



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



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



MALTEGO

E molto altro ancora...

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



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

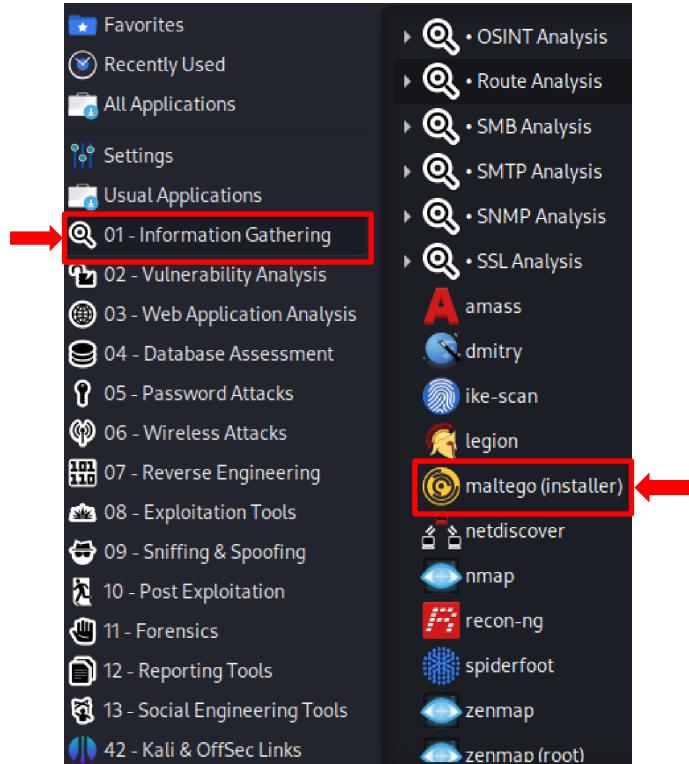


MALTEGO

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»

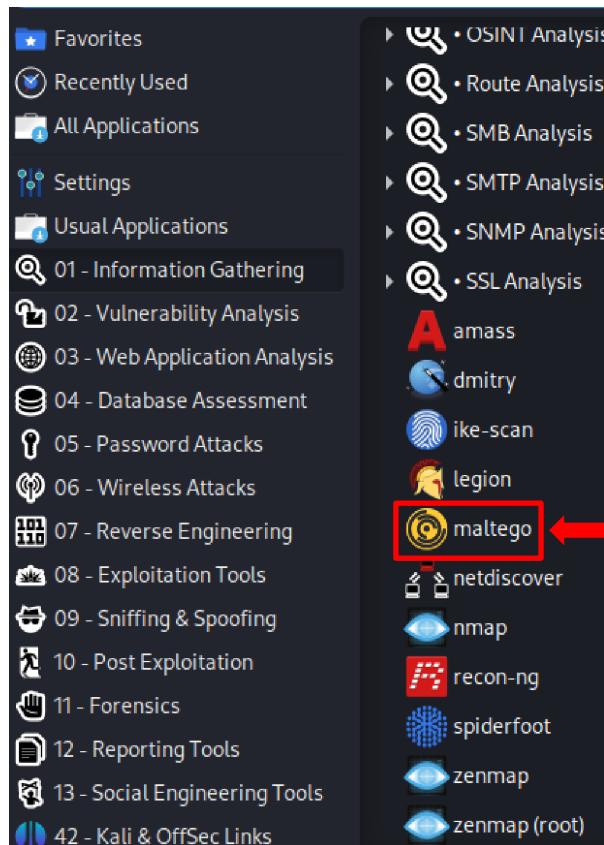


Information Gathering

Utilizzo di Crawler

Maltego – Primo Avvio

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



Utilizzo di Crawler

Maltego – Primo Avvio

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

<p>Community</p> <p>Free Community Edition (CE) for Maltego explorers</p> <p>USE FOR FREE</p> <p>The CE plan includes:</p> <ul style="list-style-type: none">● Link analysis software (limited)● Out-of-the box access to commercial data (limited)● 200 Maltego Credits● Connectors to external data (limited)● Maltego Academy with on-demand and live training <p>See all features</p>	<p>Professional</p> <p>Ideal for individuals investigators or small teams—up to 5 users (billed per seat)</p> <p>GET STARTED</p> <p>Everything in CE, plus:</p> <ul style="list-style-type: none">● Investigation tool for quick OSINT searches on the go● Unmatched access to commercial data● 20,000 Maltego Credits / month● User management system (soon)● Encrypted investigation storage (soon) <p>See all features</p>	<p>Organization</p> <p>Best for larger teams and government organizations (for teams of 5 or more users)</p> <p>CONTACT US</p> <p>Everything in Professional, plus:</p> <ul style="list-style-type: none">● Real-time social media monitoring● Deep and anonymous social network analysis● 250,000+ Maltego Credits / month● Easily integrate your own data (external and local)● Custom services● Priority support <p>See all features</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

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

Complete Your Profile

First Name *

Last Name *

Are you a student? No Yes

Country *

ⓘ Due to export laws, Maltego products are [unavailable in certain countries](#).

Area code *

Phone number *

I would like to receive updates about Maltego product updates, news, events and offers.

CONTINUE →



MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

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

Complete Your Profile

Organization Name *

Private

Organization Size *

1-10

Business Role *

Trainer

Your Role *

Professor

Organization website

e.g. <https://www.company.com>

Main Use Cases *

Penetration Testing X

How did you first learn about Maltego?

Focus of Business Unit *

Trust & Safety

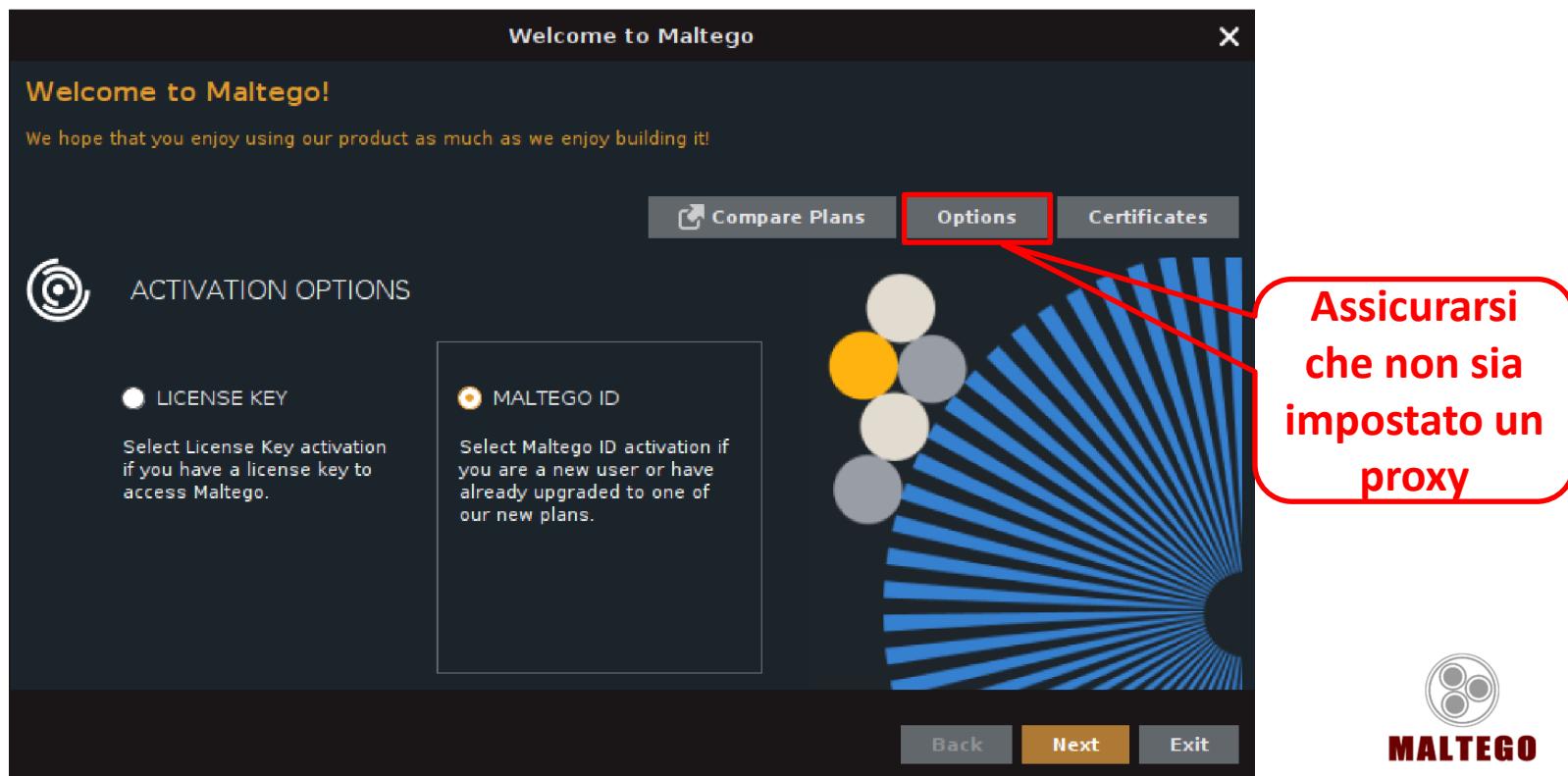
CONTINUE →



Utilizzo di Crawler

Maltego – Primo Avvio

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



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

The screenshot shows the Maltego setup process. On the left, a vertical list of steps is displayed:

- 1. License Agreement
- 2. Login Link Options
- 3. Login
- 4. Maltego ID Activation
- 5. Select Data Sources
- 6. Download Data Sources
- 7. Data Sources T&Cs
- 8. Install Data Sources
- 9. Help Improve Maltego
- 10. Web Browser Options
- 11. Privacy Mode Options
- 12. Ready

The current step, "1. License Agreement", is highlighted in orange. The main content area displays the "General Terms and Conditions for Software Licenses and Accompanying Services". The text states:

LICENSE AGREEMENT: Please read and accept the following License Agreement.

General Terms and Conditions for Software Licenses and Accompanying Services

Effective November 2022

These General Terms and Conditions for Software Licenses and Accompanying Services ("General Terms and Conditions") apply to software distributed and accompanying services provided by Maltego Technologies GmbH, a company registered in the district court Munich, Germany under no. HRB 236523 (hereinafter referred to as "Licensor") to its customers (hereinafter referred to as "Licensee").

Unless agreed otherwise Licensor distributes software licenses by way of Subscription Plans. By subscribing to a Subscription Plan Licensee acquires temporary rights to use software and will be given access to optional Accompanying Services. The specific scope of each Subscription Plan is specified on Licensor's website. In addition, these General Terms and Condition apply. (Licensor and Licensee also referred to as "Party" and collectively the "Parties").

I. Software Licenses

1. Scope of Software Licenses

1.1. By subscribing to a Subscription Plan Licensee will be granted a worldwide, non-exclusive, non-transferable and non-sublicensable right to temporarily use the respective Software for Licensee's

Accept

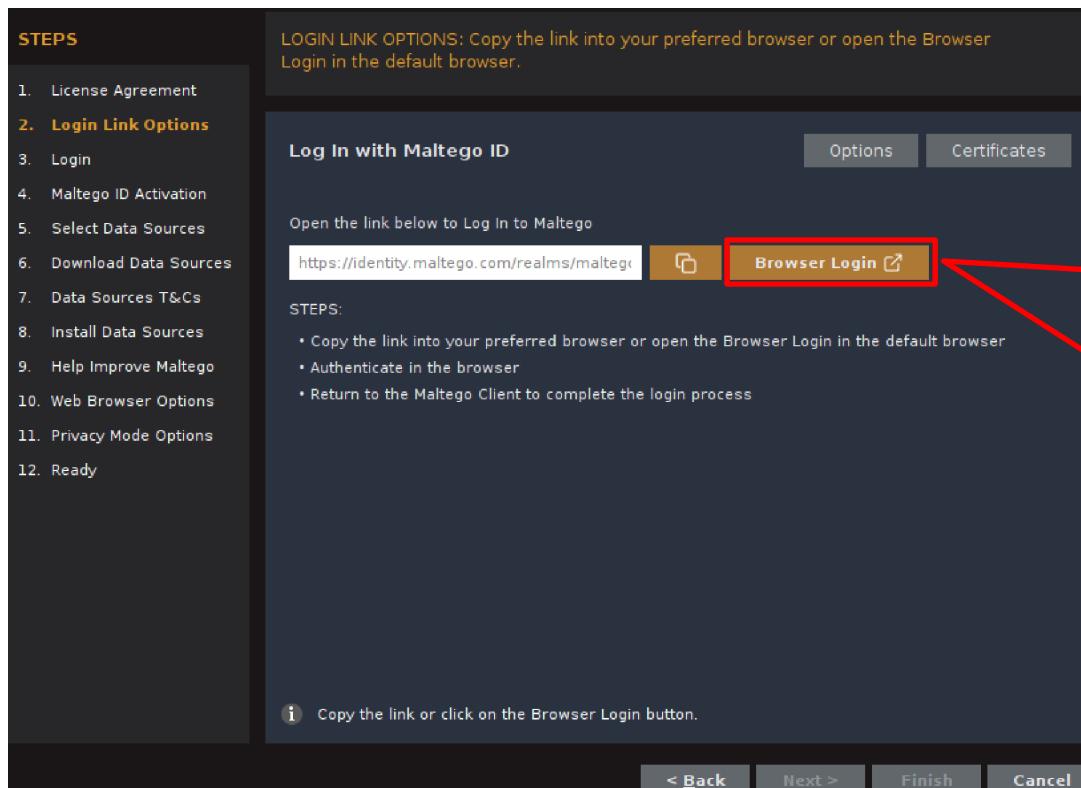
At the bottom of the screen, there are three buttons: "< Back", "Next >" (which is highlighted with a red border), and "Finish / Cancel".



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**

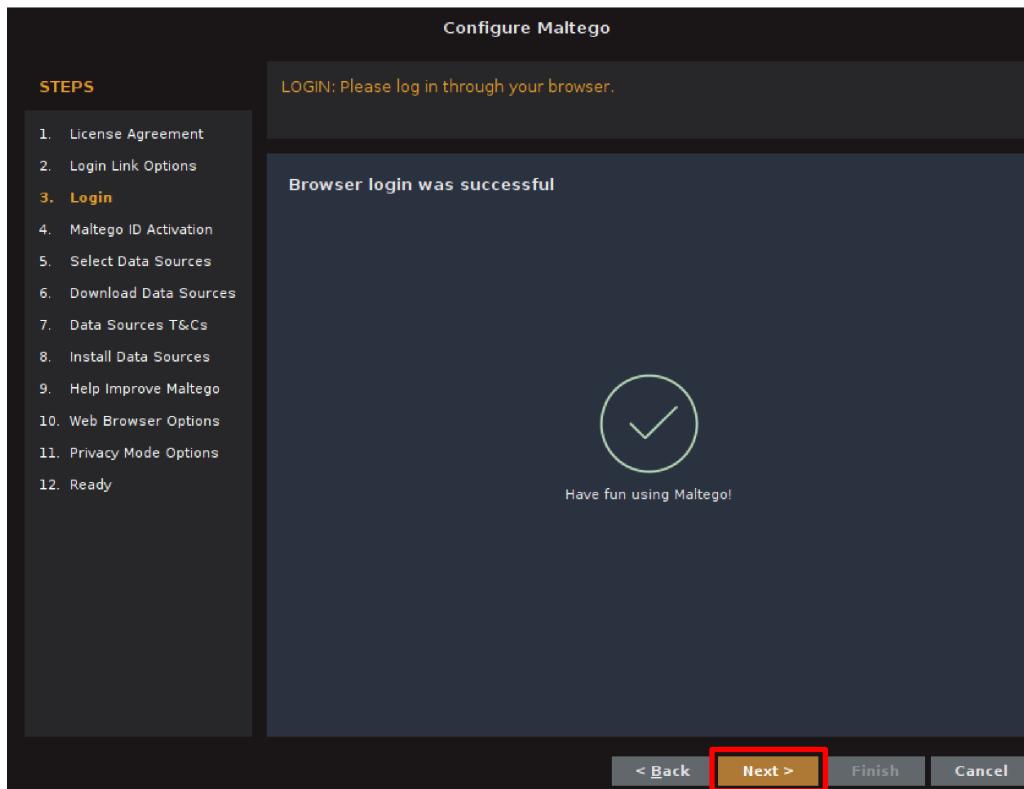


MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

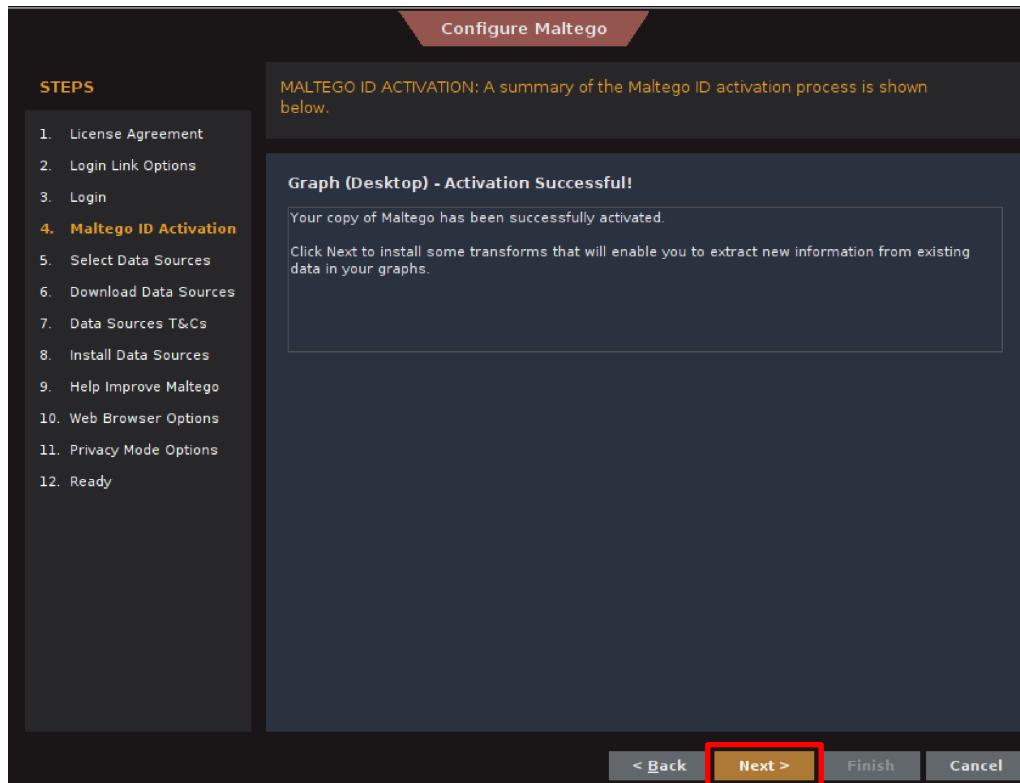
- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione



Utilizzo di Crawler

Maltego – Primo Avvio

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

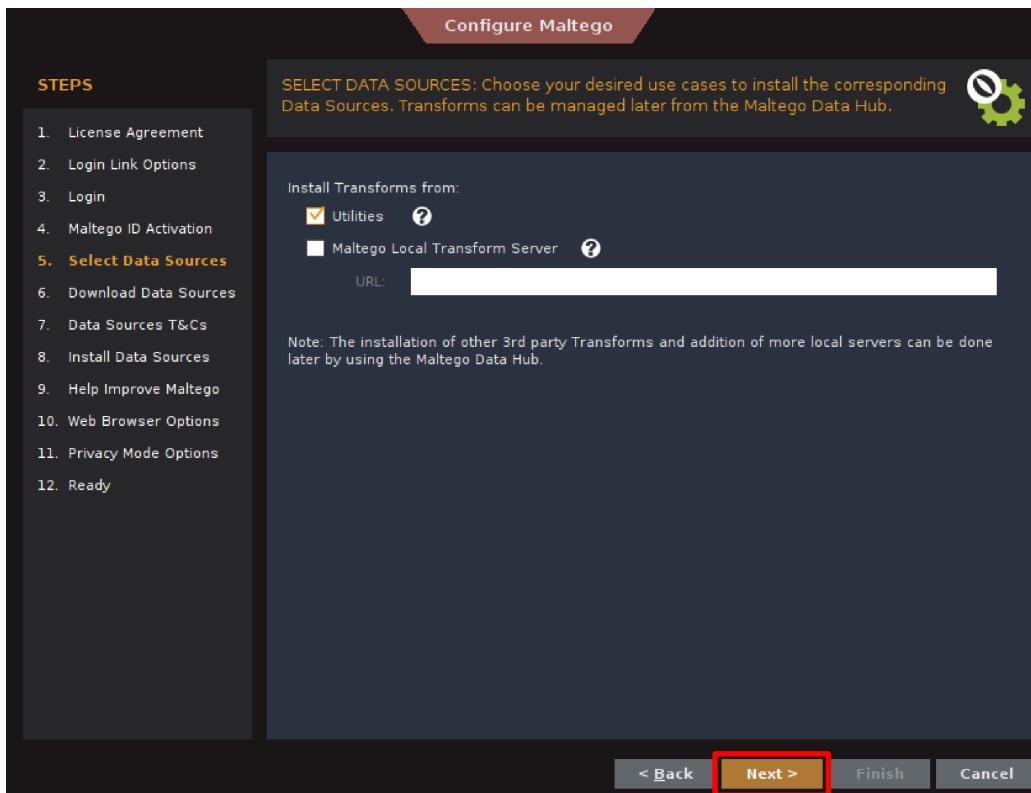


MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

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

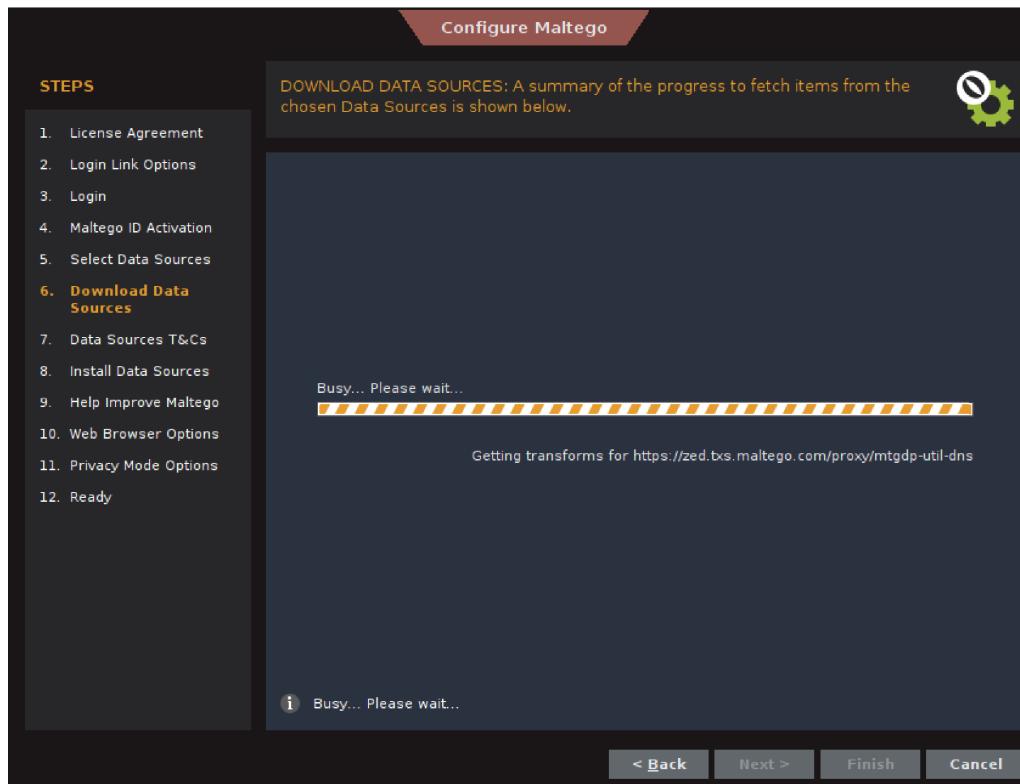


MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

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



MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

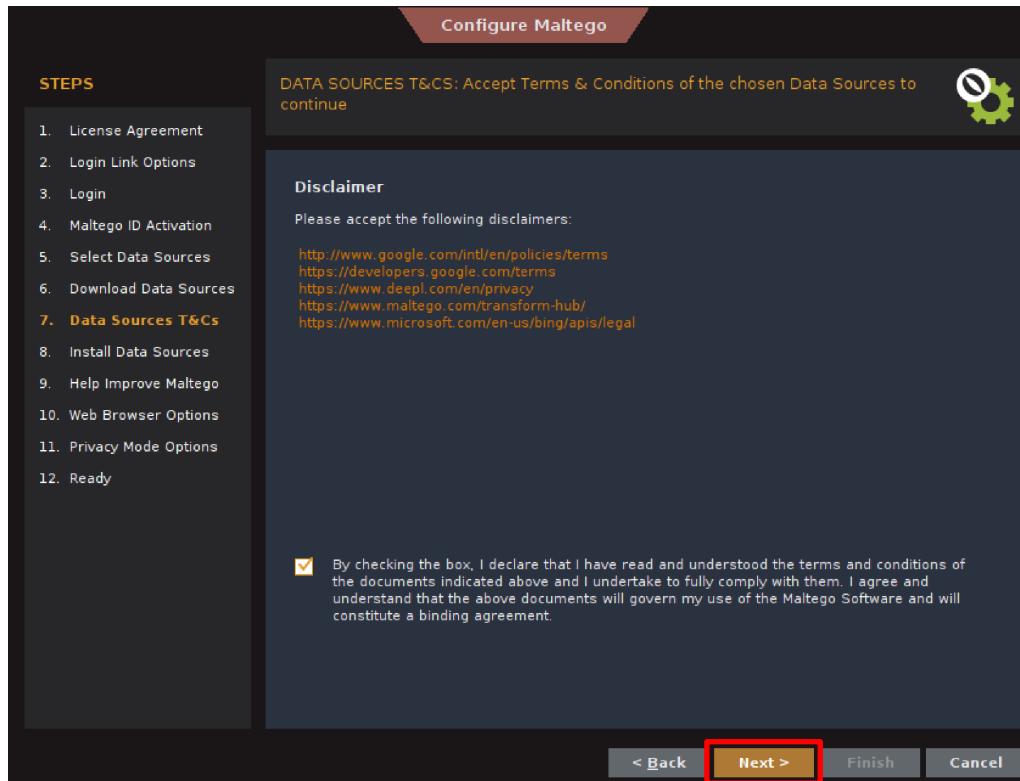
- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione



