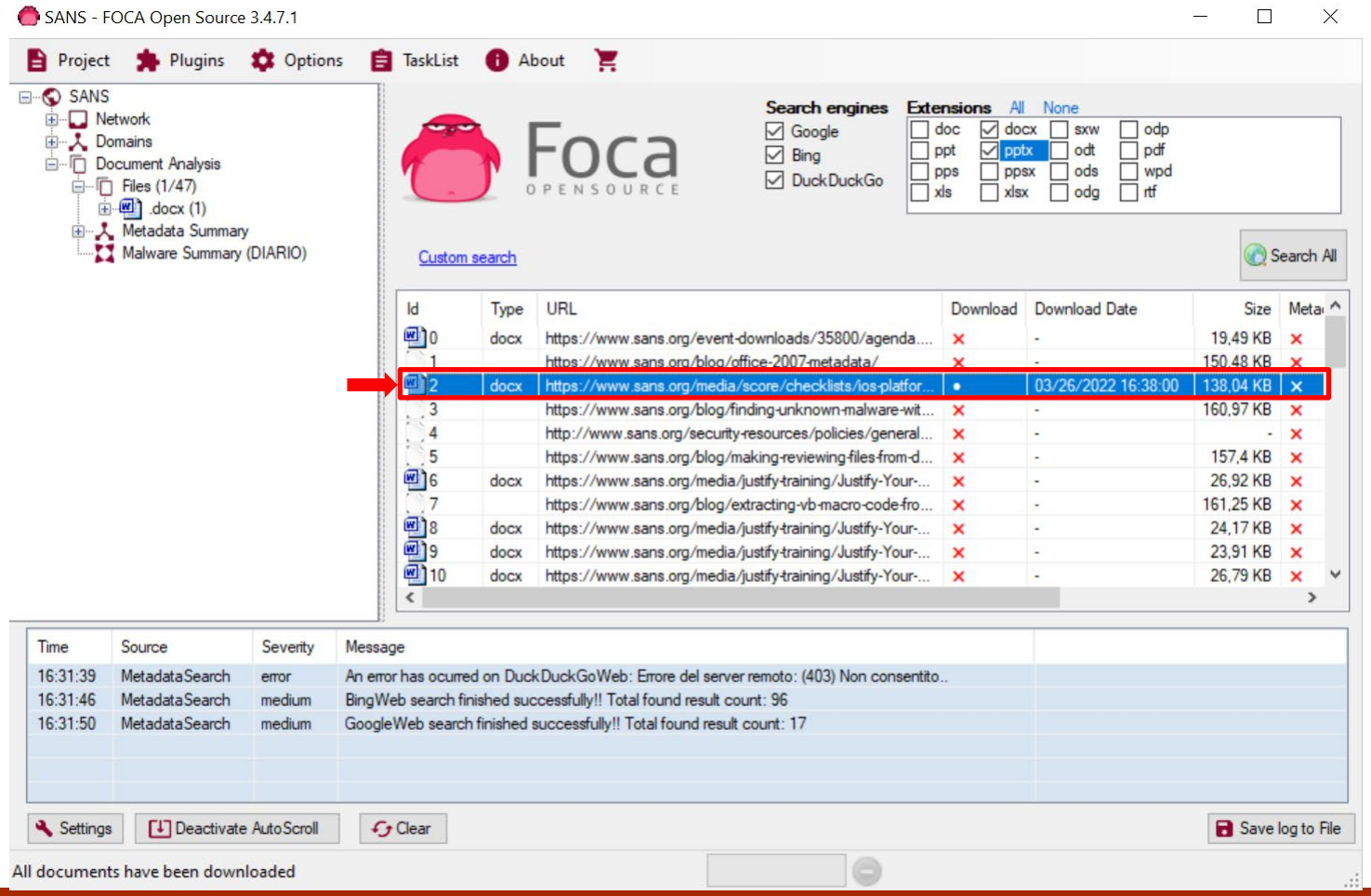
Ricerca di Metadati – FOCA – Esempio

Successivamente è possibile scaricare una o più risorse



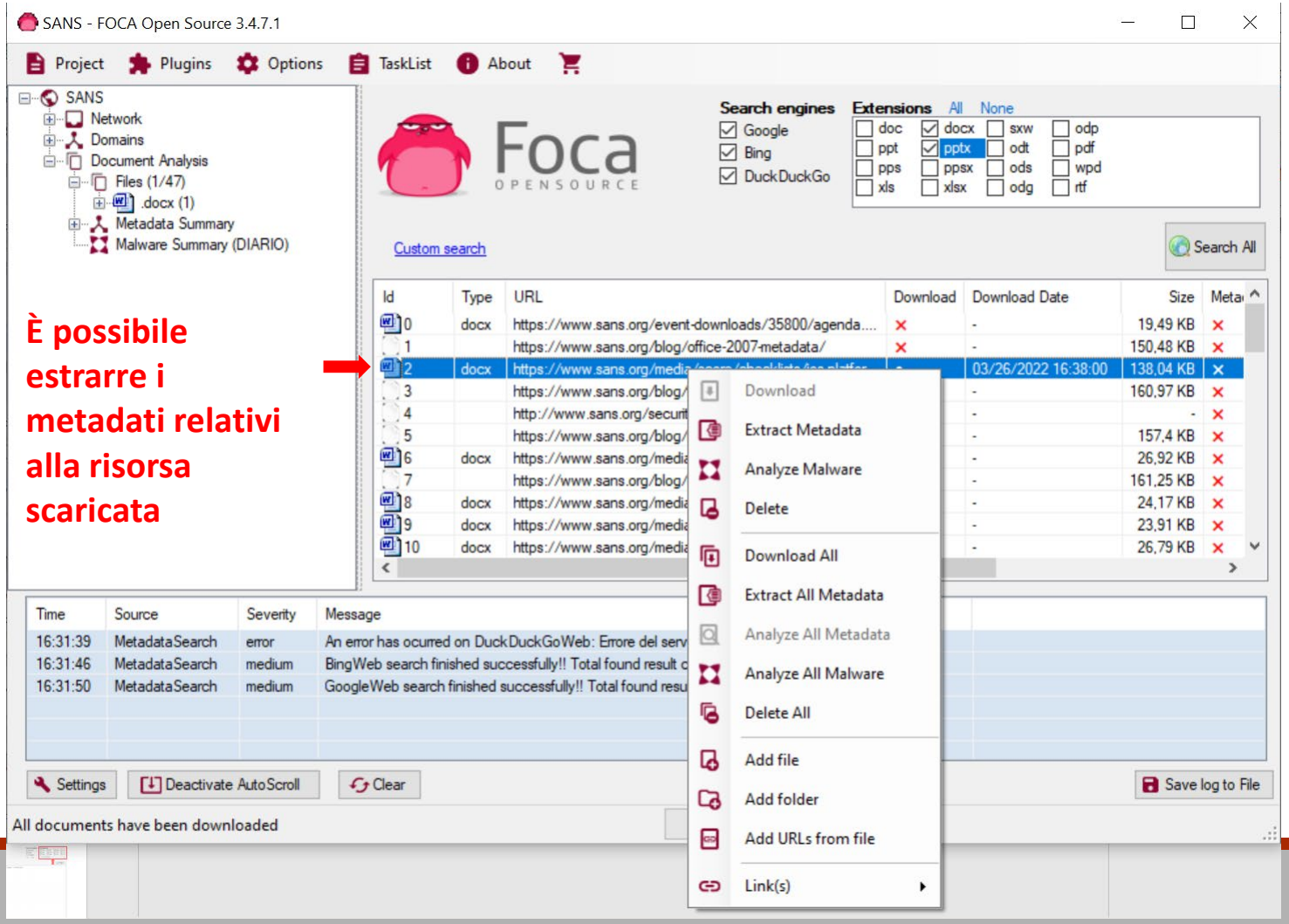
Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



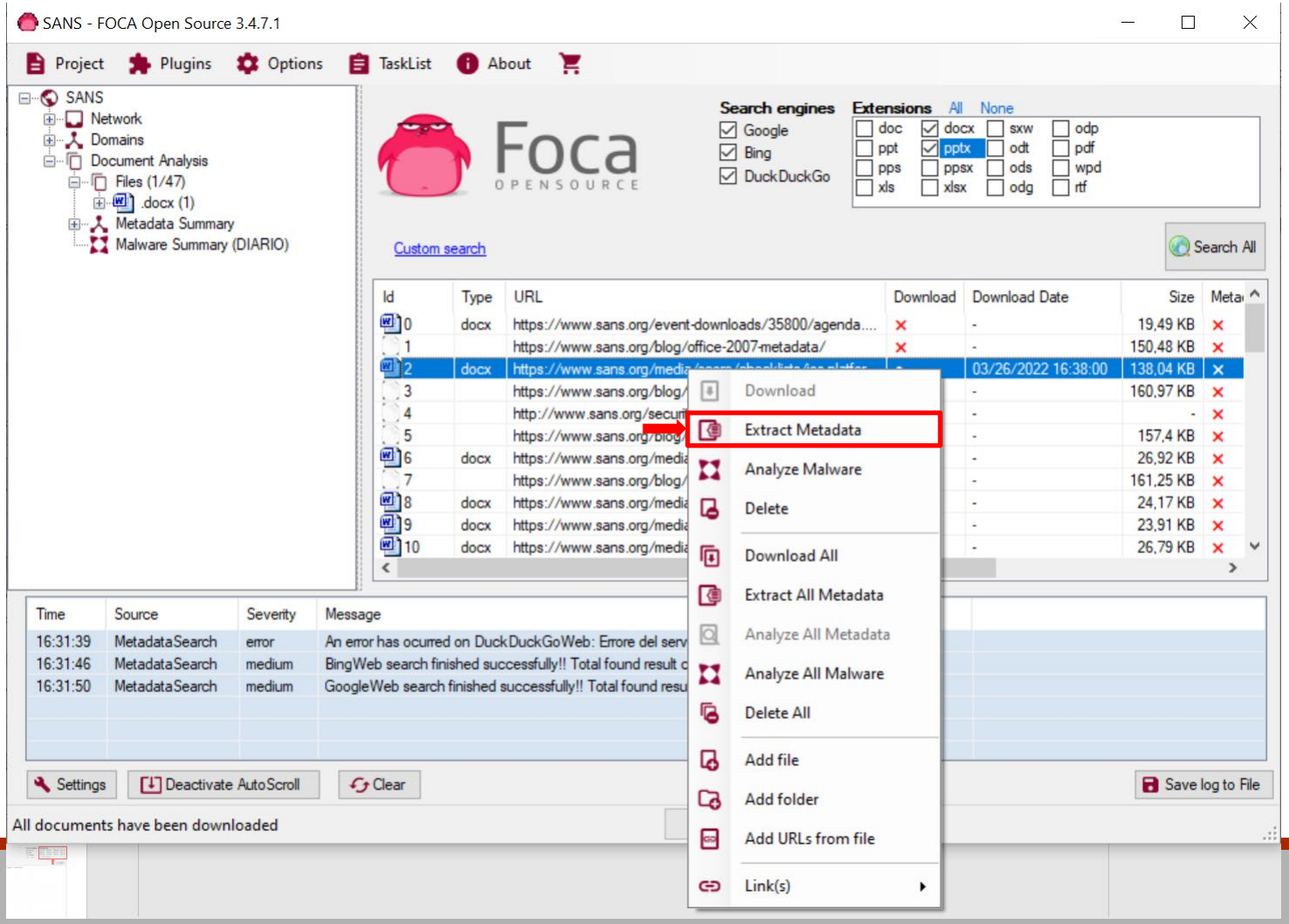
Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



