Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Information Gathering
Parte 1

Arcangelo Castiglione
arcastiglione@unisa.it

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

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

Concetti Preliminari

- Raccogliere quante più informazioni possibili sull'asset da analizzare, riguardanti
  - La **parte digitale dell'asset**
    - Domain Name System (DNS), indirizzi IP, hostname, Autonomous Systems (AS)
    - Tecnologie e configurazioni usate
    - Etc
  - Le **persone legate all'asset**
    - Informazioni di contatto, credenziali, documenti
    - Metadati
    - Etc

Concetti Preliminari

- Raccogliere quante più informazioni possibili sull'asset da analizzare, riguardanti
  - La **parte digitale dell'asset**
    - Domain Name System (DNS), indirizzi IP, hostname, Autonomous Systems (AS)
    - Tecnologie e configurazioni usate
    - Etc
  - Le **persone legate all'asset**
    - Informazioni di contatto, credenziali, documenti
    - Metadati
    - Etc

In questa fase, tutte le informazioni ottenute devono essere considerate importanti

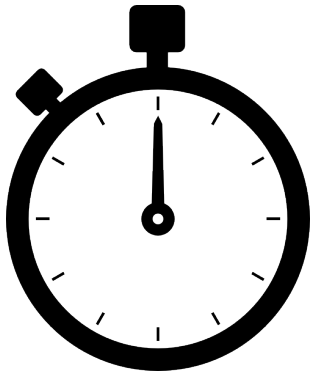
Concetti Preliminari

- Fase necessaria quando non si hanno a disposizione informazioni sull'asset da analizzare o si hanno informazioni parziali su di esso
  - Black Box e Grey Box Penetration Testing
- Utile al pentester per verificare la consistenza delle informazioni che ha ricevuto
  - White Box Penetration Testing
- Permette di caratterizzare l'asset in termini volumetrici e di enumerare le sue componenti
  - Quanti e quali sono gli indirizzi IP utilizzati dall'asset, i sottodomini, i *name server*, i *server mail*, etc
- Consente di ottenere quante più informazioni possibili su tutto ciò che ha a che fare con la componente umana che «orbita intorno» all'asset

Concetti Preliminari

- Fase anche nota come **Ricognizione** o **Footprinting**

- È stimato che circa l'80% del tempo richiesto da un tipico processo di penetration testing sia dedicato a questa fase



Concetti Preliminari

- In base al metodo utilizzato per raccogliere le informazioni, la fase di Information Gathering può essere di tipo «attivo» o «passivo»

  - **Active Information Gathering:** vengono raccolte informazioni sull'asset inviando traffico di rete verso tale asset

  - **Passive Information Gathering:** vengono raccolte informazioni sull'asset utilizzando servizi di terze parti
    - Motori di ricerca, servizi Web-based, etc

Concetti Preliminari

- **Active Information Gathering**
  - **[Pro] Permette di ottenere più informazioni**
  - **[Pro] Permette di ottenere informazioni più aggiornate e precise**
  - **[Cons] Alcuni dispositivi potrebbero intercettare questa attività**

- **Passive Information Gathering**
  - **[Pro] Permette di operare in maniera «nascosta» all'asset**
  - **[Cons] Permette di ottenere meno informazioni**
  - **[Cons] Permette di ottenere informazioni meno aggiornate e precise rispetto all'Active Information Gathering**

Concetti Preliminari

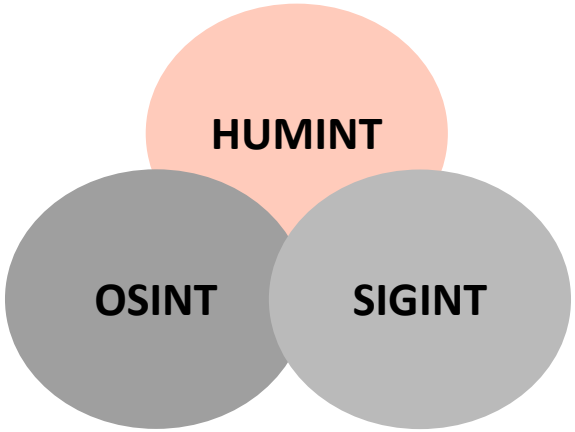
Open Source Intelligence

- La fase di Information Gathering si basa fortemente sul concetto di **O**pen **S**ource **INT**elligence (**OSINT**)
  - **Record** o **informazioni pubbliche** che le organizzazioni condividono come parte delle loro operazioni quotidiane
- OSINT permette di ottenere informazioni la cui fruizione **non è protetta da controlli di sicurezza**
  - Ad es., password, controllo accessi, etc

Concetti Preliminari

Open Source Intelligence

- Altre fonti di «intelligence»
  - Lo spionaggio che coinvolge l'interazione tra esseri umani viene definito come **HUM**an **INT**elligence (**HUMINT**)
  - La cattura di segnali radio con l'intento di violare la comunicazione prende il nome di **SIG**nal **INT**elligence (**SIGINT**)



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

Utilizzo di Risorse Web-Based

- Diverse risorse pubbliche Web-based possono essere utilizzate per raccogliere informazioni su
  - Asset di interesse (Spazio di indirizzamento IP, DNS, Autonomous System, etc)
  - Persone legate all'asset di interesse

- Il vantaggio dell'utilizzo di queste risorse è che il traffico di rete non viene inviato direttamente verso l'asset di interesse
  - Tale attività non è quindi rilevata e memorizzata dall'asset

Utilizzo di Risorse Web-Based

Google Hacking (o Google Dorking)

- Utilizzando Google in maniera opportuna è possibile ottenere informazioni molto utili ed interessanti, tra le quali
  - Username
  - Password
  - File di configurazione
  - Informazioni riservate
  - Etc

- Google permette di effettuare ricerche molto precise e «mirate» mediante opportuni operatori di ricerca
  - Detti anche *parametri* o *comandi*

Utilizzo di Risorse Web-Based

Google Hacking (o Google Dorking)

- I principali parametri di ricerca forniti da Google sono i seguenti
  - **`"frase"`** Viene ricercata esattamente la frase racchiusa tra doppi apici
  - **`+`** Forza una ricerca ad includere un singolo termine o frase
  - **`–`** Esclude dalla ricerca un singolo termine o frase
  - **`AND`** e **`OR`** logico tra due o più termini di ricerca
  - **`site`**: Limita i risultati a quelli di un sito Web specifico

Utilizzo di Risorse Web-Based

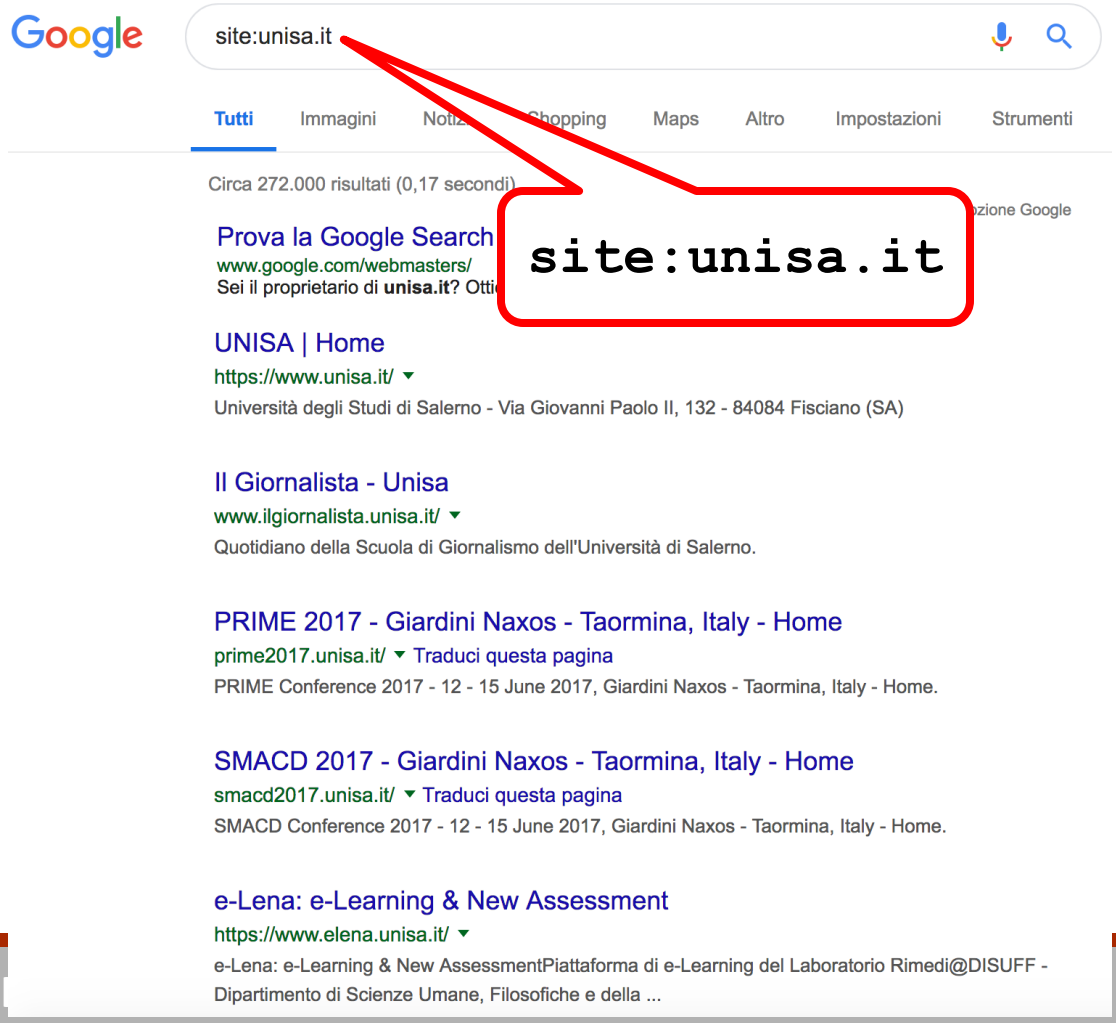
Google Hacking (o Google Dorking)

- I principali parametri di ricerca forniti da Google sono i seguenti
  - **`intitle:`** Trova le pagine con una determinata parola (o parole) nel titolo
  - **`intext:`** Trova le pagine contenenti una determinata parola (o parole) nel contenuto
  - **`inurl:`** Trova le pagine con una determinata parola (o parole) nell'URL
  - **`filetype:`** Limita i risultati a quelli di un determinato tipo di file