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

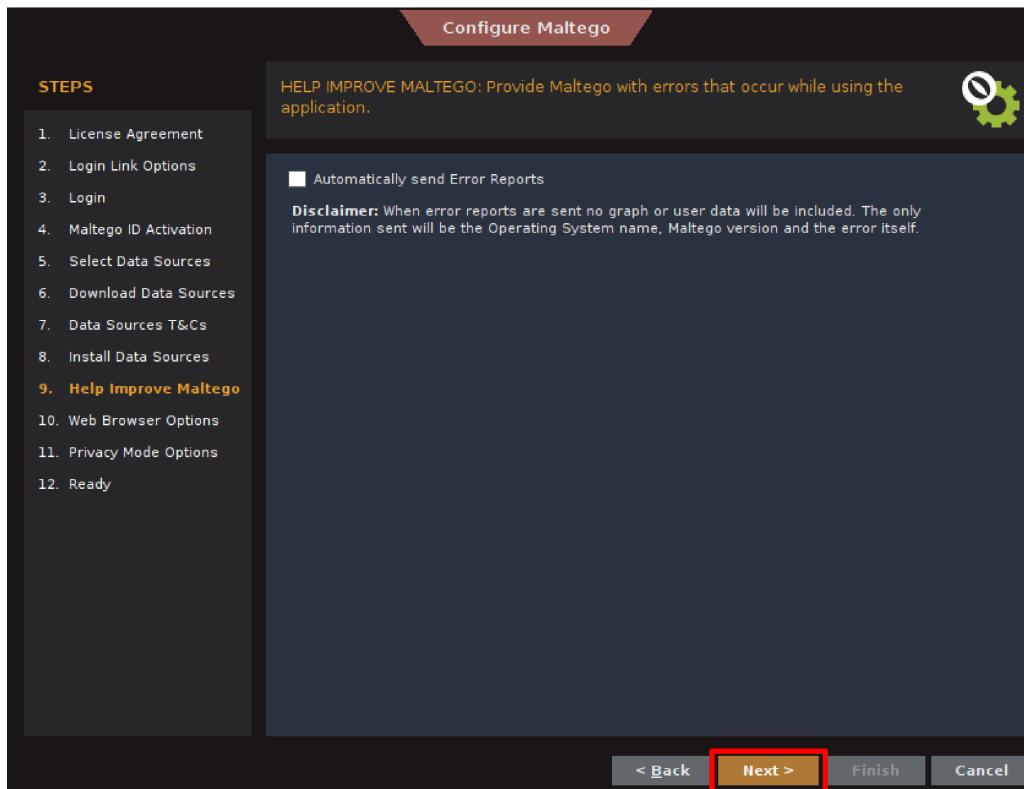
- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione



Utilizzo di Crawler

Maltego – Primo Avvio

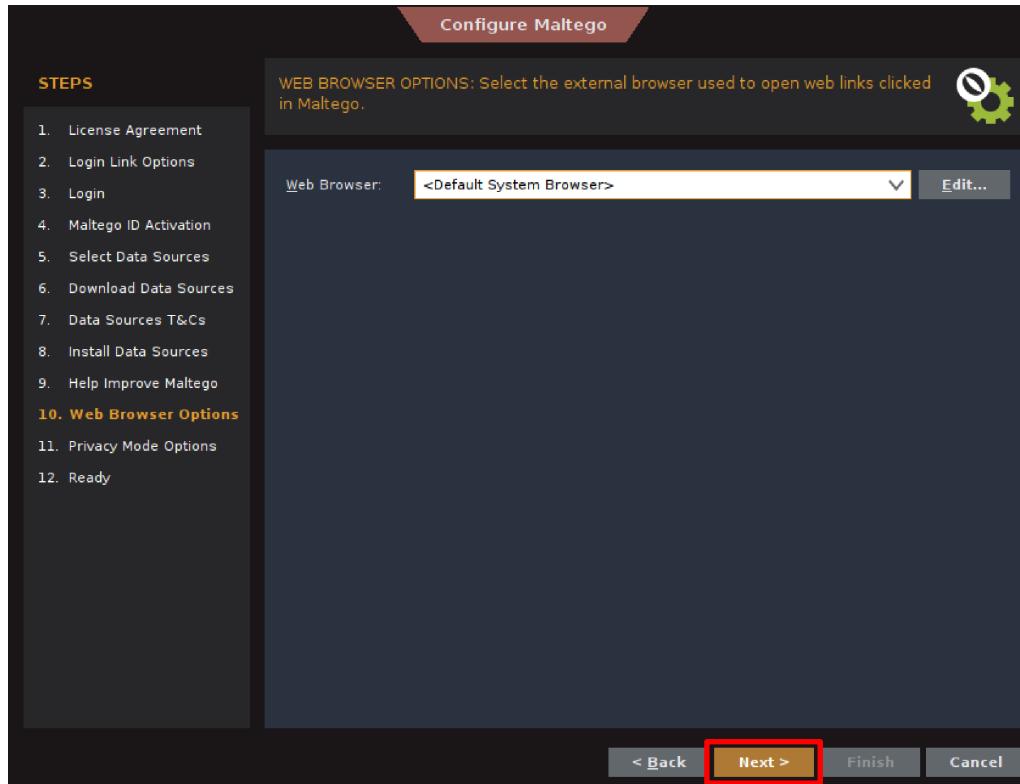
- È necessario attivare il prodotto, utilizzando le credenziali inserite in fase di registrazione



Utilizzo di Crawler

Maltego – Primo Avvio

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

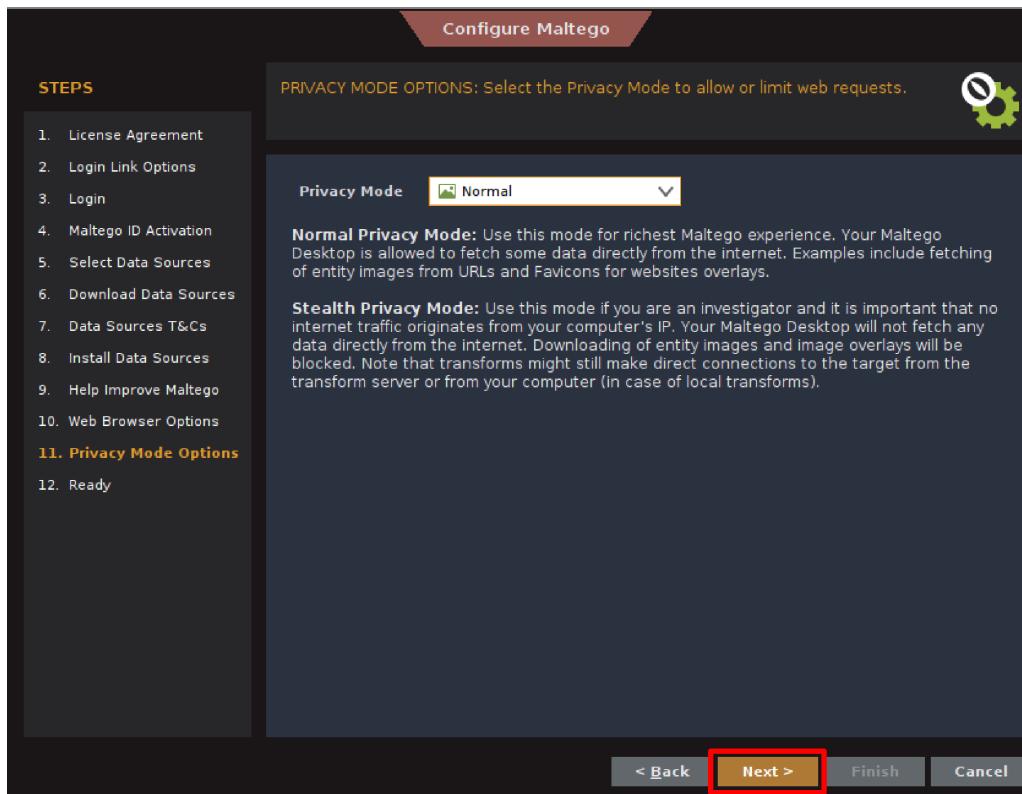


MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

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

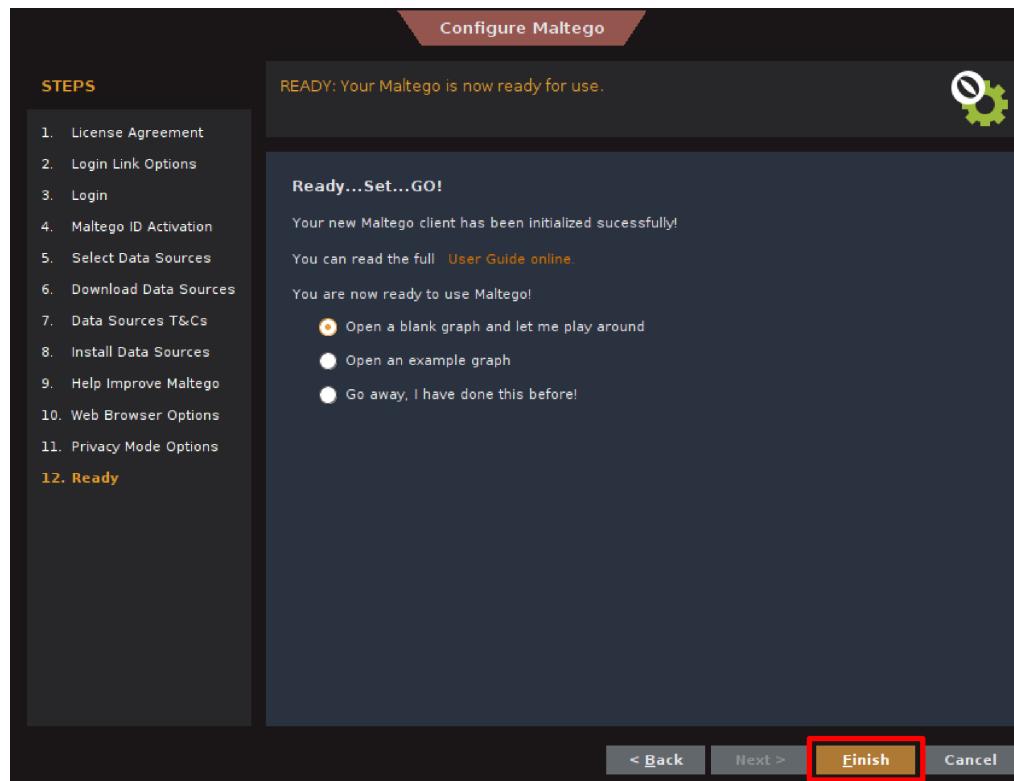


MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

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

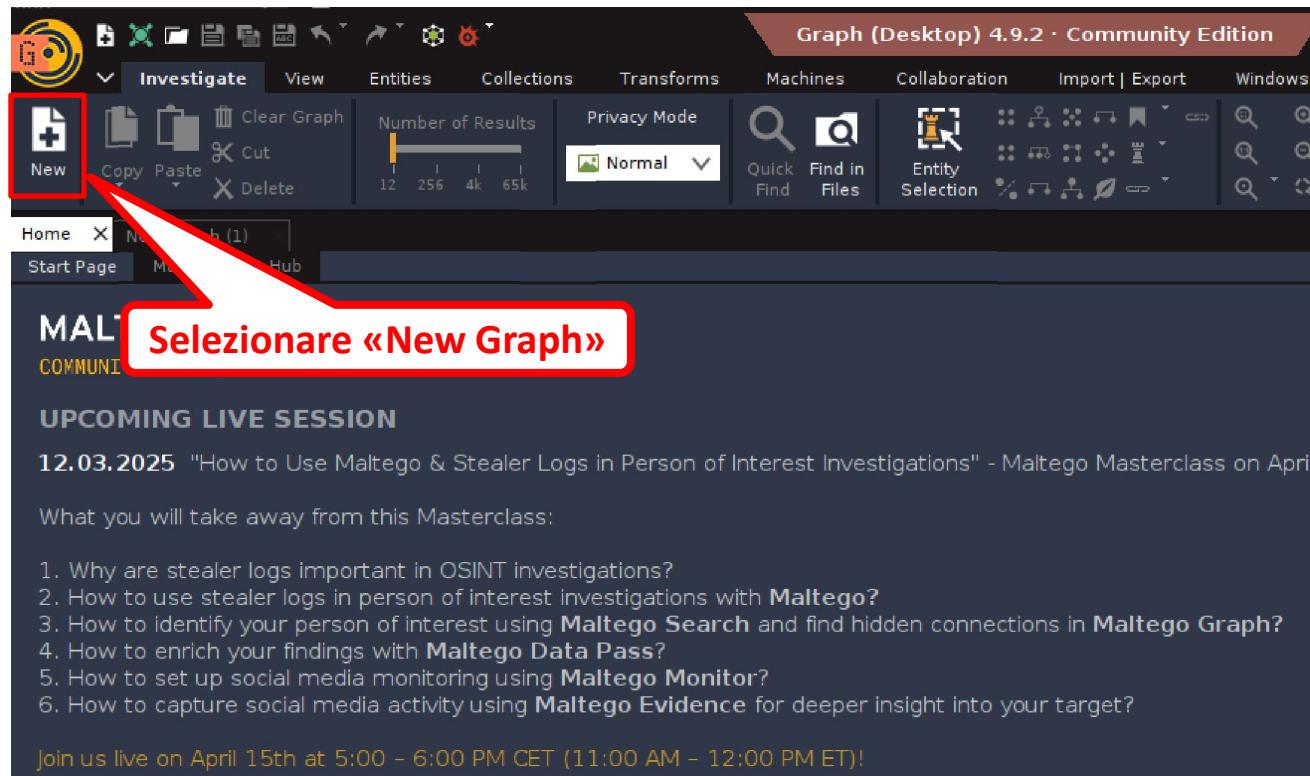


MALTEGO

Utilizzo di Crawler

Maltego – Primo Avvio

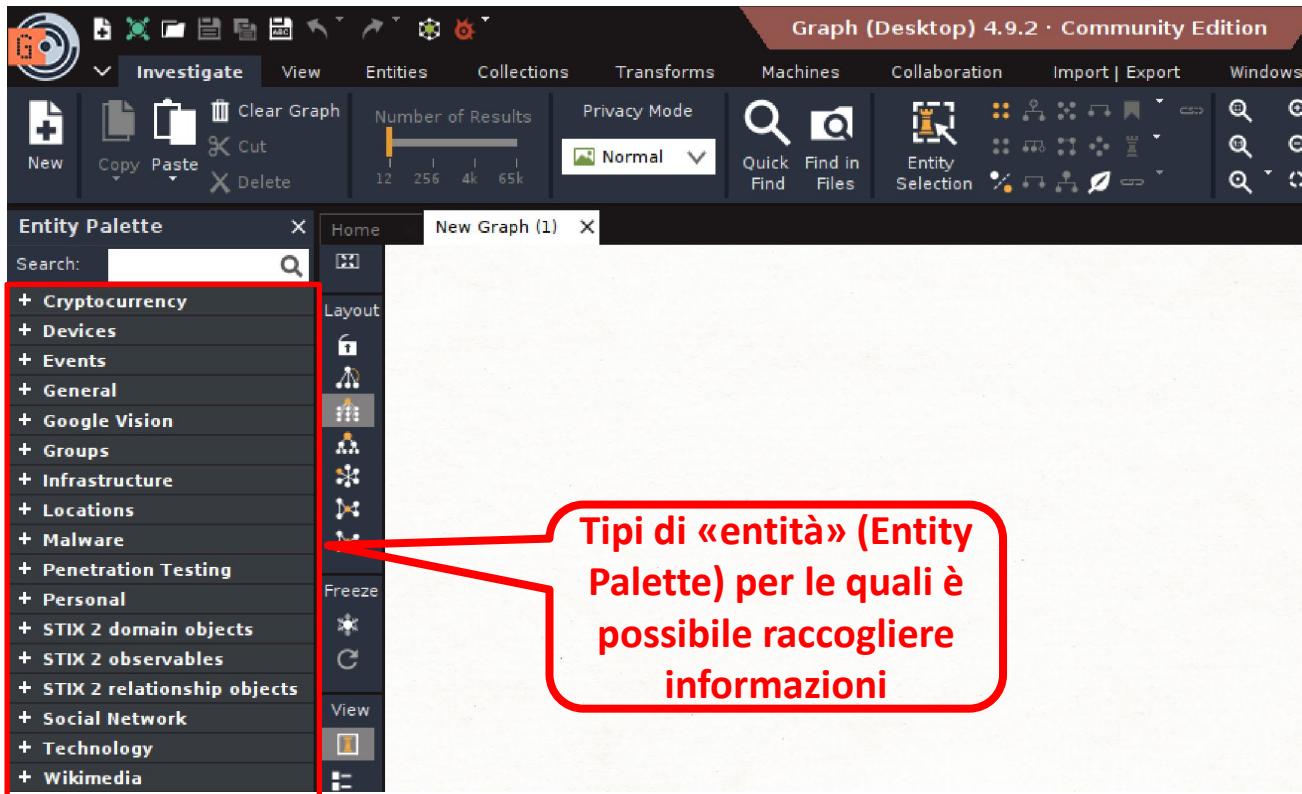
- Una volta terminata la registrazione del prodotto, è possibile tornare alla schermata di Maltego per poterlo utilizzare



Utilizzo di Crawler

Maltego – Primo Avvio

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



Entity Palette

Tipi di «entità» (Entity Palette) per le quali è possibile raccogliere informazioni



MALTEGO

Information Gathering

Utilizzo di Crawler

Maltego – Entity Palette

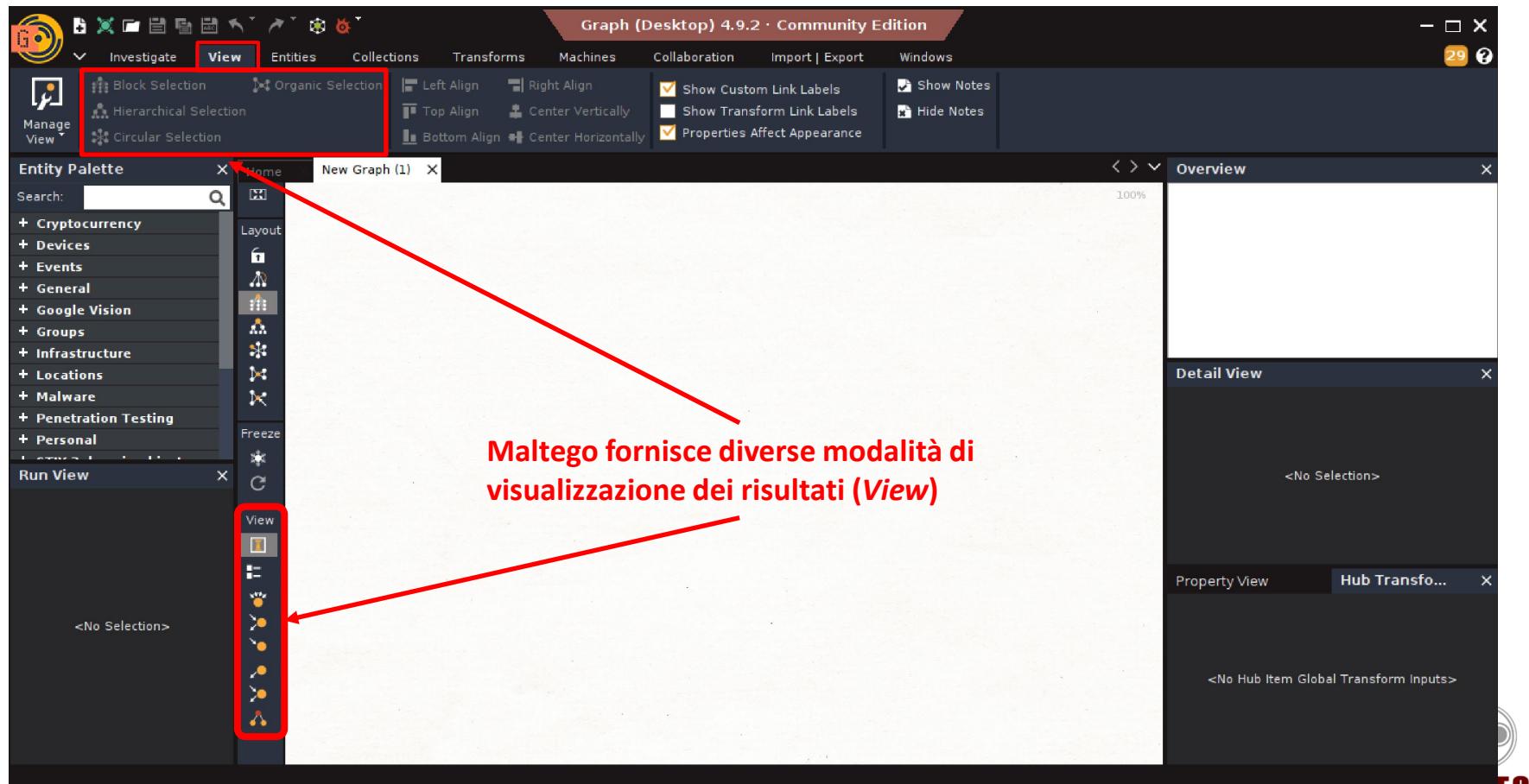
- Le entità (*Entity Palette*) sono suddivise in 17 gruppi
 - Cryptocurrency
 - Devices
 - Events
 - Groups
 - General
 - Google Vision
 - Infrastructure
 - Locations
 - Malware
 - Penetration Testing
 - Personal
 - Social Network
 - Technology
 - Wikimedia
 - STIX 2 domain objects
 - STIX 2 observables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