Utilizzo di Crawler

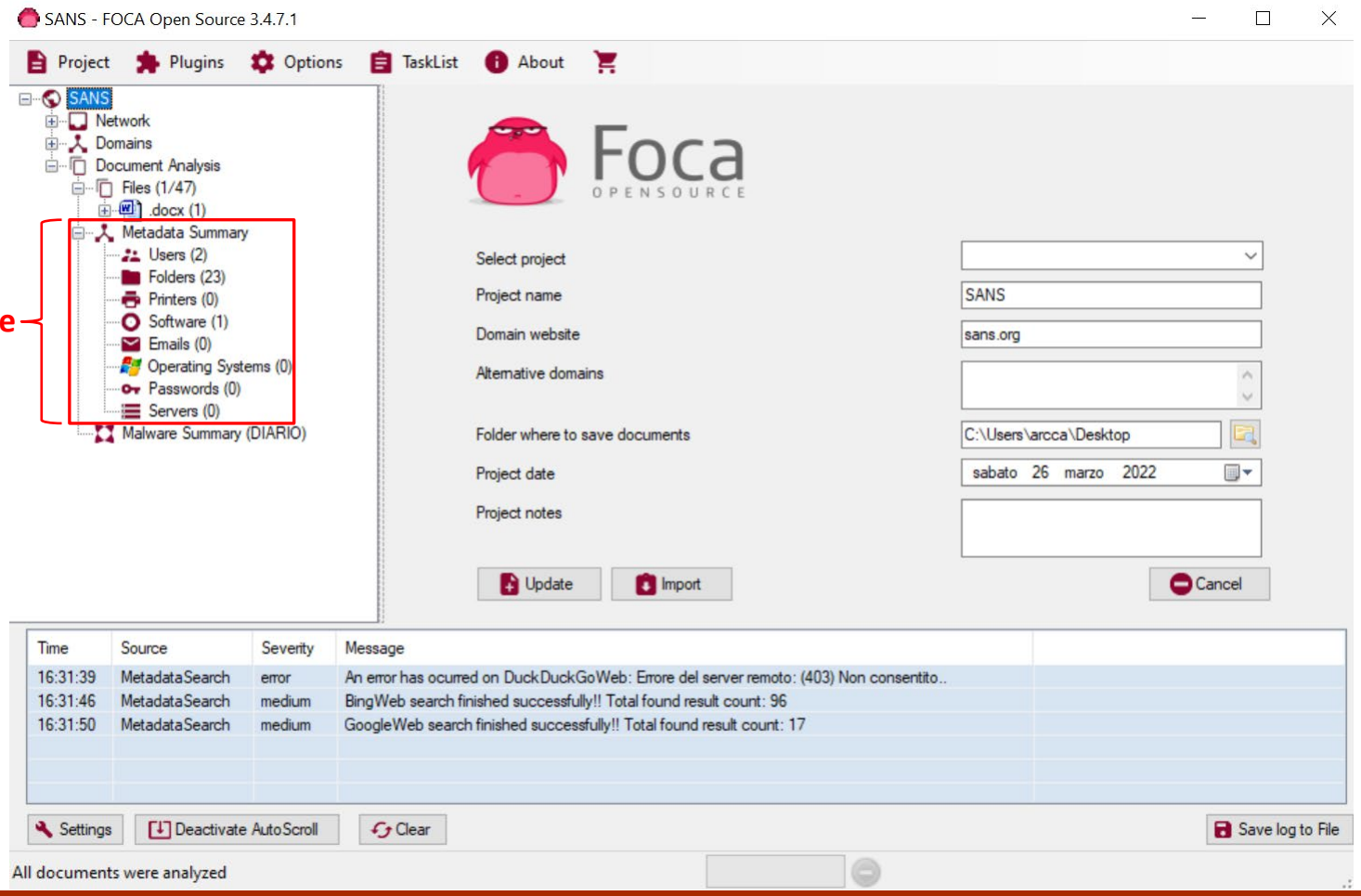
Ricerca di Metadati – FOCA – Esempio



Utilizzo di Crawler

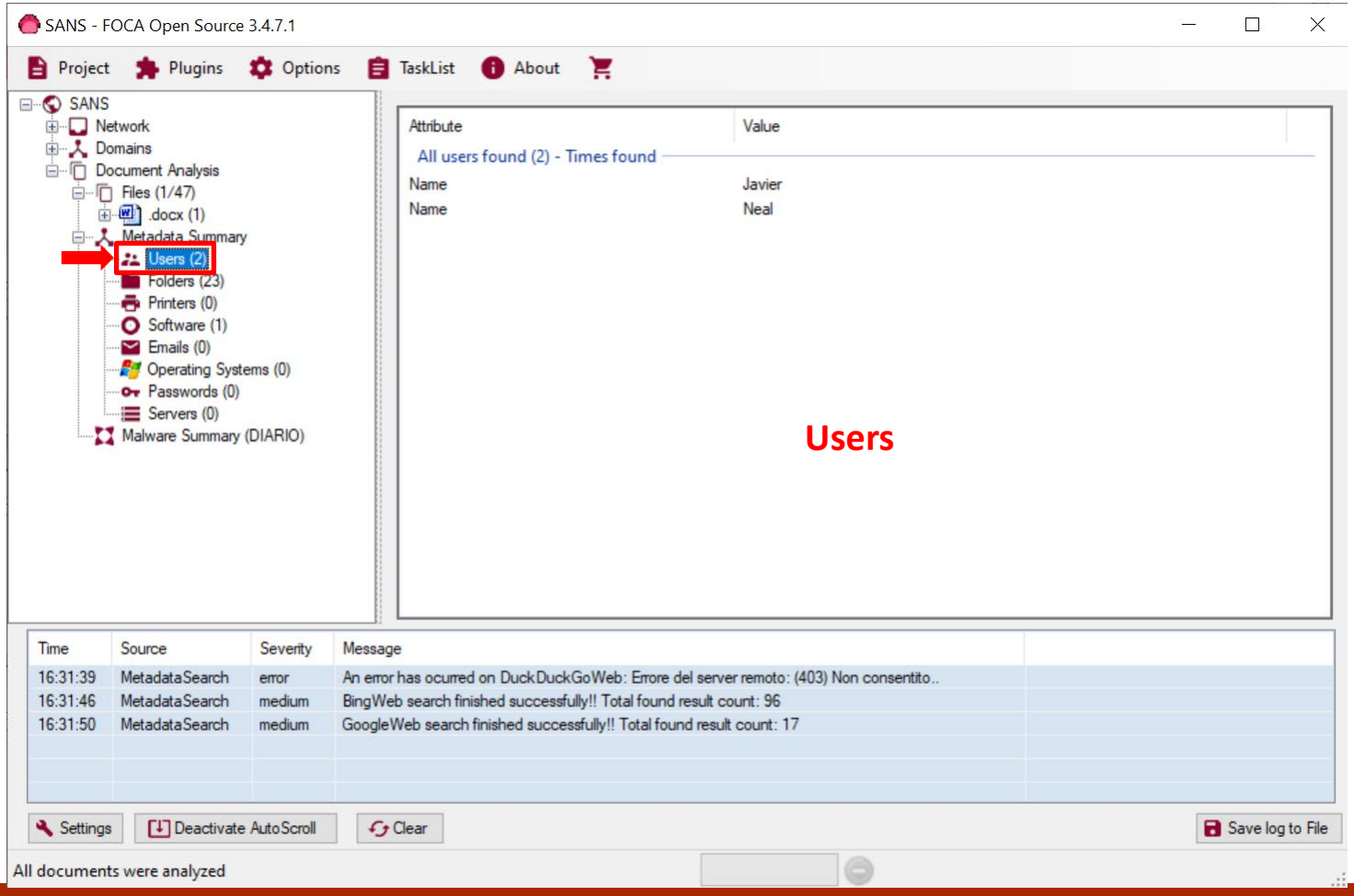
Ricerca di Metadati – FOCA – Esempio

Metadati estratti dal file selezionato



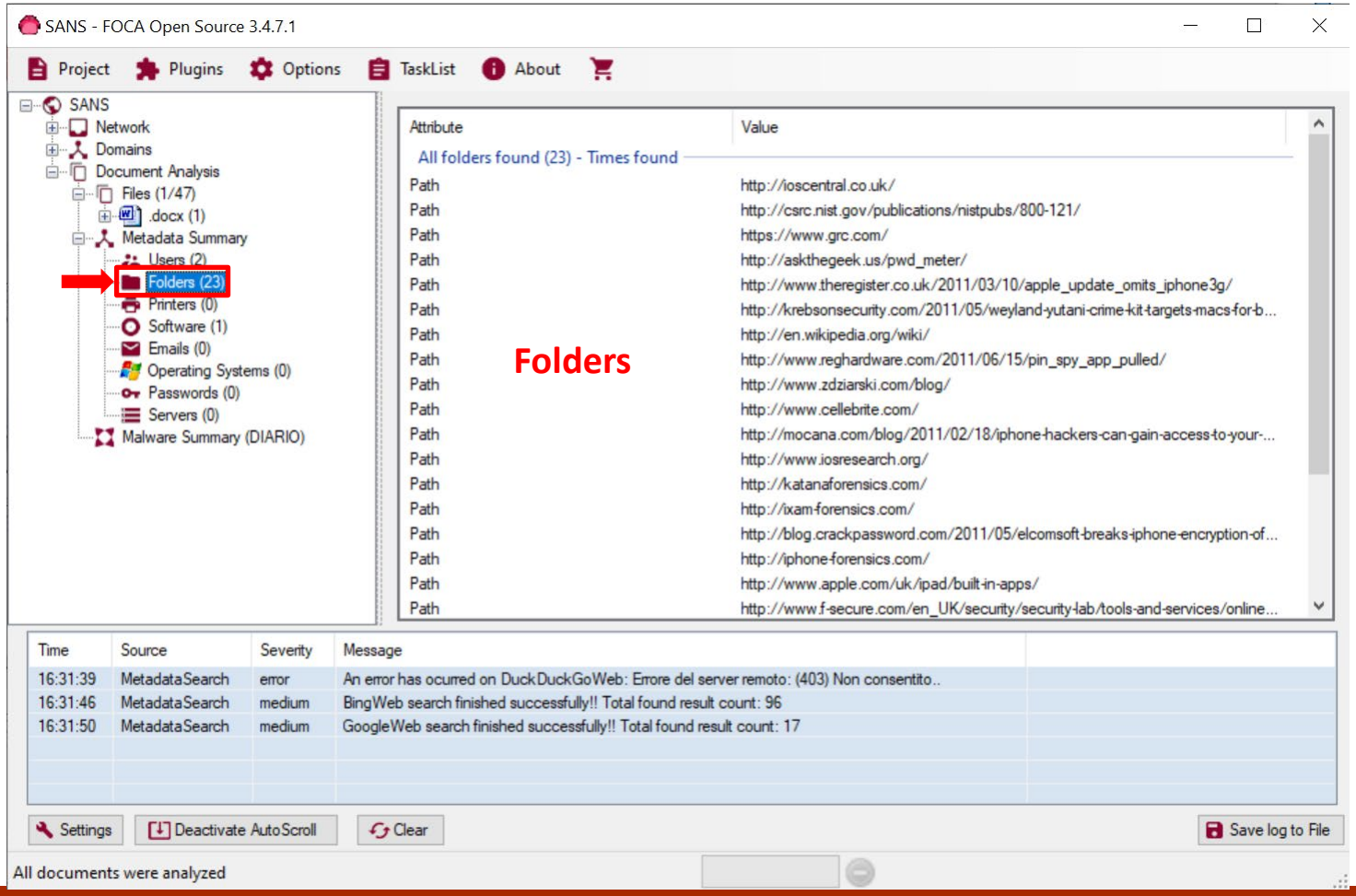
Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



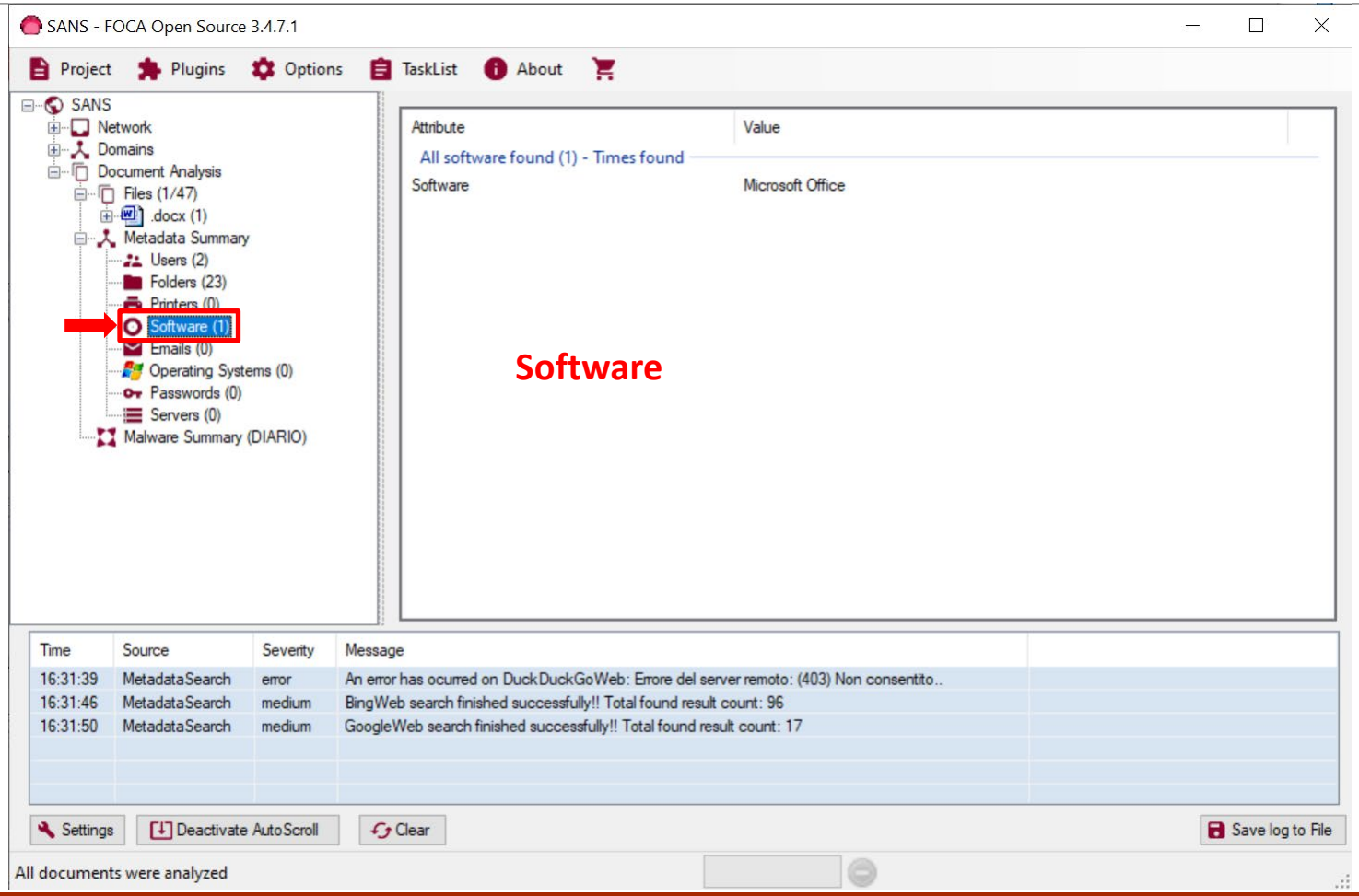
Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



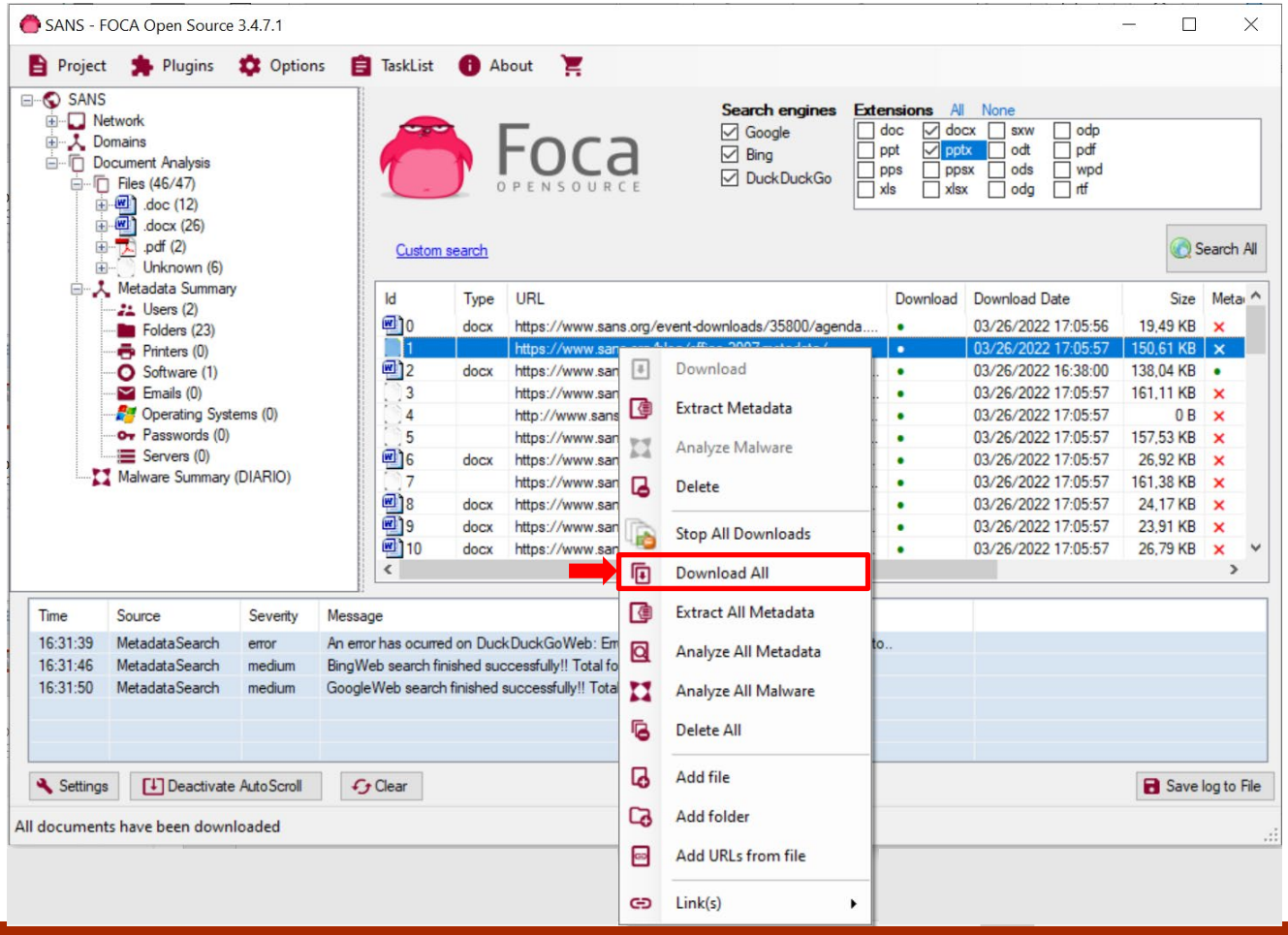
Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



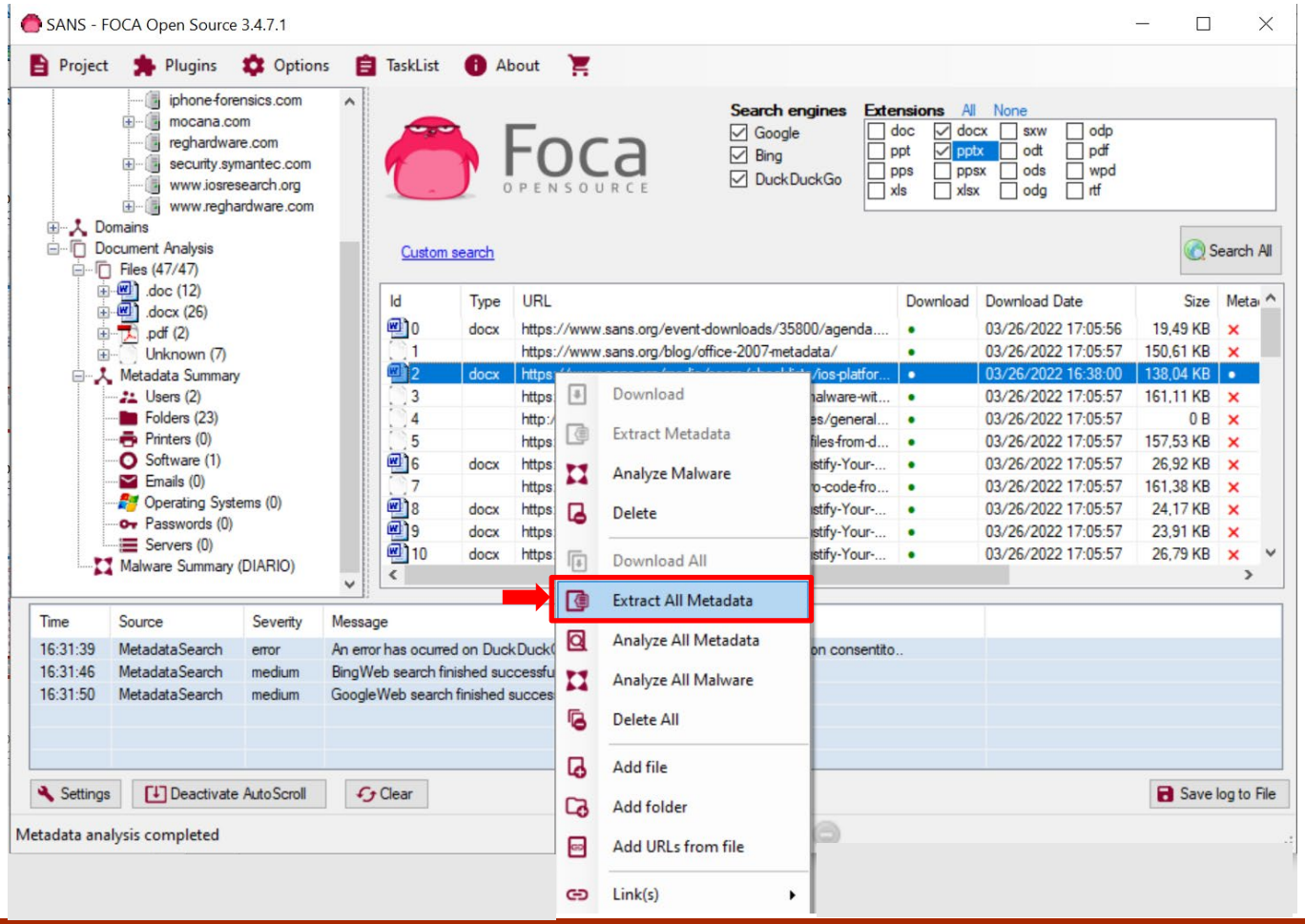
Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