Utilizzo di Risorse Web-Based

Google Hacking (o Google Dorking) – Esempio 1

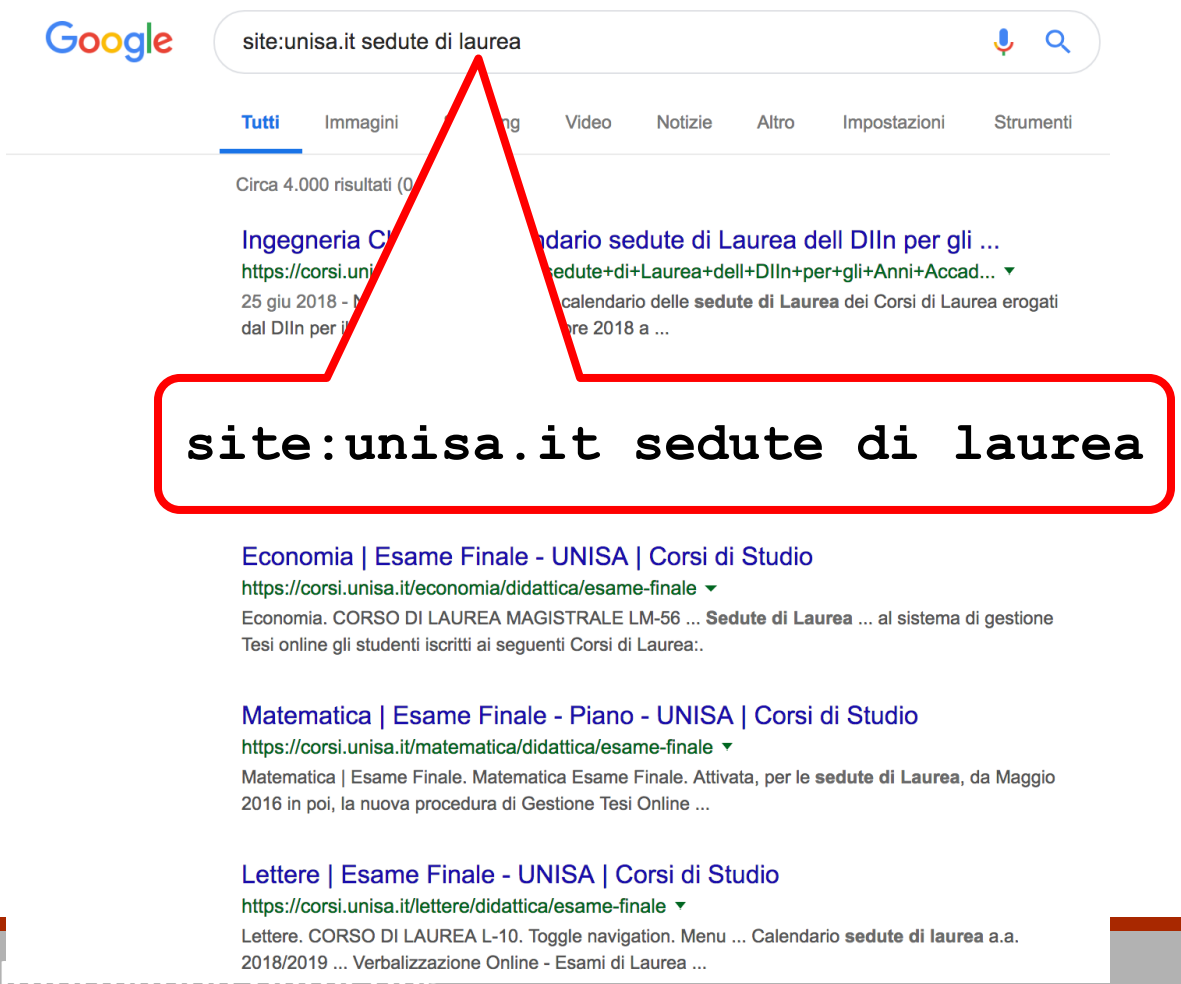
- Utilizzando il parametro **`site:`** la ricerca restituirà solo i risultati riguardanti **unisa.it**



Utilizzo di Risorse Web-Based

Google Hacking (o Google Dorking) – Esempio 2

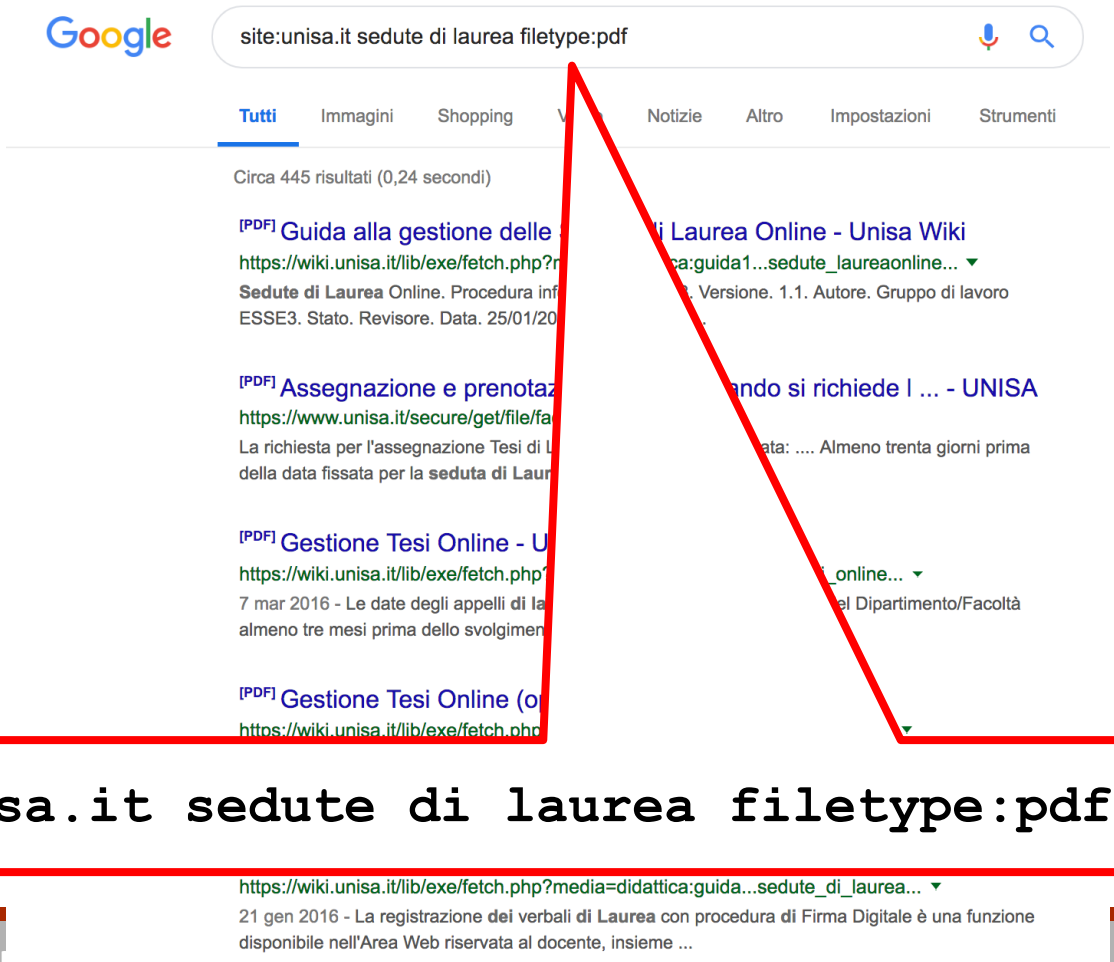
- Utilizzando il parametro **`site:`** la ricerca restituirà solo i risultati riguardanti **unisa.it**
- Cerchiamo «**sedute di laurea**» nelle pagine di **unisa.it**



Utilizzo di Risorse Web-Based

Google Hacking (o Google Dorking) – Esempio 3

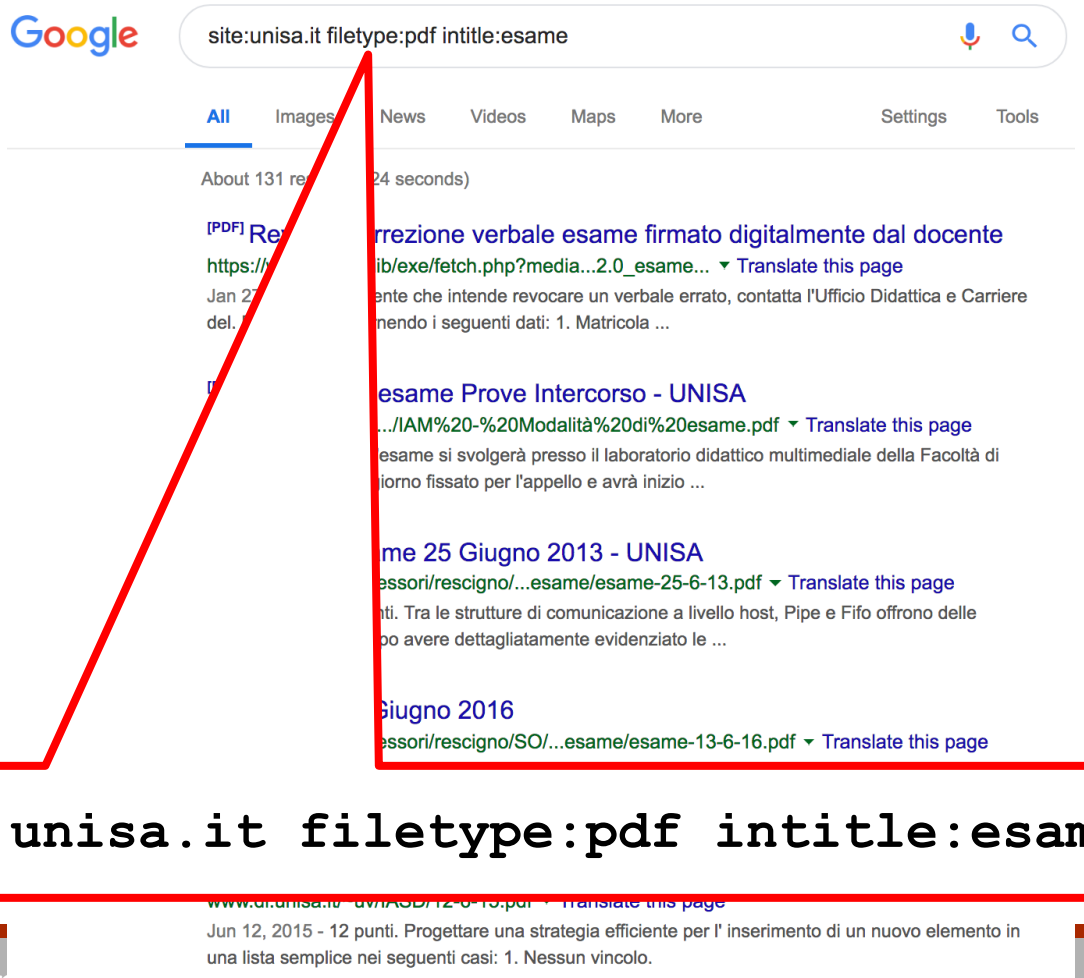
- Utilizzando il parametro **`site:`** la ricerca restituirà solo i risultati riguardanti **unisa.it**
- Cerchiamo nelle pagine di **unisa.it** tutti i **PDF** che riguardano le «**sedute di laurea**»
  - Utilizzando il parametro **`filetype:`**