MALTEGO

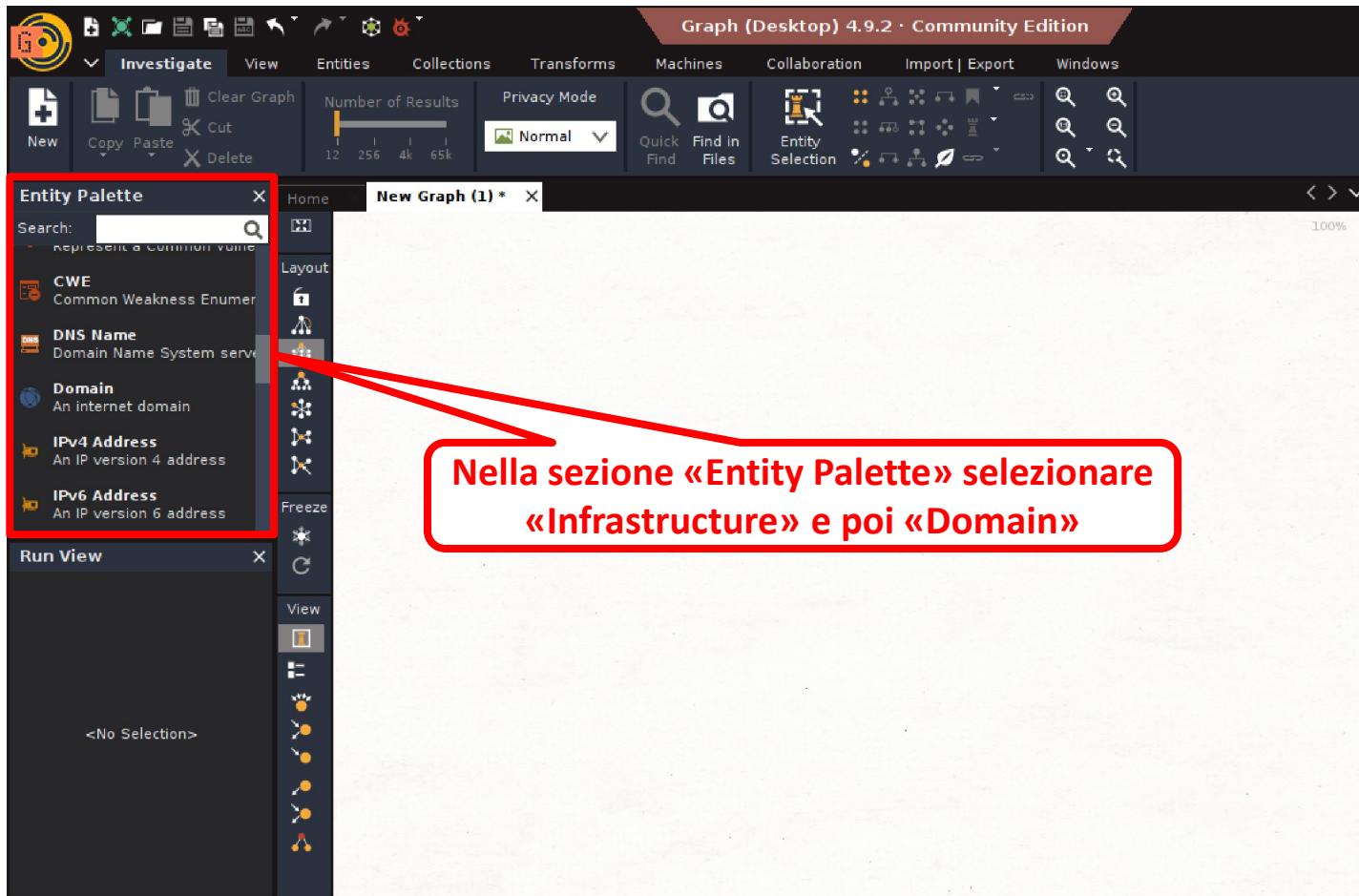
Utilizzo di Crawler

Maltego – View



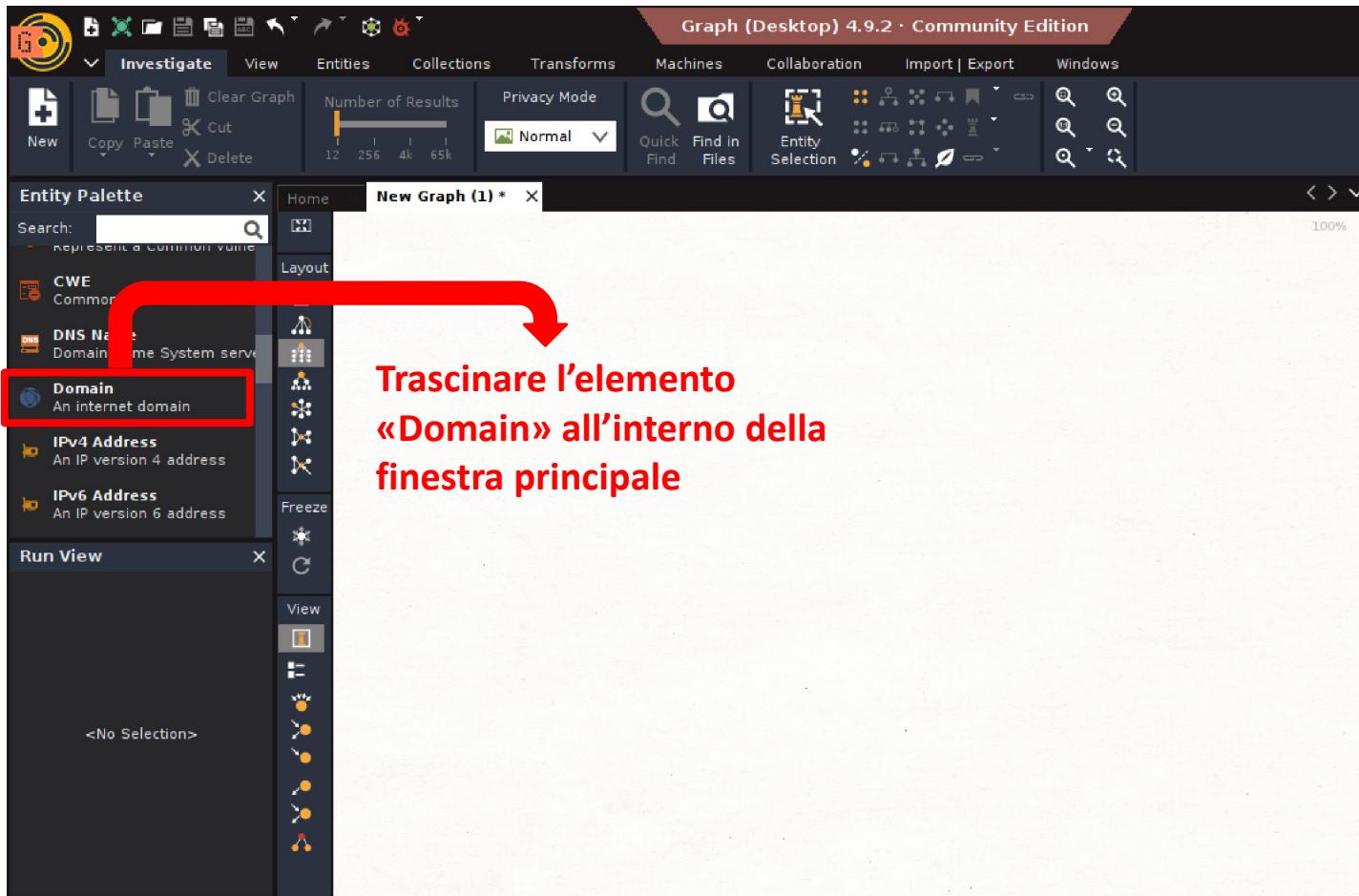
Utilizzo di Crawler

Maltego – Esempio 1



Utilizzo di Crawler

Maltego – Esempio 1



Information Gathering

Utilizzo di Crawler

Maltego – Esempio 1

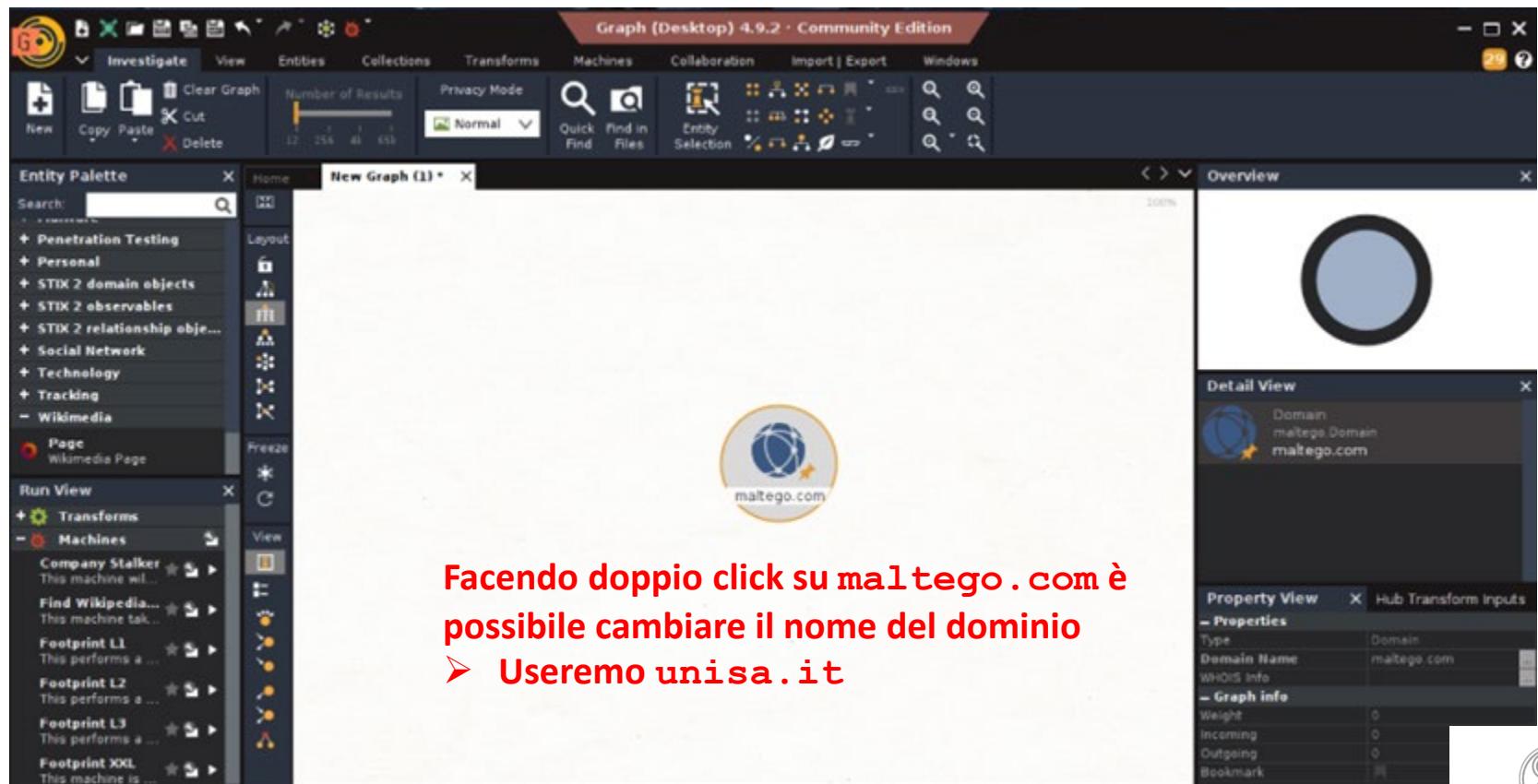
The screenshot shows the Maltego interface with the following components:

- Entity Palette:** On the left, it lists various entity types under categories like Penetration Testing, Personal, STIX, Social Network, Technology, Tracking, and Wikimedia. Under "Run View", there are sections for Transformations and Machines, with several options listed.
- Graph Area:** The central area displays a search result for "maltego.com". A large blue circular node is shown with the Maltego logo and the URL "maltego.com". Below the node, the text "Nella finestra principale comparirà un dominio, chiamato maltego . com" is overlaid in red.
- Detail View:** To the right of the graph, it shows the domain "maltego.Domain maltego.com".
- Property View:** At the bottom right, it provides detailed properties for the domain, including "Domain Name: maltego.com" and "Graph info: Weight: 0, Incoming: 0, Outgoing: 0, Bookmark: 0".