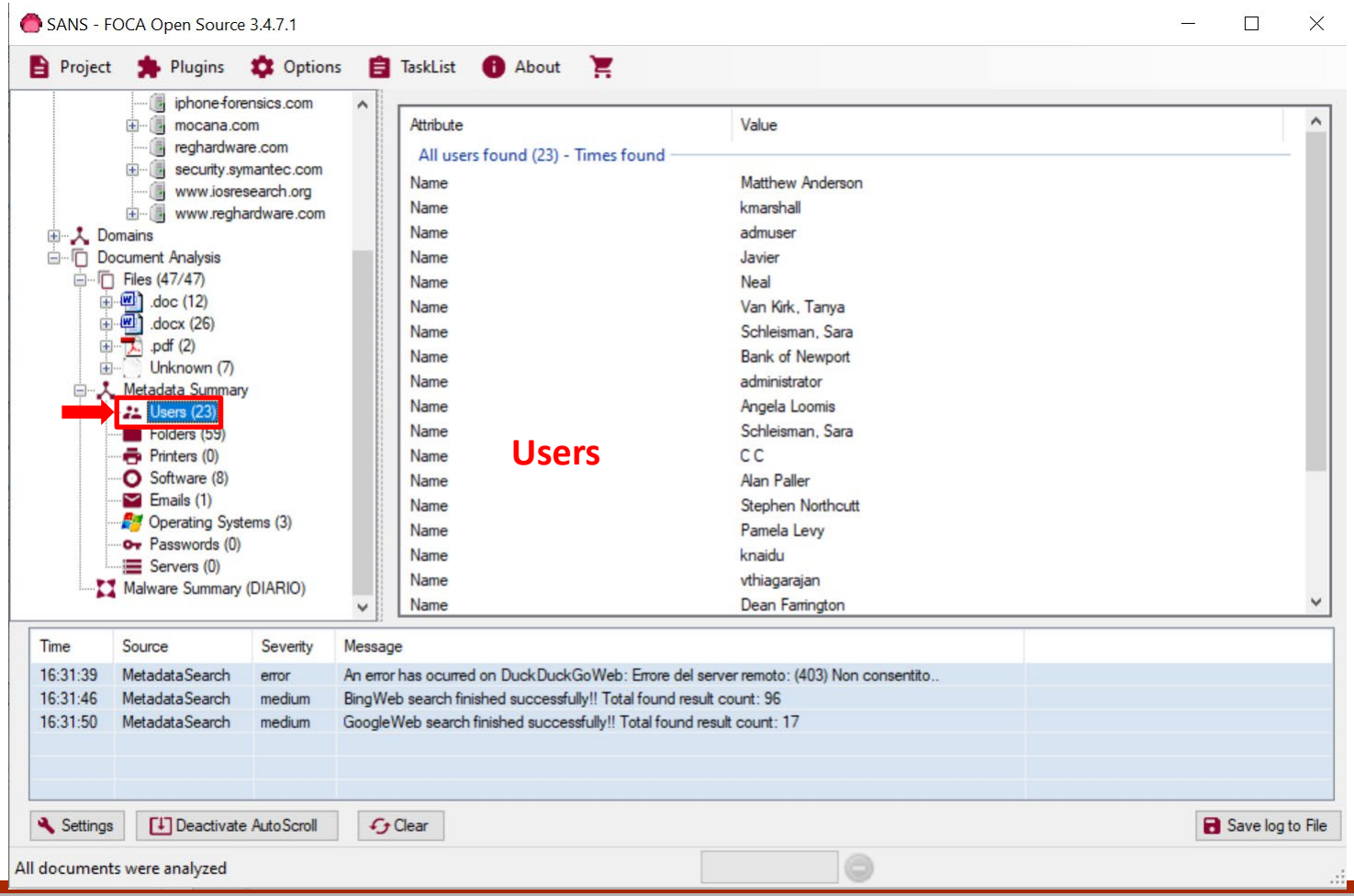
Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



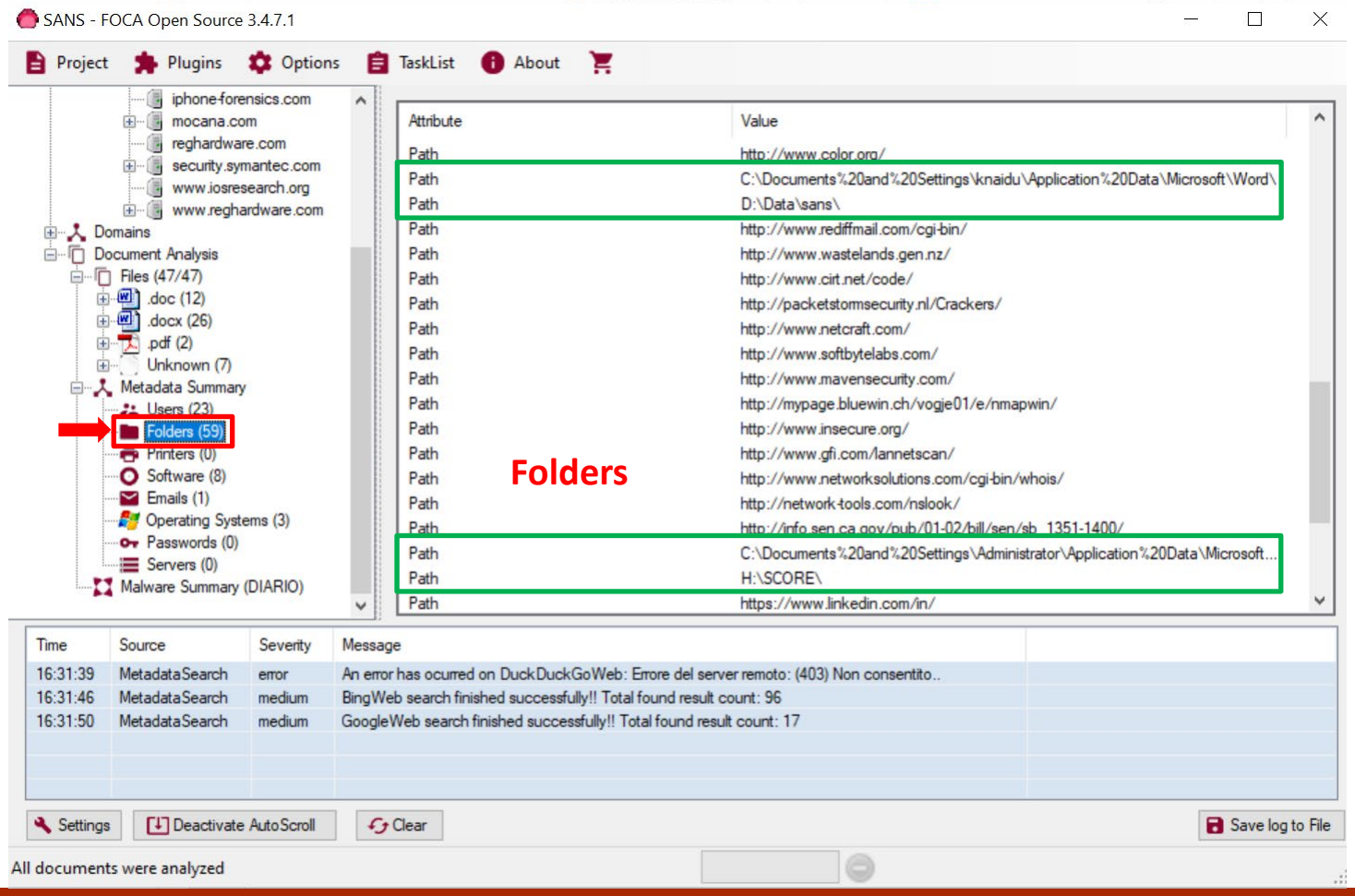
Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



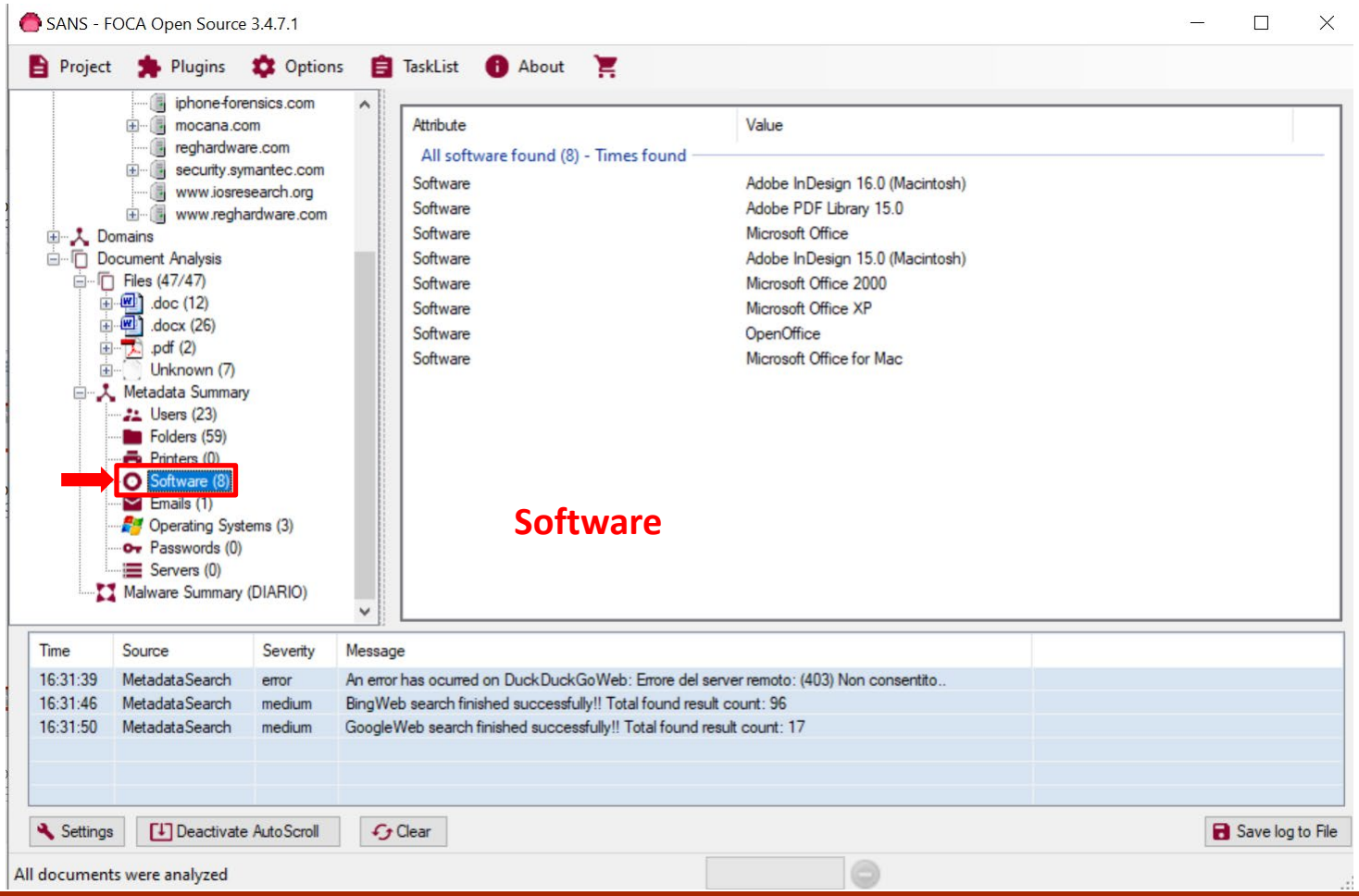
Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



Utilizzo di Crawler

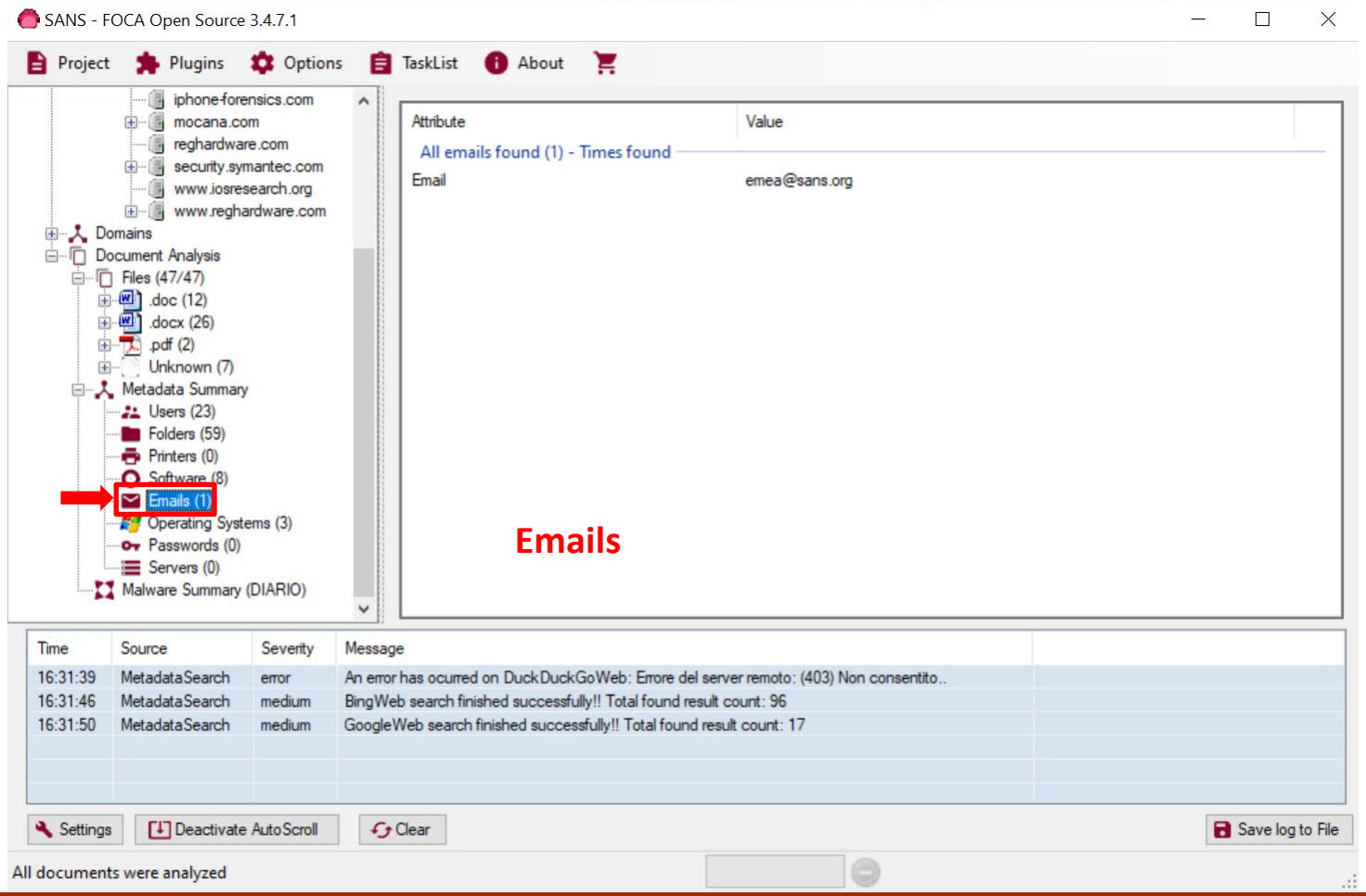
Ricerca di Metadati – FOCA – Esempio



Software

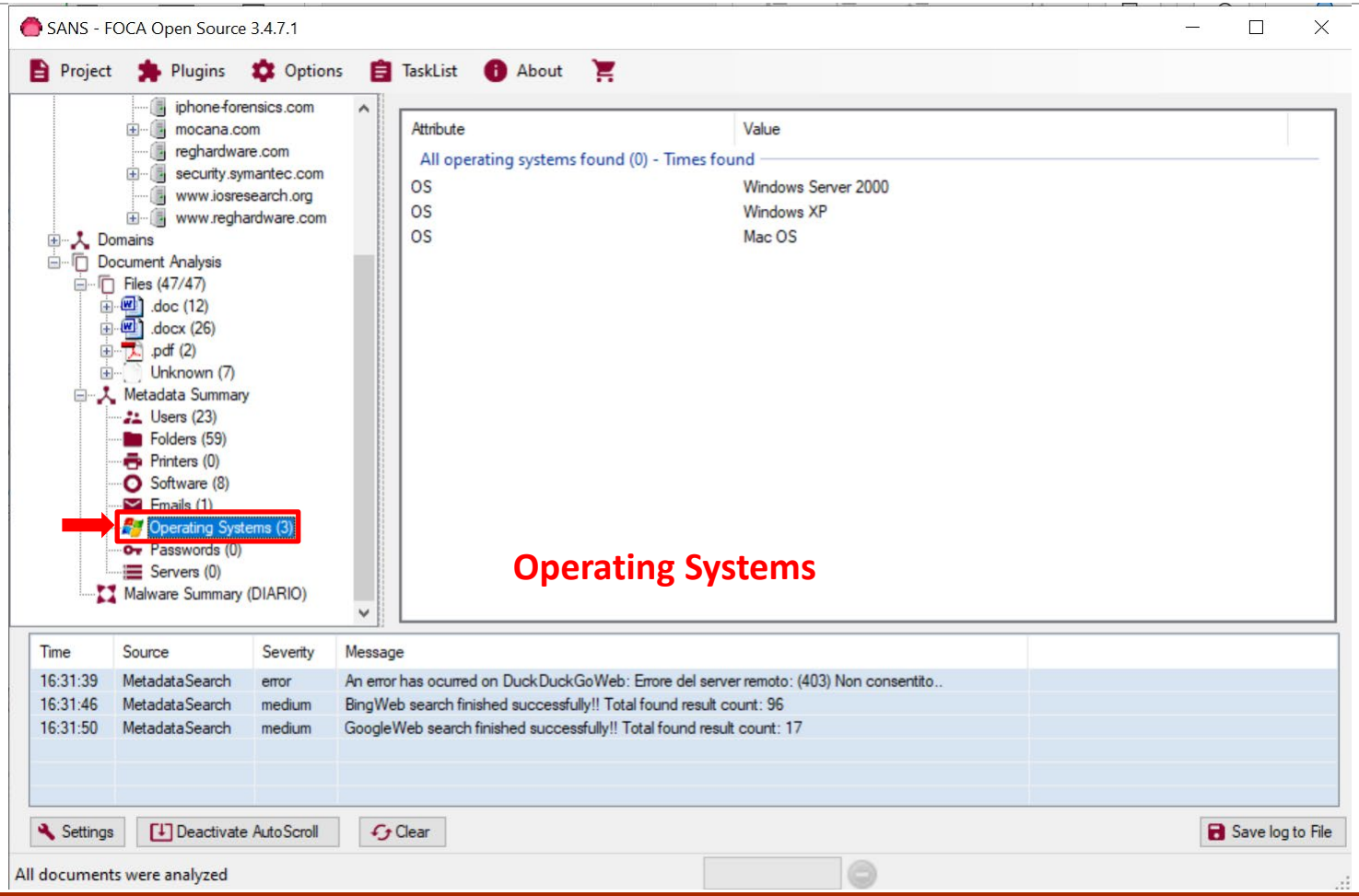
Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