Utilizzo di Risorse Web-Based

Google Hacking (o Google Dorking) – Esempio 4

- Utilizzando il parametro **`site:`** la ricerca restituirà solo i risultati riguardanti **unisa.it**
- Cerchiamo nelle pagine di **unisa.it** tutti i **PDF** (parametro **`filetype:`**) che riguardano l'esame (parametro **`intitle:`**)

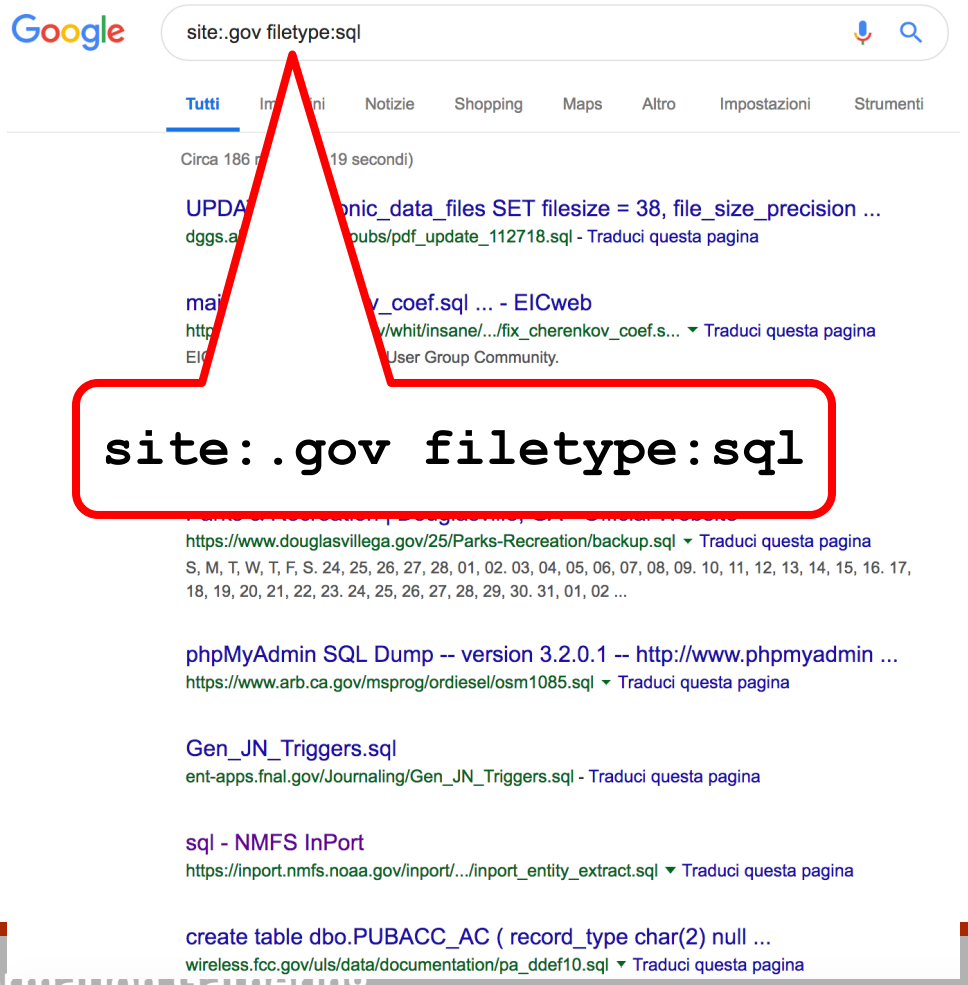


`site:unisa.it filetype:pdf intitle:esame`

Utilizzo di Risorse Web-Based

Google Hacking (o Google Dorking) – Esempio 5

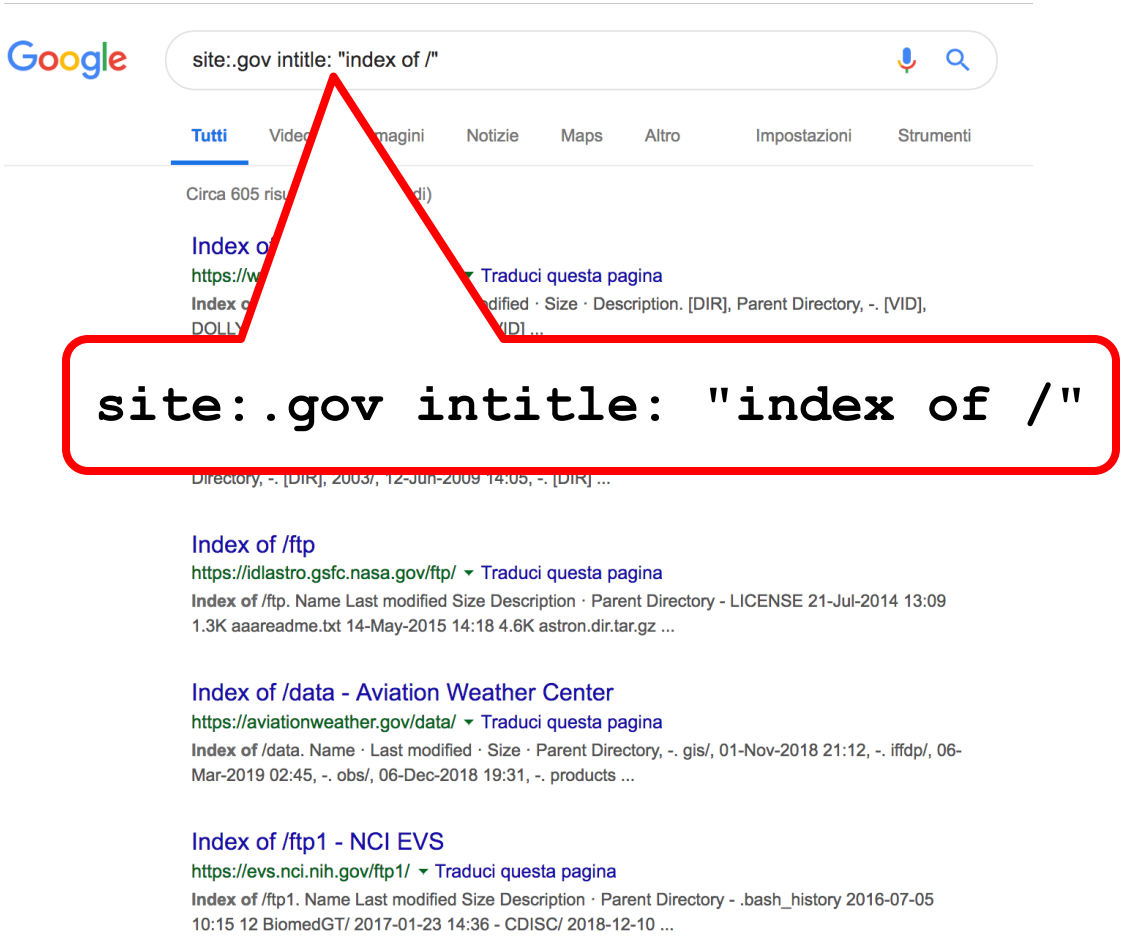
- Utilizzando il parametro **`site:`** effettuiamo una query che riguarda tutti i domini **.gov**
- Cerchiamo i file **SQL** nelle pagine con dominio **.gov**
  - Utilizzando il parametro **`filetype:`**



Utilizzo di Risorse Web-Based

Google Hacking (o Google Dorking) – Esempio 6

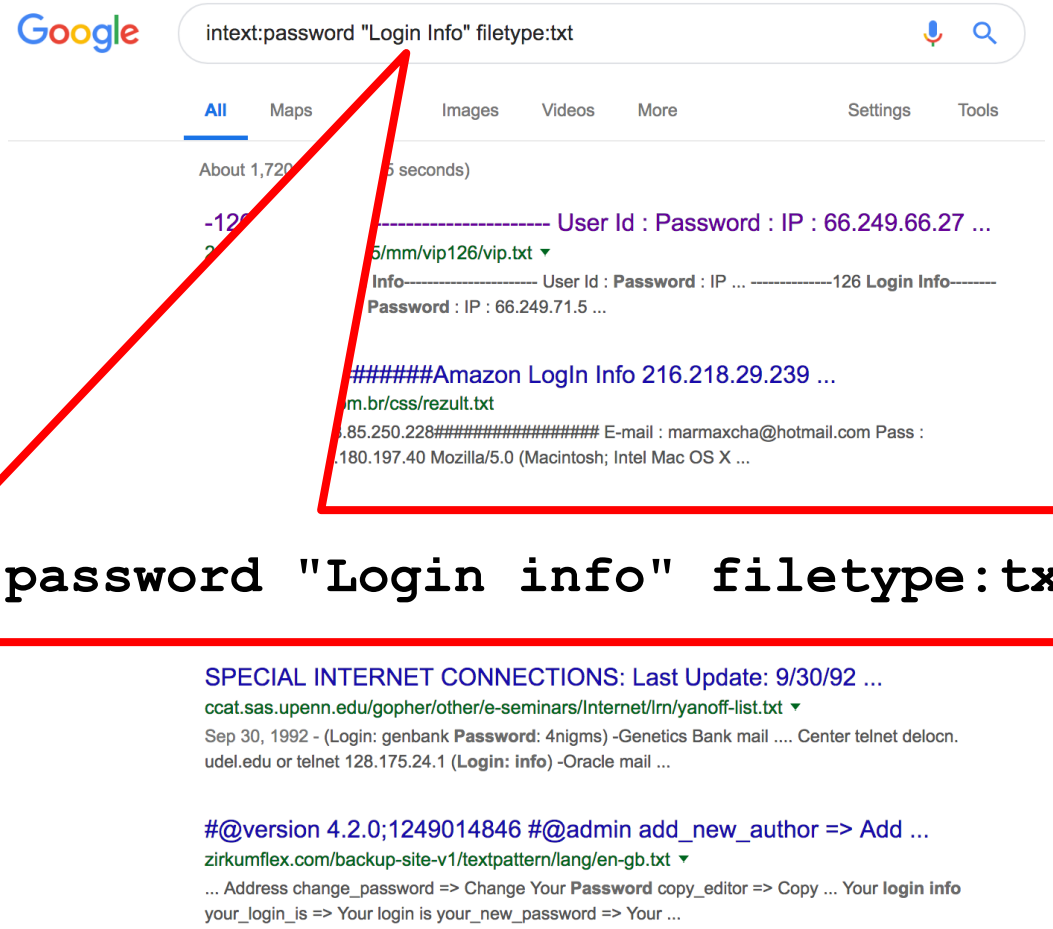
- Utilizzando il parametro **`site:`** effettuiamo una query che riguarda tutti i domini **.gov**
- Cerchiamo i **siti**, nelle pagine con dominio **.gov**, che consentano il **directory listing**
  - Utilizzando il parametro **`intitle:`**