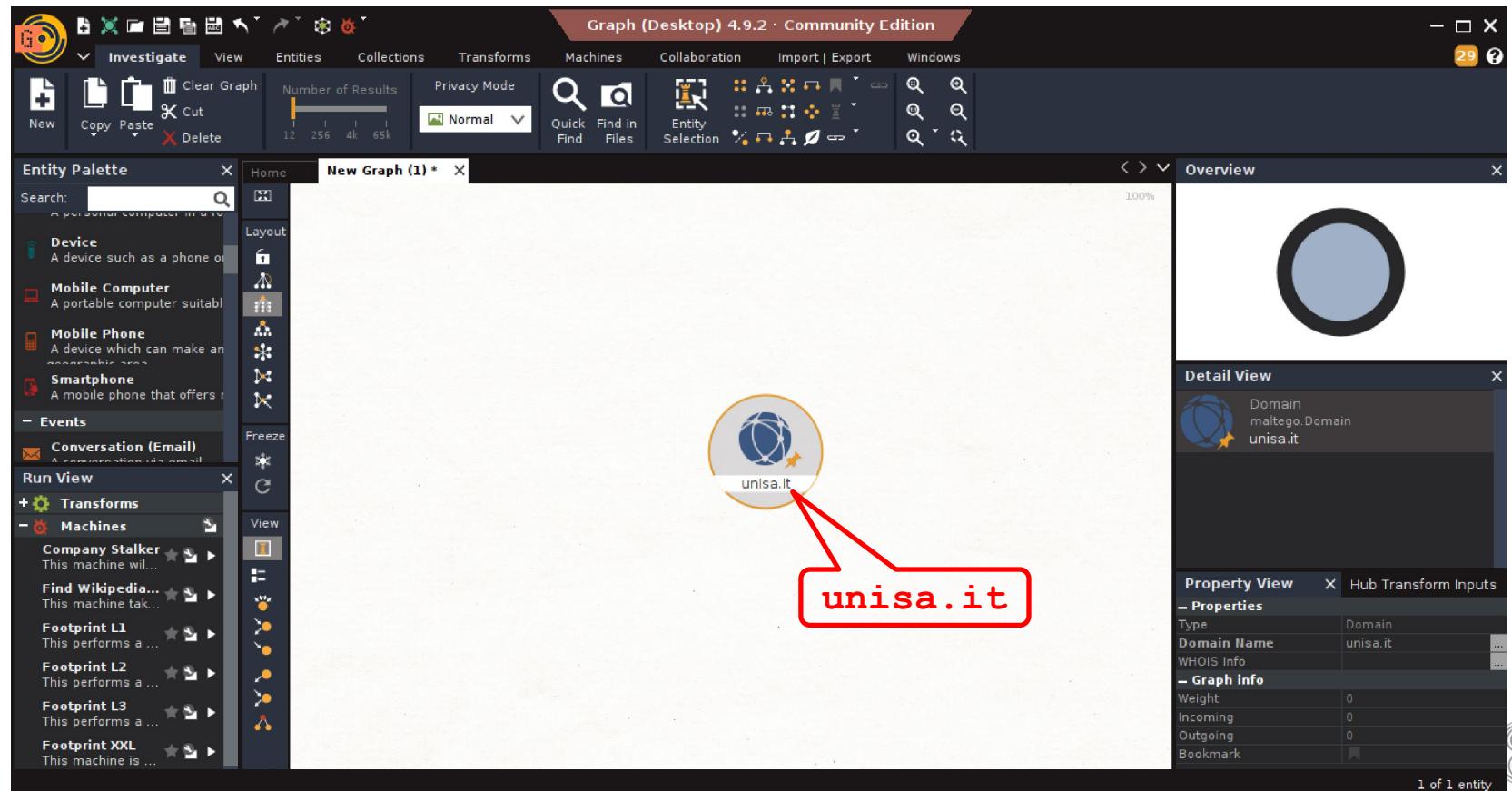
Utilizzo di Crawler

Maltego – Esempio 1



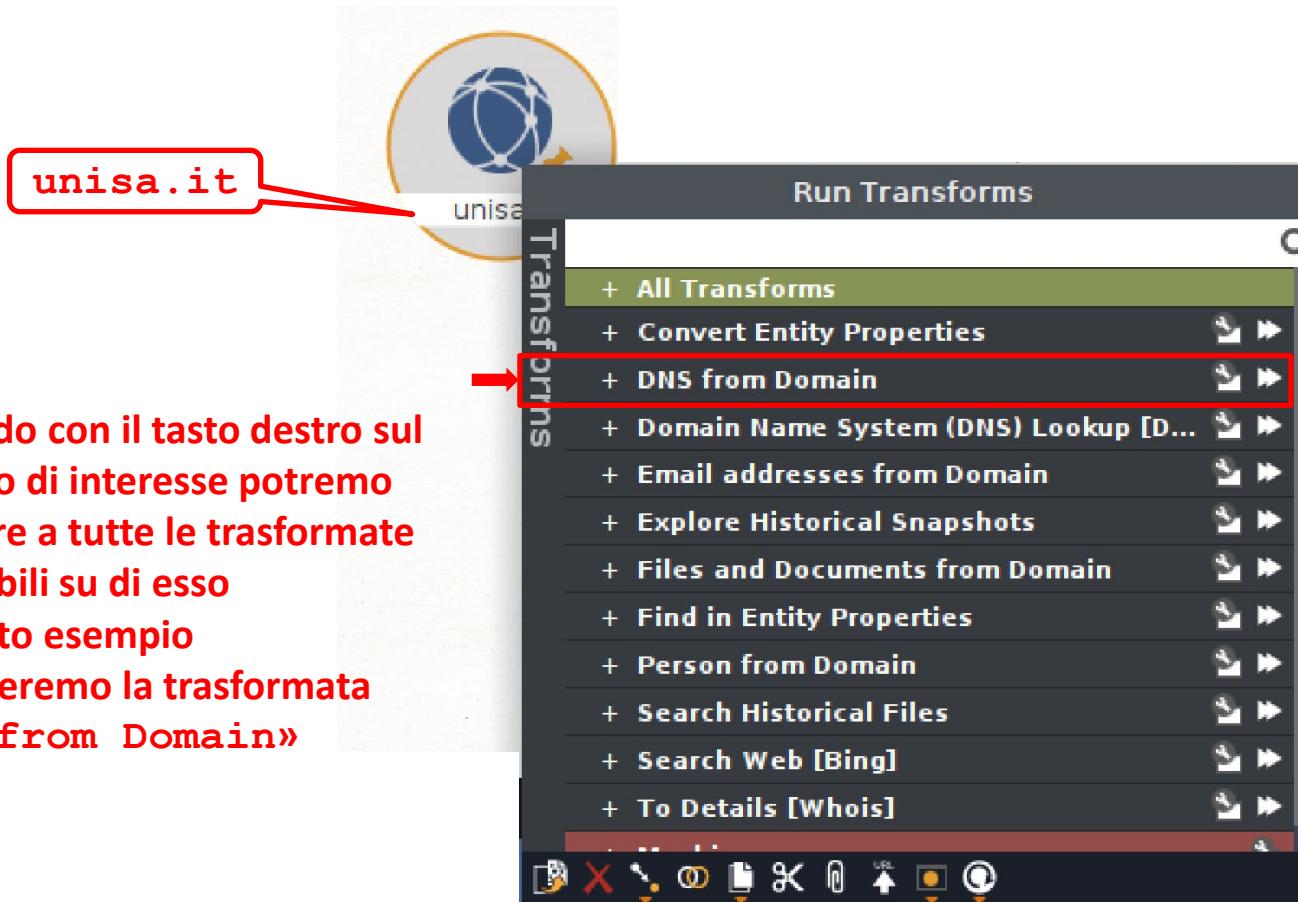
Utilizzo di Crawler

Maltego – Esempio 1



Utilizzo di Crawler

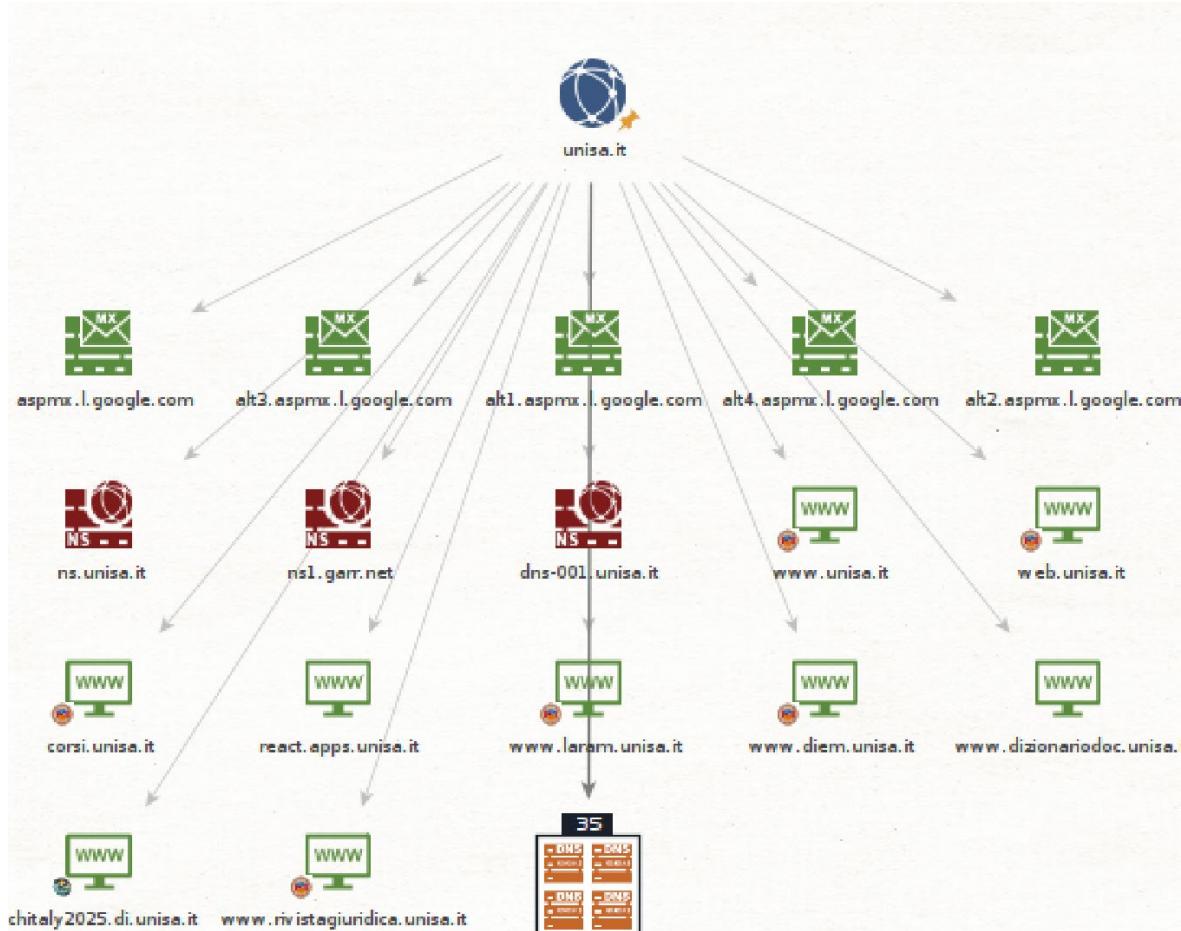
Maltego – Esempio 1



- **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»**

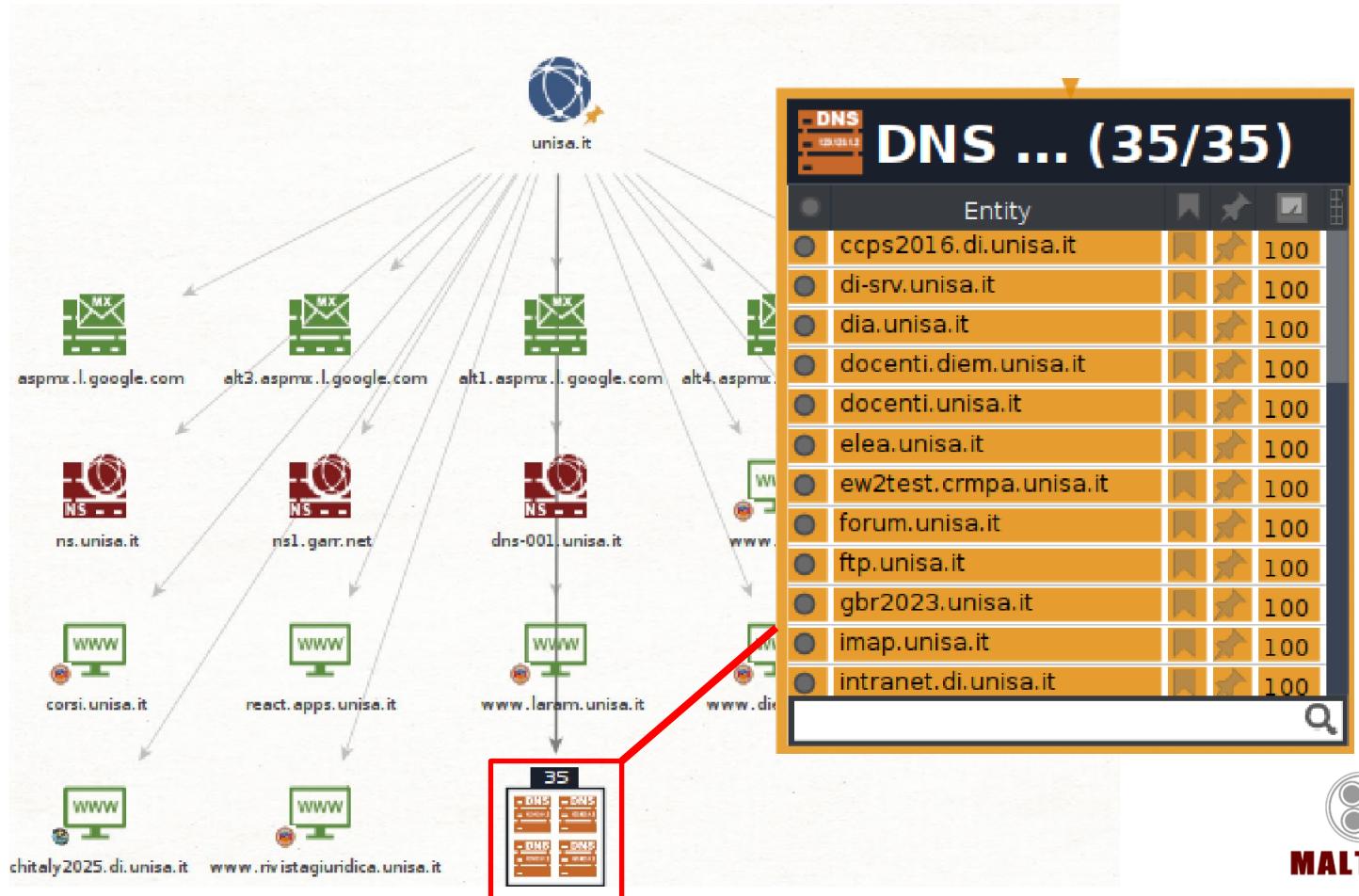
Utilizzo di Crawler

Maltego – Esempio 1



Utilizzo di Crawler

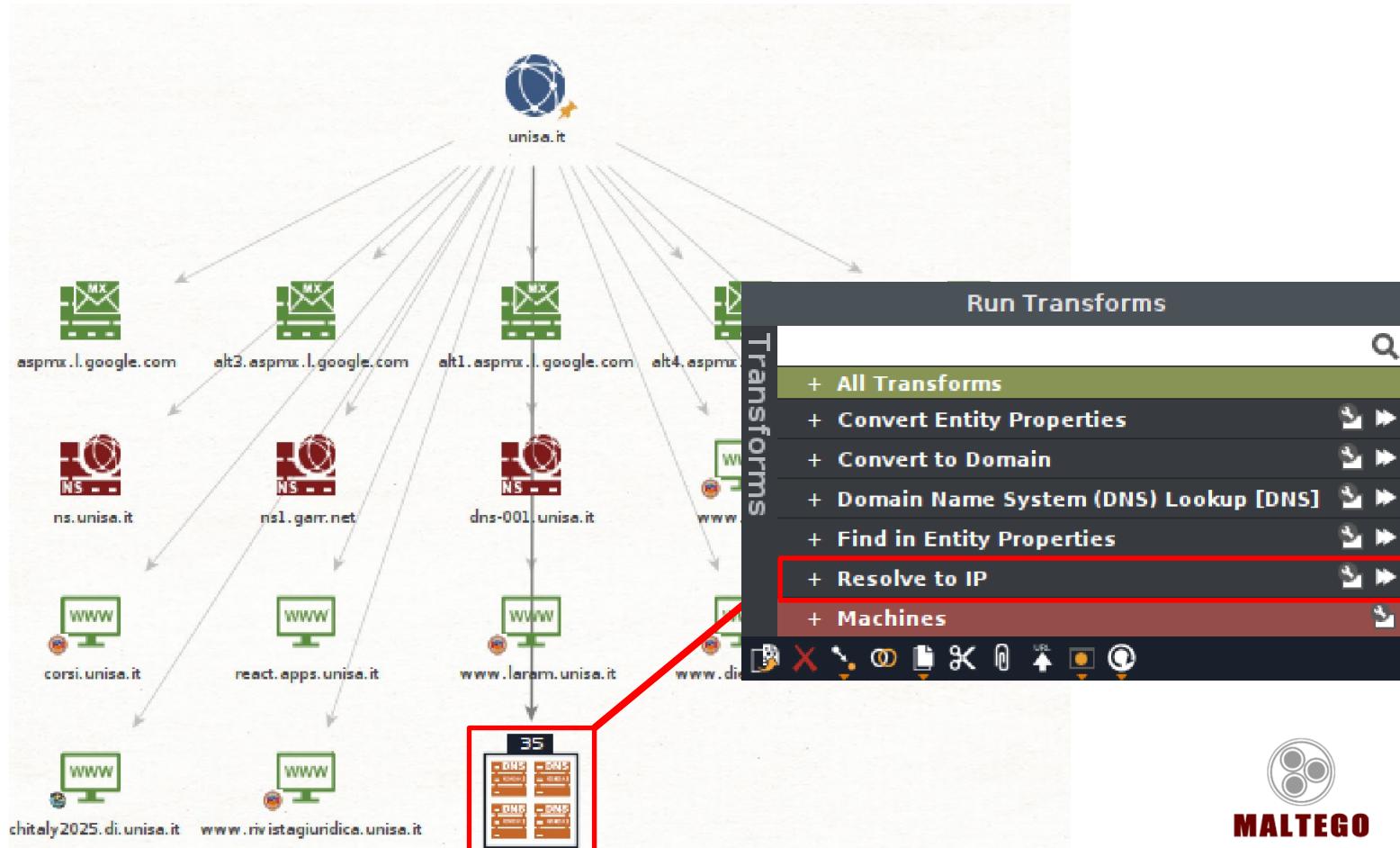
Maltego – Esempio 1



Information Gathering

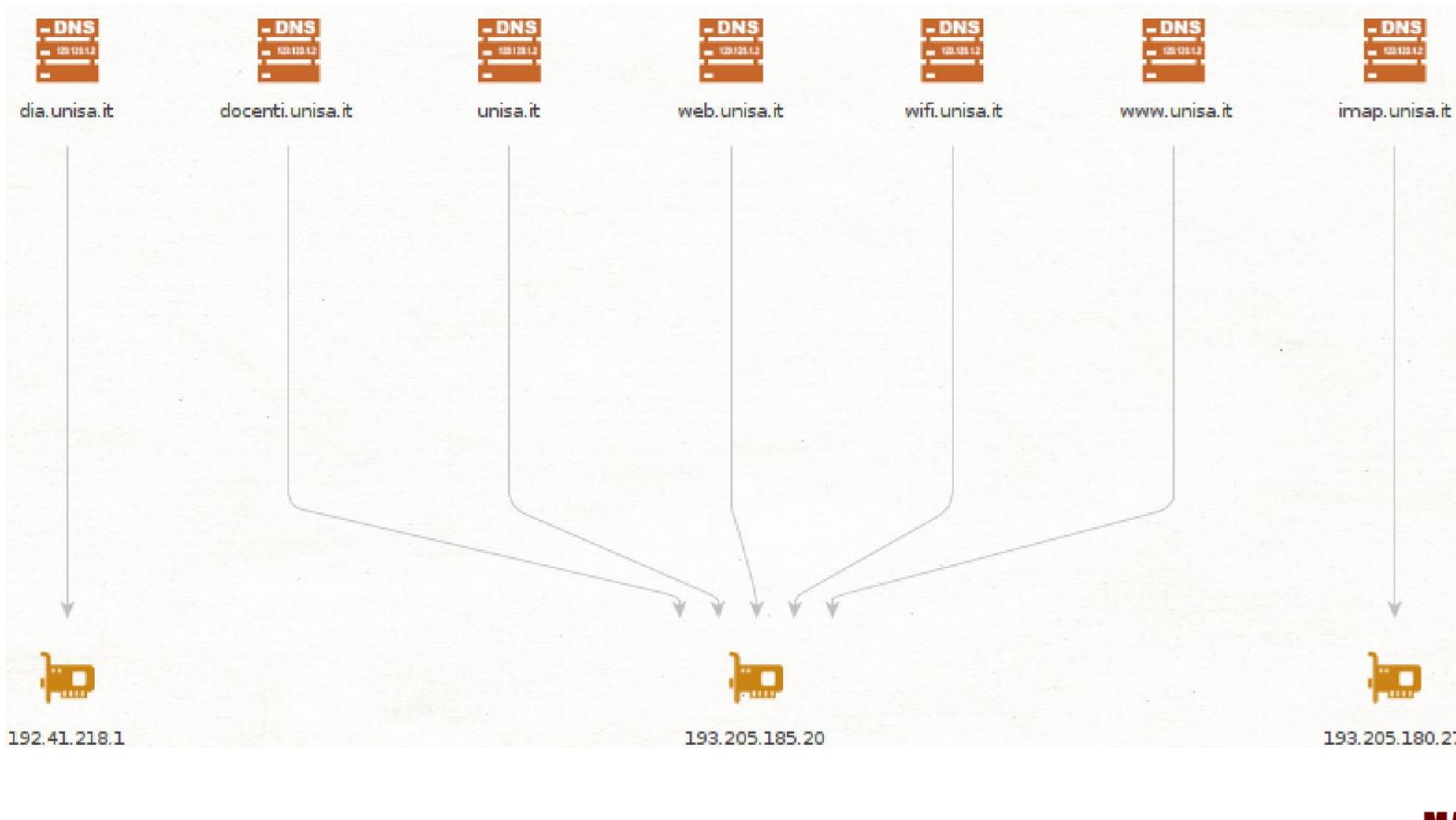
Utilizzo di Crawler

Maltego – Esempio 2



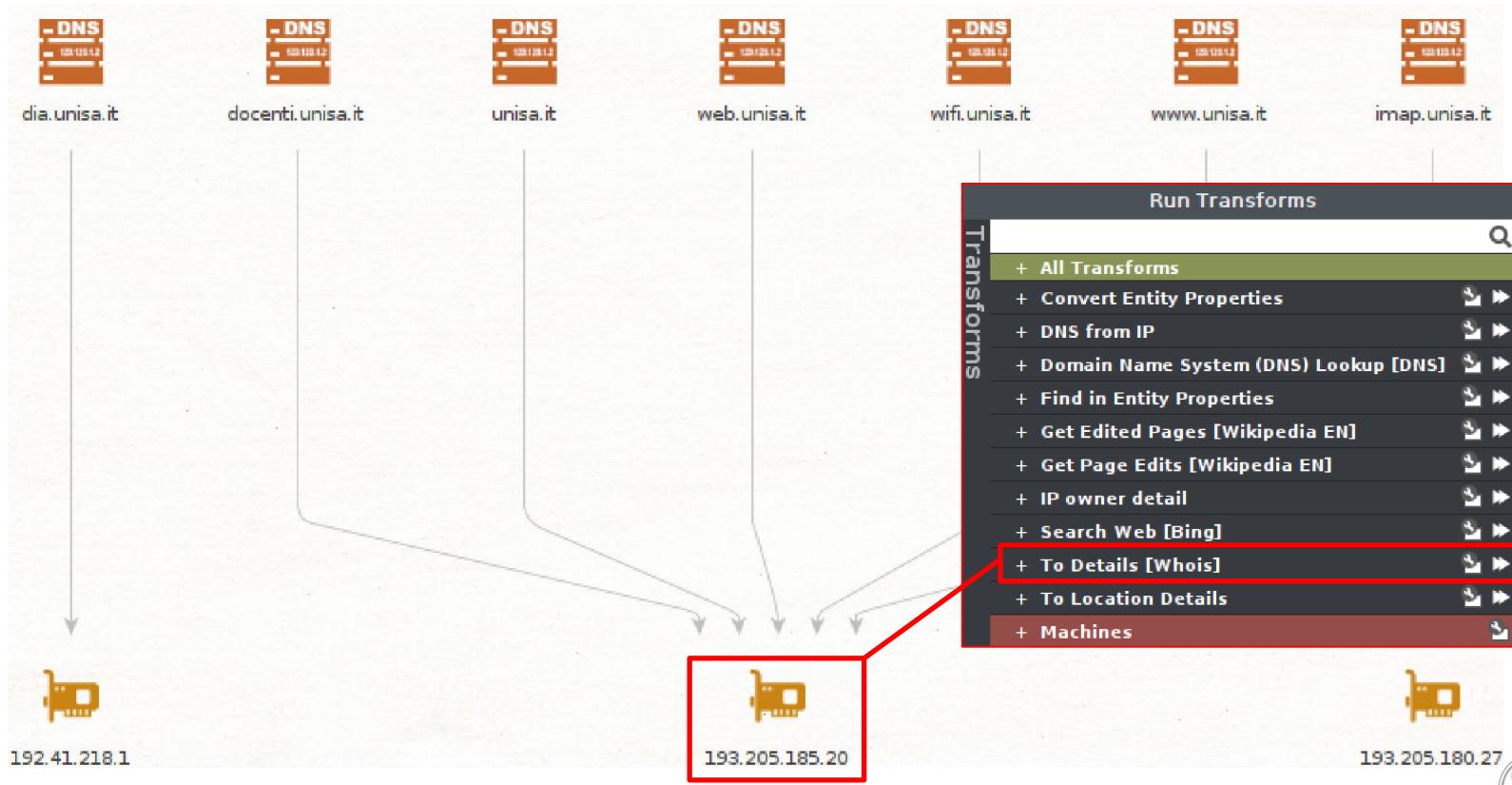
Utilizzo di Crawler

Maltego – Esempio 2



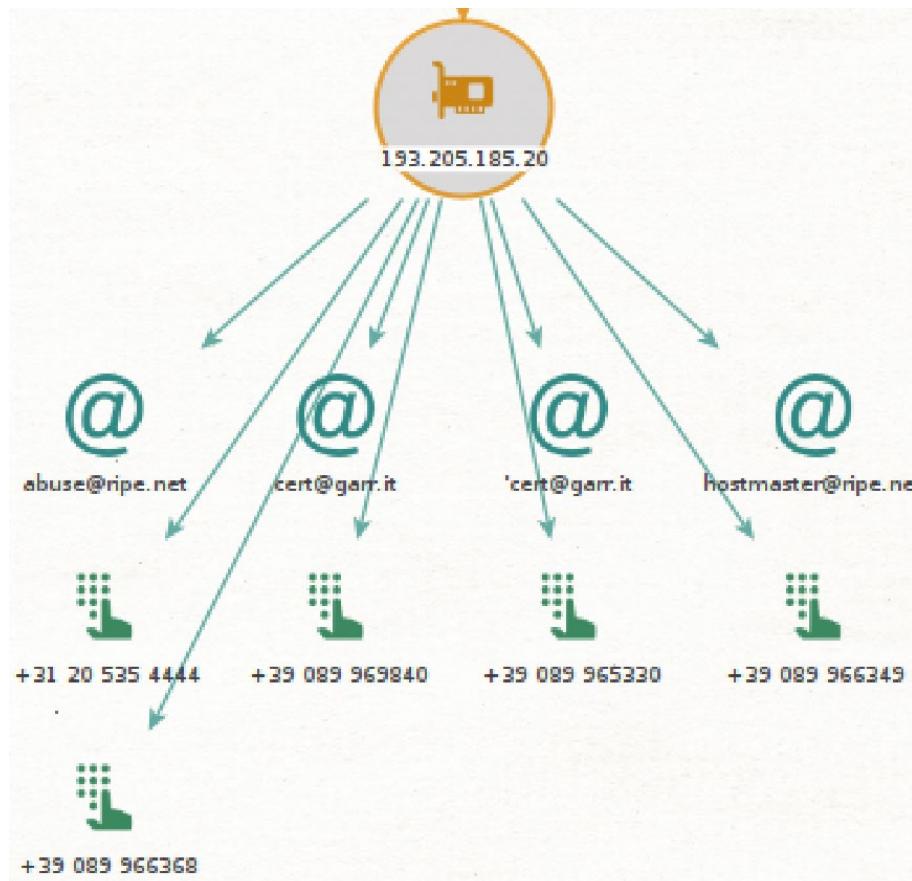
Utilizzo di Crawler

Maltego – Esempio 3



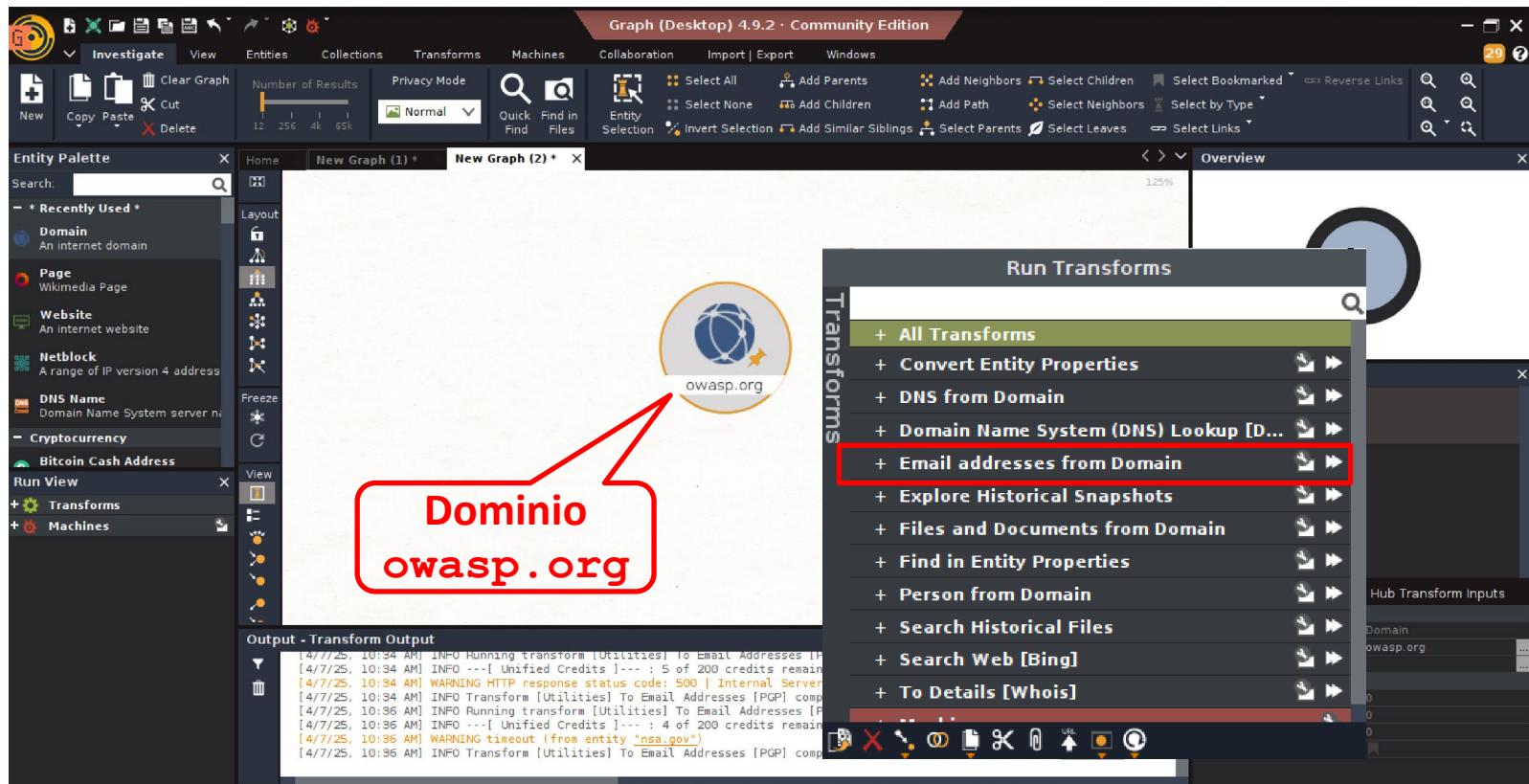
Utilizzo di Crawler

Maltego – Esempio 3



Utilizzo di Crawler

Maltego – Esempio 4



Utilizzo di Crawler

Maltego – Esempio 4



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

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

Utilizzo di Crawler

SpiderFoot – Esempio

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

```
(kali㉿kali)-[~]
$ sudo spiderfoot -l 127.0.0.1:5001
[sudo] password for kali:

*****
Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:5001/
*****
2024-04-08 12:19:15,712 [INFO] sf : Starting web server at 127.0.0.1:5001 .
..
2024-04-08 12:19:15,717 [WARNING] sf :
*****
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
*****
```

Utilizzo di Crawler

SpiderFoot – Esempio

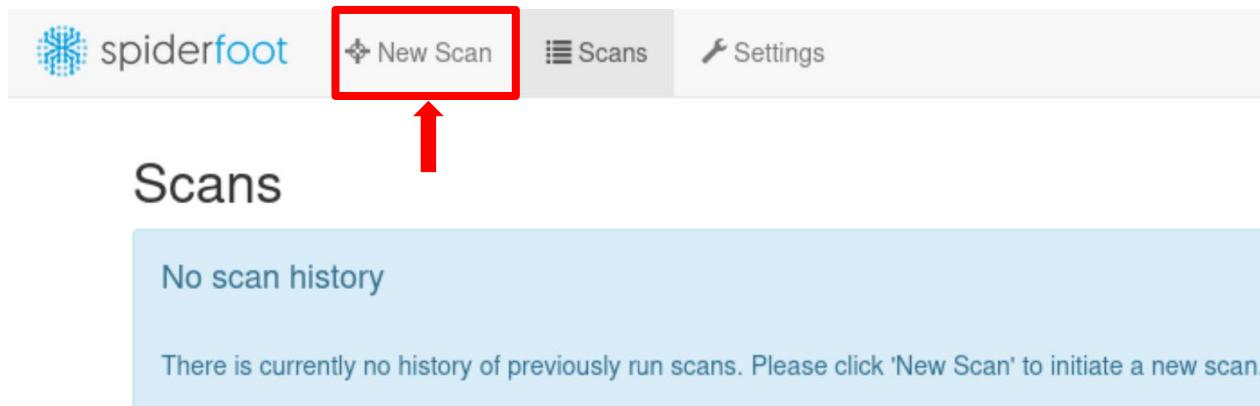
- Spiderfoot può essere utilizzato tramite Web browser, accedendo all'URL seguente
 - <http://127.0.0.1:5001/>

The screenshot shows the SpiderFoot web application interface. At the top, there is a navigation bar with the logo 'spiderfoot' (a blue stylized snowflake icon), a 'New Scan' button (with a diamond icon), a 'Scans' button (with a list icon, which is highlighted in grey), and a 'Settings' button (with a wrench icon). Below the navigation bar, the main content area has a light blue header with the title 'Scans'. Underneath, a larger light blue box contains the text 'No scan history' in a dark blue font. At the bottom of this box, a smaller message reads: 'There is currently no history of previously run scans. Please click 'New Scan' to initiate a new scan.'.

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»)

New Scan

Scan Name

The name of this scan.

Scan Target

The target of your scan.

Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:
Domain Name: e.g. example.com
IPv4 Address: e.g. 1.2.3.4
IPv6 Address: e.g. 2606:4700:4700::1111
Hostname/Sub-domain: e.g. abc.example.com
Subnet: e.g. 1.2.3.0/24
Bitcoin Address: e.g. 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R
E-mail address: e.g. bob@example.com
Phone Number: e.g. +12345678901 (E.164 format)
Human Name: e.g. "John Smith" (must be in quotes)
Username: e.g. "jsmith2000" (must be in quotes)
Network ASN: e.g. 1234

→ By Use Case

By Required Data

By Module

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

All

Get anything and everything about the target.

All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

Footprint

Understand what information this target exposes to the Internet.

Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

Investigate

Best for when you suspect the target to be malicious but need more information.

Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

Passive

When you don't want the target to even suspect they are being investigated.

As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

Run Scan Now



Utilizzo di Crawler

SpiderFoot – Esempio

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

New Scan

Scan Name

The name of this scan.

Scan Target

The target of your scan.

💡 Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:

Domain Name: e.g. example.com

IPv4 Address: e.g. 1.2.3.4

IPv6 Address: e.g. 2606:4700:4700::1111

Hostname/Sub-domain: e.g. abc.example.com

Subnet: e.g. 1.2.3.0/24

Bitcoin Address: e.g. 1HesYJSP1QqcyPEjnQ9vzBL1wuJuNGe7R

E-mail address: e.g. bob@example.com

Phone Number: e.g. +12345678901 (E.164 format)

Human Name: e.g. "John Smith" (must be in quotes)

Username: e.g. "jsmith2000" (must be in quotes)

Network ASN: e.g. 1234

→ **By Use Case**

By Required Data

By Module

All

Get anything and everything about the target.

All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

Footprint

Understand what information this target exposes to the Internet.

Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

Investigate

Best for when you suspect the target to be malicious but need more information.

Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

Passive

When you don't want the target to even suspect they are being investigated.

As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

Run Scan Now



Utilizzo di Crawler

SpiderFoot – Esempio

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

New Scan

Scan Name

Scan Target

Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:

- Domain Name: e.g. example.com
- IPv4 Address: e.g. 1.2.3.4
- IPv6 Address: e.g. 2608:4700:4700::1111
- Hostname/Sub-domain: e.g. abc.example.com
- Subnet: e.g. 1.2.3.0/24
- Bitcoin Address: e.g. 1HesYJSP1QqcyPEjnQ9vzBL1wuJruNGe7R
- E-mail address: e.g. bob@example.com
- Phone Number: e.g. +12345678901 (E.164 format)
- Human Name: e.g. "John Smith" (must be in quotes)
- Username: e.g. "jsmith2000" (must be in quotes)
- Network ASN: e.g. 1234

All

Get anything and everything about the target.

All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

Footprint

Understand what information this target exposes to the Internet.

Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

Investigate

Best for when you suspect the target to be malicious but need more information.

Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

Passive

When you don't want the target to even suspect they are being investigated.

As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

Run Scan Now

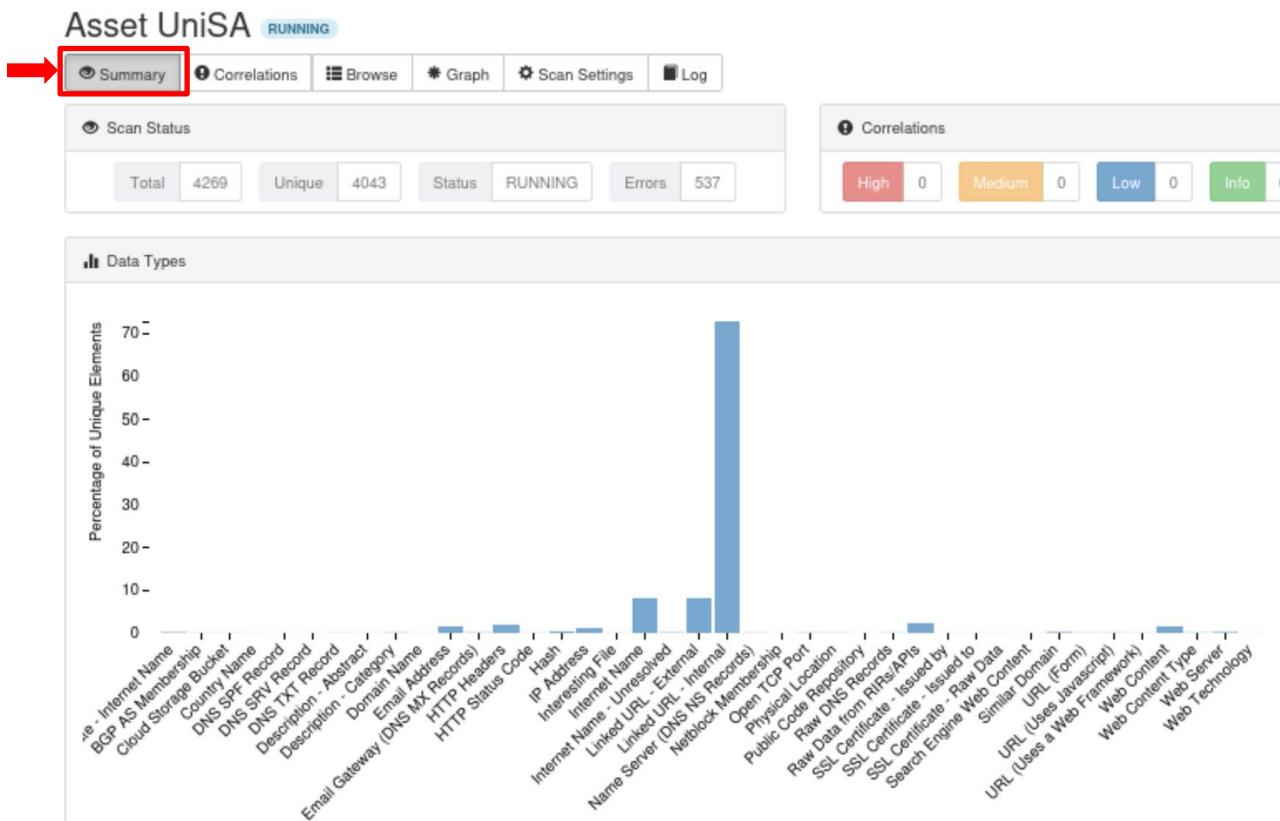
Avviato il processo di scansione, potranno subito essere visualizzati i relativi risultati intermedi



Utilizzo di Crawler

SpiderFoot – Esempio

- Riepilogo dei risultati ottenuti dalla scansione



Utilizzo di Crawler

SpiderFoot – Esempio

- Risultati ottenuti dalla scansione (*Indirizzi IP*)

Asset UniSA RUNNING

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

Utilizzo di Crawler

SpiderFoot – Esempio

- Risultati ottenuti dalla scansione (*Sottodomini*)

Asset UniSA RUNNING

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

Utilizzo di Crawler

SpiderFoot – Esempio

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

Asset UniSA RUNNING

Summary Correlations Browse Graph Scan Settings Log

Browse / Email Address

<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	20centroictstaff@unisa.it	unisa.it	sfp_emailformat	2024-03-23 07:19:07
<input type="checkbox"/>	20ritcas@unisa.it	unisa.it	sfp_emailformat	2024-03-23 07:19:07
<input type="checkbox"/>	20rpellella@unisa.it	unisa.it	sfp_emailformat	2024-03-23 07:19:07
<input type="checkbox"/>	G.MADONNA3@studenti.unisa.it	unisa.it	sfp_grep_app	2024-03-23 07:18:24
<input type="checkbox"/>	GMadonna@studenti.unisa.it	unisa.it	sfp_grep_app	2024-03-23 07:18:28
<input type="checkbox"/>	Gianni@studenti.unisa.it	unisa.it	sfp_grep_app	2024-03-23 07:18:34
<input type="checkbox"/>	GianniMorandiManiGrandi@studenti.unisa.it	unisa.it	sfp_grep_app	2024-03-23 07:18:26
<input type="checkbox"/>	ProvaUser@studenti.unisa.it	unisa.it	sfp_grep_app	2024-03-23 07:18:32
<input type="checkbox"/>	a.prova@studenti.unisa.it	unisa.it	sfp_grep_app	2024-03-23 07:18:24
<input type="checkbox"/>	a.raiola14@studenti.unisa.it	unisa.it	sfp_grep_app	2024-03-23 07:18:38

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

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

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 relativi all'asset

The screenshot shows the terminal output of the OWASP Amass project. At the top, there is a decorative banner with various symbols like dots, dashes, and numbers. Below the banner, the text "v4.2.0" and "OWASP Amass Project - @owaspamass In-depth Attack Surface Mapping and Asset Discovery" is displayed. The main content is the help text for the "amass intel" command:

```
Usage: amass intel [options]
-h      Show the program usage message
--help   Show the program usage message
--version
        Print the version number of this Amass binary

Subcommands:
amass intel - Discover targets for enumerations
amass enum  - Perform enumerations and network mapping
```