Utilizzo di Crawler

Ricerca di Metadati – Metagoofil

- Strumento basato su Google Dork che permette di scaricare determinati tipi di file dall'asset
  - Originariamente permetteva anche di ottenere i relativi metadati

- Supporta vari tipi di file
  - *Word document* (*.docx*, *.doc*)
  - *Spreadsheet document* (*.xlsx*, *.xls*, *.ods*)
  - *Presentation file* (*.pptx*, *.ppt*, *.odp*)
  - *PDF file* (*.pdf*)

Utilizzo di Crawler

Ricerca di Metadati – Metagoofil

- Metagoofil effettua le seguenti azioni
  1. Cerca nel dominio analizzato alcuni o tutti i tipi di file mostrati in precedenza
     - Utilizzando query Google
  2. Scarica sul disco locale tutti i file trovati

- I file recuperati tramite Metagoofil possono essere successivamente valutati tramite altri strumenti per l'analisi dei metadati
  - Ad es., https://www.metadata2go.com/

Utilizzo di Crawler

Ricerca di Metadati – Metagoofil

- Le informazioni ricavate mediante Metagoofil possono essere di aiuto per le fasi successive del processo di penetration testing
  - In particolare per il Social Engineering ed il Post-Exploitation

- Metagoofil non è installato di default in Kali Linux
  - `apt-get install metagoofil`

Utilizzo di Crawler

Ricerca di Metadati – Metagoofil

- Per maggiori informazioni sul comando **`metagoofil`** è sufficiente digitarlo
  - **`metagoofil -h`**

```
usage: metagoofil.py [-h] -d DOMAIN [-e DELAY] [-f] [-i URL_TIMEOUT]
                     [-l SEARCH_MAX] [-n DOWNLOAD_FILE_LIMIT] [-o SAVE_DIRECTORY]
                     [-r NUMBER_OF_THREADS] -t FILE_TYPES [-u [USER_AGENT]] [-w]

Metagoofil - Search and download specific filetypes

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN             Domain to search.
  -e DELAY              Delay (in seconds) between searches. If it's too small
                        Google may block your IP, too big and your searchmay take
                        a while. Default: 30.0
  -f                    Save the html links to html_links_<TIMESTAMP>.txt file.
  -i URL_TIMEOUT        Number of seconds to wait before timeout for
                        unreachable/stale pages. Default: 15
  -l SEARCH_MAX         Maximum results to search. Default: 100
  -n DOWNLOAD_FILE_LIMIT
                        Maximum number of files to download per filetype. Default
                        100
  -o SAVE_DIRECTORY     Directory to save downloaded files. Default is current
                        working directory, "."
  -r NUMBER_OF_THREADS  Number of downloader threads. Default: 8
  -t FILE_TYPES         file_types to download
                        (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx). To search all
                        17,576 three-letter file extensions, type "ALL"
  -u [USER_AGENT]       User-Agent for file retrieval against -d domain.
```

Utilizzo di Crawler

Ricerca di Metadati – Metagoofil – Esempio

- **`metagoofil -d nist.gov -t pdf,doc -l 30 -n 30 -o metagoofil_nist -w`**
  - **`-d nist.gov`** Dominio su cui effettuare la ricerca
  - **`-t doc,pdf`** Tipi di file da scaricare (*doc* e *pdf*)
  - **`-l 30`** Limite sul numero di risultati da cercare. Di default è *100*
  - **`-n 30`** Limite sul numero di file da scaricare. Di default è *100*
  - **`-o metagoofil_nist`** Directory dove memorizzare i file scaricati
  - **`-w`** I file trovati vengono scaricati nella directory che segue il parametro **`-o`**

Utilizzo di Crawler

Ricerca di Metadati – Metagoofil – Esempio

Output parziale

- `metagoofil -d nist.gov -t pdf,doc -l 30 -n 30 -o metagoofil_nist -w`

Ricerca e download di file PDF

```
[*] Downloaded files will be saved here: metagoofil_nist
[*] Searching for 30 .pdf files and waiting 30.0 seconds between searches
[+] Downloading file - [378775 bytes] https://www.nist.gov/document/eppendorf
5415rcentrifugemanualpdf
[+] Downloading file - [66449 bytes] https://math.nist.gov/~BAlpert/evolution
.pdf
[+] Downloading file - [1460582 bytes] https://www.nist.gov/document/measureo
fsecuritywithcoverpagesjuly22finalpdf
[+] Downloading file - [180600 bytes] https://emtoolbox.nist.gov/Publications
/NISTTechnicalNote1297s.pdf
[+] Downloading file - [1207384 bytes] https://www.nist.gov/document/smartgri
dinteroperabilitypdf
[+] Downloading file - [452543 bytes] https://www.nist.gov/document/cybersecu
rityframework6thworkshopintelcorppdf
[+] Downloading file - [233702 bytes] https://www.nist.gov/document-10863
[+] Downloading file - [270673 bytes] https://math.nist.gov/~BAlpert/nrbc2.pd
f
[+] Downloading file - [213999 bytes] https://www.nist.gov/document/r0001214p
df
[+] Downloading file - [1430251 bytes] https://www.nist.gov/document/4se7seal
sysengveefinalpdf
```

Utilizzo di Crawler

Ricerca di Metadati – Metagoofil – Esempio

Output parziale

- `metagoofil -d nist.gov -t pdf,doc -l 30 -n 30 -o metagoofil_nist -w`

Ricerca e download di file doc

```
[*] Searching for 30 .doc files and waiting 30.0 seconds between searches
[+] Downloading file - [373248 bytes] https://www.nist.gov/document/appenadoc
[+] Downloading file - [38400 bytes] https://www.nist.gov/document/ststelecon
20060531doc
[+] Downloading file - [67584 bytes] https://www.nist.gov/document/ineap2011j
ulyfdoc
[+] Downloading file - [417280 bytes] https://www.nist.gov/document/oktextsit
esurveysdoc
[+] Downloading file - [98816 bytes] https://www.nist.gov/document/massachuse
ttsdoc
[+] Downloading file - [178688 bytes] https://www.nist.gov/document/procedure
13v401d03doc
[+] Downloading file - [4774400 bytes] https://www.nist.gov/document-15900
[+] Downloading file - [113664 bytes] https://www.nist.gov/document-11796
[+] Downloading file - [437760 bytes] https://www.nist.gov/document/xscript20
050118doc
[+] Downloading file - [98816 bytes] https://www.nist.gov/document-4050
[+] Downloading file - [51200 bytes] https://www.nist.gov/document/20050929pr
elimhfdoc
[+] Downloading file - [48640 bytes] https://www.nist.gov/document-14120
[+] Downloading file - [4760064 bytes] https://www.nist.gov/document-16197
[+] Downloading file - [68096 bytes] https://www.nist.gov/document/citationsp
art8doc
```

Outline

- Concetti Preliminari
- Raccolta di Informazioni da Risorse Web-Based
- Raccolta delle Informazioni di Registrazione
- Raccolta delle Informazioni di Routing
- Raccolta di Informazioni dall'Analisi dei Record DNS
- Raccolta di Informazioni mediante Crawler
- **Raccolta di informazioni dal Dark Web**
- Altri Strumenti e Servizi per Raccogliere Informazioni

Dark Web


Surface Web
<10% of Internet
– Indexed Internet
Deep Web
>90% of Internet
– Unindexed Internet
Dark Web (Darknet)
– Subset of Deep Web
– Hidden Services
YouTube
Gmail
TIMES NOW
TOI
I2P
freenet
Tor


The Dark Web

Dark Web

- Il Dark Web
  - Permette di accedere ad informazioni potenzialmente riservate
  - Rappresenta un'area della rete Internet che non è indicizzata da motori di ricerca quali Google, Bing, Yandex, Baidu, etc

- In quest'area gli hacker si scambiano (o acquistano) informazioni su
  - Vulnerabilità
  - Exploit
  - Malware
  - Credenziali
  - Etc

Tipicamente 0-day

Dark Web

- Il Dark Web ha una struttura diversa dal World Wide Web
  - I siti del Dark Web non sono indicizzati dai motori di ricerca e possono essere acceduti solo in modo diretto, digitando il loro URL
  - L'URL associato ad un sito nel Dark Web è costituito da una stringa (apparentemente) casuale seguita dal dominio di primo livello **`.onion`**

Dark Web

- **[Pro]** Il Dark Web potrebbe fornire informazioni che normalmente non si otterrebbero attraverso normali ricerche

- **[Cons]** Tuttavia
  - Il Dark Web potrebbe essere spesso popolato anche da cyber-criminali
    - E da criminali «non cyber»
  - Bisogna quindi fare molta attenzione
    - Possibilità di incorrere in truffe, raggiri, etc

Dark Web

TOR Browser

- Per accedere ai siti del Dark Web è necessario conoscere il loro URL
  - Non viene usato il DNS per la risoluzione dei nomi

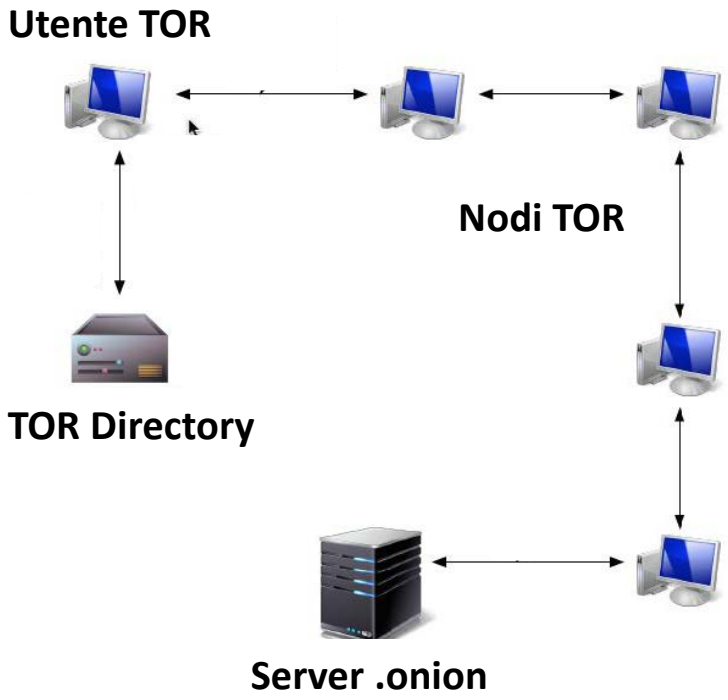
- Il Dark Web può essere acceduto utilizzando il *The Onion Router (TOR)* Browser

- Il TOR Browser
  - È basato su Mozilla Firefox
  - Permette di accedere sia a siti con dominio **`.onion`** che a siti Web indicizzati in maniera convenzionale

Dark Web

TOR Browser

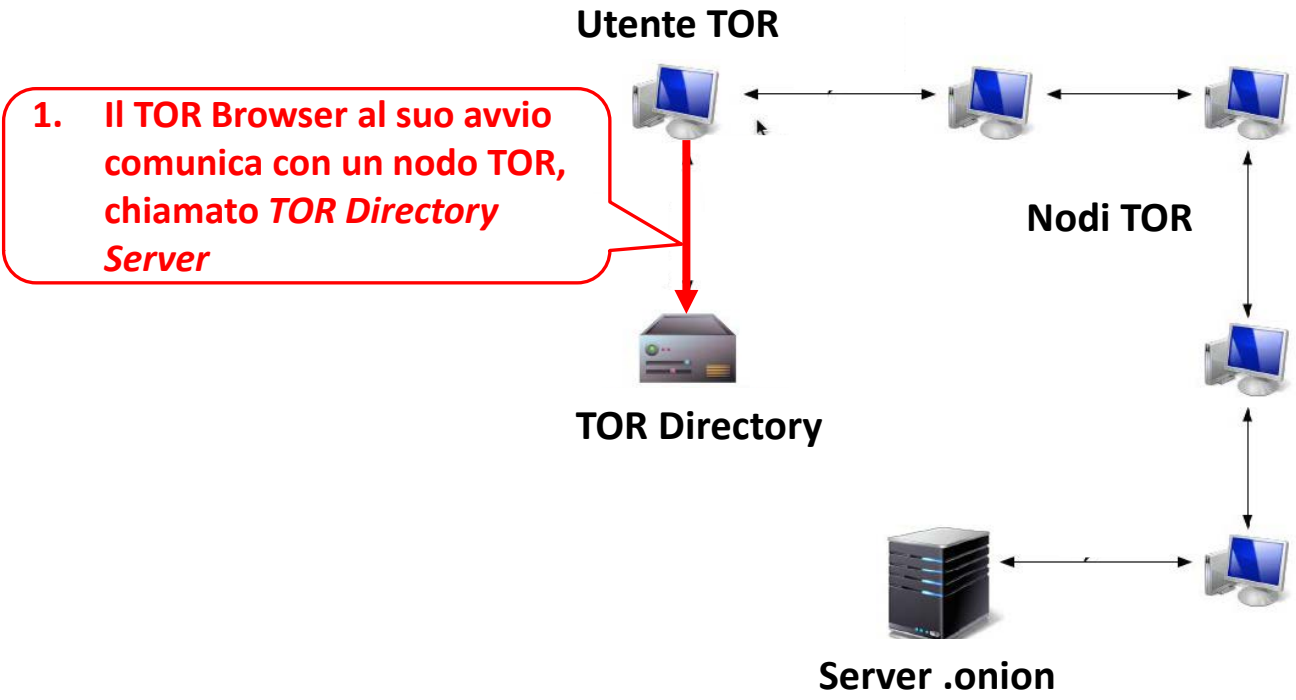
- Il TOR Browser accede ad un server contenente un sito con dominio `.onion` nel modo seguente



Dark Web

TOR Browser

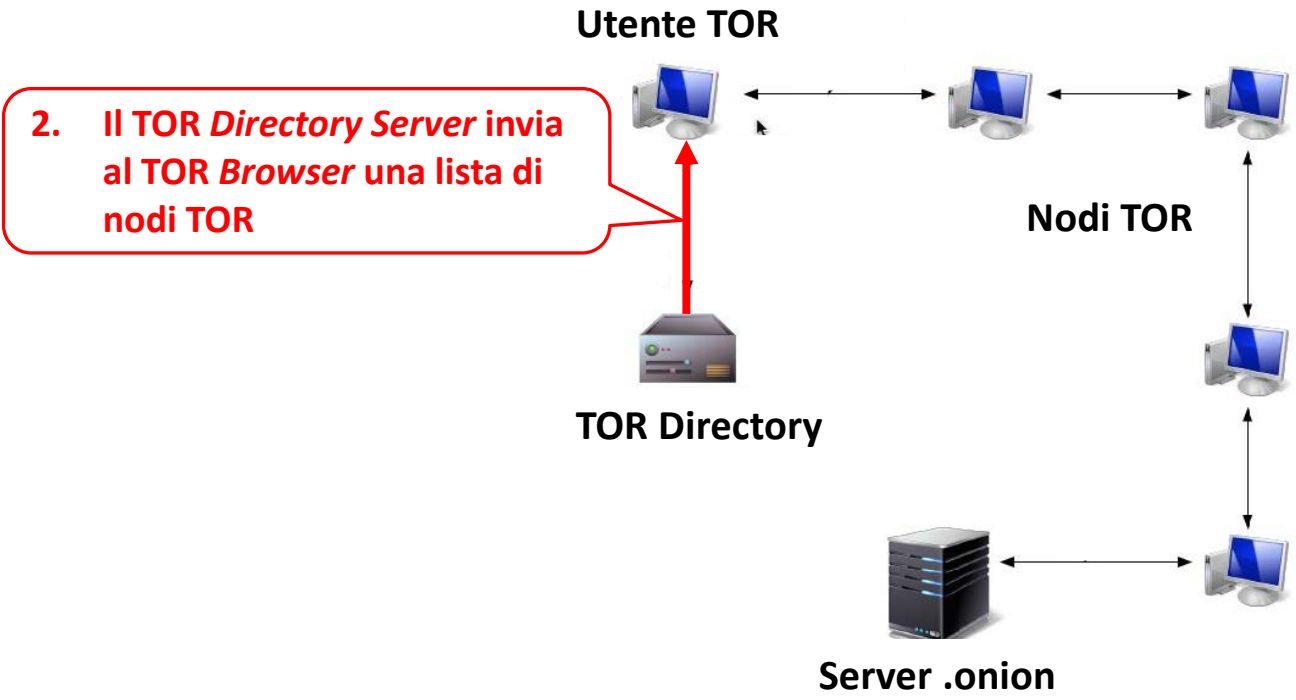
- Il TOR Browser accede ad un server contenente un sito con dominio `.onion` nel modo seguente