Utilizzo di Risorse Web-Based

Google Hacking (o Google Dorking) – Esempio 7

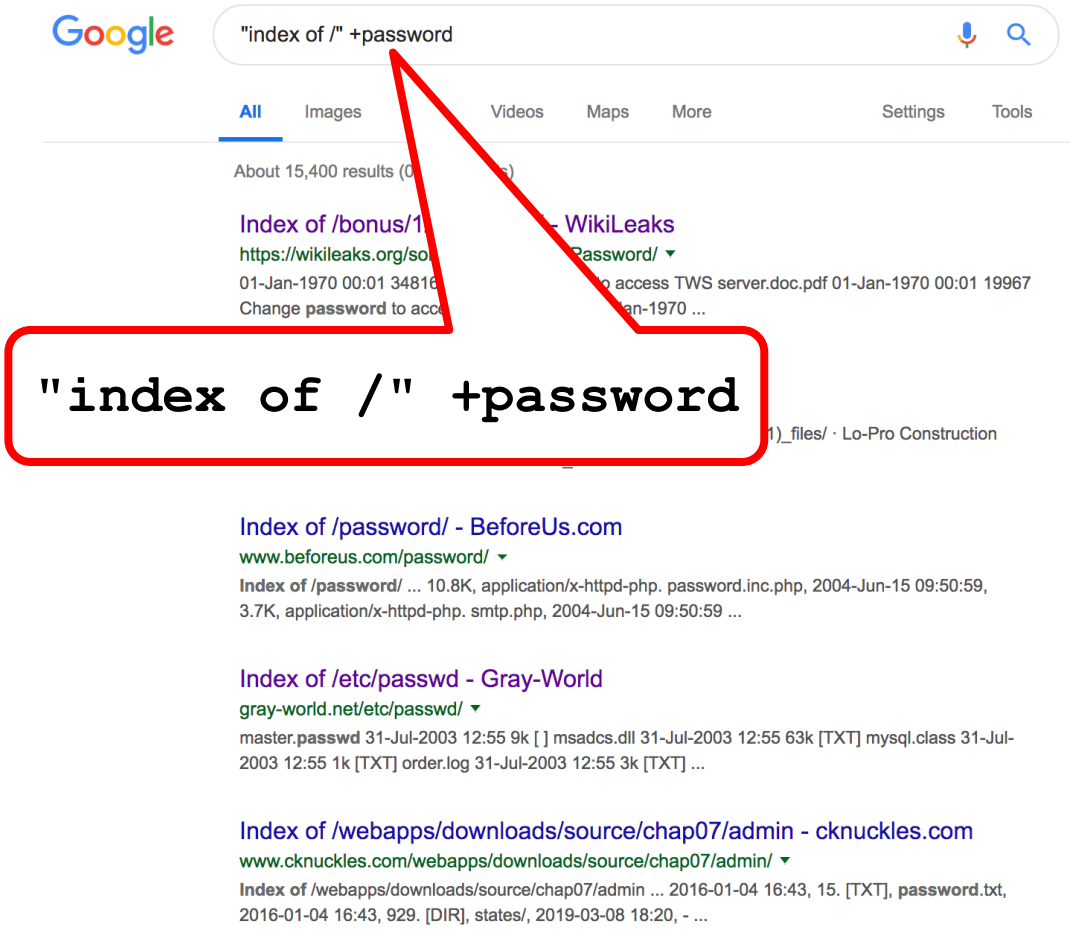
- Utilizzando i parametri **`intext:`** e **`filetype:`** cerchiamo tutti i file testuali contenenti credenziali di accesso
  - username e password



Utilizzo di Risorse Web-Based

Google Hacking (o Google Dorking) – Esempio 8

- Operatori "" e +



Utilizzo di Risorse Web-Based

Google Hacking – Ulteriori Esempi " Index of /"

- **Index of /admin**
- **Index of /passwd**
- **Index of /password**
- **Index of /mail**
- **"Index of /" +password.txt**
- **"Index of /" +.htaccess**

Utilizzo di Risorse Web-Based

Google Hacking – Ulteriori Esempi " Index of /"

- **"Index of /secret"**
- **"Index of /confidential"**
- **"Index of /root"**
- **"Index of /cgi-bin"**
- **"Index of /logs"**
- **"Index of /config"**

Utilizzo di Risorse Web-Based

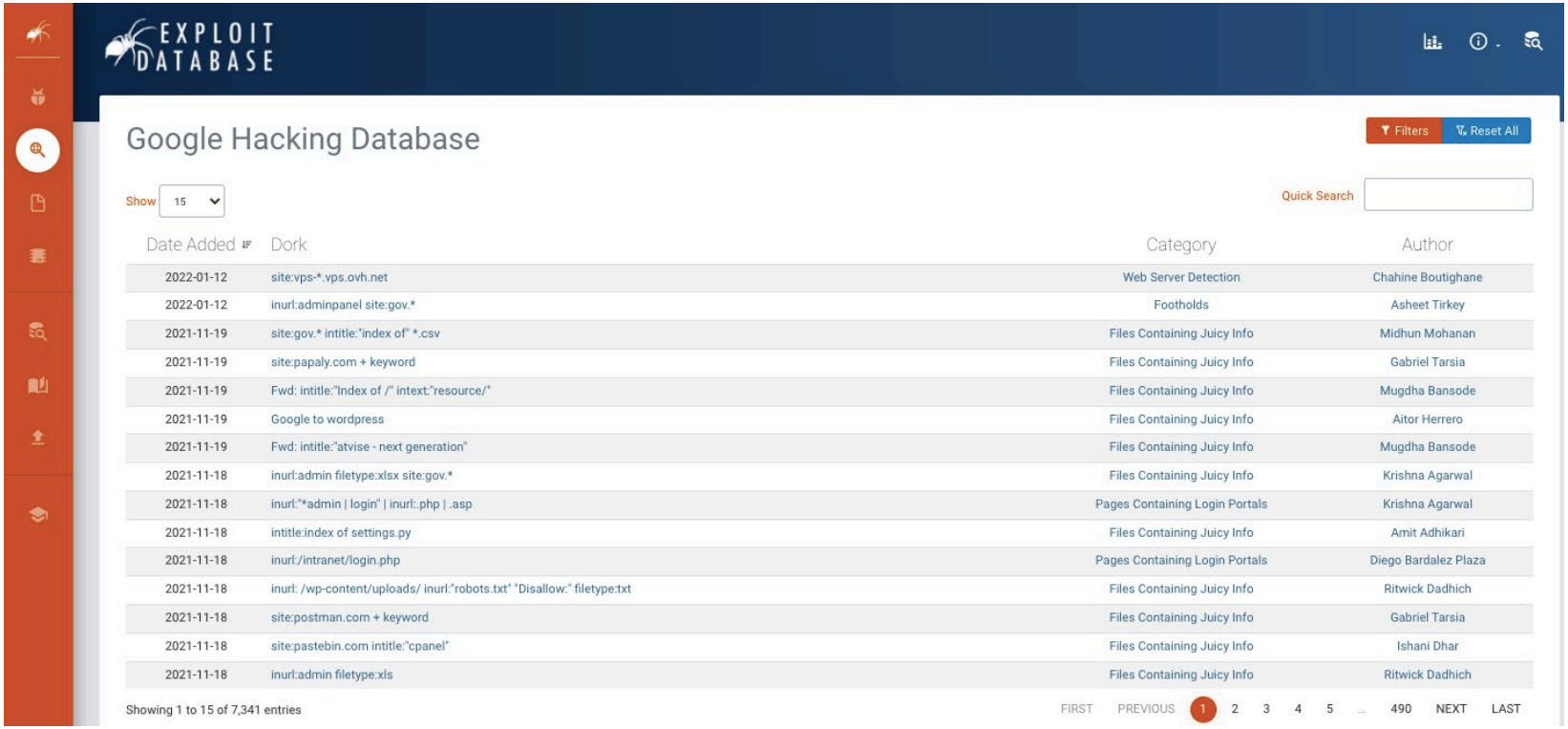
Google Hacking Database (GHDB)

- https://www.exploit-db.com/google-hacking-database

- Database collaborativo contenente complesse query Google «preconfezionate» chiamate **dork**
  - Aggiornate costantemente (fino al 28 agosto 2024)
  - Utilizzano determinati operatori per trovare informazioni specifiche