Amass
OWASP®

Utilizzo di Crawler

OWASP Amass – Comando intel

➤ **amass intel -h**

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

      -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)
archeo5dbc.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)
```

Utilizzo di Crawler

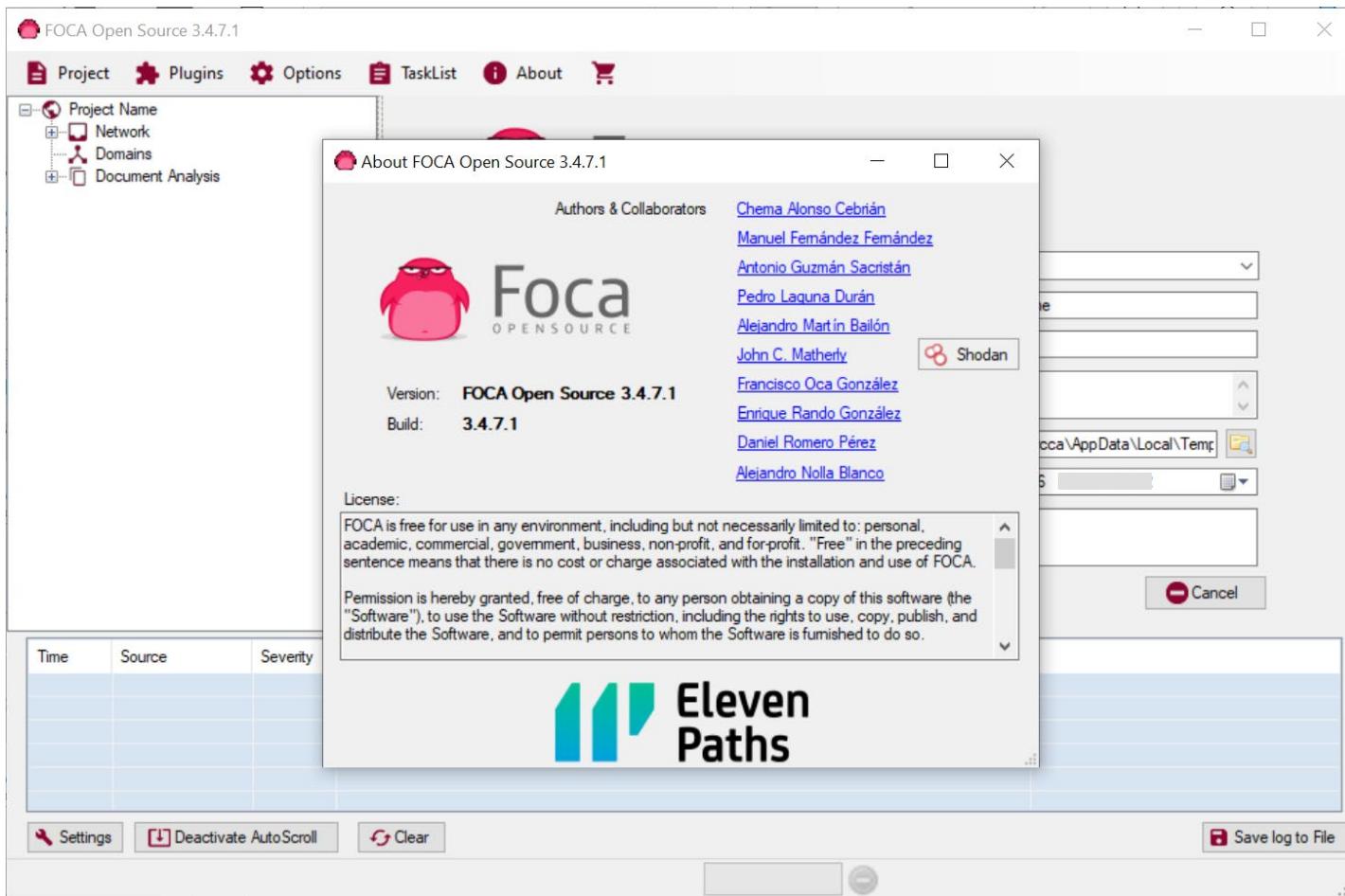
Ricerca di Metadati – FOCA

- ***FOCA (Fingerprinting Organizations with Collected Archives)***
 - 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>



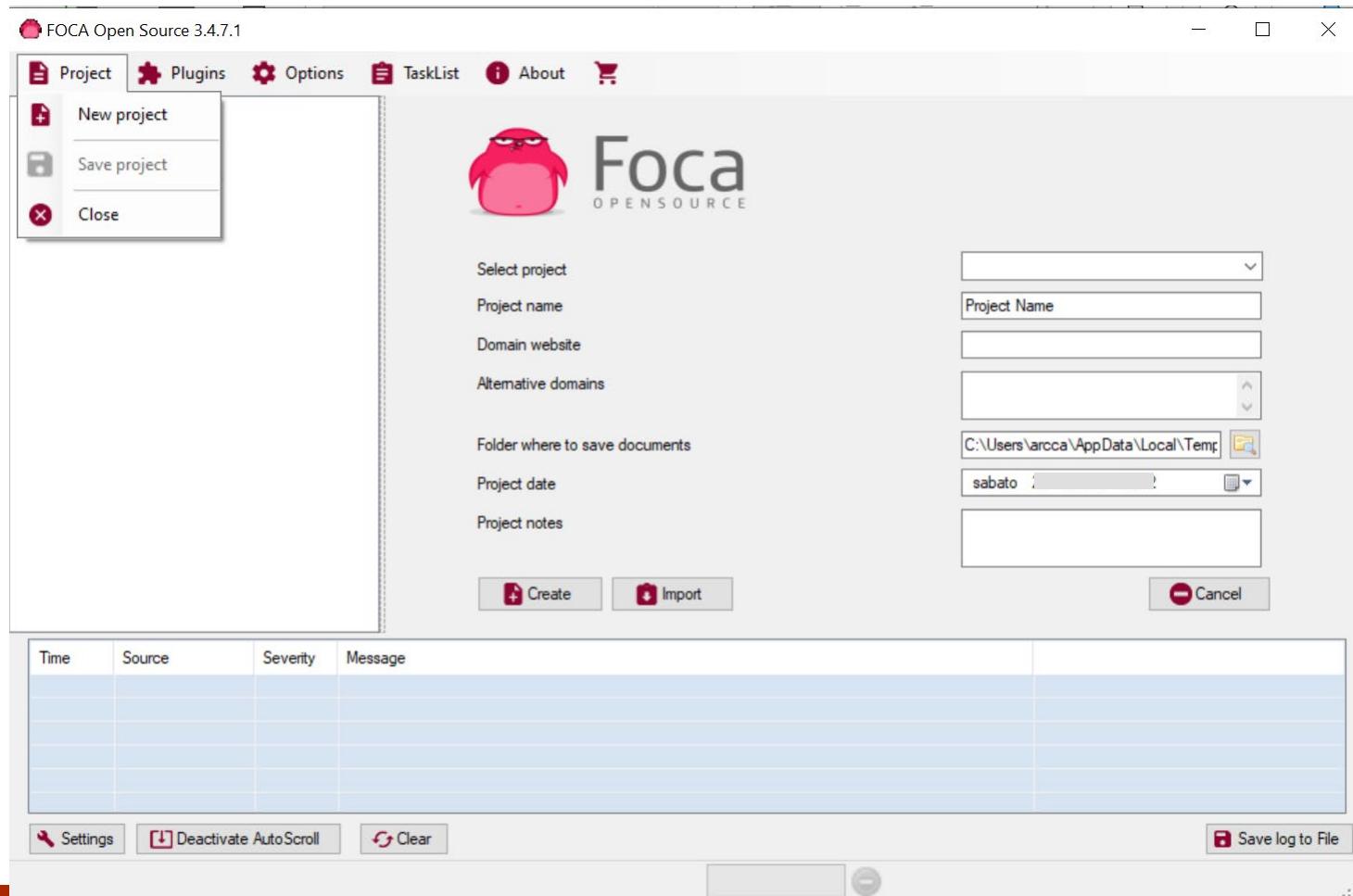
Utilizzo di Crawler

Ricerca di Metadati – FOCA



Utilizzo di Crawler

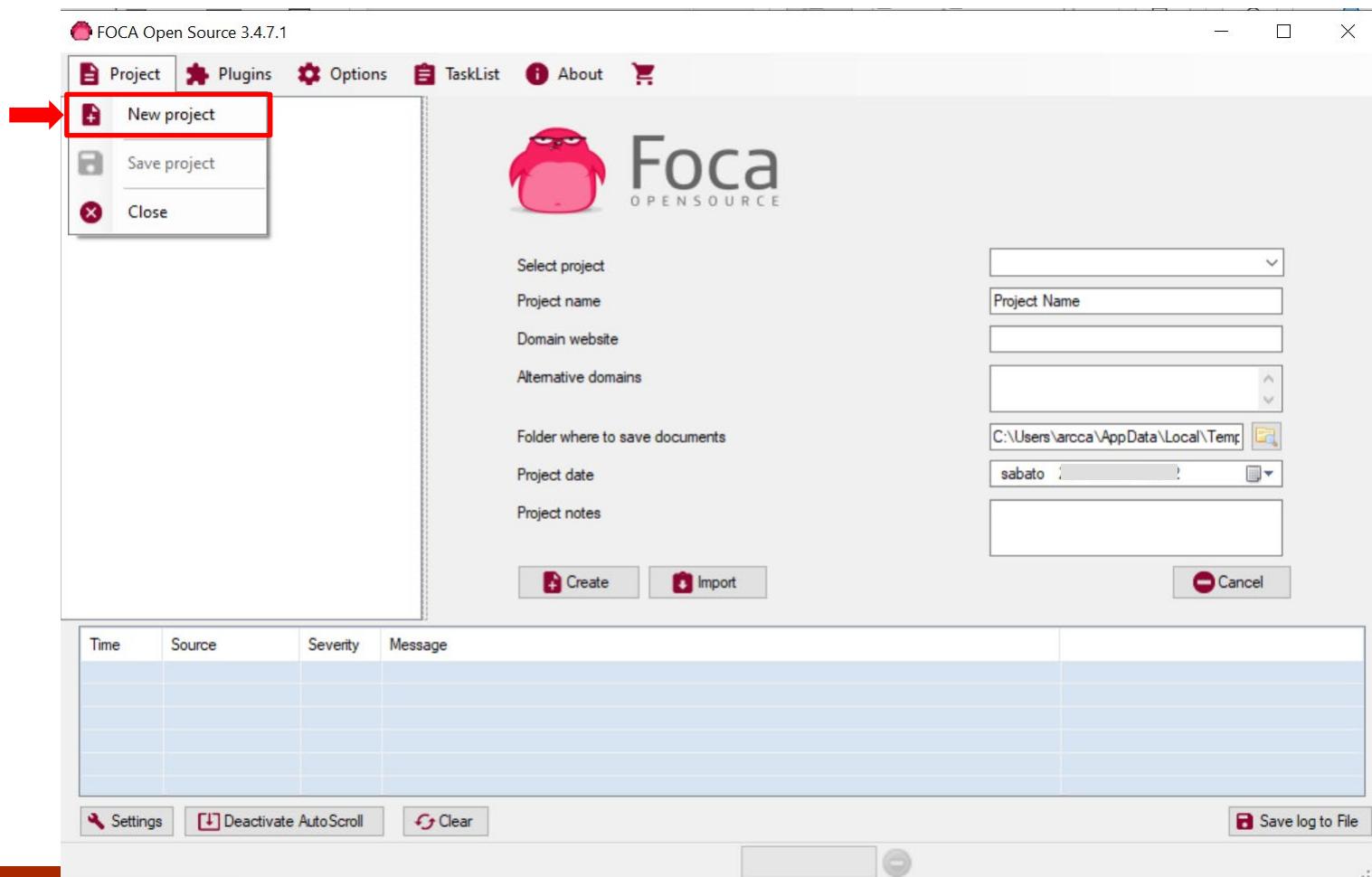
Ricerca di Metadati – FOCA



Information Gathering

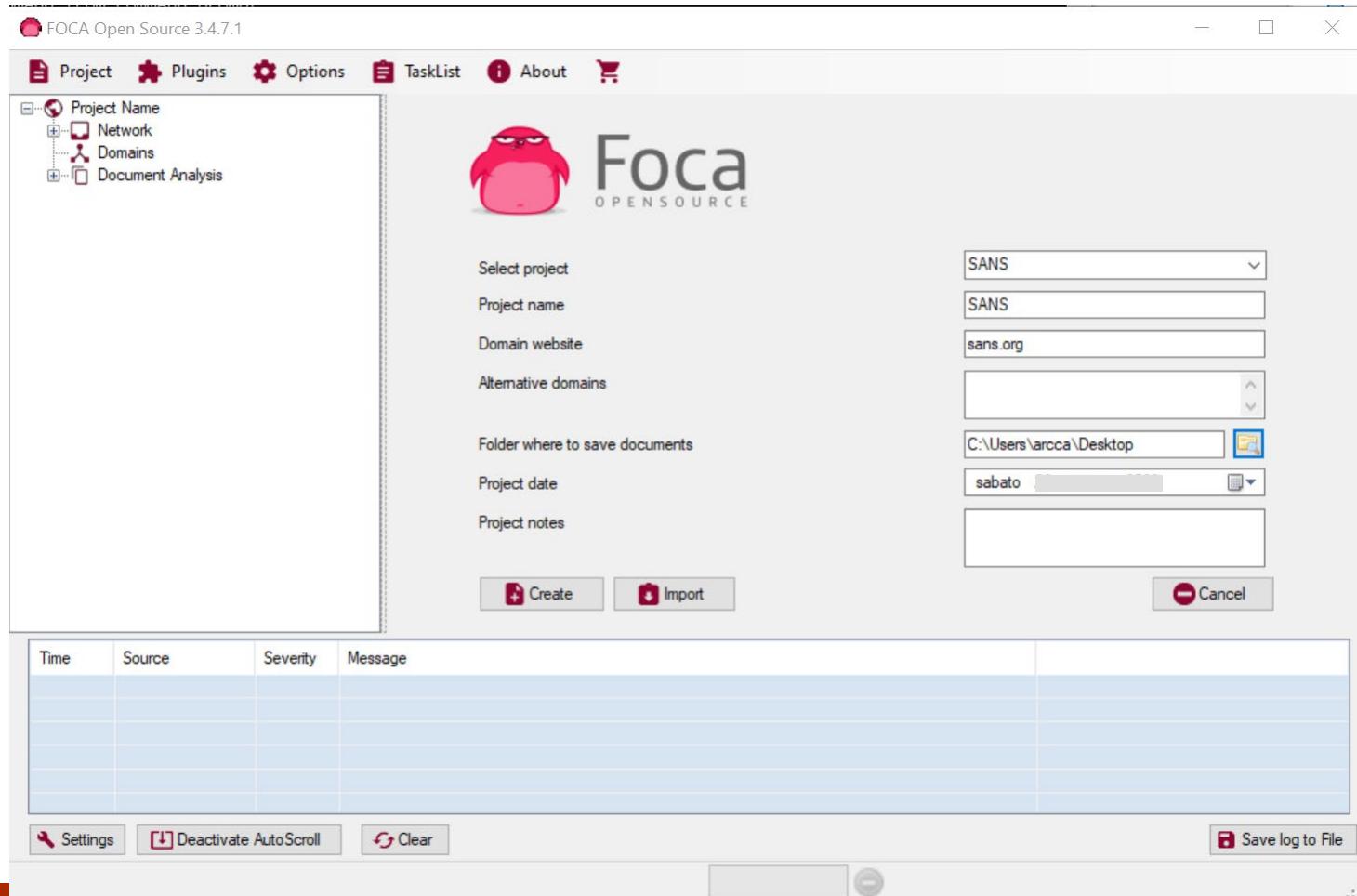
Utilizzo di Crawler

Ricerca di Metadati – FOCA



Utilizzo di Crawler

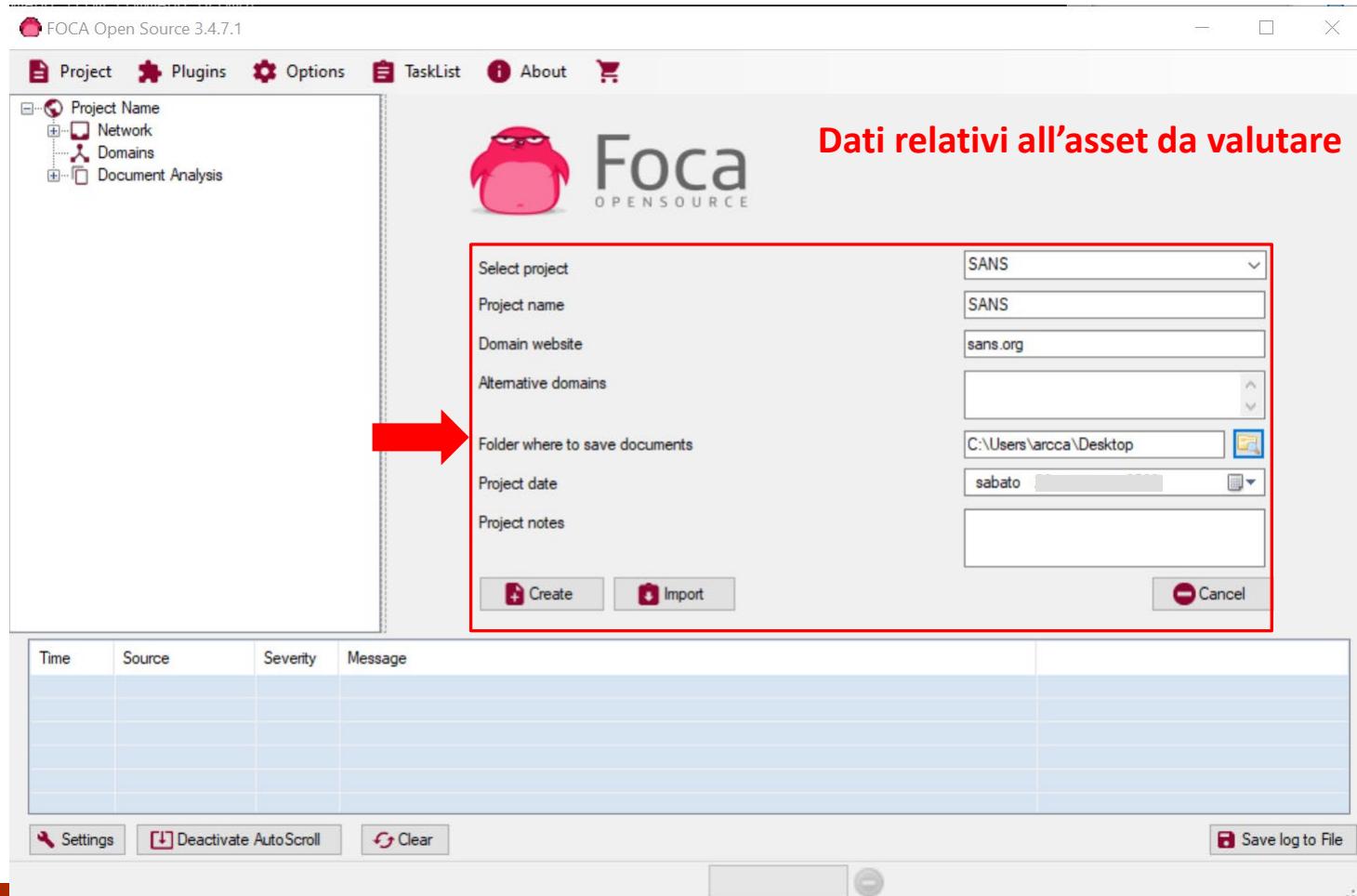
Ricerca di Metadati – FOCA – Esempio



Information Gathering

Utilizzo di Crawler

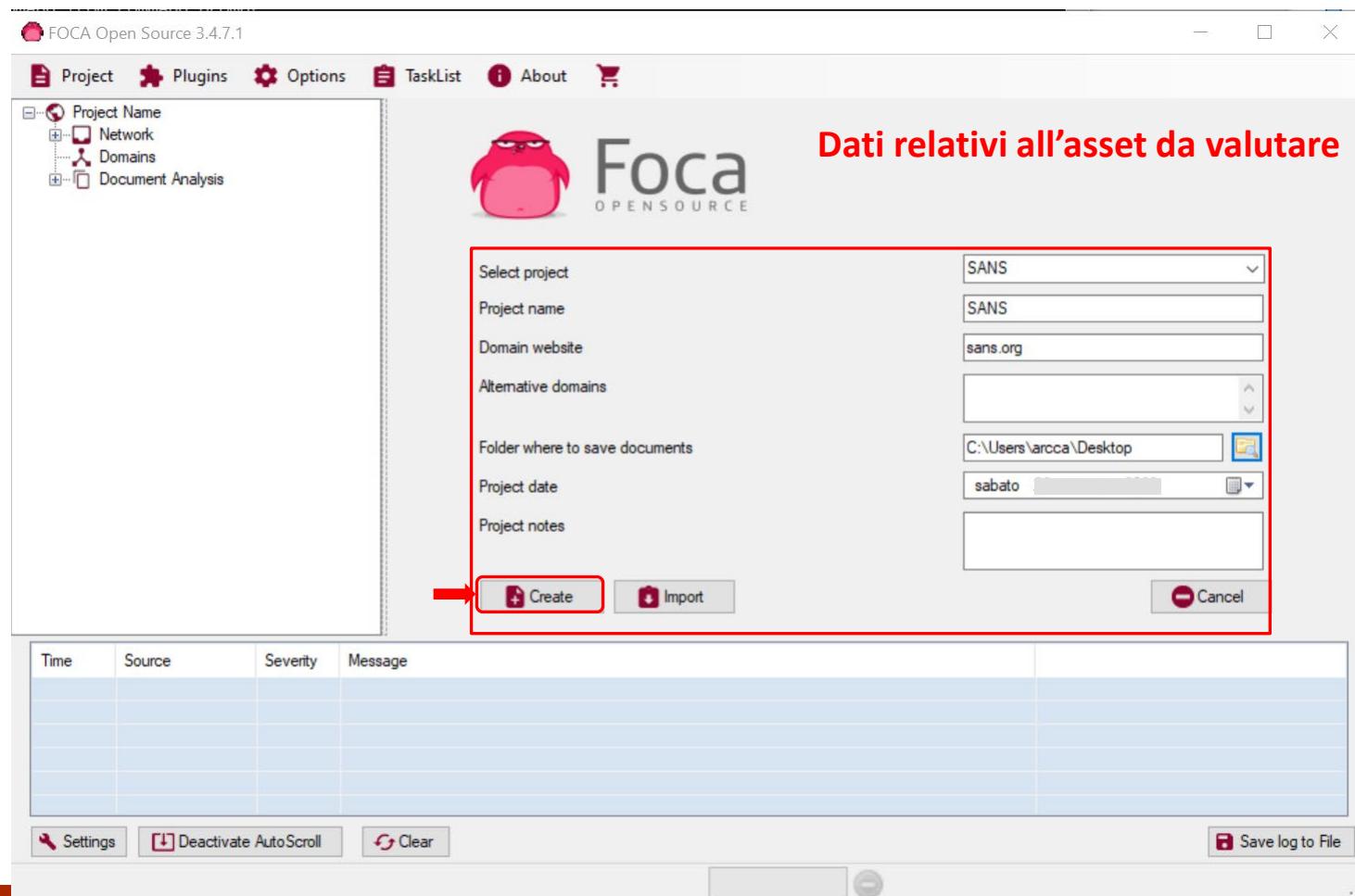
Ricerca di Metadati – FOCA – Esempio



Information Gathering

Utilizzo di Crawler

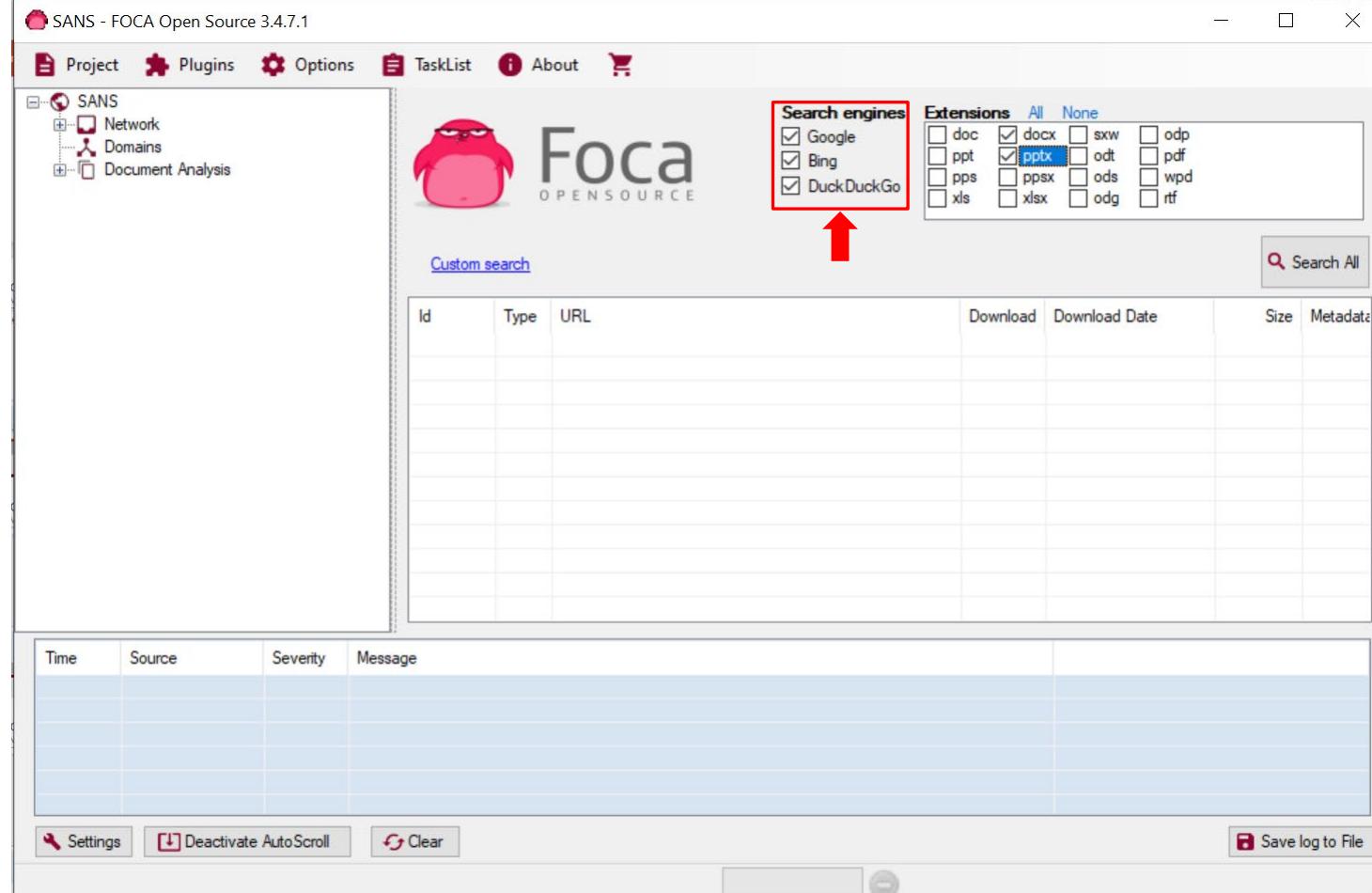
Ricerca di Metadati – FOCA – Esempio



Information Gathering

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio



The screenshot shows the FOCA Open Source 3.4.7.1 application window. The top menu bar includes Project, Plugins, Options, TaskList, About, and a shopping cart icon. The left sidebar displays a tree view with a single node labeled "SANS" expanded, showing "Network", "Domains", and "Document Analysis". The main area features a Foca OpenSource logo with a pink penguin icon and a "Custom search" link. To the right of the logo is a search engines configuration panel with three checkboxes: Google, Bing, and DuckDuckGo, all of which are checked and highlighted with a red box. Below this is a "Extensions" section with three tabs: All, None, and ppbx (which is selected). A red arrow points from the text "Search engines" in the previous slide to the "ppbx" tab here. A "Search All" button is located at the bottom right of this panel. At the bottom of the window is a log table with columns for Time, Source, Severity, and Message, and a "Save log to File" button.

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

The screenshot shows the FOCA Open Source 3.4.7.1 application window. At the top, there is a menu bar with icons for Project, Plugins, Options, TaskList, About, and a shopping cart. Below the menu is a sidebar titled "SANS" containing "Network", "Domains", and "Document Analysis". The main area features a logo for "Foca OPEN SOURCE" with a pink cartoon character. On the right side, there is a "Search engines" section with checkboxes for Google, Bing, and DuckDuckGo. Below it is a "Extensions" section with checkboxes for various file types. A red box highlights the "Extensions" section, and a red arrow points upwards from the bottom of the slide towards this box. At the bottom of the main pane, there is a table with columns for Id, Type, URL, Download, Download Date, Size, and Metadata. The bottom-most section contains a table for logs with columns for Time, Source, Severity, and Message, along with buttons for Settings, Deactivate Auto Scroll, Clear, and Save log to File.

Id	Type	URL	Download	Download Date	Size	Metadata

Time	Source	Severity	Message

Custom search

Search engines

Extensions All None

Google

Bing

DuckDuckGo

doc docx sxw odp

ppt pptx odt pdf

pps ppsx ods wpd

xls xlsx odg rtf

Custom search

Search All

Time Source Severity Message

Settings Deactivate Auto Scroll Clear Save log to File

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

The screenshot shows the FOCA Open Source 3.4.7.1 application window. The top menu bar includes Project, Plugins, Options, TaskList, About, and a shopping cart icon. The left sidebar displays a project structure under 'SANS': Network, Domains, and Document Analysis. The main area features a Foca logo and search engines (Google, Bing, DuckDuckGo) and extensions (doc, ppt, pps, xls, docx, pptx, ppsx, xlsx, sxw, odt, ods, odg, odp, pdf, wpd, rtf). A red arrow points to the 'Search All' button. Below this, a table lists search results with columns: Id, Type, URL, Download, Download Date, Size, and Metadata. A large red text overlay in the center of the results table reads: "La prima fase dello strumento è quella di spidering, che sostanzialmente si occupa della visita ricorsiva del sito web e dell'individuazione delle risorse". At the bottom, there is a log table with columns: Time, Source, Severity, and Message, along with buttons for Settings, Deactivate Auto Scroll, Clear, and Save log to File.

La prima fase dello strumento è quella di *spidering*, che sostanzialmente si occupa della visita ricorsiva del sito web e dell'individuazione delle risorse

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

SANS - FOCA Open Source 3.4.7.1

Project Plugins Options TaskList About

SANS Network Domains Document Analysis

Search engines Extensions All None

Google Bing DuckDuckGo doc docx sxw odp
ppt pptx odt pdf
pps ppsx ods wpd
xls xlsx odg rtf

Custom search

File docx e pptx individuati sull'asset

Id Type URL Download Download Date Size Meta

0	docx	https://www.sans.org/event-downloads/35800/agenda....	x	-	19,49 KB	x
1		https://www.sans.org/blog/office-2007-metadata/	x	-	150,48 KB	x
2	docx	https://www.sans.org/media/score/checklists/ios-platfor...	x	-	138,04 KB	x
3		https://www.sans.org/blog/finding-unknown-malware-wit...	x	-	160,97 KB	x
4		http://www.sans.org/security-resources/policies/general...	x	-	-	x
5		https://www.sans.org/blog/making-reviewing-files-from-d...	x	-	157,4 KB	x
6	docx	https://www.sans.org/media/justify-training/Justify-Your...	x	-	26,92 KB	x
7		https://www.sans.org/blog/extracting-vb-macro-code-fro...	x	-	161,25 KB	x
8	docx	https://www.sans.org/media/justify-training/Justify-Your...	x	-	24,17 KB	x
9	docx	https://www.sans.org/media/justify-training/Justify-Your...	x	-	23,91 KB	x
10	docx	https://www.sans.org/media/justify-training/Justify-Your...	x	-	26,79 KB	x

Time Source Severity Message

16:31:39	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: Error from the remote server: (403) Forbidden..
16:31:46	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 96
16:31:50	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 17

Settings Deactivate AutoScroll Clear Save log to File

All searchers have finished

Time	Source	Severity	Message
16:31:39	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: Error from the remote server: (403) Forbidden..
16:31:46	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 96
16:31:50	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 17

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

Successivamente è possibile scaricare una o più risorse

The screenshot shows the FOCA Open Source 3.4.7.1 application window. At the top, there's a navigation bar with Project, Plugins, Options, TaskList, About, and a shopping cart icon. Below the navigation is a sidebar titled 'SANS' containing Network, Domains, and Document Analysis. The main area features a logo for 'Foca OPEN SOURCE' and a 'Custom search' section. A table lists search results with columns for Id, Type, URL, Download, Download Date, Size, and Meta. The row at Id 2 is highlighted with a blue selection bar. A context menu is open over this row, with the 'Download' option highlighted by a red box and a red arrow pointing to it. Other options in the menu include Extract Metadata, Analyze Malware, Delete, Download All, Extract All Metadata, Analyze All Metadata, Analyze All Malware, Delete All, Add file, Add folder, Add URLs from file, and Link(s). At the bottom of the interface, there's a log table showing search activity and a 'Save log to File' button.

Time	Source	Severity	Message
16:31:39	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: Error
16:31:46	MetadataSearch	medium	BingWeb search finished successfully!! Total fo
16:31:50	MetadataSearch	medium	GoogleWeb search finished successfully!! Total

All searchers have finished

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

SANS - FOCA Open Source 3.4.7.1

Project Plugins Options TaskList About

SANS

- Network
- Domains
- Document Analysis
 - Files (1/47)
 - .docx (1)
 - Metadata Summary
 - Malware Summary (DIARIO)

Foca
OPENSOURCE

Search engines Extensions All None

Google doc docx sxw odp
 Bing ppt ptx odt pdf
 DuckDuckGo pps ppsx ods wpd
 xls xlsx odg rtf

Custom search

Id	Type	URL	Download	Download Date	Size	Meta
0	docx	https://www.sans.org/event-downloads/35800/agenda...	x	-	19,49 KB	x
1		https://www.sans.org/blog/office-2007-metadata/	x	-	150,48 KB	x
2	docx	https://www.sans.org/media/score/checklists/ios-platfor...	*	03/26/2022 16:38:00	138,04 KB	x
3		https://www.sans.org/blog/finding-unknown-malware-with...	x	-	160,97 KB	x
4		http://www.sans.org/security-resources/policies/general...	x	-	-	x
5		https://www.sans.org/blog/making-reviewing-files-from-d...	x	-	157,4 KB	x
6	docx	https://www.sans.org/media/justify-training/Justify-Your...	x	-	26,92 KB	x
7		https://www.sans.org/blog/extracting-vb-macro-code-fro...	x	-	161,25 KB	x
8	docx	https://www.sans.org/media/justify-training/Justify-Your...	x	-	24,17 KB	x
9	docx	https://www.sans.org/media/justify-training/Justify-Your...	x	-	23,91 KB	x
10	docx	https://www.sans.org/media/justify-training/Justify-Your...	x	-	26,79 KB	x

Time Source Severity Message

16:31:39 MetadataSearch error An error has occurred on DuckDuckGoWeb: Error del server remoto: (403) Non consentito..

16:31:46 MetadataSearch medium BingWeb search finished successfully!! Total found result count: 96

16:31:50 MetadataSearch medium GoogleWeb search finished successfully!! Total found result count: 17

Settings Deactivate AutoScroll Clear Save log to File

All documents have been downloaded

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

È possibile estrarre i metadati relativi alla risorsa scaricata

The screenshot shows the SANS - FOCA Open Source 3.4.7.1 application window. On the left, there's a tree view under 'Project' labeled 'SANS' with nodes like 'Network', 'Domains', 'Document Analysis', 'Files (1/47)', 'Metadata Summary', and 'Malware Summary (DIARIO)'. In the center, there's a logo for 'Foca OPEN SOURCE' with a red penguin icon. On the right, there are sections for 'Search engines' (Google, Bing, DuckDuckGo) and 'Extensions' (All or None). A 'Custom search' bar has a 'Search All' button. Below these are two tables: one for 'Download' and one for 'Extract Metadata'. A context menu is open over a row in the 'Download' table, listing options: Download, Extract Metadata, Analyze Malware, Delete, Download All, Extract All Metadata, Analyze All Metadata, Analyze All Malware, Delete All, Add file, Add folder, Add URLs from file, and Link(s). At the bottom, there's a log table with columns for Time, Source, Severity, and Message, and buttons for Settings, Deactivate AutoScroll, Clear, and Save log to File.

Time	Source	Severity	Message
16:31:39	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: Errore del serv
16:31:46	MetadataSearch	medium	BingWeb search finished successfully!! Total found result c
16:31:50	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found resu

All documents have been downloaded

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