Dark Web

TOR Browser

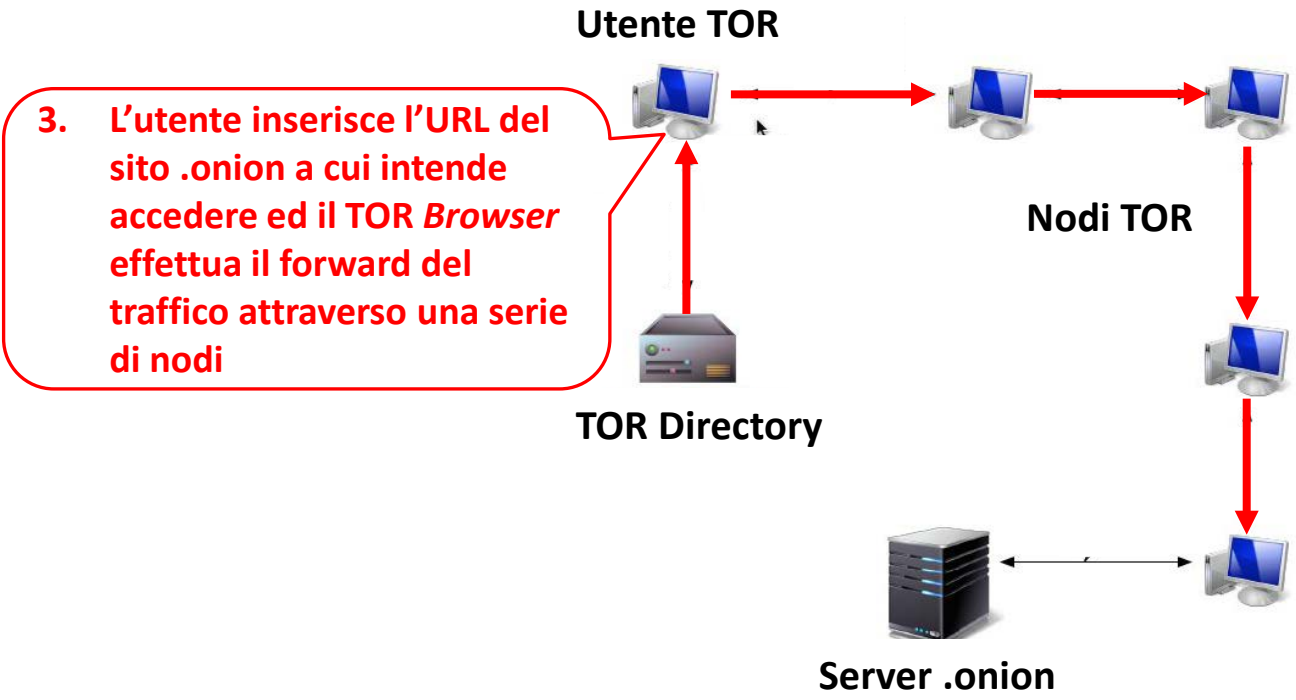
- Il TOR Browser accede ad un server contenente un sito con dominio `.onion` nel modo seguente



Dark Web

TOR Browser

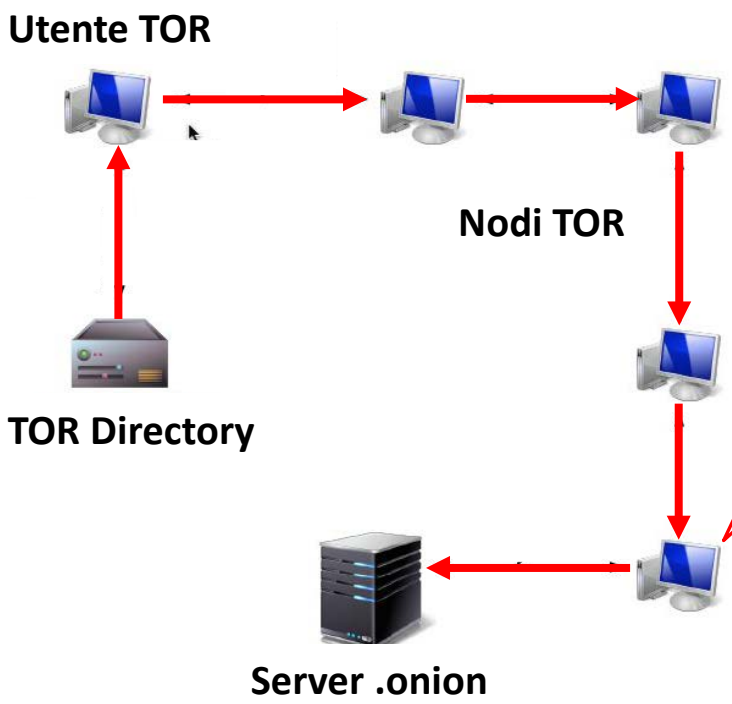
- Il TOR Browser accede ad un server contenente un sito con dominio `.onion` nel modo seguente



Dark Web

TOR Browser

- Il TOR Browser accede ad un server contenente un sito con dominio `.onion` nel modo seguente



4. **L'ultimo nodo si connette al server .onion**
   - **Da questo punto in poi, tutto il traffico viene reinstradato al *Browser* dell'utente attraverso i nodi TOR**

Dark Web
TOR Browser

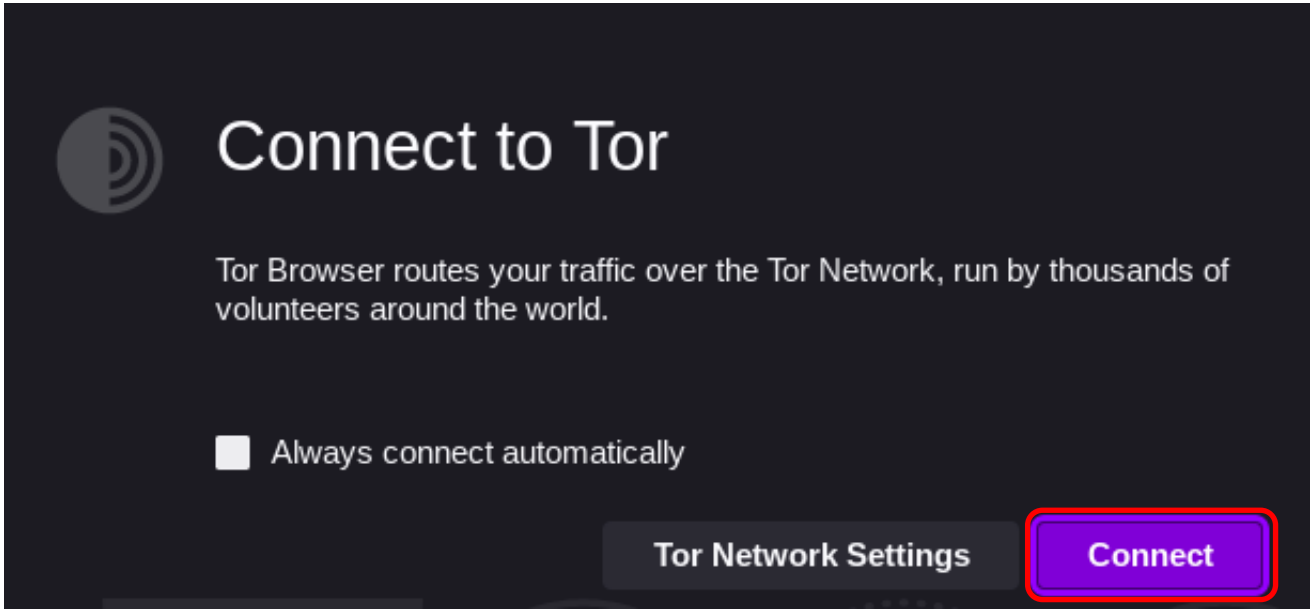
- Grazie al TOR Browser
  - La connessione tra tutti i nodi appartenenti al percorso di routing è protetta
    - Tranne quella tra l'ultimo nodo (*exit node* o *exit relay*) ed il Server **`.onion`**
  - Il Server **`.onion`** sarà a conoscenza solo dell'indirizzo IP dell'ultimo nodo

- Il TOR browser permette anche di anonimizzare il traffico verso i siti del World Wide Web (WWW)
  - Al browser verrà assegnato un indirizzo IP anonimo

Dark Web

TOR Browser – Installazione ed Utilizzo

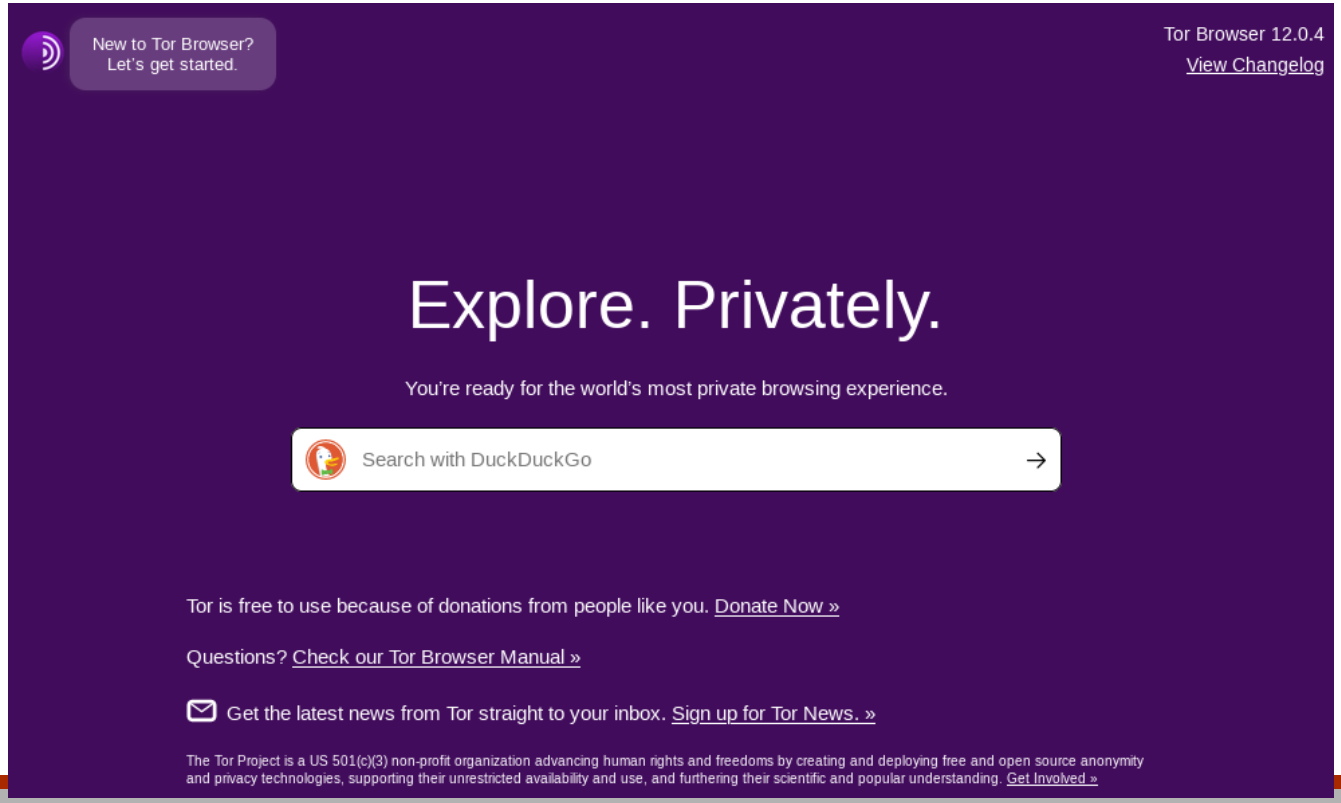
- Per avviare il TOR Browser è sufficiente digitare il seguente comando (non presente di default in Kali Linux)
  - `torbrowser-launcher`



Dark Web

TOR Browser – Installazione ed Utilizzo

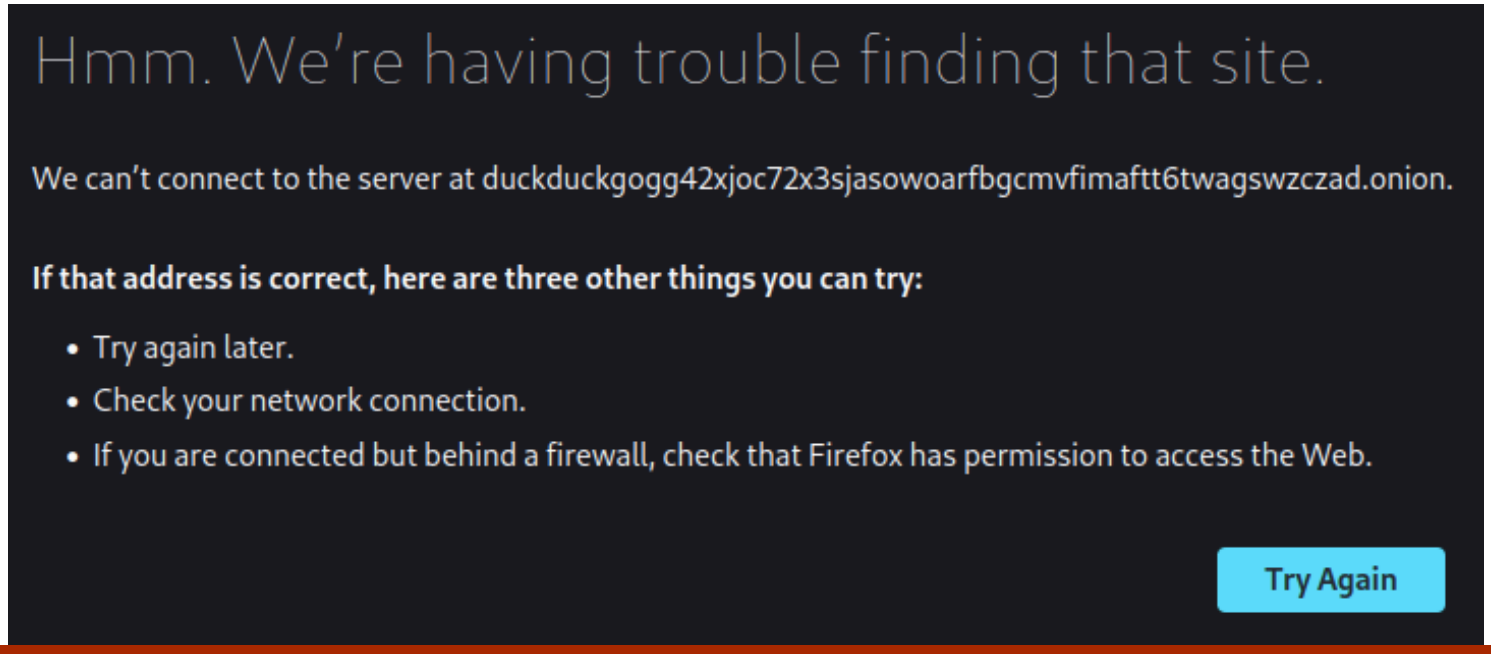
6. Avviare il TOR Browser
   - **`torbrowser-launcher`**



Dark Web

Esempio 1 – Motori di Ricerca per il Dark Web

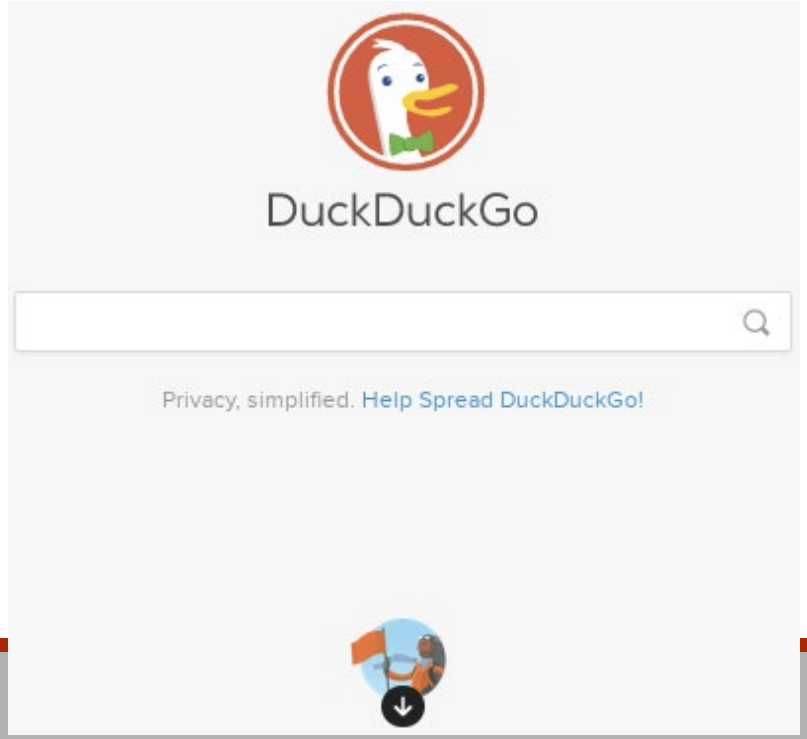
- DuckDuckGo (Accesso tramite Mozilla Firefox)
  - **`https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/`**



Dark Web

Esempio 1 – Motori di Ricerca per il Dark Web

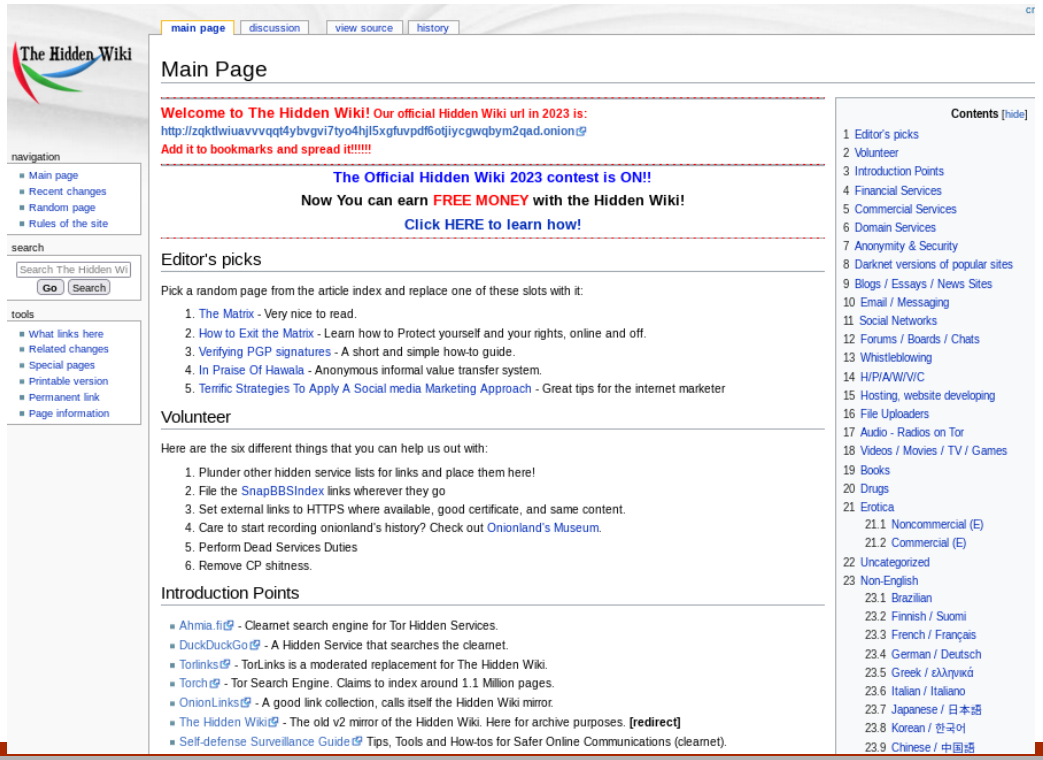
- DuckDuckGo (Accesso tramite TOR Browser)
  - **`https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/`**