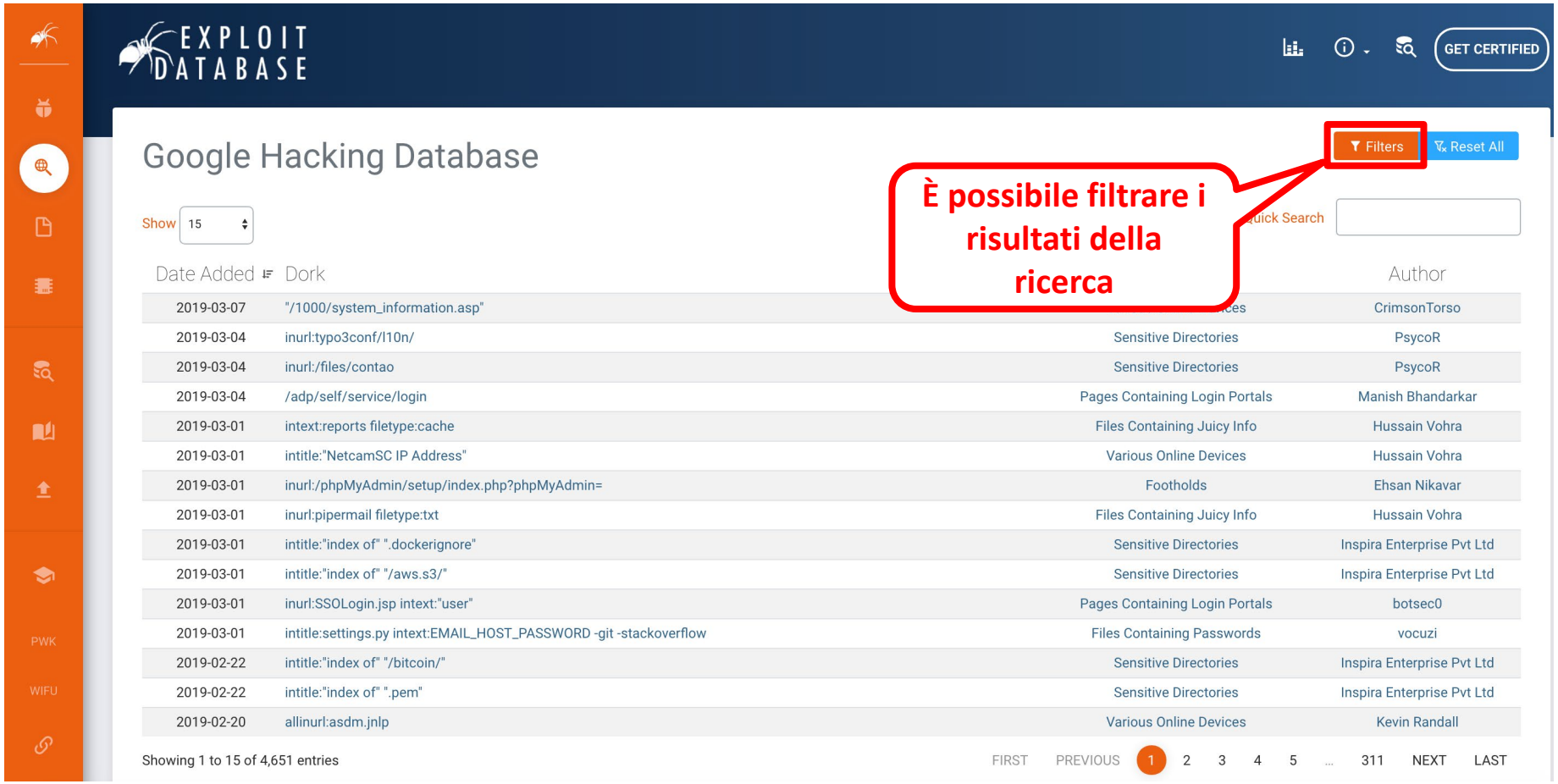
Utilizzo di Risorse Web-Based

Google Hacking Database (GHDB)



Utilizzo di Risorse Web-Based

Google Hacking Database (GHDB)



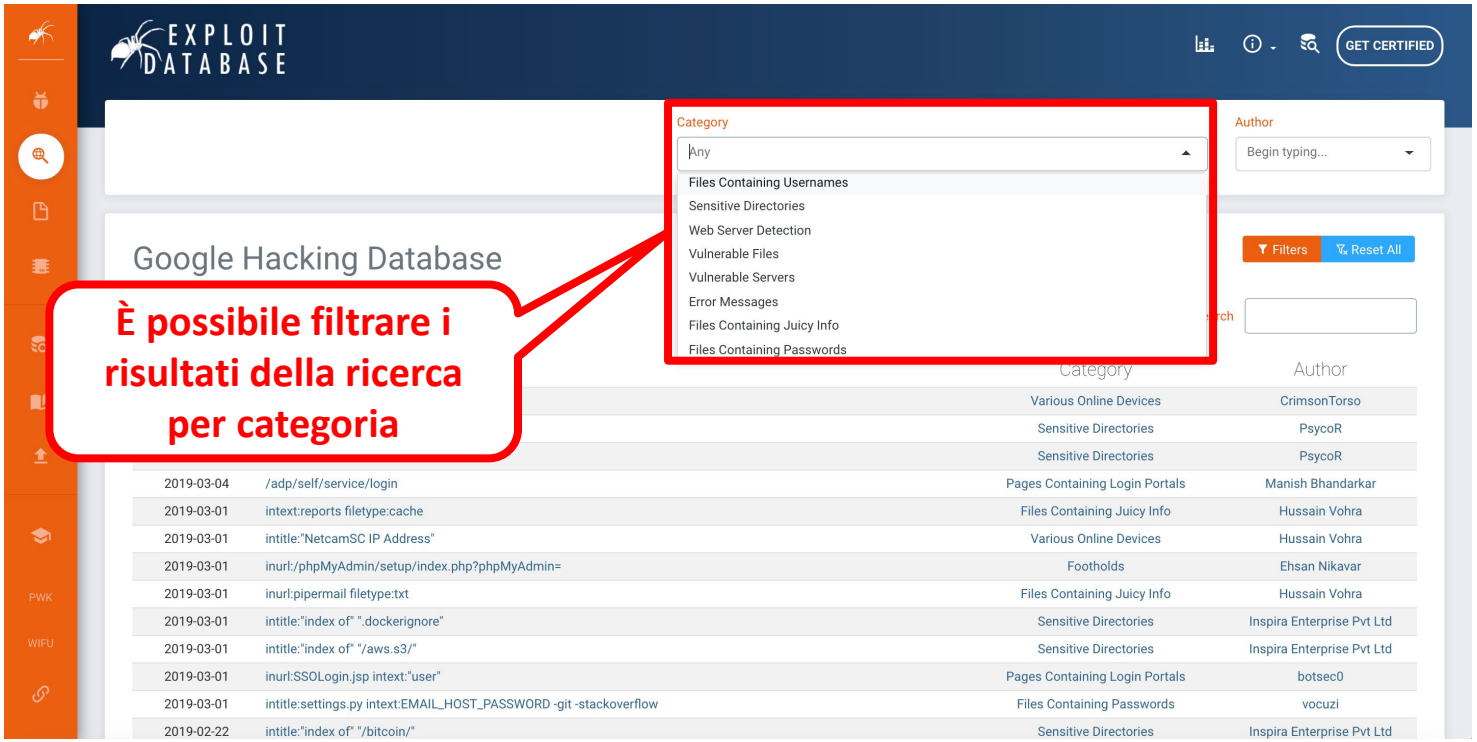
Date Added	Dork		Author
2019-03-07	"/1000/system_information.asp"		CrimsonTorso
2019-03-04	inurl:typo3conf/l10n/	Sensitive Directories	PsycoR
2019-03-04	inurl:/files/contao	Sensitive Directories	PsycoR
2019-03-04	/adp/self/service/login	Pages Containing Login Portals	Manish Bhandarkar
2019-03-01	intext:reports filetype:cache	Files Containing Juicy Info	Hussain Vohra
2019-03-01	intitle:"NetcamSC IP Address"	Various Online Devices	Hussain Vohra
2019-03-01	inurl:/phpMyAdmin/setup/index.php?phpMyAdmin=	Footholds	Ehsan Nikavar
2019-03-01	inurl:pipermail filetype:txt	Files Containing Juicy Info	Hussain Vohra
2019-03-01	intitle:"index of" ".dockerignore"	Sensitive Directories	Inspira Enterprise Pvt Ltd
2019-03-01	intitle:"index of" "/aws.s3/"	Sensitive Directories	Inspira Enterprise Pvt Ltd
2019-03-01	inurl:SSOLogin.jsp intext:"user"	Pages Containing Login Portals	botsec0
2019-03-01	intitle:settings.py intext:EMAIL_HOST_PASSWORD -git -stackoverflow	Files Containing Passwords	vocuzi
2019-02-22	intitle:"index of" "/bitcoin/"	Sensitive Directories	Inspira Enterprise Pvt Ltd
2019-02-22	intitle:"index of" ".pem"	Sensitive Directories	Inspira Enterprise Pvt Ltd
2019-02-20	allinurl:asdm.jnlp	Various Online Devices	Kevin Randall

Showing 1 to 15 of 4,651 entries

FIRST PREVIOUS 1 2 3 4 5 ... 311 NEXT LAST

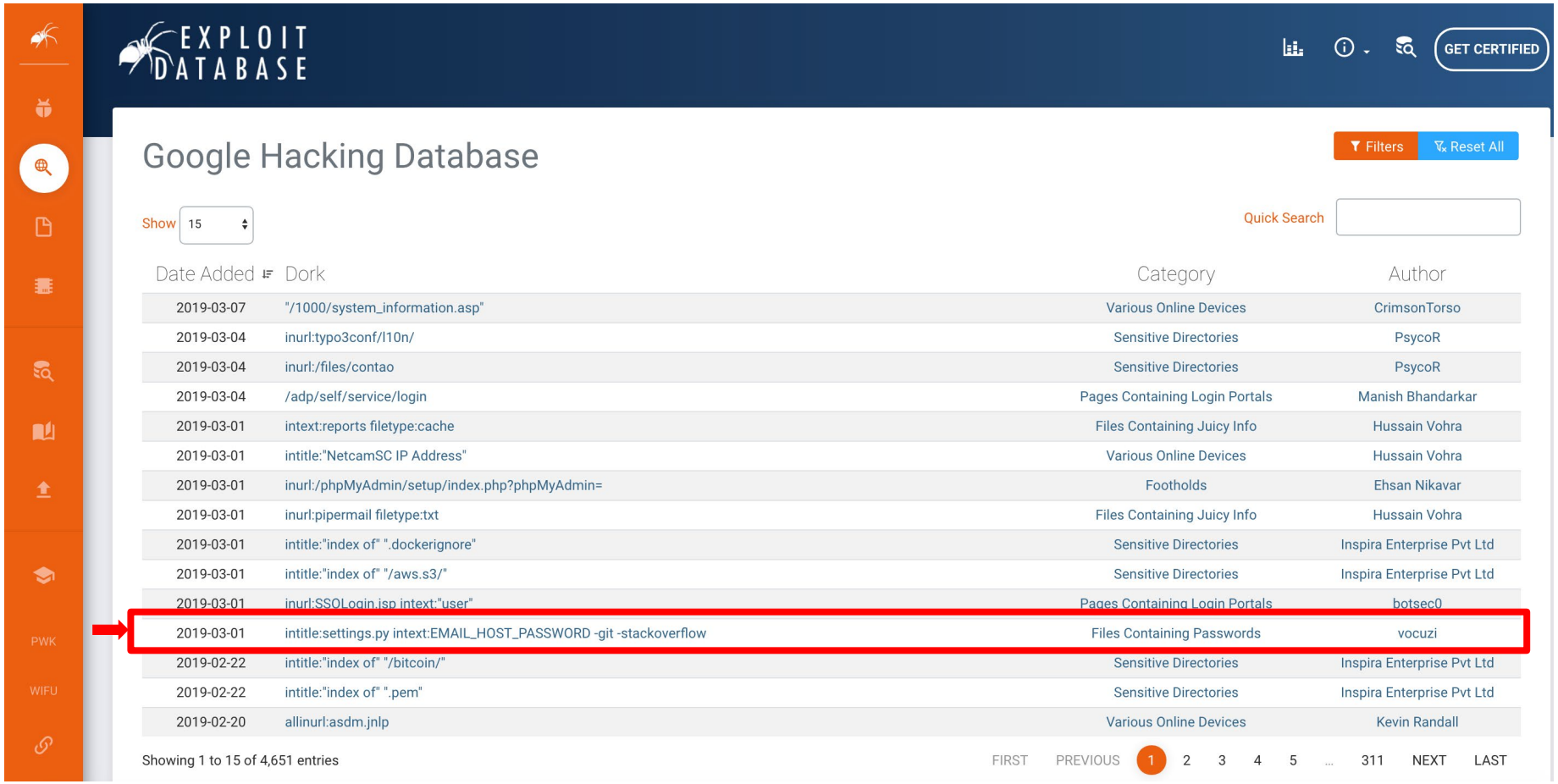
Utilizzo di Risorse Web-Based

Google Hacking Database (GHDB)