The screenshot shows the FOCA Open Source application interface. The left sidebar contains a tree view with nodes like 'SANS' (selected), 'Network', 'Domains', 'Document Analysis' (with 'Files (1/47)' and '.docx (1)'), 'Metadata Summary', and 'Malware Summary (DIARIO)'. The main area features a logo for 'Foca OPEN SOURCE' with a red penguin icon. Below it is a 'Custom search' section with a search bar labeled 'Search All'. A central table lists 11 downloaded files, each with a preview icon, file type ('docx'), URL, download status ('Download'), download date ('Download Date'), size ('Size'), and metadata status ('Metadata'). A context menu is open over the second file in the list, showing options: 'Download', 'Extract Metadata' (highlighted with a red box and arrow), 'Analyze Malware', 'Delete', 'Download All', 'Extract All Metadata', 'Analyze All Metadata', 'Analyze All Malware', 'Delete All', 'Add file', 'Add folder', 'Add URLs from file', and 'Link(s)'. At the bottom, there's a log table with columns 'Time', 'Source', 'Severity', and 'Message', and buttons for 'Settings', 'Deactivate AutoScroll', 'Clear', and 'Save log to File'.

Time	Source	Severity	Message
16:31:39	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: Error del servidor
16:31:46	MetadataSearch	medium	BingWeb search finished successfully!! Total found result 0
16:31:50	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result 0

All documents have been downloaded

Search engines: Google, Bing, DuckDuckGo

Extensions: All, None

- doc docx sxw odp
- ppt pptx odt pdf
- pps ppsx ods wpd
- xls xlsx odg rtf

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

Metadati
estratti dal file
selezionato

The screenshot shows the FOCA Open Source 3.4.7.1 application window. On the left, there is a tree view of a project named "SANS". A red box highlights the "Metadata Summary" node under "Document Analysis", which contains items like "Users (2)", "Folders (23)", "Printers (0)", etc. Below the tree view, a message says "All documents were analyzed".

The main area has a logo for "Foca OPEN SOURCE". It includes fields for "Select project" (set to "SANS"), "Project name" ("sans.org"), "Domain website" ("sans.org"), "Alternative domains", "Folder where to save documents" ("C:\Users\varcca\Desktop"), "Project date" ("sabato 26 marzo 2022"), and "Project notes". There are "Update" and "Import" buttons at the bottom.

Time	Source	Severity	Message
16:31:39	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: Error del server remoto: (403) Non consentito..
16:31:46	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 96
16:31:50	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 17

At the bottom, there are buttons for "Settings", "Deactivate AutoScroll", "Clear", and "Save log to File".

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

The screenshot shows the SANS - FOCA Open Source 3.4.7.1 application window. The left sidebar displays a tree view of analysis results under the 'SANS' project:

- Network
- Domains
- Document Analysis
 - Files (1/47)
 - .docx (1)
 - Metadata Summary
 - Users (2)** (highlighted with a red arrow)
 - Folders (23)
 - Printers (0)
 - Software (1)
 - Emails (0)
 - Operating Systems (0)
 - Passwords (0)
 - Servers (0)
 - Malware Summary (DIARIO)

The right panel shows a table of found users:

Attribute	Value
All users found (2) - Times found	
Name	Javier
Name	Neal

A large red arrow points to the 'Users (2)' node in the tree view. The word 'Users' is also highlighted in red at the bottom center of the right panel.

At the bottom, a log table shows search activity:

Time	Source	Severity	Message
16:31:39	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: Error del server remoto: (403) Non consentito..
16:31:46	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 96
16:31:50	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 17

Buttons at the bottom include: Settings, Deactivate AutoScroll, Clear, Save log to File, and a status message: All documents were analyzed.

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

The screenshot shows the SANS - FOCA Open Source 3.4.7.1 application window. The left sidebar displays a tree view of analysis results under the 'SANS' project, including Network, Domains, Document Analysis (with sub-options like Files, Metadata Summary, Users, Printers, Software, Emails, Operating Systems, Passwords, Servers), and Malware Summary (DIARIO). A red arrow points to the 'Folders (23)' item under Document Analysis. The main pane shows a table of found folders:

Attribute	Value
All folders found (23) - Times found	
Path	http://ioscentral.co.uk/
Path	http://csrc.nist.gov/publications/nistpubs/800-121/
Path	https://www.grc.com/
Path	http://askthegeek.us/pwd_meter/
Path	http://www.theregister.co.uk/2011/03/10/apple_update_omits_iphone3g/
Path	http://krebsonsecurity.com/2011/05/weyland-yutani-crime-kit-targets-macs-for-b.../
Path	http://en.wikipedia.org/wiki/
Path	http://www.reghardware.com/2011/06/15/pin_spy_app_pulled/
Path	http://www.zdziarski.com/blog/
Path	http://www.cellebrite.com/
Path	http://mocana.com/blog/2011/02/18/iphone-hackers-can-gain-access-to-your-...
Path	http://www.iosresearch.org/
Path	http://katanaforensics.com/
Path	http://ixam-forensics.com/
Path	http://blog.crackpassword.com/2011/05/elcomsoft-breaks-iphone-encryption-of...
Path	http://iphone-forensics.com/
Path	http://www.apple.com/uk/ipad/built-in-apps/
Path	http://www.f-secure.com/en_UK/security/lab/tools-and-services/online...

Folders

At the bottom, there is a TaskList table showing search logs:

Time	Source	Severity	Message
16:31:39	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: Error del server remoto: (403) Non consentito..
16:31:46	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 96
16:31:50	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 17

Buttons at the bottom include: Settings, Deactivate AutoScroll, Clear, Save log to File, and a status message: All documents were analyzed.

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

The screenshot shows the FOCA software interface. On the left, a tree view displays a project named "SANS" with various sections like Network, Domains, Document Analysis, and Software. A red arrow points to the "Software (1)" node under Document Analysis. The main pane on the right shows a table of found software:

Attribute	Value
All software found (1) - Times found	
Software	Microsoft Office

The word "Software" is highlighted in red at the bottom of this table. Below the table is a log window showing search results:

Time	Source	Severity	Message
16:31:39	MetadataSearch	error	An error has occured on DuckDuckGoWeb: Errore del server remoto: (403) Non consentito..
16:31:46	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 96
16:31:50	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 17

At the bottom, there are buttons for Settings, Deactivate AutoScroll, Clear, and Save log to File. The status bar at the bottom says "All documents were analyzed".

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

The screenshot shows the FOCA Open Source 3.4.7.1 application window. On the left, there's a tree view of a project named 'SANS' containing 'Network', 'Domains', 'Document Analysis' (with 'Files (46/47)' including 'doc' (12), 'docx' (26), 'pdf' (2), 'Unknown' (6)), and 'Metadata Summary' (with 'Users (2)', 'Folders (23)', 'Printers (0)', 'Software (1)', 'Emails (0)', 'Operating Systems (0)', 'Passwords (0)', 'Servers (0)', and 'Malware Summary (DIARIO)'). The main area features a Foca logo and a 'Custom search' section. A context menu is open over a list of 11 downloaded files, with the 'Download All' option highlighted by a red arrow. The file list includes:

ID	Type	URL	Download	Date	Size	Meta
0	docx	https://www.sans.org/event-downloads/35800/agenda....	.	03/26/2022 17:05:56	19,49 KB	x
1	docx	https://www.sans.org/event-downloads/35800/agenda....	.	03/26/2022 17:05:57	150,61 KB	x
2	docx	https://www.sans.org/event-downloads/35800/agenda....	.	03/26/2022 16:38:00	138,04 KB	•
3		https://www.sans.org/event-downloads/35800/agenda....	.	03/26/2022 17:05:57	161,11 KB	x
4		http://www.sans.org/event-downloads/35800/agenda....	.	03/26/2022 17:05:57	0 B	x
5		https://www.sans.org/event-downloads/35800/agenda....	.	03/26/2022 17:05:57	157,53 KB	x
6	docx	https://www.sans.org/event-downloads/35800/agenda....	.	03/26/2022 17:05:57	26,92 KB	x
7		https://www.sans.org/event-downloads/35800/agenda....	.	03/26/2022 17:05:57	161,38 KB	x
8	docx	https://www.sans.org/event-downloads/35800/agenda....	.	03/26/2022 17:05:57	24,17 KB	x
9	docx	https://www.sans.org/event-downloads/35800/agenda....	.	03/26/2022 17:05:57	23,91 KB	x
10	docx	https://www.sans.org/event-downloads/35800/agenda....	.	03/26/2022 17:05:57	26,79 KB	x

At the bottom, a log table shows:

Time	Source	Severity	Message
16:31:39	MetadataSearch	error	An error has occured on DuckDuckGoWeb: Error
16:31:46	MetadataSearch	medium	BingWeb search finished successfully!! Total fo
16:31:50	MetadataSearch	medium	GoogleWeb search finished successfully!! Total fo

Buttons at the bottom include 'Settings', 'Deactivate AutoScroll', and 'Clear'. A message at the bottom states 'All documents have been downloaded'.

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

The screenshot shows the FOCA Open Source 3.4.7.1 application interface. On the left, there is a tree view of domains and analysis results. The main area displays a search results table with columns: Id, Type, URL, Download, Download Date, Size, and Meta. A context menu is open over a row with Id 2, Type docx, and URL https://www.sans.org/... . The menu items include Extract All Metadata (highlighted with a red arrow), Analyze All Metadata, Analyze All Malware, Delete All, Add file, Add folder, Add URLs from file, and Link(s). At the bottom, there is a log table with entries and buttons for Settings, Deactivate AutoScroll, and Clear.

ID	Type	URL	Download	Download Date	Size	Meta
0	docx	https://www.sans.org/event-downloads/35800/agenda....	.	03/26/2022 17:05:56	19,49 KB	X
1		https://www.sans.org/blog/office-2007-metadata/	.	03/26/2022 17:05:57	150,61 KB	X
2	docx	https://www.sans.org/.../ios-platform.../malware-wit...	.	03/26/2022 16:38:00	138,04 KB	.
3		https://www.sans.org/.../es/general.../files-from-d...	.	03/26/2022 17:05:57	161,11 KB	X
4		https://www.sans.org/.../stify-Your.../o-code-fro...	.	03/26/2022 17:05:57	157,53 KB	X
5		https://www.sans.org/.../stify-Your.../o-code-fro...	.	03/26/2022 17:05:57	26,92 KB	X
6	docx	https://www.sans.org/.../stify-Your.../o-code-fro...	.	03/26/2022 17:05:57	161,38 KB	X
7		https://www.sans.org/.../stify-Your.../o-code-fro...	.	03/26/2022 17:05:57	24,17 KB	X
8	docx	https://www.sans.org/.../stify-Your.../o-code-fro...	.	03/26/2022 17:05:57	23,91 KB	X
9	docx	https://www.sans.org/.../stify-Your.../o-code-fro...	.	03/26/2022 17:05:57	26,79 KB	X
10	docx	https://www.sans.org/.../stify-Your.../o-code-fro...	.	03/26/2022 17:05:57	26,79 KB	X

Extract All Metadata

Analyze All Metadata

Analyze All Malware

Delete All

Add file

Add folder

Add URLs from file

Link(s)

Save log to File

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

The screenshot shows the FOCA application interface. On the left, a tree view displays analyzed domains and files. A red arrow points to the 'Users (23)' node under the 'Document Analysis' section. The main pane shows a table of found users with their names listed. At the bottom, a log table shows search progress, and a status bar indicates 'All documents were analyzed'.

Users

Attribute	Value
All users found (23) - Times found	
Name	Matthew Anderson
Name	kmarshall
Name	admuser
Name	Javier
Name	Neal
Name	Van Kirk, Tanya
Name	Schleisman, Sara
Name	Bank of Newport
Name	administrator
Name	Angela Loomis
Name	Schleisman, Sara
Name	C C
Name	Alan Paller
Name	Stephen Northcutt
Name	Pamela Levy
Name	knaidu
Name	vthiagarajan
Name	Dean Farnington

Time	Source	Severity	Message
16:31:39	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: Error del server remoto: (403) Non consentito..
16:31:46	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 96
16:31:50	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 17

All documents were analyzed

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