Dark Web

Esempio 2 – Motori di Ricerca per il Dark Web

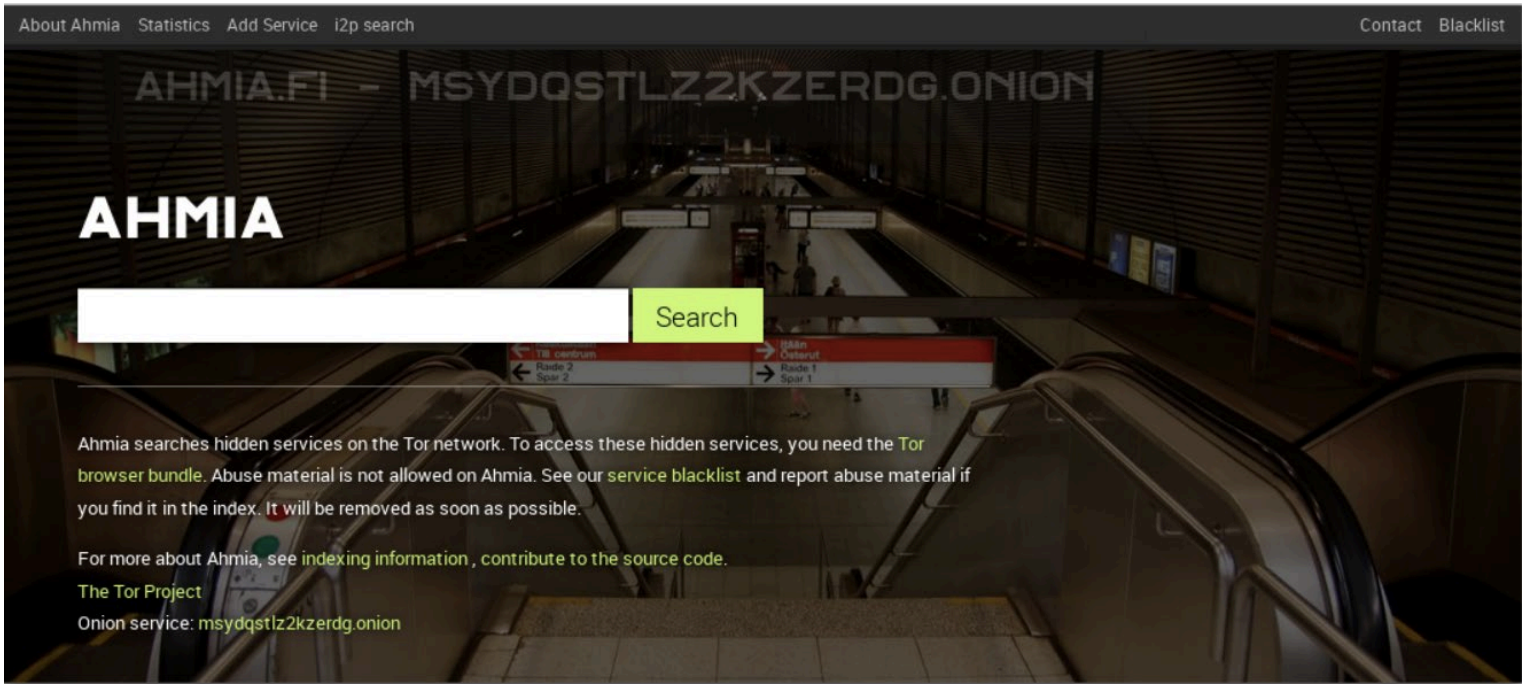
- The Hidden Wiki
  - **http://s4k4ceiapwwgcm3mkb6e4diqecpo7kvdnfr5gg7sph7jjppqkvwwqtyd.onion/**



Dark Web

Esempio 3 – Motori di Ricerca per il Dark Web

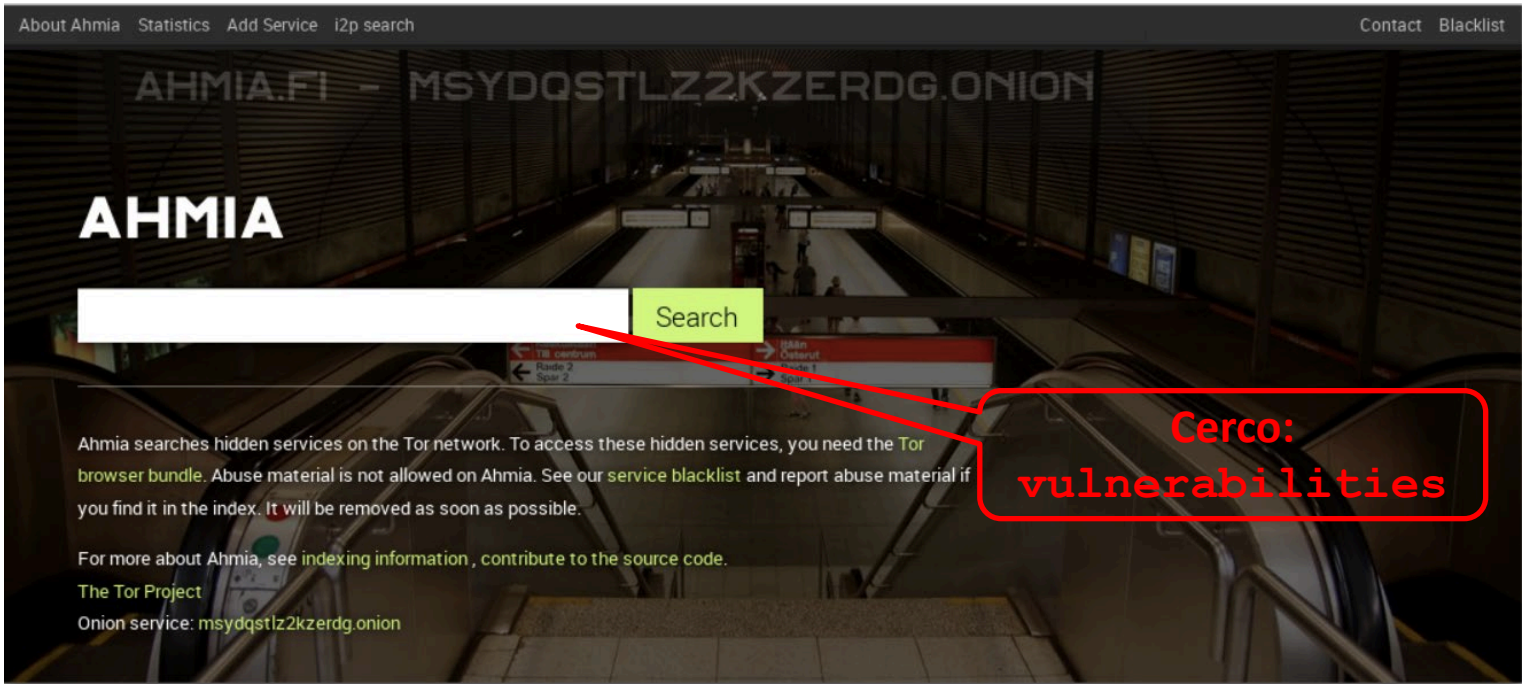
- Ahmia
  - **http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/**



Dark Web

Esempio 3 – Motori di Ricerca per il Dark Web

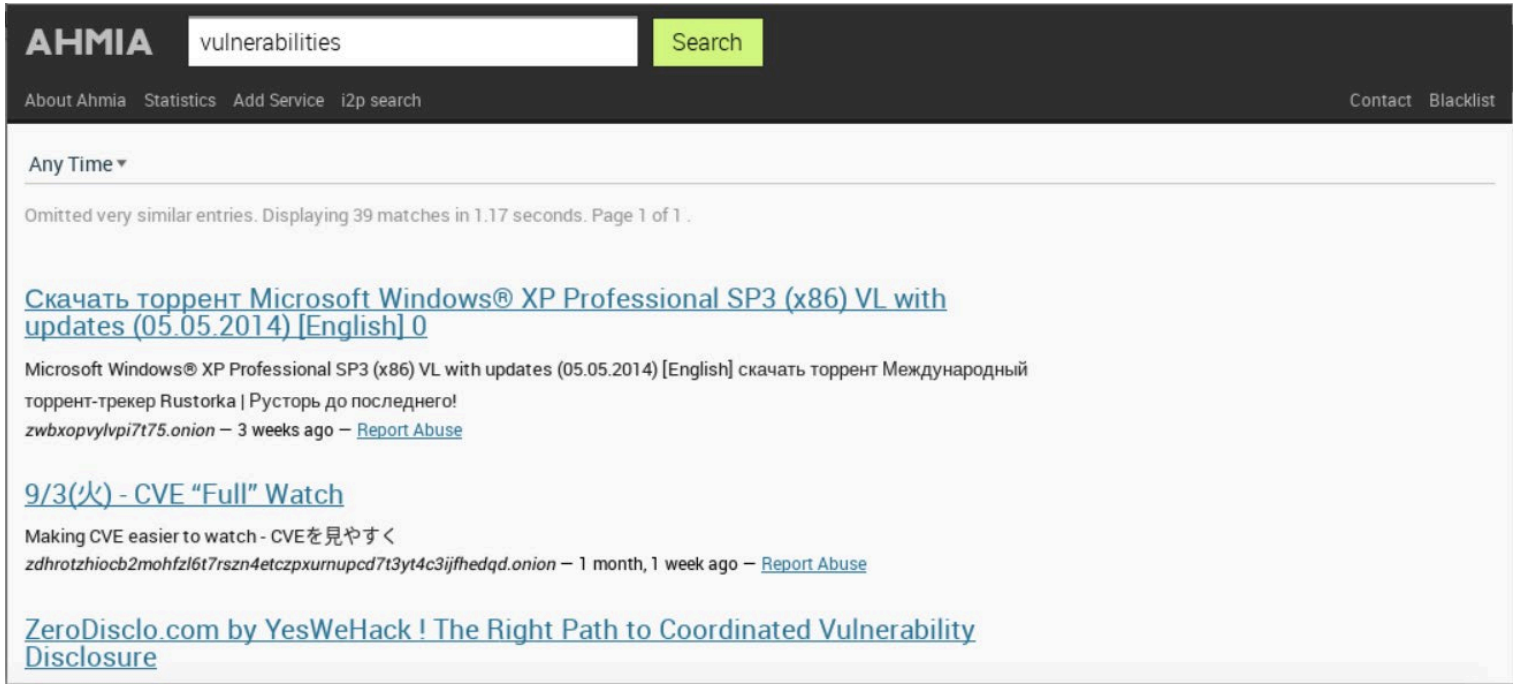
- Ahmia
  - **http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/**



Dark Web

Esempio 3 – Motori di Ricerca per il Dark Web

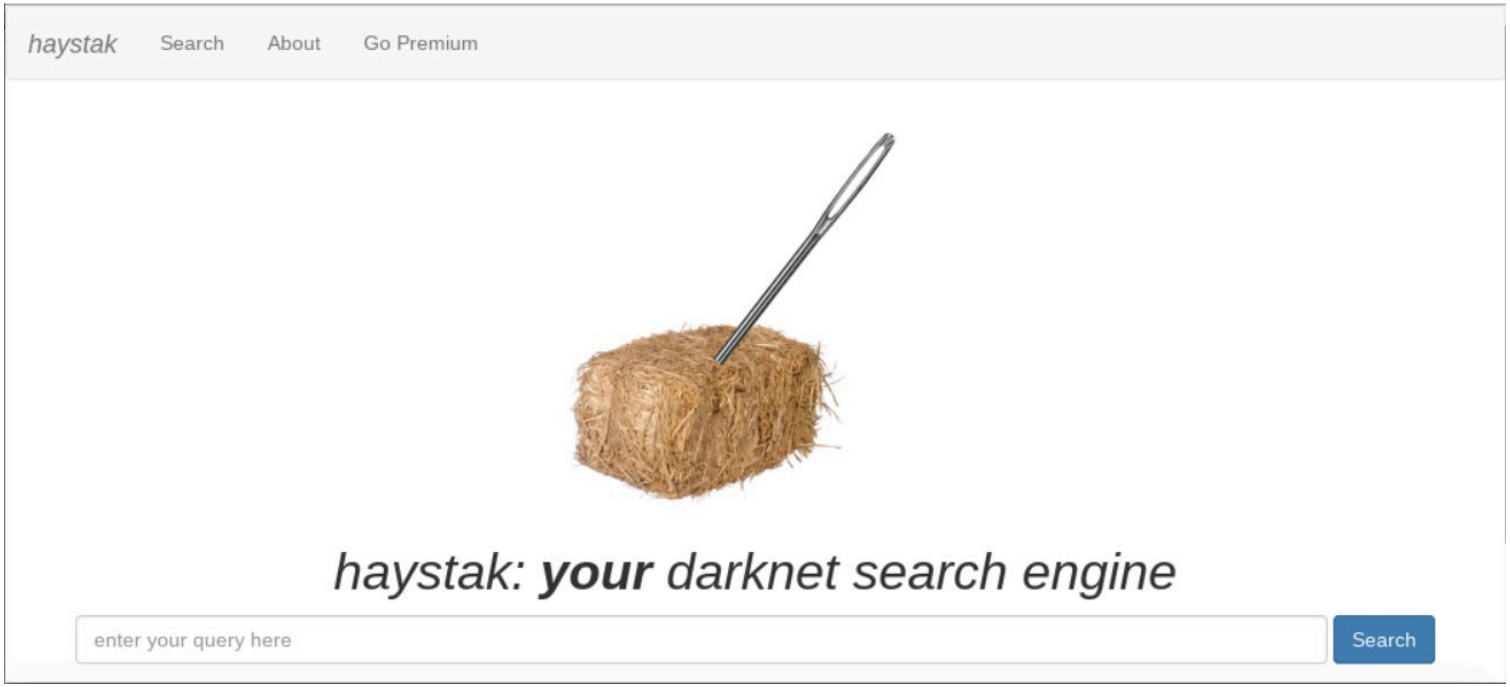
- Ahmia
  - **http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/**



Dark Web

Esempio 4 – Motori di Ricerca per il Dark Web

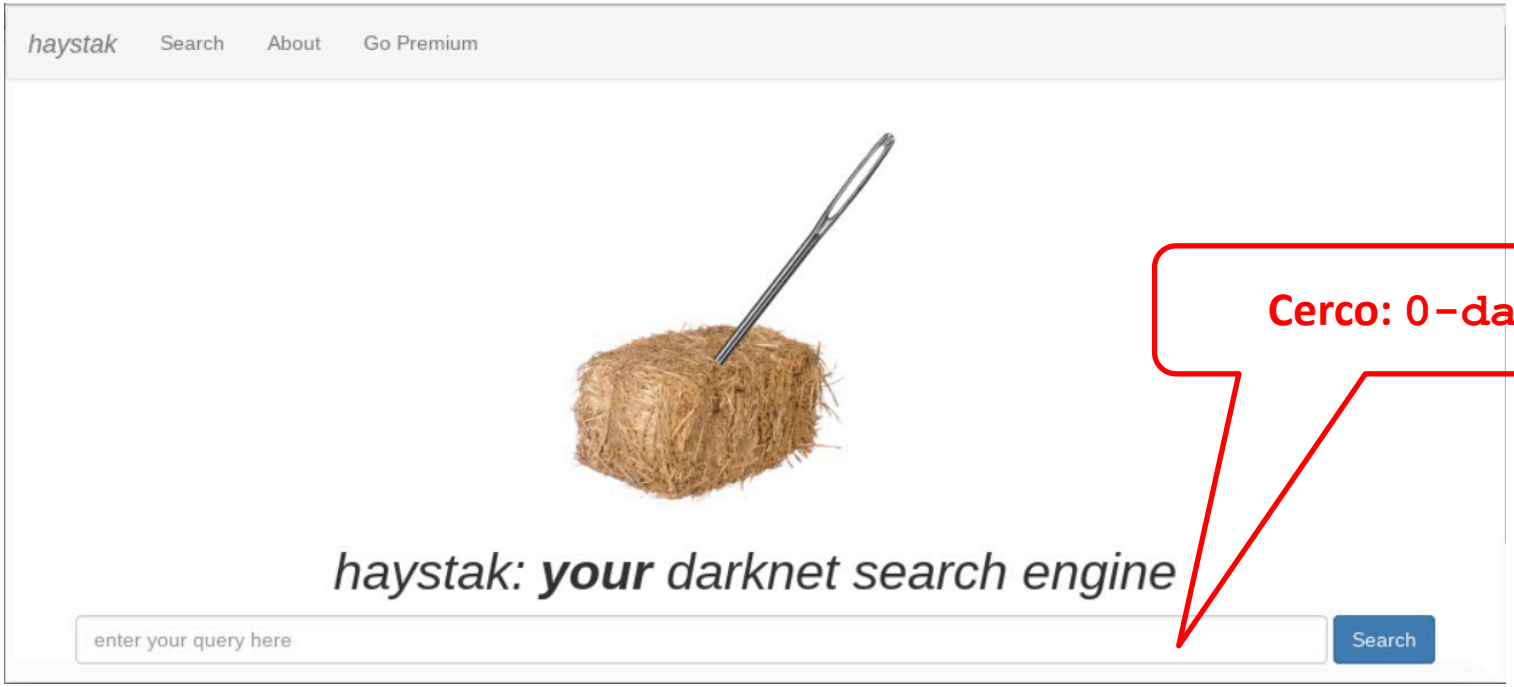
- Haystak
  - **http://haystak5njsmn2hqkewecpaxetahtwhsbsa64jom2k22z5afxhnpxfid.onion/**