Utilizzo di Risorse Web-Based

Google Hacking Database (GHDB)



Utilizzo di Risorse Web-Based

Google Hacking Database (GHDB)

intitle:settings.py intext:EMAIL_HOST_PASSWORD -git -stackoverflow

GHDB-ID: 5141

Author: VOCUZI

Published: 2019-03-01

Google Dork Description:

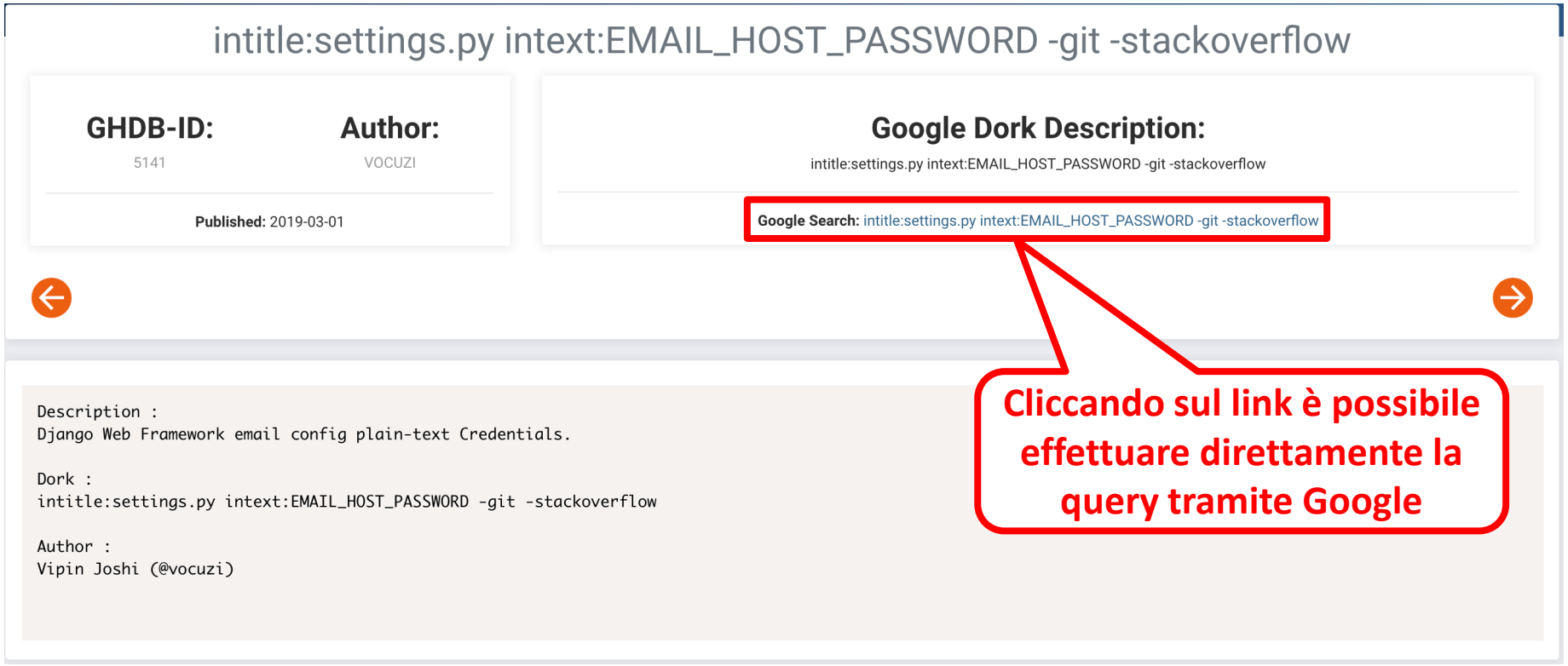
intitle:settings.py intext:EMAIL_HOST_PASSWORD -git -stackoverflow

Google Search: intitle:settings.py intext:EMAIL_HOST_PASSWORD -git -stackoverflow

```
Description :
Django Web Framework email config plain-text Credentials.

Dork :
intitle:settings.py intext:EMAIL_HOST_PASSWORD -git -stackoverflow

Author :
Vipin Joshi (@vocuzi)
```

Utilizzo di Risorse Web-Based

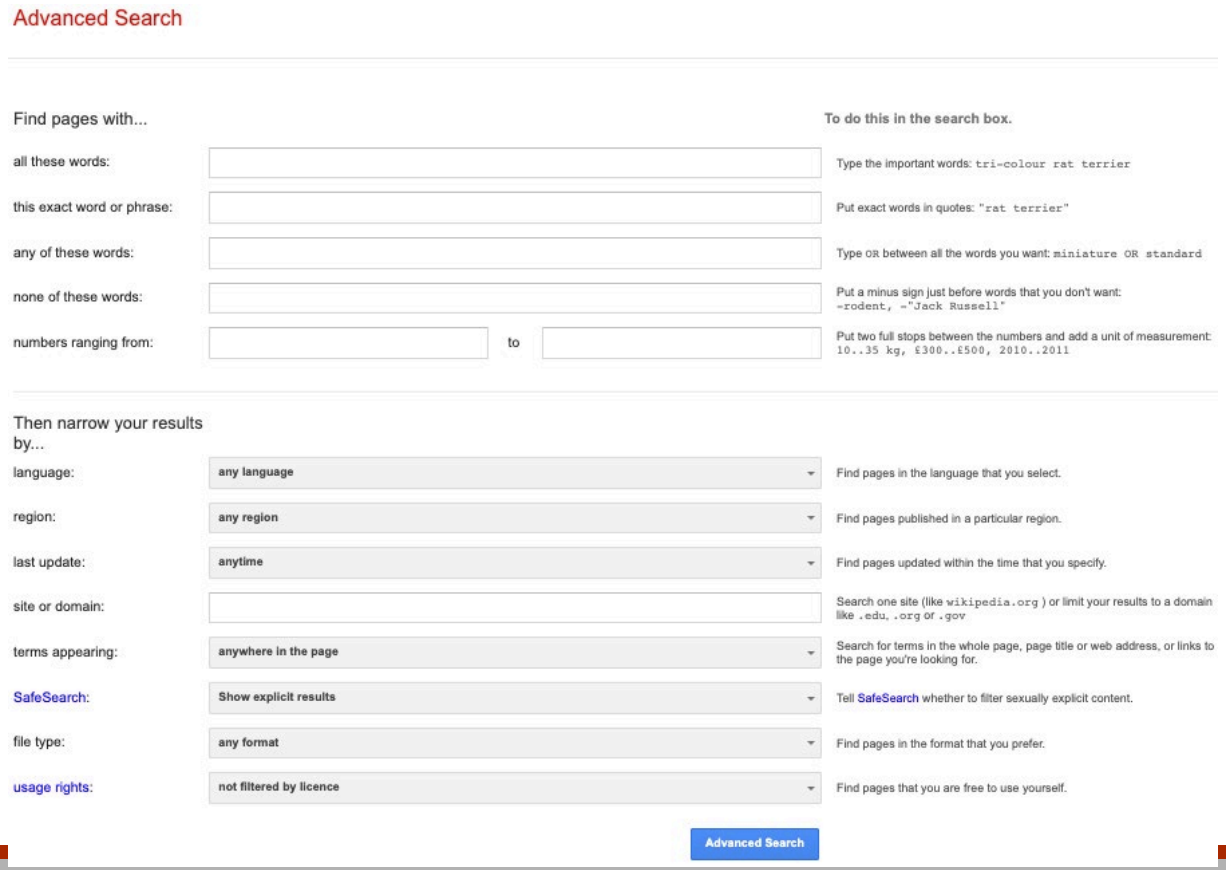
Google Hacking Database (GHDB)



Utilizzo di Risorse Web-Based

Google Advanced Search

- https://www.google.com/advanced_search



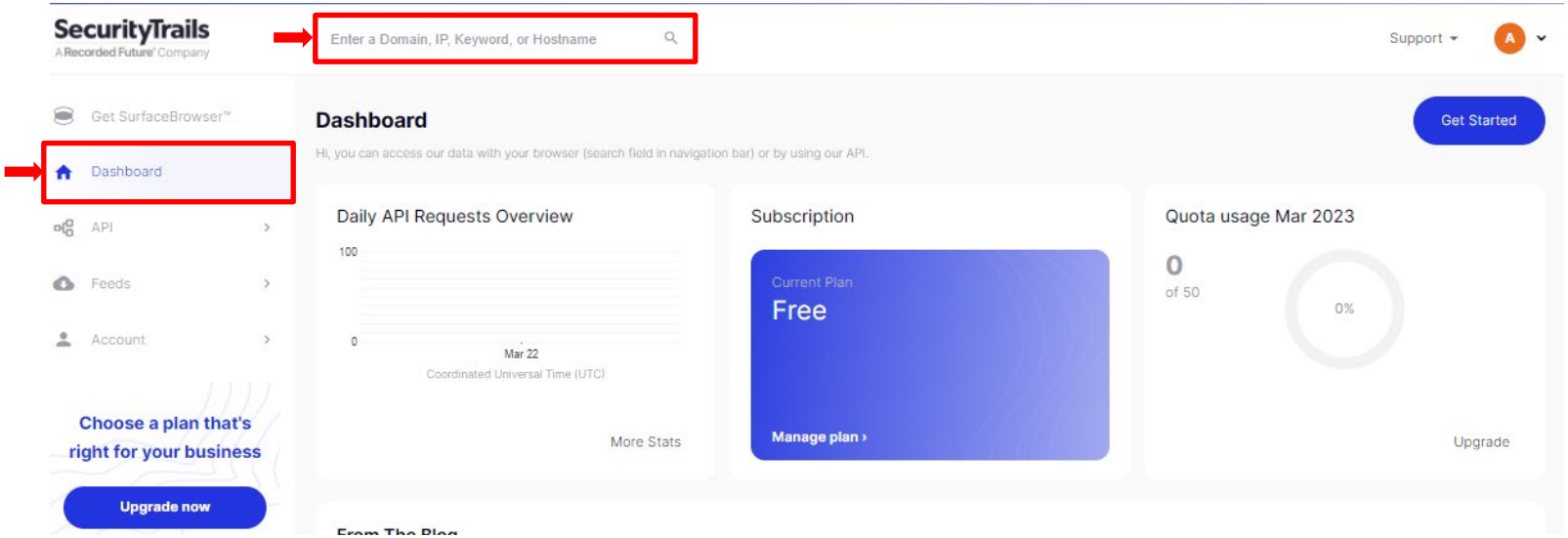
Utilizzo di Risorse Web-Based

Asset Discovery – SecurityTrails

- https://securitytrails.com/
  - Servizio che raccoglie e fornisce dati riguardanti DNS (ad es., sottodomini), indirizzi IP, *whois*, ed altri servizi di rete
  - Parte dei dati viene fornita gratuitamente su una piattaforma Web per ricerche e indagini
  - Oltre alla piattaforma gratuita, tutti i dati raccolti vengono forniti tramite API a pagamento