The screenshot shows the FOCA application interface. On the left, there's a navigation tree with sections like Domains, Document Analysis (containing Files, PDFs, Unknown, and Folders), Metadata Summary (Users, Folders, Printers, Software, Emails, Operating Systems, Passwords, Servers), and Malware Summary (DIARIO). A red arrow points to the 'Folders (59)' item under the Document Analysis section. The main pane displays a table of search results:

Attribute	Value
Path	http://www.color.org/
Path	C:\Documents%20and%20Settings\knaidu\Application%20Data\Microsoft\Word\
Path	D:\Data\sans\
Path	http://www.rediffmail.com/cgi-bin/
Path	http://www.wastelands.gen.nz/
Path	http://www.cirt.net/code/
Path	http://packetstormsecurity.nl/Crackers/
Path	http://www.netcraft.com/
Path	http://www.softbytelabs.com/
Path	http://www.mavensecurity.com/
Path	http://mypage.bluewin.ch/vogje01/e/nmapwin/
Path	http://www.insecure.org/
Path	http://www.gfi.com/lannetscan/
Path	http://www.networksolutions.com/cgi-bin/whois/
Path	http://network-tools.com/nslookup/
Path	http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/
Path	C:\Documents%20and%20Settings\Administrator\Application%20Data\Microsoft...
Path	H:\SCOREV
Path	https://www.linkedin.com/in/

Below the table, a message states "All documents were analyzed". At the bottom, there are buttons for Settings, Deactivate AutoScroll, Clear, and Save log to File.

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

The screenshot shows the FOCA software interface. On the left, a tree view displays analyzed domains and files. A red arrow points to the 'Software (8)' node under the 'Metadata Summary' section. The main pane shows a table of found software with their corresponding values. At the bottom, a log table lists search activities, and a status bar at the bottom indicates 'All documents were analyzed'.

Software

Attribute	Value
All software found (8) - Times found	
Software	Adobe InDesign 16.0 (Macintosh)
Software	Adobe PDF Library 15.0
Software	Microsoft Office
Software	Adobe InDesign 15.0 (Macintosh)
Software	Microsoft Office 2000
Software	Microsoft Office XP
Software	OpenOffice
Software	Microsoft Office for Mac

Time	Source	Severity	Message
16:31:39	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: Errore del server remoto: (403) Non consentito..
16:31:46	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 96
16:31:50	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 17

Settings Deactivate AutoScroll Clear Save log to File

All documents were analyzed

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

The screenshot shows the FOCA application interface. On the left, a tree view displays analyzed domains and their metadata. A red arrow points to the 'Emails (1)' node under the 'Metadata Summary' section. The right panel shows a table of found emails with one entry: 'emea@sans.org'. Below the tree view, a log table lists three entries from a 'MetadataSearch' task.

Emails

Time	Source	Severity	Message
16:31:39	MetadataSearch	error	An error has occured on DuckDuckGoWeb: Errore del server remoto: (403) Non consentito..
16:31:46	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 96
16:31:50	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 17

All documents were analyzed

Utilizzo di Crawler

Ricerca di Metadati – FOCA – Esempio

The screenshot shows the FOCA application interface. On the left, a tree view displays analyzed domains and their sub-components. A red arrow points to the 'Operating Systems' node under the 'Metadata Summary' section. The main pane on the right shows a table of operating system findings:

Attribute	Value
All operating systems found (0) - Times found	
OS	Windows Server 2000
OS	Windows XP
OS	Mac OS

Below this, a table of log entries is shown:

Time	Source	Severity	Message
16:31:39	MetadataSearch	error	An error has occured on DuckDuckGoWeb: Errore del server remoto: (403) Non consentito..
16:31:46	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 96
16:31:50	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 17

At the bottom, there are buttons for Settings, Deactivate AutoScroll, Clear, and Save log to File. The status bar at the bottom left says "All documents were analyzed".

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 search may 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/smartergi
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



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

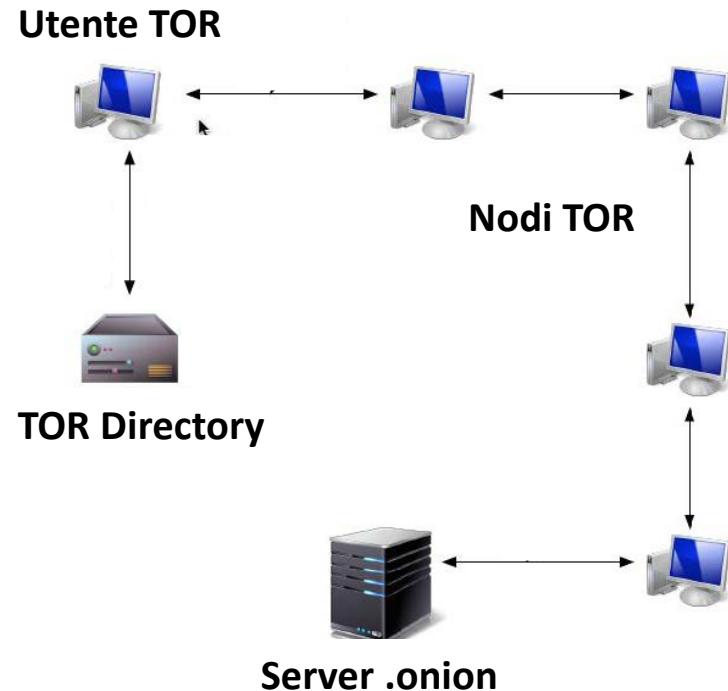
- Per accedere ai siti del Dark Web è necessario conoscere il loro URL
 - Non viene usato il DNS per la risoluzione dei nomi
- Il Dark Web può essere acceduto utilizzando il *The Onion Router (TOR) Browser*
- Il TOR Browser
 - È basato su Mozilla Firefox
 - Permette di accedere sia a siti con dominio **.onion** che a siti Web indicizzati in maniera convenzionale



Dark Web

TOR Browser

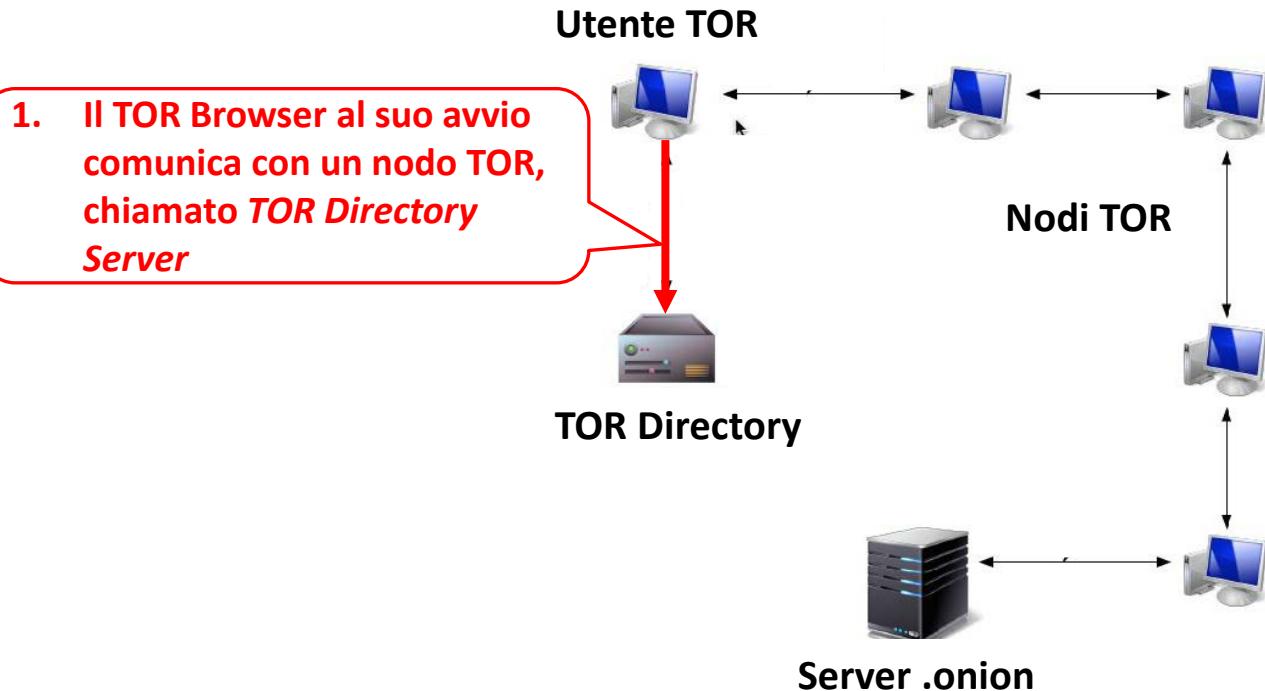
- Il TOR Browser accede ad un server contenente un sito con dominio **.onion** nel modo seguente



Dark Web

TOR Browser

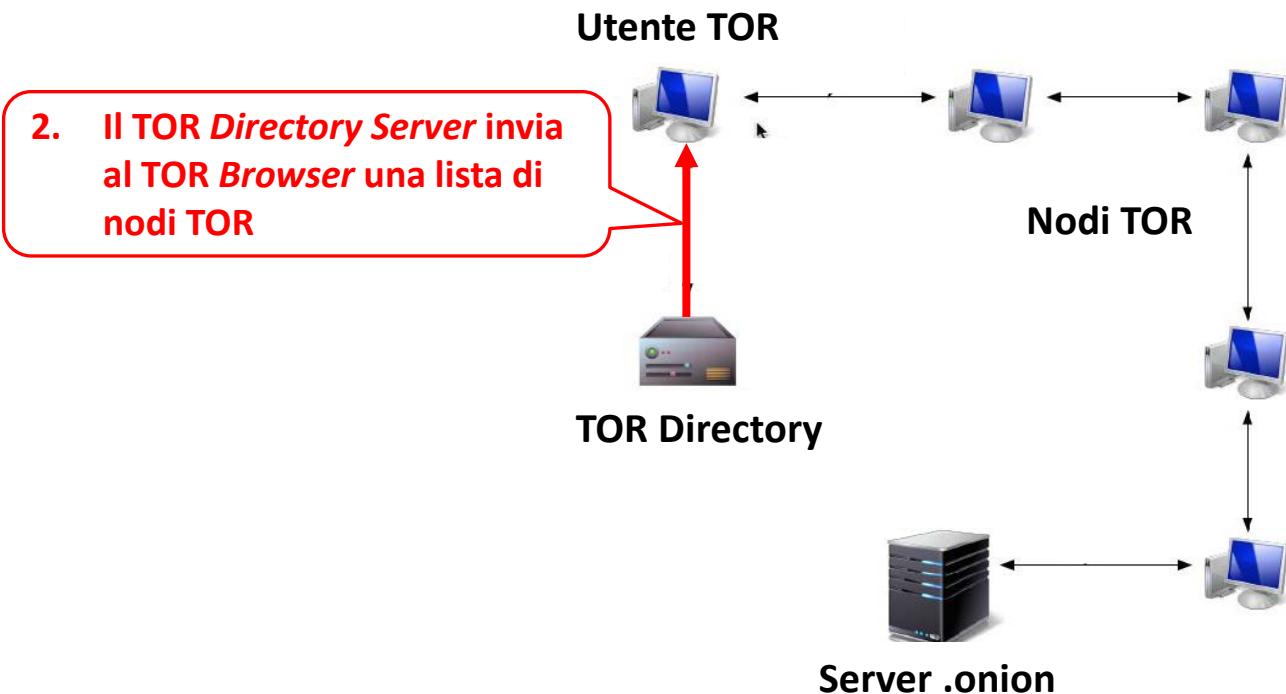
- Il TOR Browser accede ad un server contenente un sito con dominio **.onion** nel modo seguente



Dark Web

TOR Browser

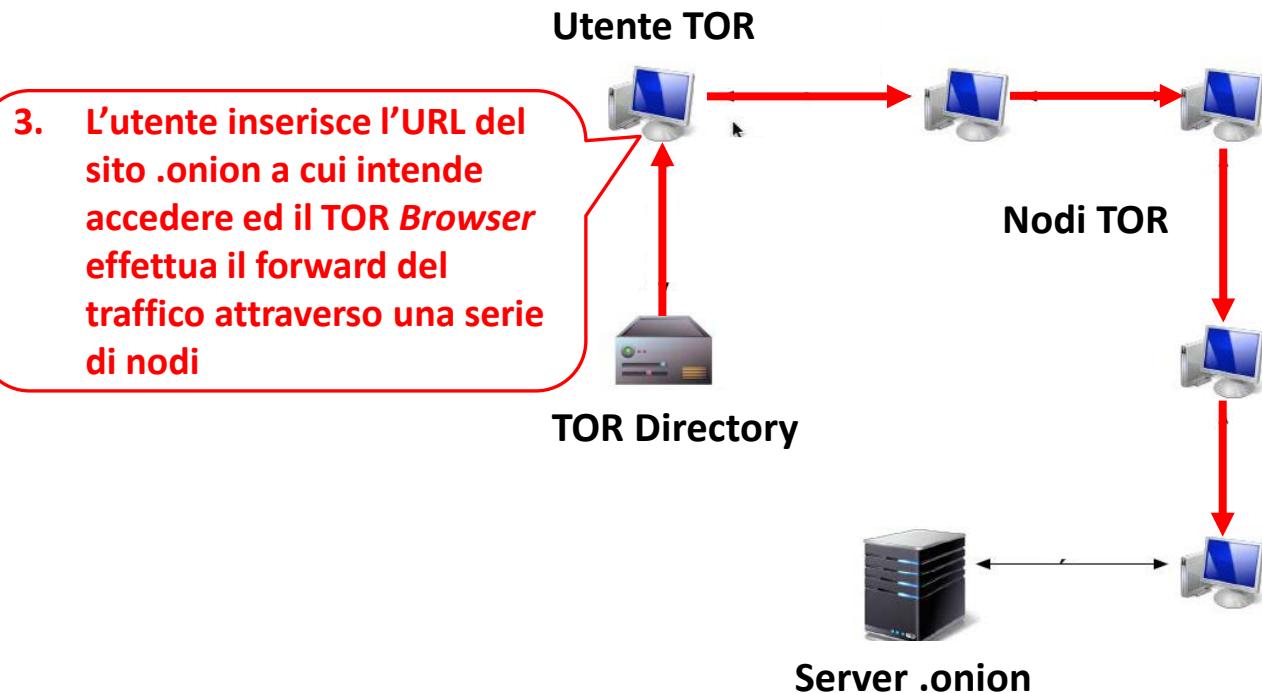
- Il TOR Browser accede ad un server contenente un sito con dominio **.onion** nel modo seguente



Dark Web

TOR Browser

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

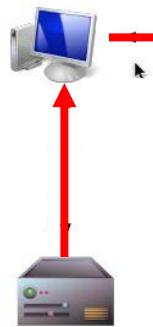


Dark Web

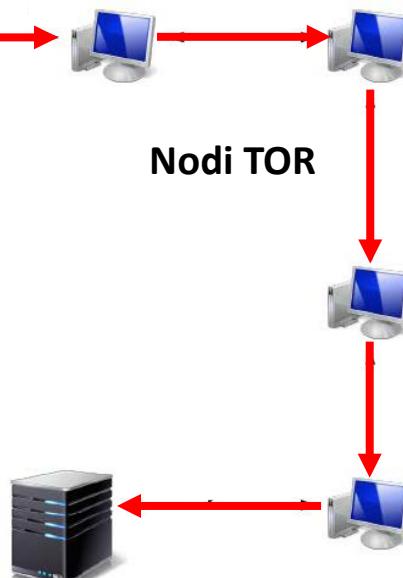
TOR Browser

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

Utente TOR



Nodi TOR



TOR Directory

Server .onion

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

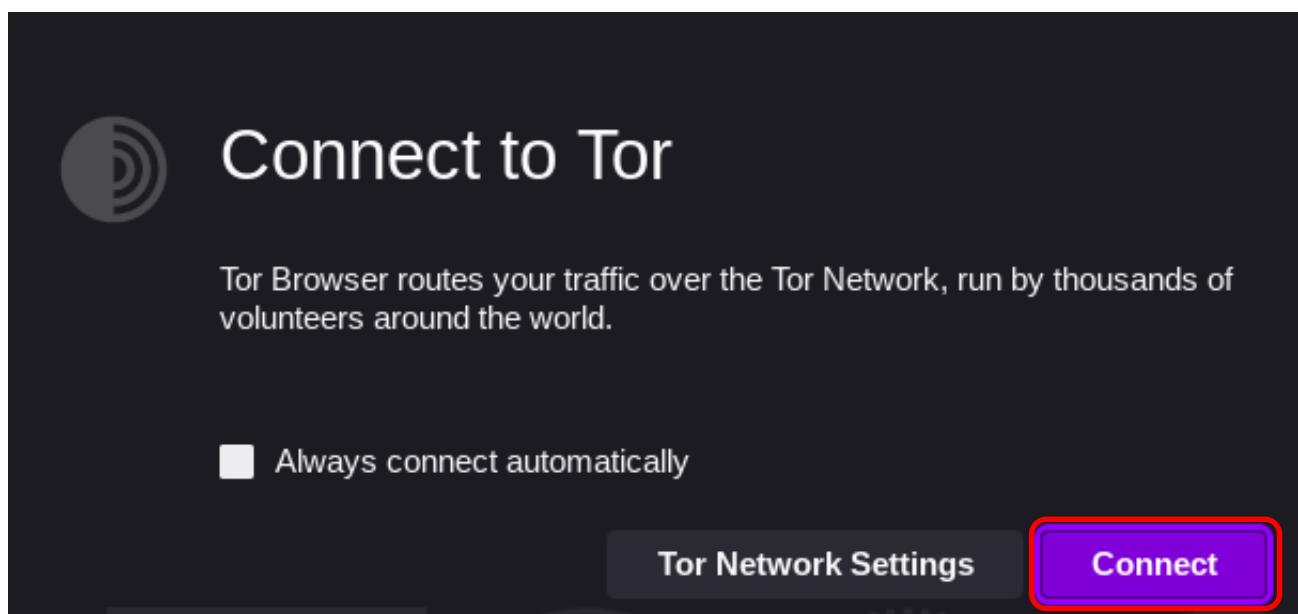
TOR Browser

- 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**

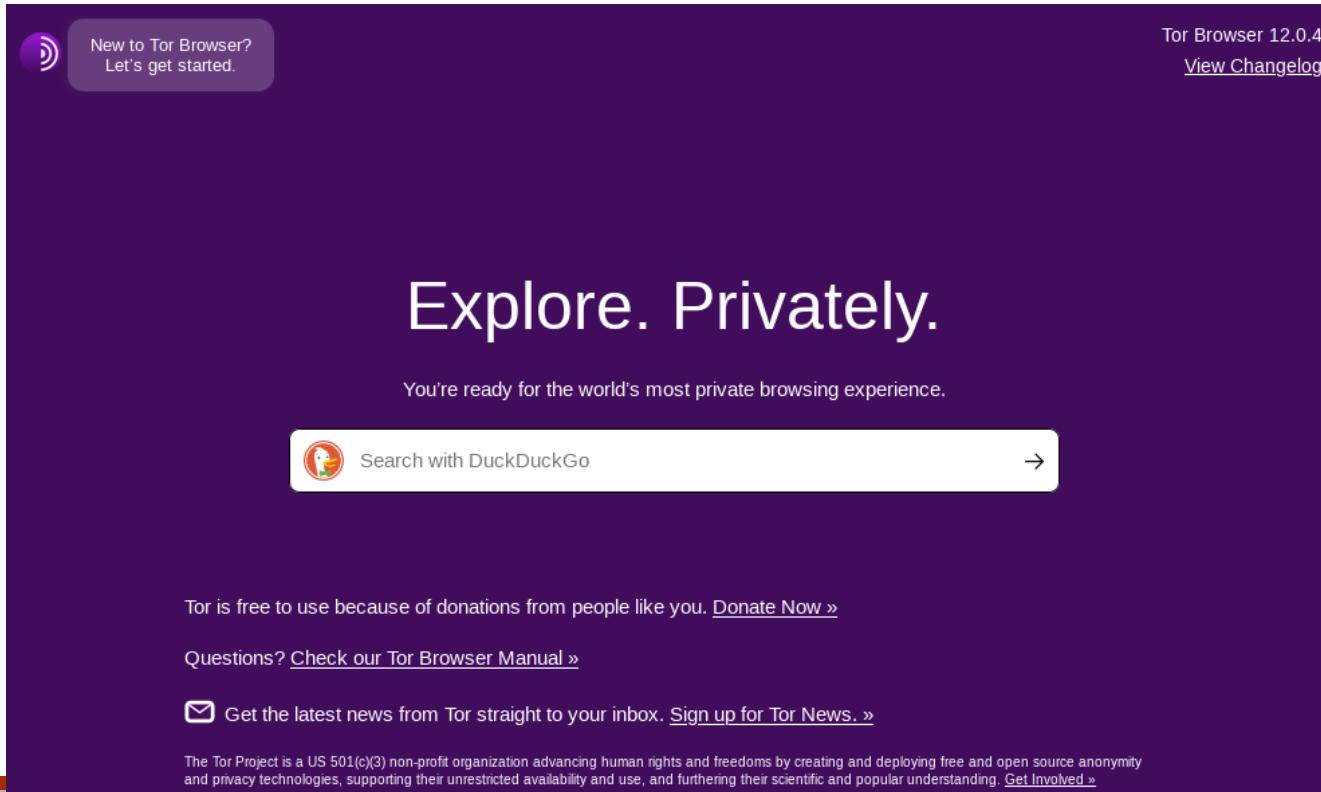


Dark Web

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://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswczad.onion/>

Hmm. We're having trouble finding that site.

We can't connect to the server at duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswczad.onion.

If that address is correct, here are three other things you can try:

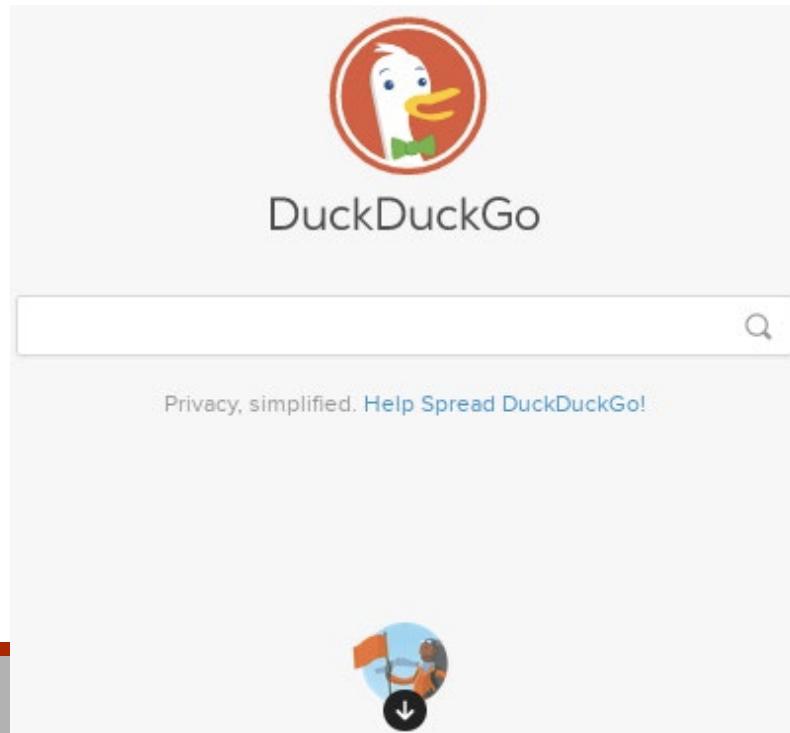
- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

Try Again

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/>

The screenshot shows the main page of The Hidden Wiki. At the top, there is a navigation bar with links for 'main page', 'discussion', 'view source', and 'history'. The main content area has a header 'Main Page' and a welcome message: 'Welcome to The Hidden Wiki! Our official Hidden Wiki url in 2023 is: http://zgktliwuvavvqqt4ybvgvi7yo4hjl5xgfuvpdf6otjyicgwqbym2quad.onion'. It also mentions a contest and a link to learn how. Below this, there is a section titled 'Editor's picks' with a list of links. Further down is a 'Volunteer' section with instructions. On the right side, there is a 'Contents' sidebar with a list of categories from 1 to 23, including 'Editor's picks', 'Volunteer', 'Introduction Points', and 'Non-English'.

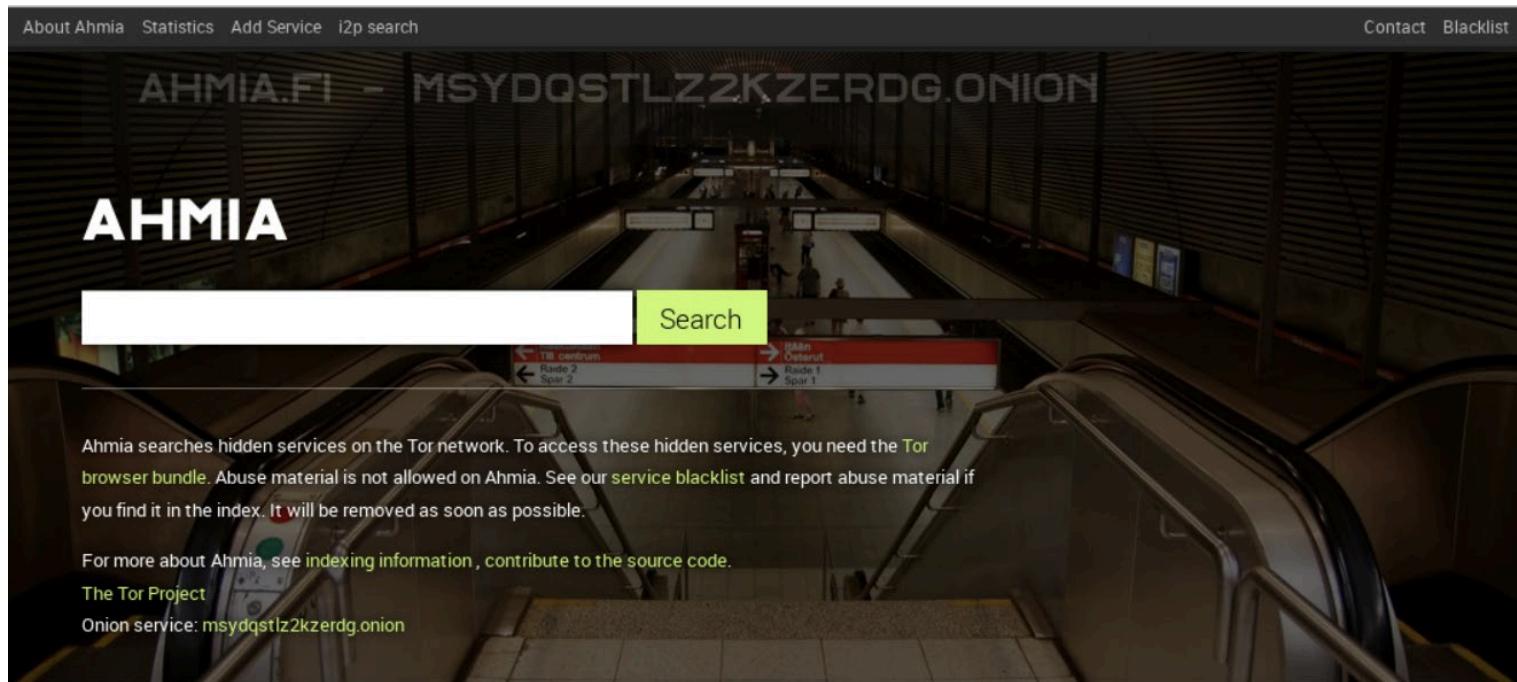
- 1 Editor's picks
- 2 Volunteer
- 3 Introduction Points
- 4 Financial Services
- 5 Commercial Services
- 6 Domain Services
- 7 Anonymity & Security
- 8 Darknet versions of popular sites
- 9 Blogs / Essays / News Sites
- 10 Email / Messaging
- 11 Social Networks
- 12 Forums / Boards / Chats
- 13 Whistleblowing
- 14 H/P/I/A/W/C
- 15 Hosting, website developing
- 16 File Uploaders
- 17 Audio - Radios on Tor
- 18 Videos / Movies / TV / Games
- 19 Books
- 20 Drugs
- 21 Erotica
 - 21.1 Noncommercial (E)
 - 21.2 Commercial (E)
- 22 Uncategorized
- 23 Non-English
 - 23.1 Brazilian
 - 23.2 Finnish / Suomi
 - 23.3 French / Français
 - 23.4 German / Deutsch
 - 23.5 Greek / Ελληνικά
 - 23.6 Italian / Italiano
 - 23.7 Japanese / 日本語
 - 23.8 Korean / 한국어
 - 23.9 Chinese / 中国語

Dark Web

Esempio 3 – Motori di Ricerca per il Dark Web

➤ Ahmia

➤ <http://juhanurmihxlp77nkq76byazcldy2h1movfu2epvl5ankdibsot4csyd.onion/>

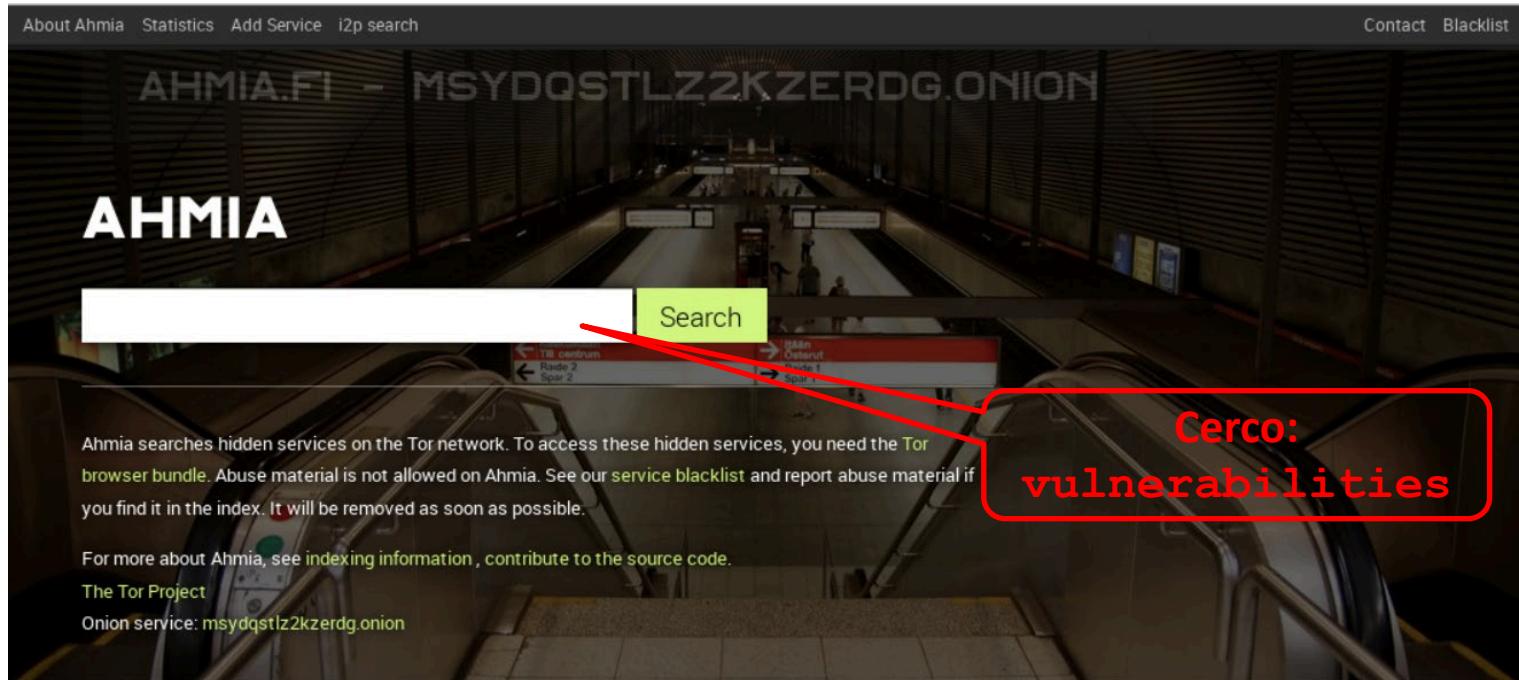


Dark Web

Esempio 3 – Motori di Ricerca per il Dark Web

➤ Ahmia

➤ <http://juhanurmihxlp77nkq76byazcldy2h1movfu2epvl5ankdibsot4csyd.onion/>



Dark Web

Esempio 3 – Motori di Ricerca per il Dark Web

➤ Ahmia

➤ <http://juhanurmihxlp77nkq76byazcldy2h1movfu2epvl5ankdibsot4csyd.onion/>

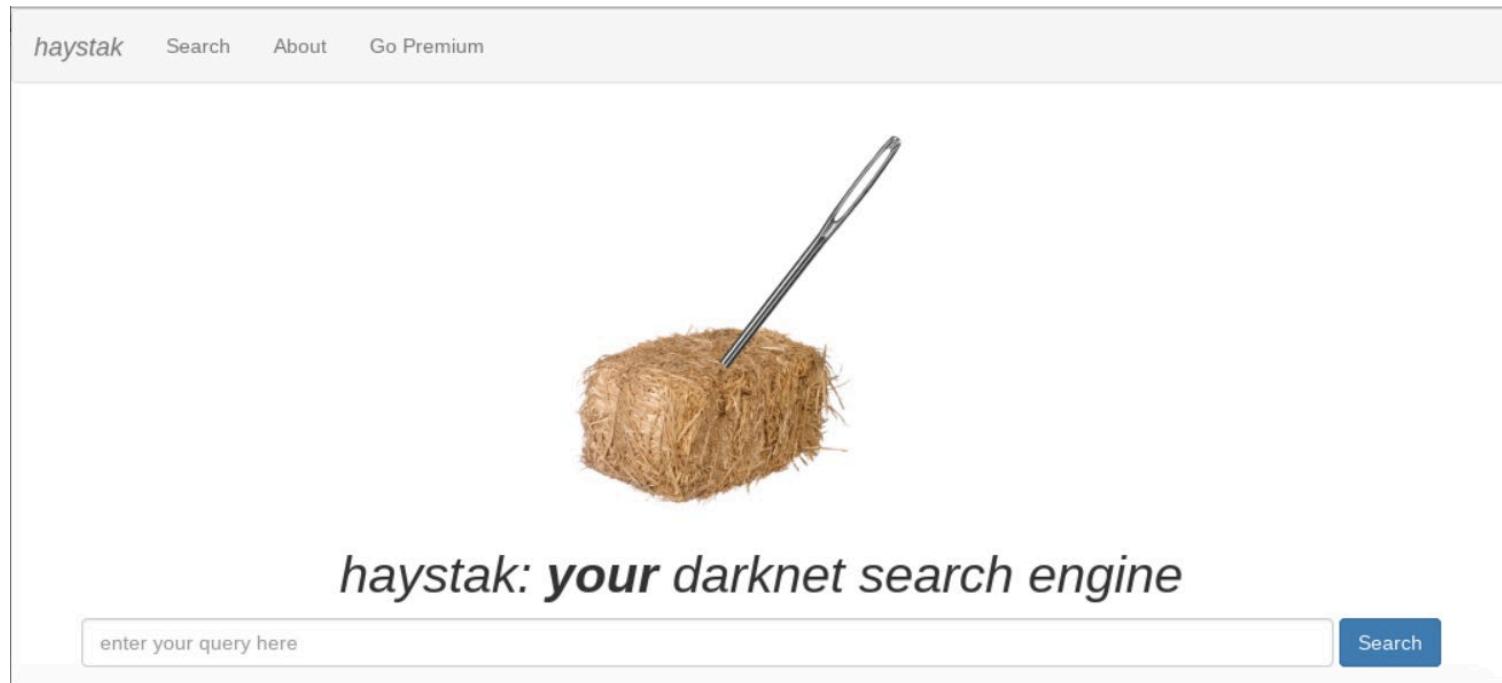
The screenshot shows the Ahmia search engine interface. At the top, there is a navigation bar with links for 'About Ahmia', 'Statistics', 'Add Service', 'i2p search', 'Contact', and 'Blacklist'. The main search bar contains the URL 'vulnerabilities' and a green 'Search' button. Below the search bar, a dropdown menu shows 'Any Time'. The search results page displays 39 matches found in 1.17 seconds, on page 1 of 1. The first result is a link to a torrent for 'Microsoft Windows® XP Professional SP3 (x86) VL with updates (05.05.2014) [English] 0'. Below the link, there is a snippet of text in Russian: 'Microsoft Windows® XP Professional SP3 (x86) VL with updates (05.05.2014) [English] скачать торрент Международный торрент-трекер Rustorka | Русторк до последнего! zwbxoprylvpit7t75.onion – 3 weeks ago – Report Abuse'. There are also other links for '9/3(火) - CVE "Full" Watch' and 'ZeroDisco.com by YesWeHack ! The Right Path to Coordinated Vulnerability Disclosure'.

Dark Web

Esempio 4 – Motori di Ricerca per il Dark Web

- Haystak

- **<http://haystak5njsmn2hqkewecpaxetahtwhsbsa64jom2k22z5afxhnpxfid.onion/>**

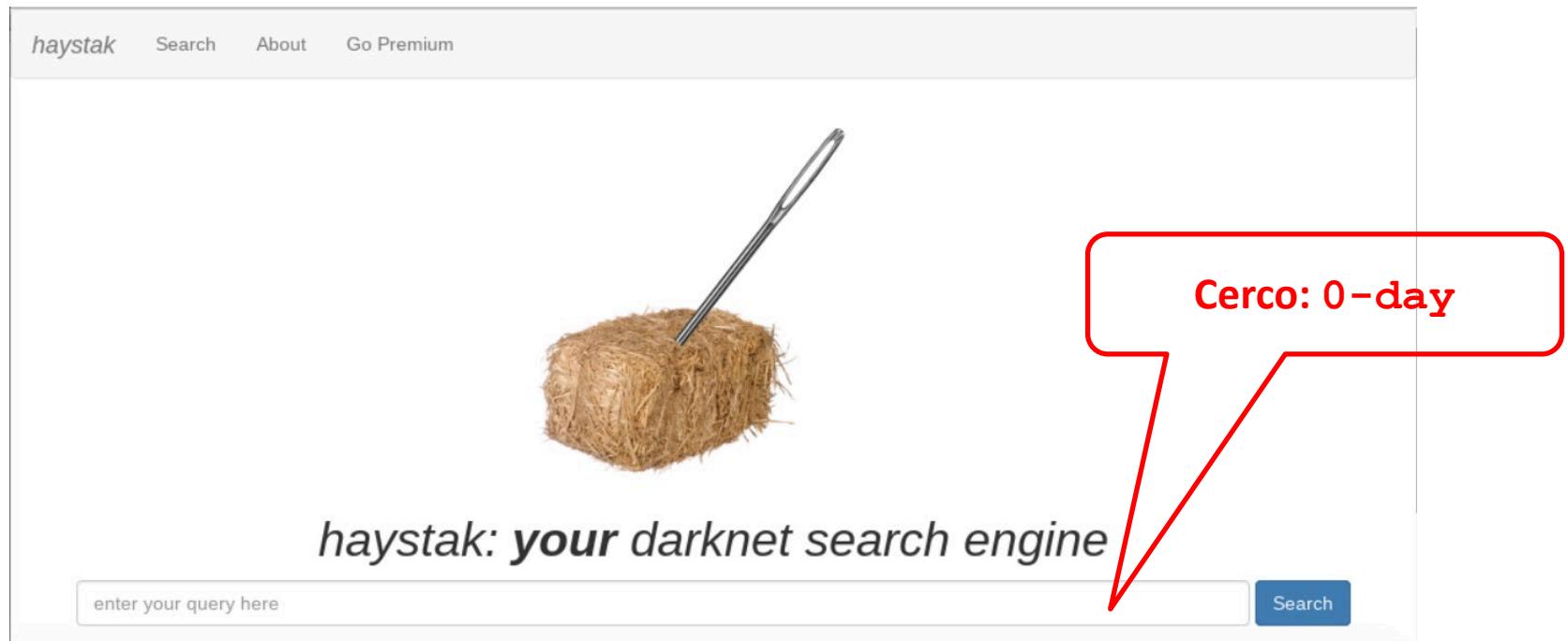


Dark Web

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/**

The screenshot shows the Haystak search engine interface. At the top, there is a navigation bar with links for 'haystak', 'Search', 'About', and 'Go Premium'. Below the navigation bar is a search form with a placeholder 'enter your query here' and a blue 'Search' button. The main content area is titled 'Search' and displays the results for the query 'exploit 0 day'. The results are listed as follows:

- Found Array results.
- Advertise here - contact us via the form
- exploit 0 day**
http://damagelabraahzcu.onion/index.php?topic=27345.msg149910%3Btopicseen
exploit 0 day * ĐĐ"ÑĐ"Đ"Đ% [http://damagelabraahzcu.onion/index.php] * ĐÑĐ%Đ' [http://damagelabraahzcu.onion
board=56.0] » * exploit 0 day [http://damagelabraahzcu.onion/index.php?
action=printpage;topic=27345.0] Đ|ÑÑĐ"Đ%Đ,ÑÑ: [1] ĐĐ²ÑĐ%Ñ ĐCĐµĐ%Đ": exploit 0 day (ĐÑĐ%ÑĐ
action=profile;u=172692] * [http:] exploit 0 day [http://damagelabraahzcu.onion/index.php?
board=56.0] » * exploit 0 day [http://damagelabraahzcu.onion/index.php?
exploit 0 day
- Cached version - Historical versions - Datapoints (e.g. bitcoin addresses) - Report for removal
- exploit 0 day**
http://damagelabraahzcu.onion/index.php?topic=27345.msg149910
exploit 0 day * ĐĐ"ÑĐ"Đ"Đ% [http://damagelabraahzcu.onion/index.php] * ĐÑĐ%Đ' [http://damagelabraahzcu.onion
board=56.0] » * exploit 0 day [http://damagelabraahzcu.onion/index.php?
action=printpage;topic=27345.0] Đ|ÑÑĐ"Đ%Đ,ÑÑ: [1] ĐĐ²ÑĐ%Ñ ĐCĐµĐ%Đ": exploit 0 day (ĐÑĐ%ÑĐ
action=profile;u=172692] * [http:] exploit 0 day [http://damagelabraahzcu.onion/index.php?

Dark Web

Esempio 5 – Motori di Ricerca per il Dark Web

➤ Torch

➤ <http://xmh57jrknzhv6y3ls3ubitzfqnkrxhopf5aygthi7d6rplyvk3noyd.onion/>

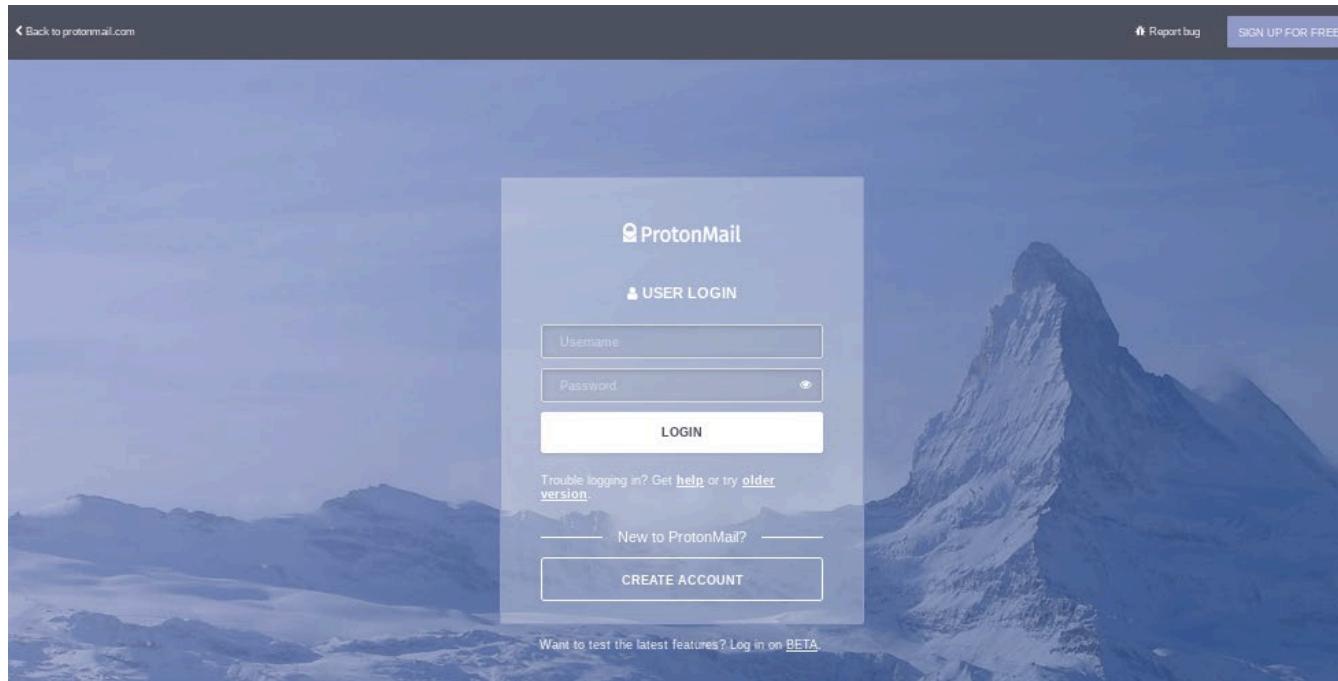


Dark Web

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

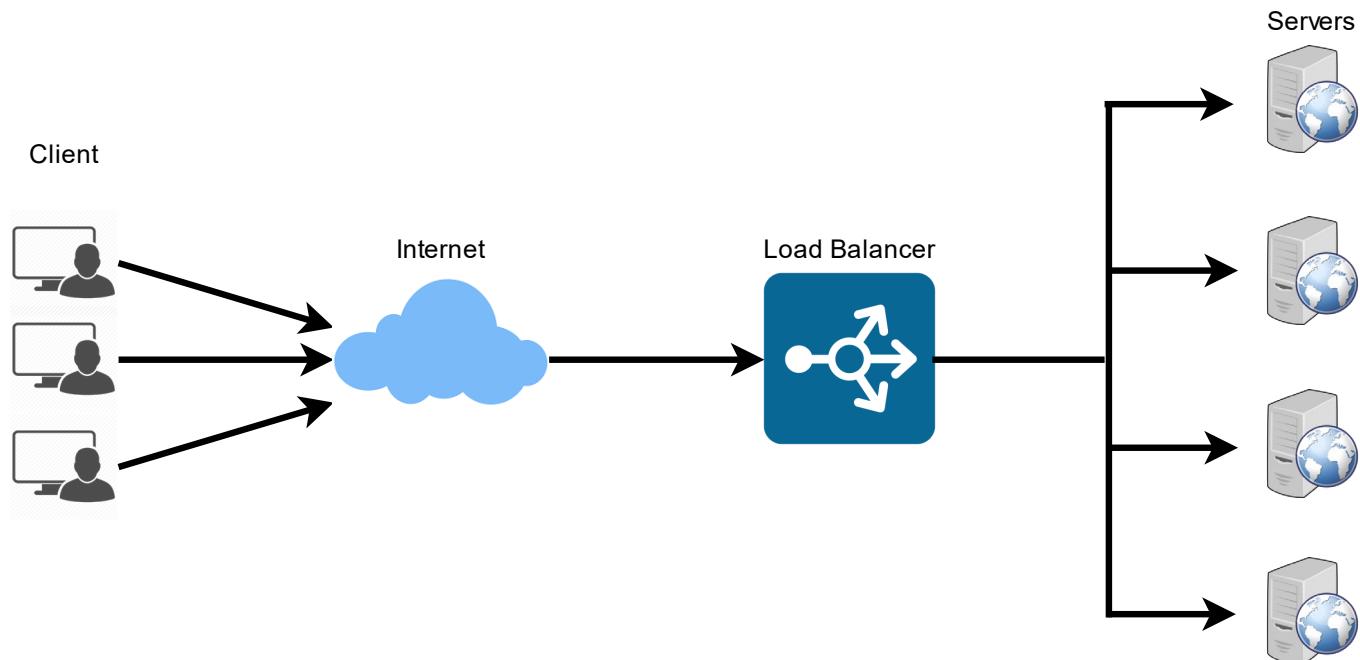
Altri Strumenti

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 **load balancer detector** (comando **ldb**)
 - **ldb** 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, 07:42:13, 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, 07:42:16, 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, 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**