Dark Web

Esempio 4 – Motori di Ricerca per il Dark Web

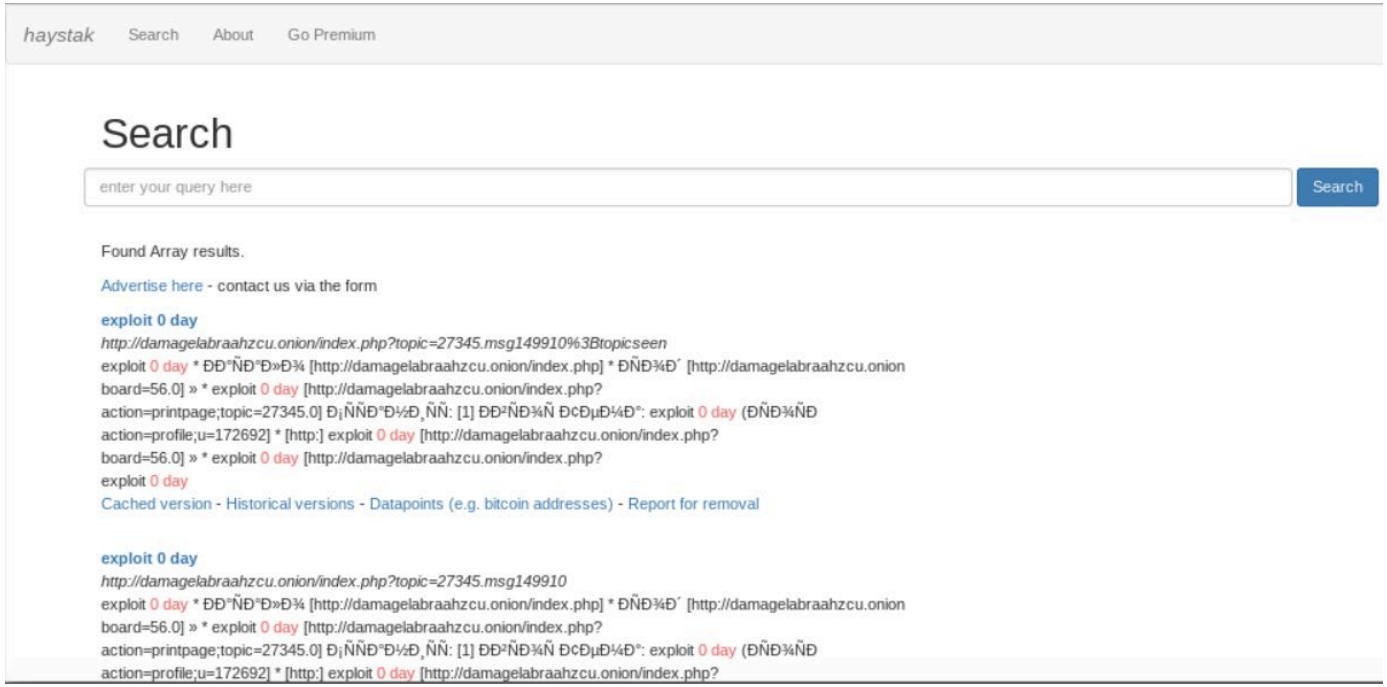
- Haystak
  - **`http://haystak5njsmn2hqkewecpaxetahtwhsbsa64jom2k22z5afxhnpxfid.onion/`**



Dark Web

Esempio 4 – Motori di Ricerca per il Dark Web

- Haystak
  - **http://haystak5njsmn2hqkewecpaxetahtwhsbsa64jom2k22z5afxhnpxfid.onion/**



Dark Web

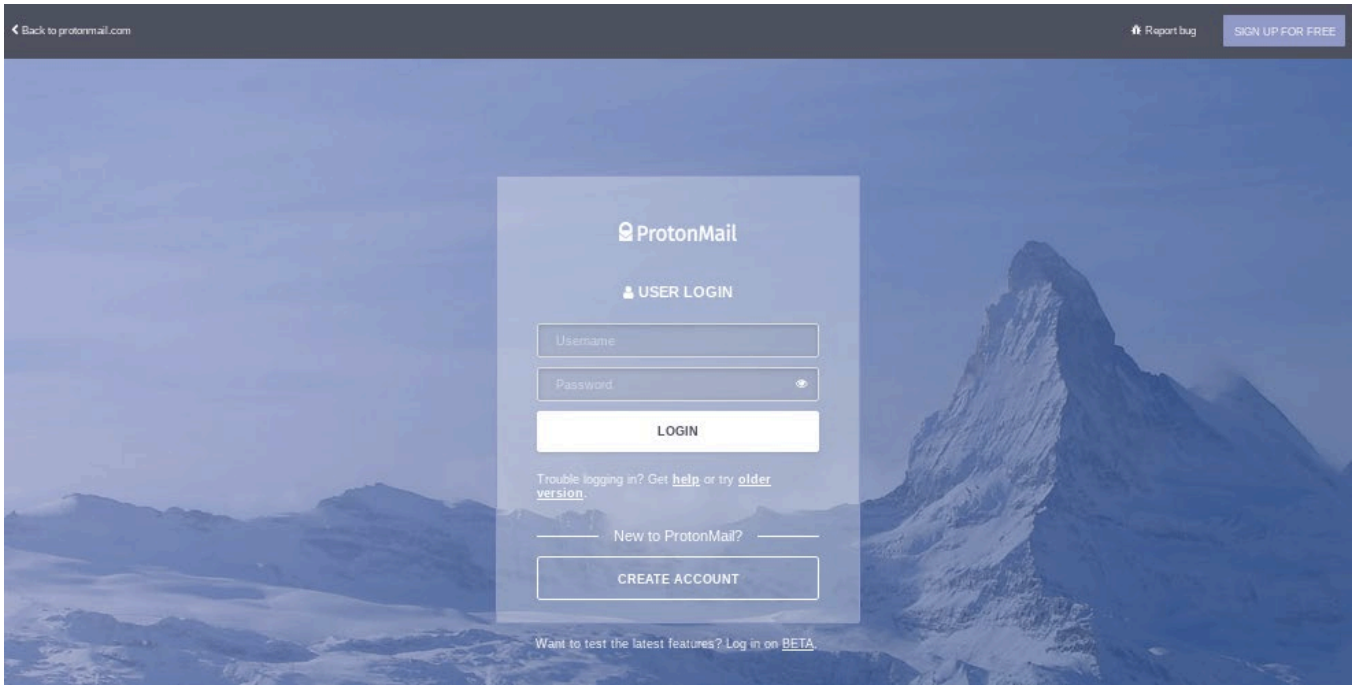
Esempio 5 – Motori di Ricerca per il Dark Web

- Torch
  - **http://xmh57jrknzkhv6y3ls3ubitzfqnkrwxhopf5aygthi7d6rplyvk3noyd.onion/**

Dark Web

Esempio 6 – Servizi E-mail

- ProtonMail
  - **https://protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion/**



Outline

- Concetti Preliminari
- Raccolta di Informazioni da Risorse Web-Based
- Raccolta delle Informazioni di Registrazione
- Raccolta delle Informazioni di Routing
- Raccolta di Informazioni dai Record DNS
- Raccolta di Informazioni mediante Crawler
- Raccolta di informazioni dal Dark Web
- **Altri Strumenti e Servizi per Raccogliere Informazioni**

Altri Strumenti

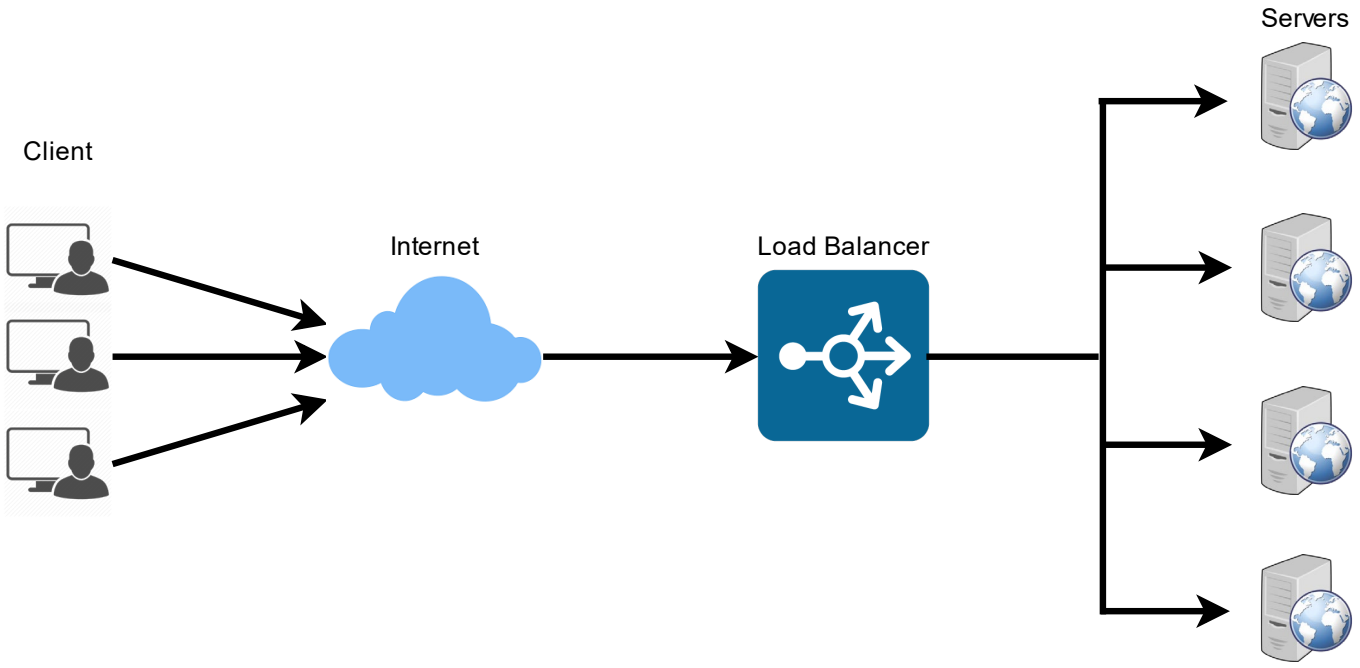
Rilevamento Load Balancer

- Il *Load Balancing* è un metodo utilizzato per distribuire il carico applicativo su più Server
  - Permettendo alle applicazioni di funzionare in modo più efficiente ed affidabile

- I *Load Balancer* sono generalmente classificati in due categorie in base al protocollo utilizzato per effettuare il *Load Balancing*
  - *DNS Load Balancer*
  - *HTTP Load Balancer*

Altri Strumenti

Rilevamento Load Balancer



Rilevamento Load Balancer

Comando `ldb`

- **Idea:** Di solito se un singolo host è risolto in più indirizzi IP probabilmente sta utilizzando un servizio di *Load Balancing*

- Esiste uno strumento specifico per la rilevazione dei *Load Balancer*, chiamato **l**oad **b**alancer **d**etector (comando **`lbd`**)
  - **`lbd`** è in grado di rilevare *DNS load balancer* ed *HTTP load balancer*

Rilevamento Load Balancer

Comando `lbd` – Esempio 1

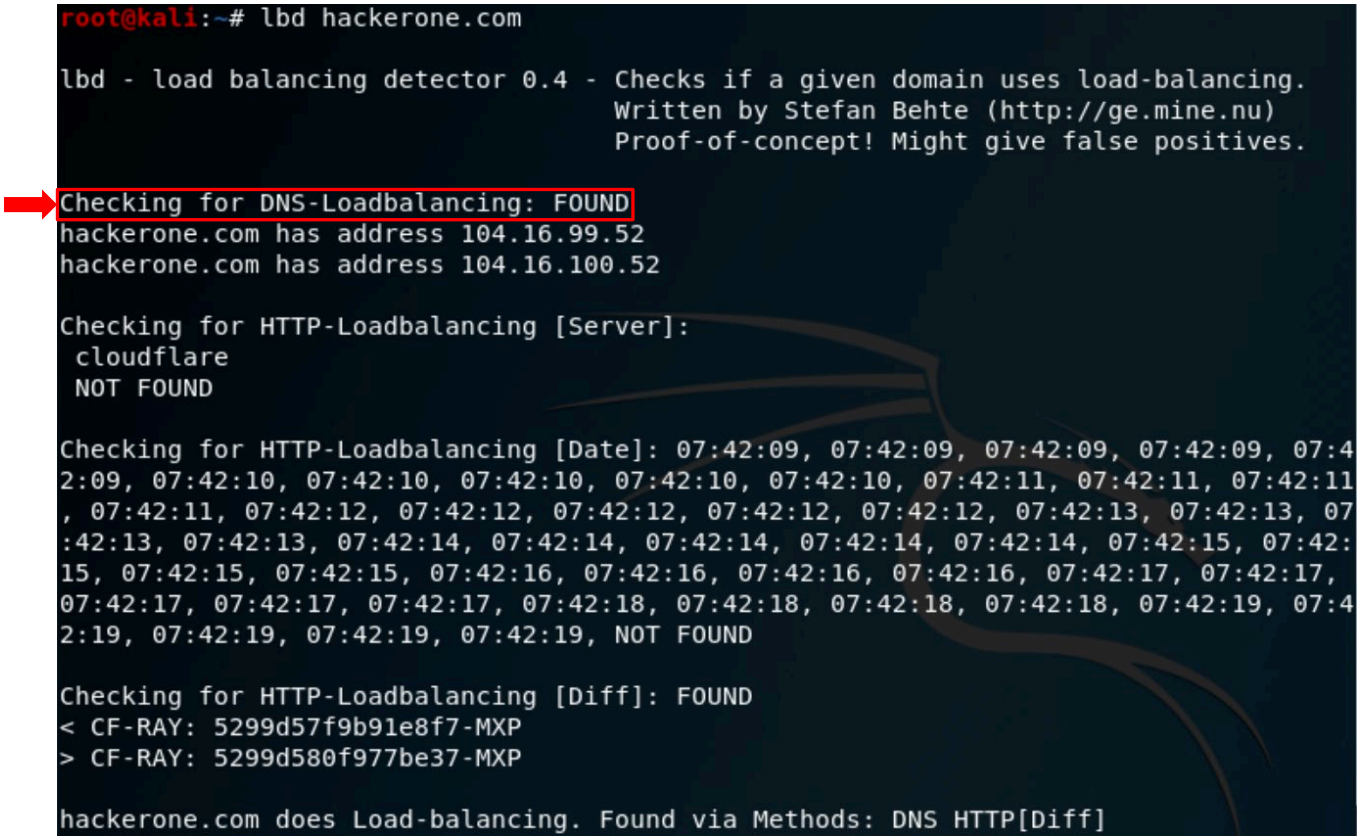
- **`lbd hackerone.com`**

```
root@kali:~# lbd hackerone.com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
                                    Written by Stefan Behte (http://ge.mine.nu)
                                    Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: FOUND
hackerone.com has address 104.16.99.52
hackerone.com has address 104.16.100.52

Checking for HTTP-Loadbalancing [Server]:
 cloudflare
 NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 07:42:09, 07:42:09, 07:42:09, 07:42:09, 07:4
2:09, 07:42:10, 07:42:10, 07:42:10, 07:42:10, 07:42:10, 07:42:11, 07:42:11, 07:42:11
, 07:42:11, 07:42:12, 07:42:12, 07:42:12, 07:42:12, 07:42:12, 07:42:13, 07:42:13, 07
:42:13, 07:42:13, 07:42:14, 07:42:14, 07:42:14, 07:42:14, 07:42:14, 07:42:15, 07:42:
15, 07:42:15, 07:42:15, 07:42:16, 07:42:16, 07:42:16, 07:42:16, 07:42:17, 07:42:17,
07:42:17, 07:42:17, 07:42:17, 07:42:18, 07:42:18, 07:42:18, 07:42:18, 07:42:19, 07:4
2:19, 07:42:19, 07:42:19, 07:42:19, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< CF-RAY: 5299d57f9b91e8f7-MXP
> CF-RAY: 5299d580f977be37-MXP

hackerone.com does Load-balancing. Found via Methods: DNS HTTP[Diff]
```