Utilizzo di Risorse Web-Based

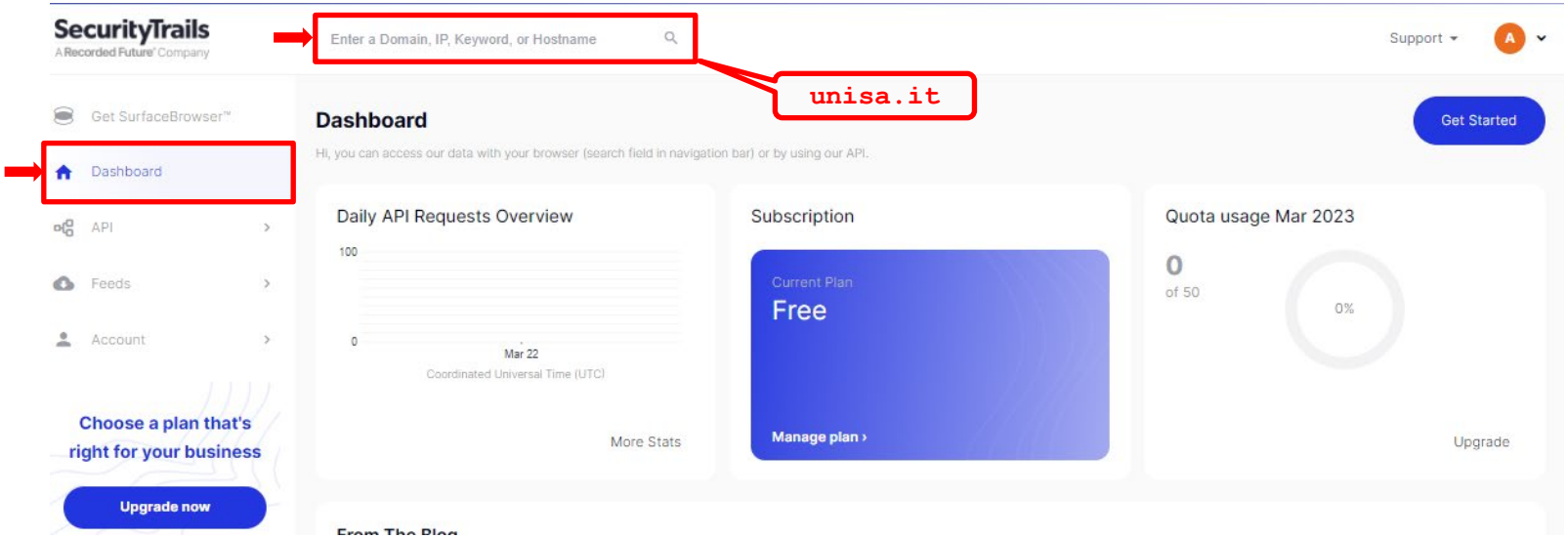
Asset Discovery – SecurityTrails



Dashboard

Utilizzo di Risorse Web-Based

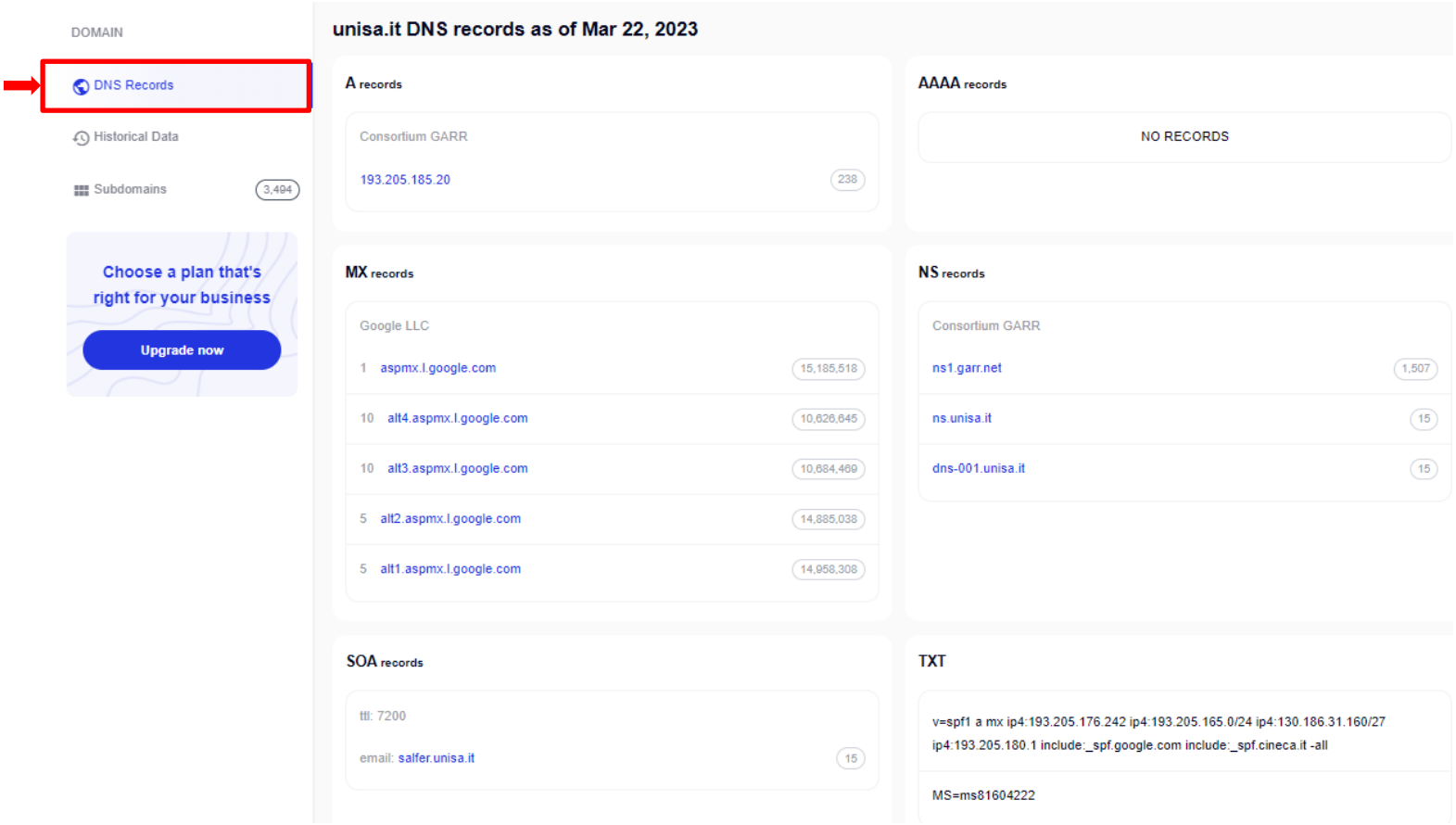
Asset Discovery – SecurityTrails – Esempio