```
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, 07:42:13, 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, 07:42:16, 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, 07:42:19, 07:4
2:19, 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 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, 22:59:06, 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: 0BdVFFZYKF0S8YaHSSk648dbbywg2Z+S/yggkezC6tGRUc8iRcRmudKy+2gAShNwf3skr/Tl6ycQ=
< x-amz-request-id: CBC674B1AF90703E
> x-amz-id-2: PxgW5sOnjuMQzpa3fS9ei39paKKlDtFu/tkGxphH8J6nvUzxRywmkj uRWckV0vRKAYTK4JqgZB0=
> 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: 0BdVFFZYKF0S8YaHSSk648dbbywg2Z+S/yggkezC6tGRUc8iRcRmudKy+2gAShNwf3skr/Tl6ycQ=
< x-amz-request-id: CBC674B1AF90703E
> x-amz-id-2: PxgW5sOnjuMQzpa3fS9ei39paKKlDtFu/tkGxphH8J6nvUzxRywmkj uRWckV0vRKAYTK4JqgZB0=
> x-amz-request-id: 117EB5353727DDCE

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

Altri Strumenti

Comando ss1scan

- Permette di analizzare il supporto SSL/TLS lato server
 - Per maggiori informazioni su **ssllscan**
 - **ssllscan -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/>

The screenshot shows the Qualys SSL Server Test interface. At the top, there's a navigation bar with links for Home, Projects, Qualys Free Trial, and Contact. The main content area has a red header bar. Below it, the Qualys logo and "SSL Labs" are displayed. A breadcrumb trail indicates the user is at Home > Projects > SSL Server Test. The main title is "SSL Server Test". A note below the title states: "This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will." There's a form to enter a hostname with a "Submit" button and a checkbox for "Do not show the results on the boards". Below the form, three panels show "Recently Seen", "Recent Best", and "Recent Worst" hosts, each with their respective URLs and grades (e.g., A+, A, B).

Recently Seen	Recent Best	Recent Worst
blog.ironcorelabs.com	mahealthconnector.optum.com A+	mail.abuld.co.nz F
cdn.ppzrlp9.life	1-2-3.tv A	rosadabelle.com T
giancarlov.com	bainelconfort.be A	cbarei.com T
api.ppzrlp9.life	cash.xpresspay.bg A	southwestwater.co.uk T
www.mass.gov	cls1bg.casino-technology.com A	giancarlov.com T
ppzrlp9.life	durancefm.com A	update.filezilla-project.org T
cdn.ppyf5b8y.life	simple.glebgg.ru A	joscanconsultoria.com.mx T
api.ppyf5b8y.life	sms.pro-code.net A	update.senduitelive.com F
ppyf5b8y.life	cms.casino-technology.com A	www.algoritmsb.ru T
po.cbre.com	www.descubretualentadorideia ... B	filicheta.msk.ru T

Altri Strumenti

Qualys – SSL Server Test

➤ <https://www.ssllabs.com/ssltest/>

The screenshot shows the Qualys SSL Labs website. At the top, there's a red header bar with the Qualys logo and the text "SSL Labs". Below it is a navigation bar with links for "Home", "Projects", "Qualys Free Trial", and "Contact". The main content area has a breadcrumb trail: "You are here: Home > Projects > SSL Server Test".

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname: Submit Do not show the results on the boards

Recently Seen

- blog.ironcorelabs.com
- cdn.ppzrlp9.life
- giancarlov.com
- api.ppzrlp9.life
- www.mass.gov
- ppzrlp9.life
- cdn.ppyf5b8y.life
- api.ppyf5b8y.life
- ppyf5b8y.life
- po.cbre.com

Recent Best

Domain	Grade
mahealthconnector.optum.com	A+
1-2-3.tv	A
bainelconfort.be	A
cash.xpresspay.bg	A
cls1bg.casino-technology.com	A
durancefm.com	A
simple.glebgg.ru	A
sms.pro-code.net	A
cms.casino-technology.com	A
www.descubretualentadoridea...	B

Recent Worst

Domain	Grade
mail.abudefduf.org	T
rosadabelle.com	T
cbarei.com	T
southwestwater.co.uk	T
giancarlov.com	T
update.filezilla-project.org	T
joscancosultoria.com.mx	T
update.senduitelive.com	F
www.algoritmsb.ru	T
filicheta.msk.ru	T

www.unisa.it

Altri Strumenti

Qualys – SSL Server Test – Esempio

➤ <https://www.ssllabs.com/ssltest/>

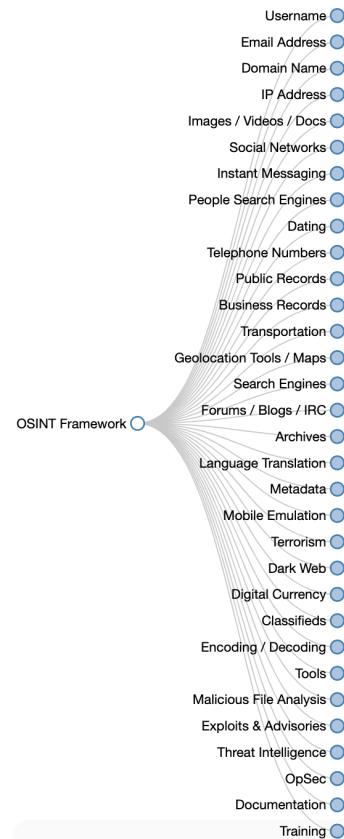
The screenshot shows the Qualys SSL Report interface for the domain www.unisa.it. The report is dated Fri, 24 Mar 2023 17:58:47 UTC. The overall rating is an **A**, indicated by a large green button. The summary section includes four horizontal bars representing different security metrics: Certificate (green), Protocol Support (green), Key Exchange (green), and Cipher Strength (green). Below the chart, a yellow box contains the text: "Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#)."

Metric	Score
Certificate	~95
Protocol Support	~95
Key Exchange	~88
Cipher Strength	~88

Altri Strumenti

OSINT Framework

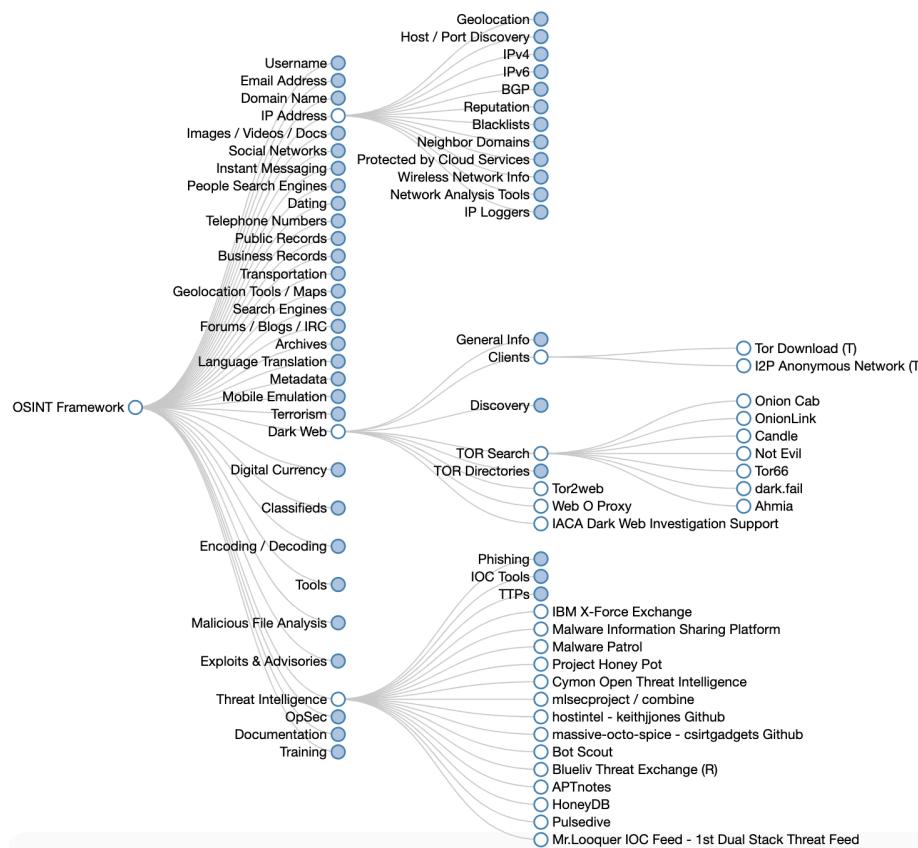
➤ <https://osintframework.com/>



Altri Strumenti

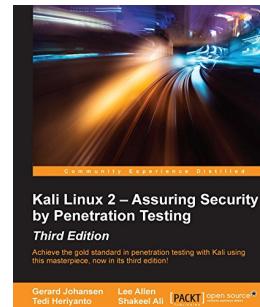
OSINT Framework

➤ <https://osintframework.com/>

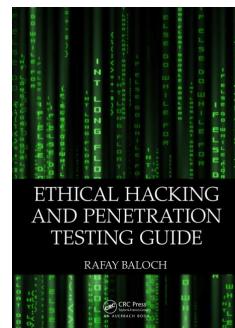


Bibliografia

- **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/>