Rilevamento Load Balancer

Comando `lbd` – Esempio 1

- **`lbd hackerone.com`**



Rilevamento Load Balancer

Comando `lbd` – Esempio 2

- **`lbd dazn.com`**

```
root@kali:~# lbd dazn.com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
                                    Written by Stefan Behte (http://ge.mine.nu)
                                    Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:
 AmazonS3
 NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 22:58:32, 22:58:33, 22:58:33, 22:58:34, 22:58:35, 22:58:
36, 22:58:37, 22:58:37, 22:58:38, 22:58:39, 22:58:40, 22:58:41, 22:58:42, 22:58:43, 22:58:44, 22
:58:44, 22:58:45, 22:58:46, 22:58:47, 22:58:47, 22:58:48, 22:58:49, 22:58:50, 22:58:51, 22:58:52
, 22:58:53, 22:58:54, 22:58:55, 22:58:56, 22:58:56, 22:58:57, 22:58:58, 22:58:59, 22:59:05, 22:5
9:06, 22:59:06, 22:59:07, 22:59:08, 22:59:09, 22:59:10, 22:59:10, 22:59:11, 22:59:12, 22:59:13,
22:59:14, 22:59:15, 22:59:16, 22:59:17, 22:59:18, 22:59:18, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< x-amz-id-2: 0BdVFfZYKF0S8YaHSSk648dbywg2Z+S/yggkezC6tGRUc8iRcRmudKy+2gAShNWf3skr/Tl6ycQ=
< x-amz-request-id: CBC674B1AF90703E
> x-amz-id-2: PxgW5sOnjuMQzpa3fS9ei39paKKlDtFu/tkGxphH8J6nvUzxRywmkjuRWckV0vRKAyTK4JqgZB0=
> x-amz-request-id: 117EB5353727DDCE

dazn.com does Load-balancing. Found via Methods: HTTP[Diff]
```

Rilevamento Load Balancer

Comando `lbd` – Esempio 2

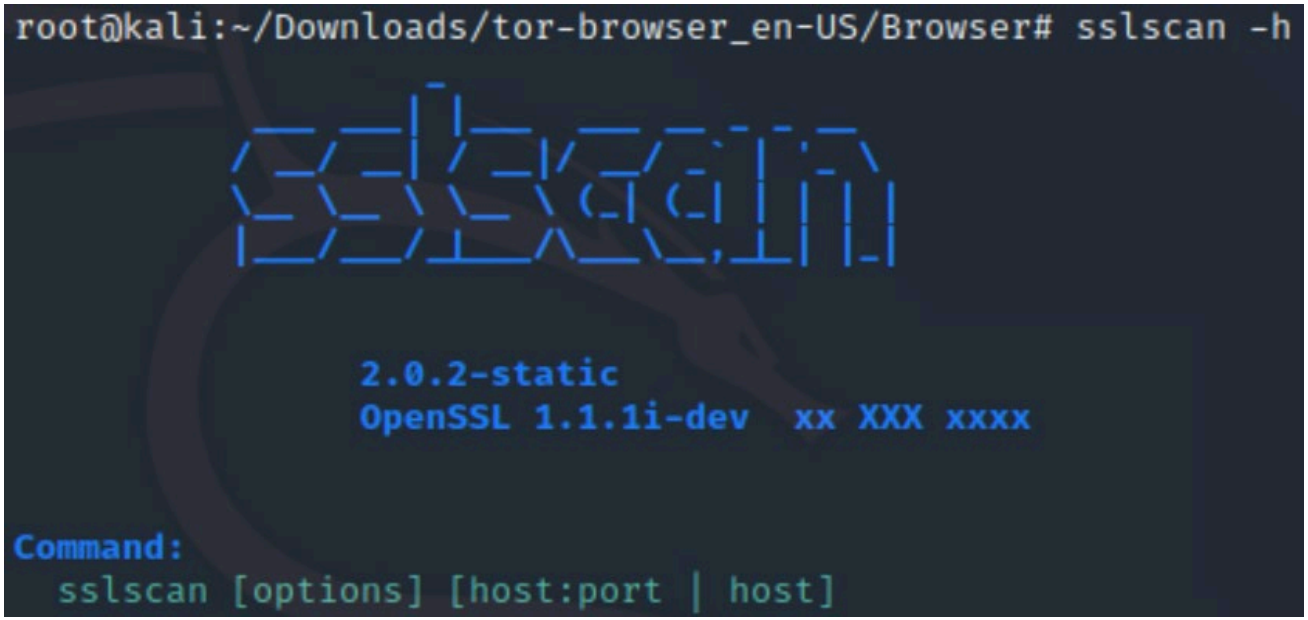
- **`lbd dazn.com`**

```
root@kali:~# lbd dazn.com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
                                    Written by Stefan Behte (http://ge.mine.nu)
                                    Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:
 AmazonS3
 NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 22:58:32, 22:58:33, 22:58:33, 22:58:34, 22:58:35, 22:58:
36, 22:58:37, 22:58:37, 22:58:38, 22:58:39, 22:58:40, 22:58:41, 22:58:42, 22:58:43, 22:58:44, 22
:58:44, 22:58:45, 22:58:46, 22:58:47, 22:58:47, 22:58:48, 22:58:49, 22:58:50, 22:58:51, 22:58:52
, 22:58:53, 22:58:54, 22:58:55, 22:58:56, 22:58:56, 22:58:57, 22:58:58, 22:58:59, 22:59:05, 22:5
9:06, 22:59:06, 22:59:07, 22:59:08, 22:59:09, 22:59:10, 22:59:10, 22:59:11, 22:59:12, 22:59:13,
22:59:14, 22:59:15, 22:59:16, 22:59:17, 22:59:18, 22:59:18, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< x-amz-id-2: 0BdVFfZYKF0S8YaHSSk648dbywg2Z+S/yggkezC6tGRUc8iRcRmudKy+2gAShNWf3skr/Tl6ycQ=
< x-amz-request-id: CBC674B1AF90703E
> x-amz-id-2: PxgW5sOnjuMQzpa3fS9ei39paKKlDtFu/tkGxphH8J6nvUzxRywmkjuRWckV0vRKAyTK4JqgZB0=
> x-amz-request-id: 117EB5353727DDCE

dazn.com does Load-balancing. Found via Methods: HTTP[Diff]
```

Altri Strumenti

Comando `sslscan`

- Permette di analizzare il supporto SSL/TLS lato server
  - Per maggiori informazioni su **`sslscan`**
    - **`sslscan -h`**



Altri Strumenti

Comando `sslscan` - Esempio

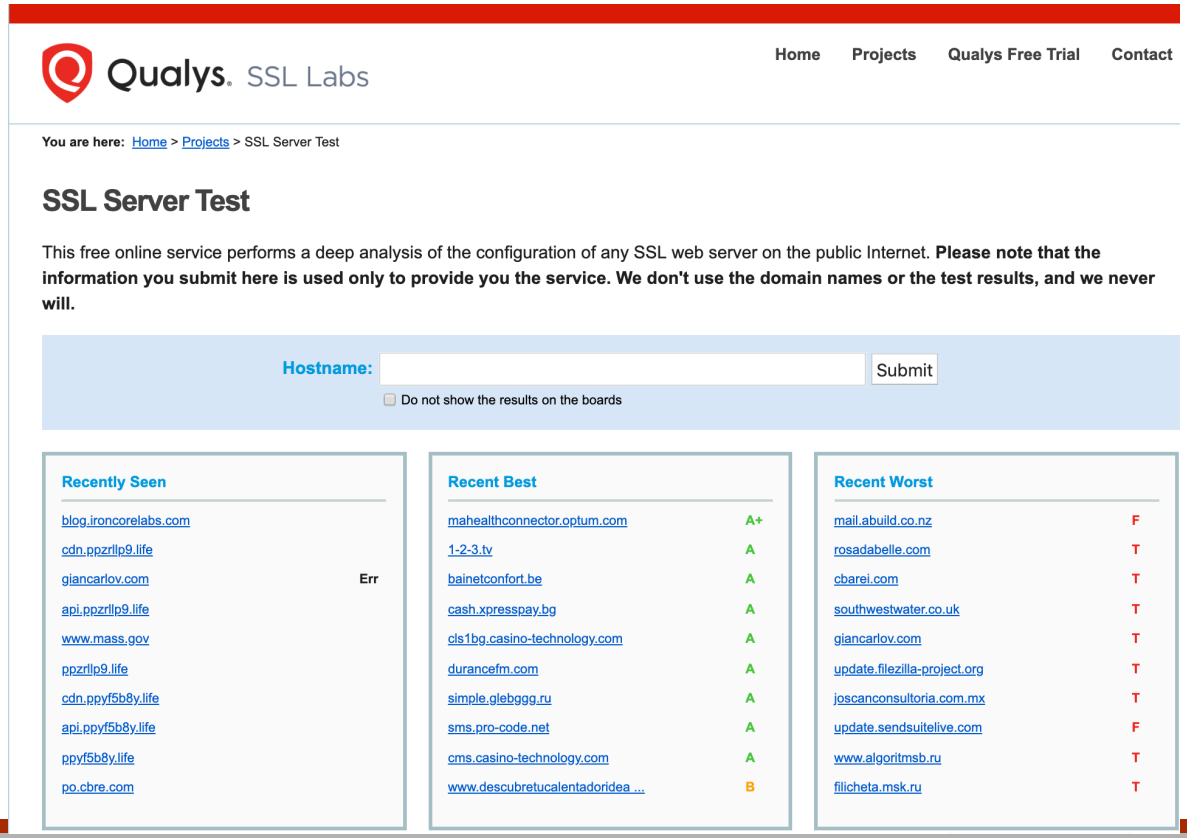
- Utilizzo del comando **`sslscan`** sul dominio **`unisa.it`**
  - **`sslscan unisa.it`**

```
root@kali:~/Downloads/tor-browser_en-US/Browser# sslscan unisa.it
Version: 2.0.2-static
OpenSSL 1.1.1i-dev  xx XXX xxxx

Connected to 193.205.185.20

Testing SSL server unisa.it on port 443 using SNI name unisa.it

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   disabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled
```

Altri Strumenti

Qualys – SSL Server Test

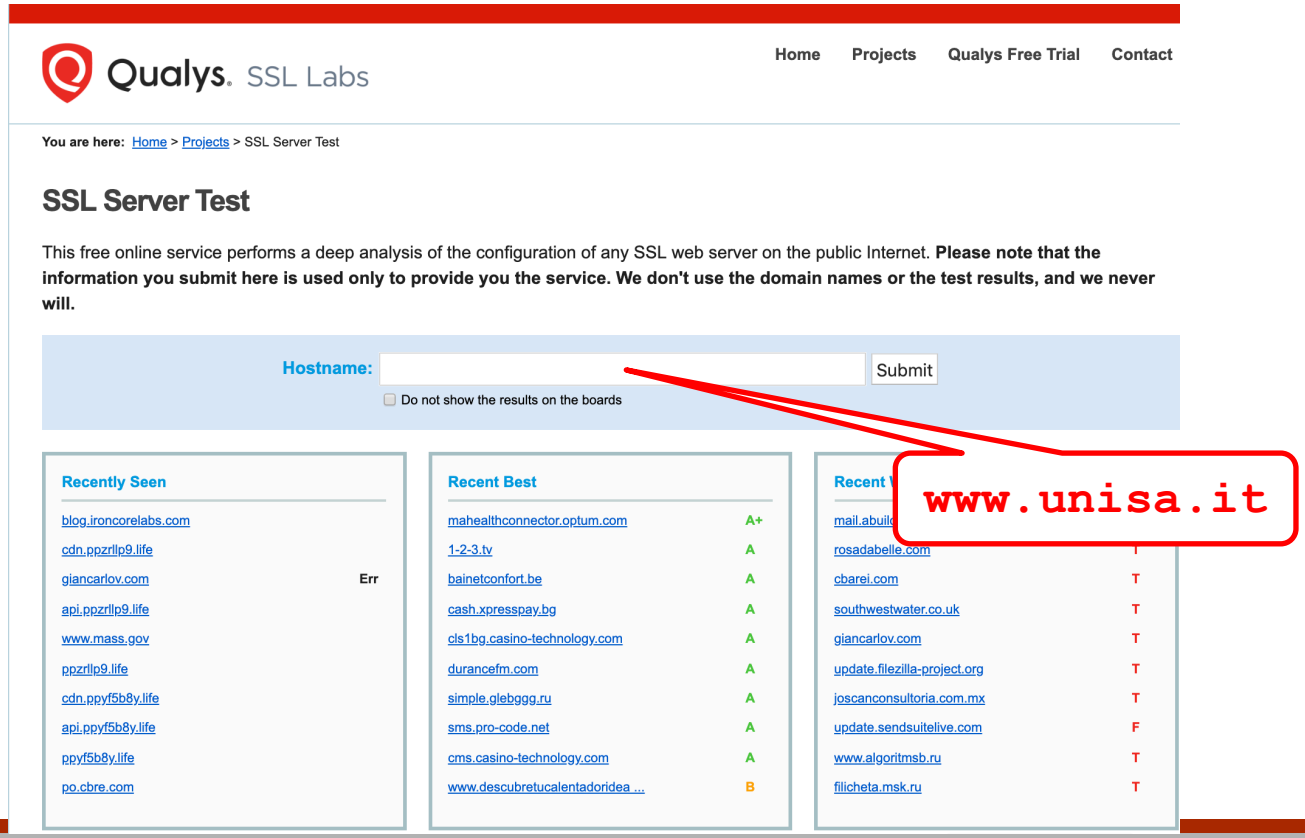
- **`https://www.ssllabs.com/ssltest/`**



Altri Strumenti

Qualys – SSL Server Test

- **`https://www.ssllabs.com/ssltest/`**



Altri Strumenti

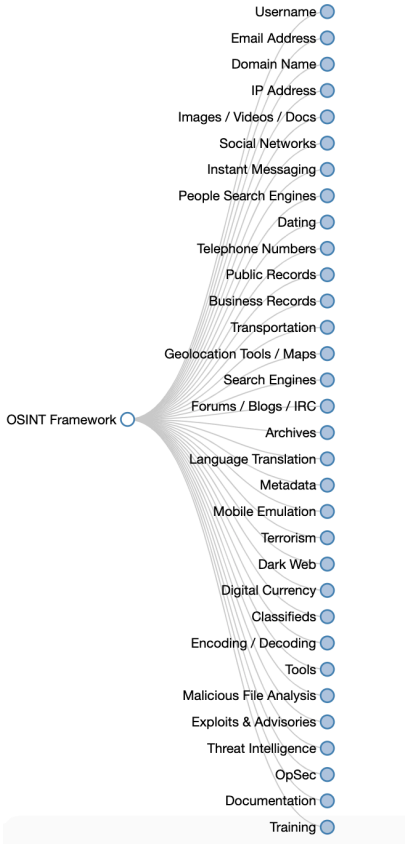
Qualys – SSL Server Test – Esempio

- **`https://www.ssllabs.com/ssltest/`**

Altri Strumenti

OSINT Framework

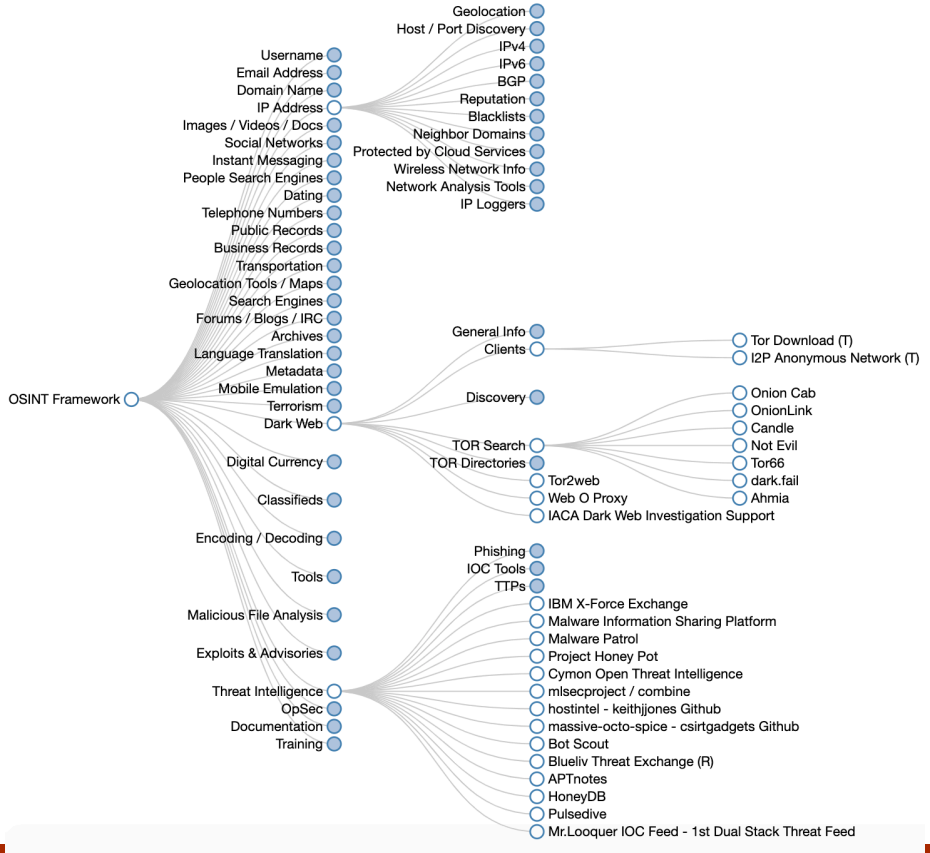
- **`https://osintframework.com/`**



Altri Strumenti

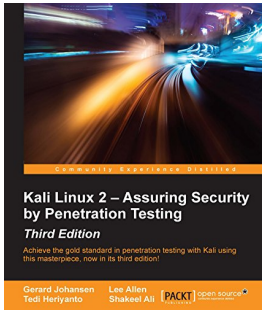
OSINT Framework

- **`https://osintframework.com/`**

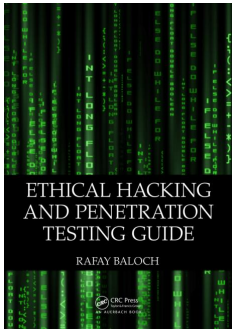


Bibliografia

- **Kali Linux 2 - Assuring Security by Penetration Testing. Third Edition**. Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali. Packt Publishing. 2016
  - Capitolo 4



- **Ethical Hacking and Penetration Testing Guide**. Rafay Baloch. CRC Press. 2014
  - Capitolo 3



Bibliografia

- **Google Search Operators**
  - https://www.indeed.com/career-advice/finding-a-job/google-search-operators
  - https://ahrefs.com/blog/google-advanced-search-operators/