Dashboard

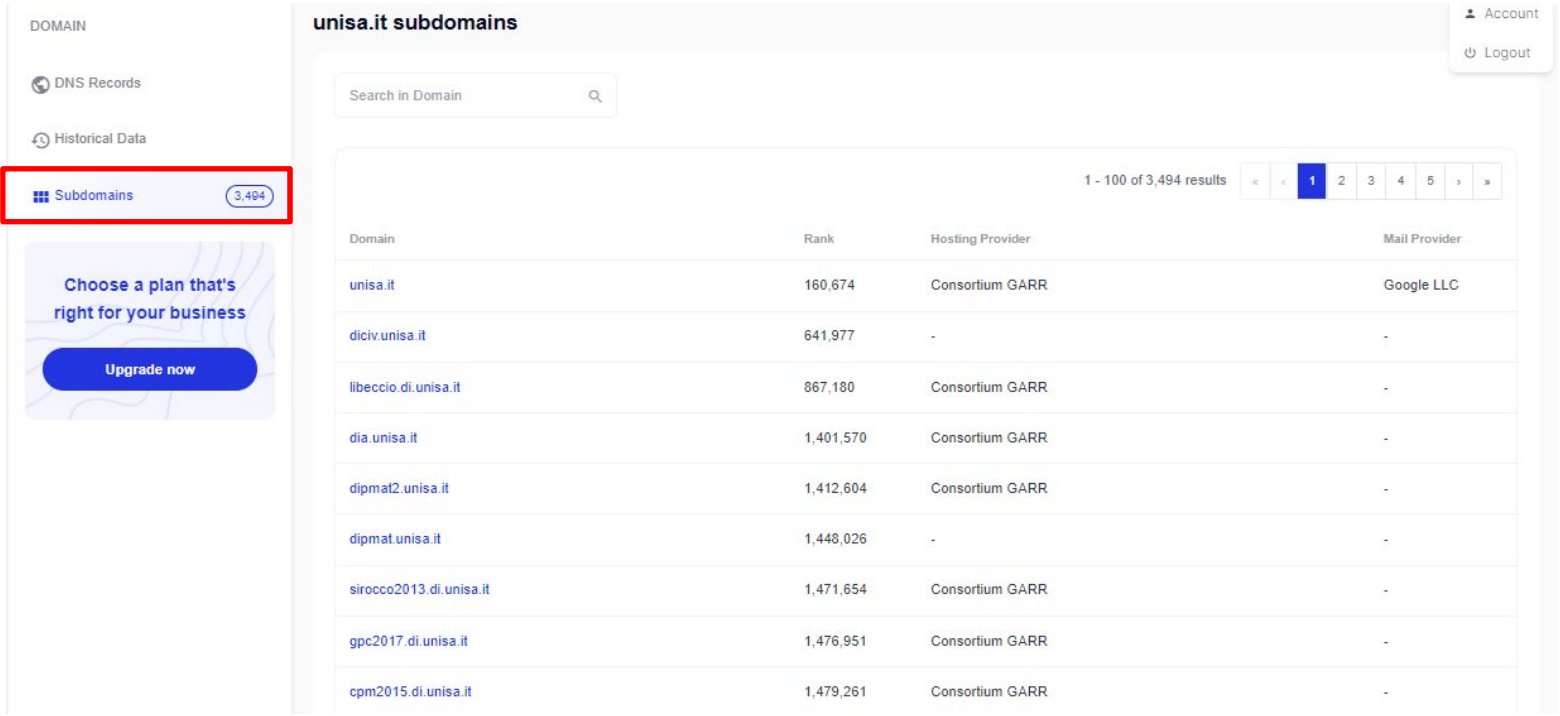
Utilizzo di Risorse Web-Based

Asset Discovery – SecurityTrails – Esempio



Utilizzo di Risorse Web-Based

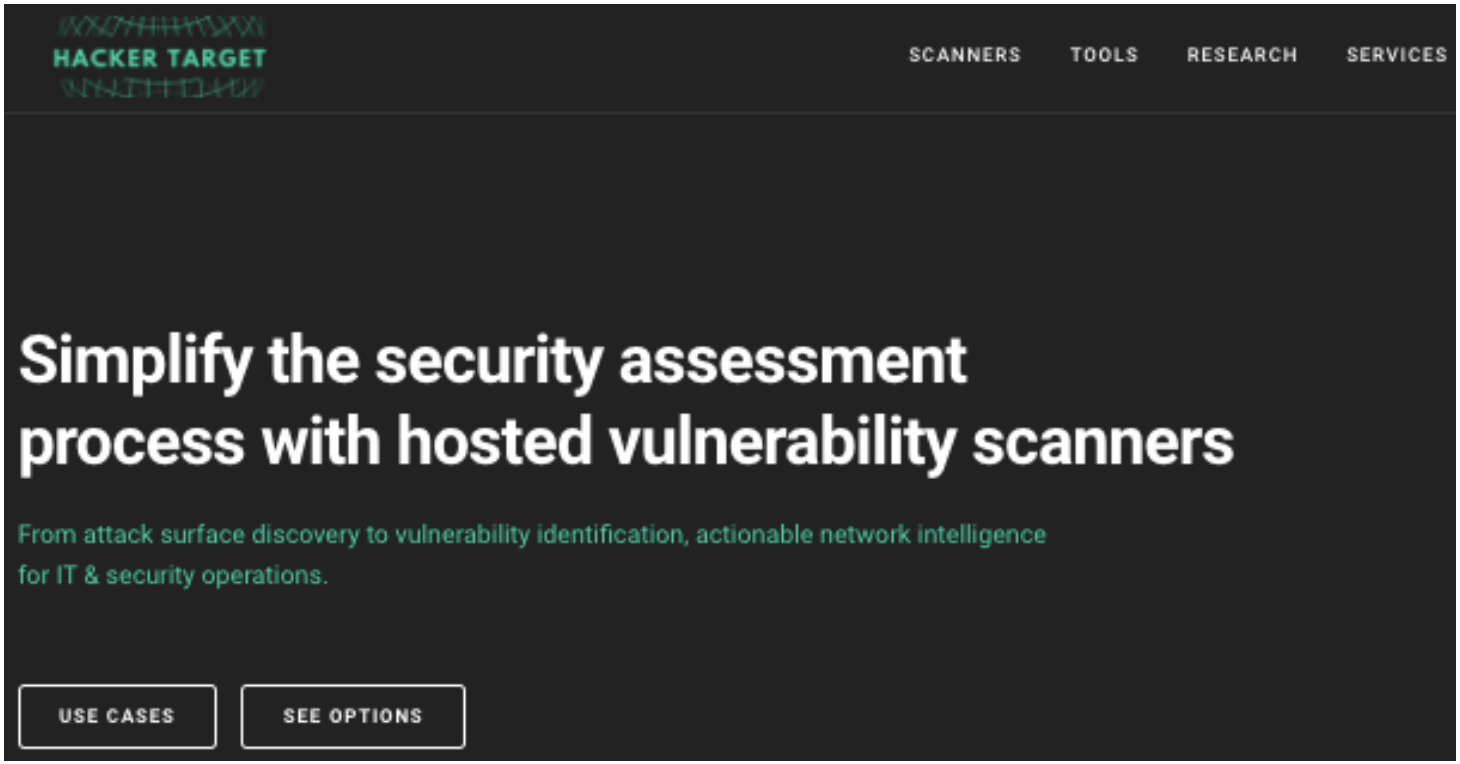
Asset Discovery – SecurityTrails – Esempio



Utilizzo di Risorse Web-Based

Asset Discovery – Hacker Target

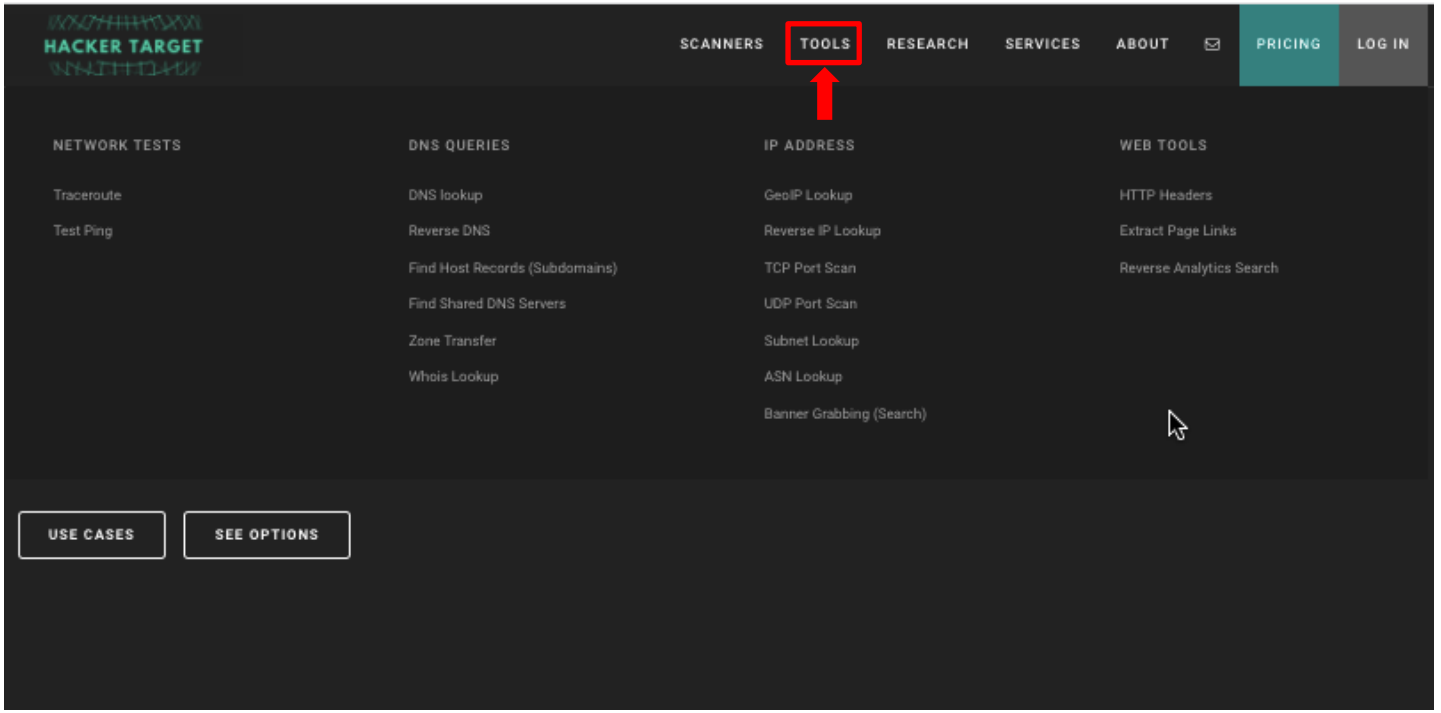
- https://hackertarget.com/
  - Permette di cercare informazioni riguardo domini e servizi di rete



Utilizzo di Risorse Web-Based

Asset Discovery – Hacker Target

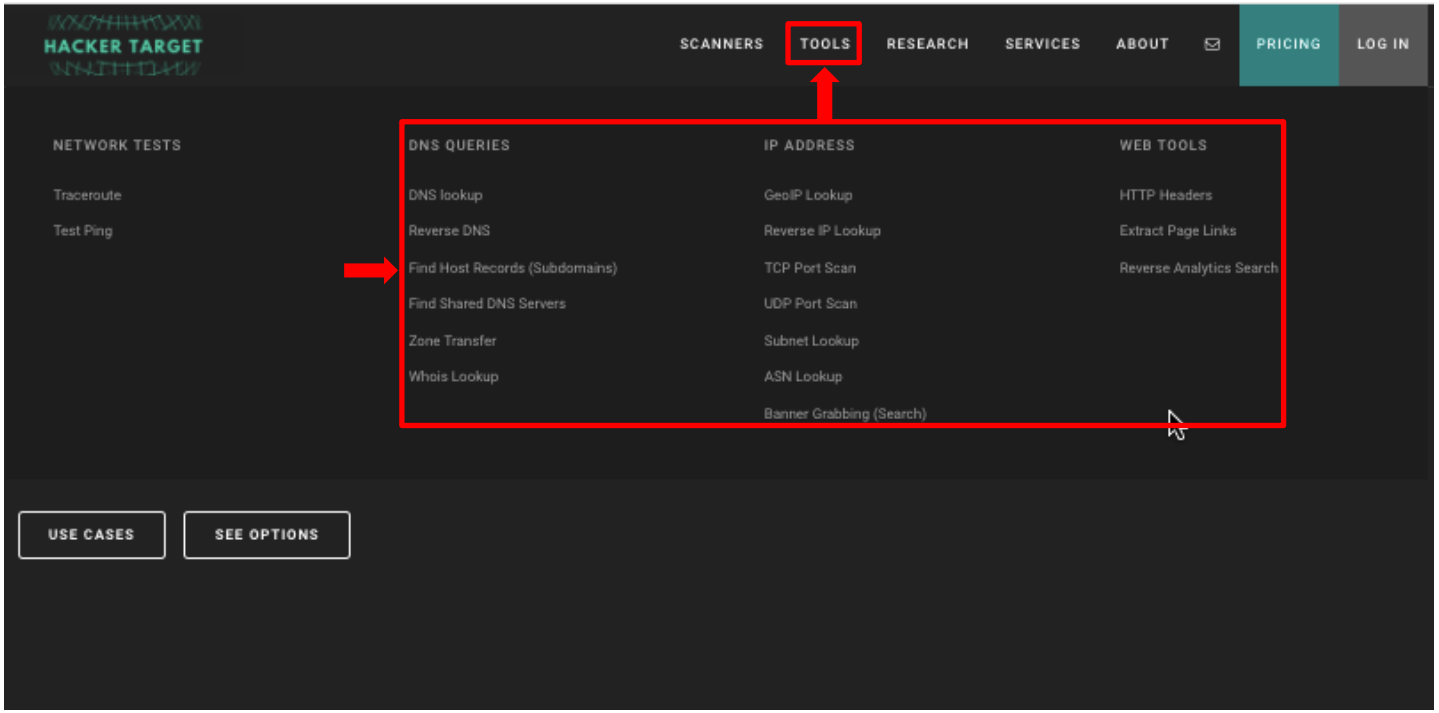
- https://hackertarget.com/
  - Permette di cercare informazioni riguardo domini e servizi di rete



Utilizzo di Risorse Web-Based

Asset Discovery – Hacker Target

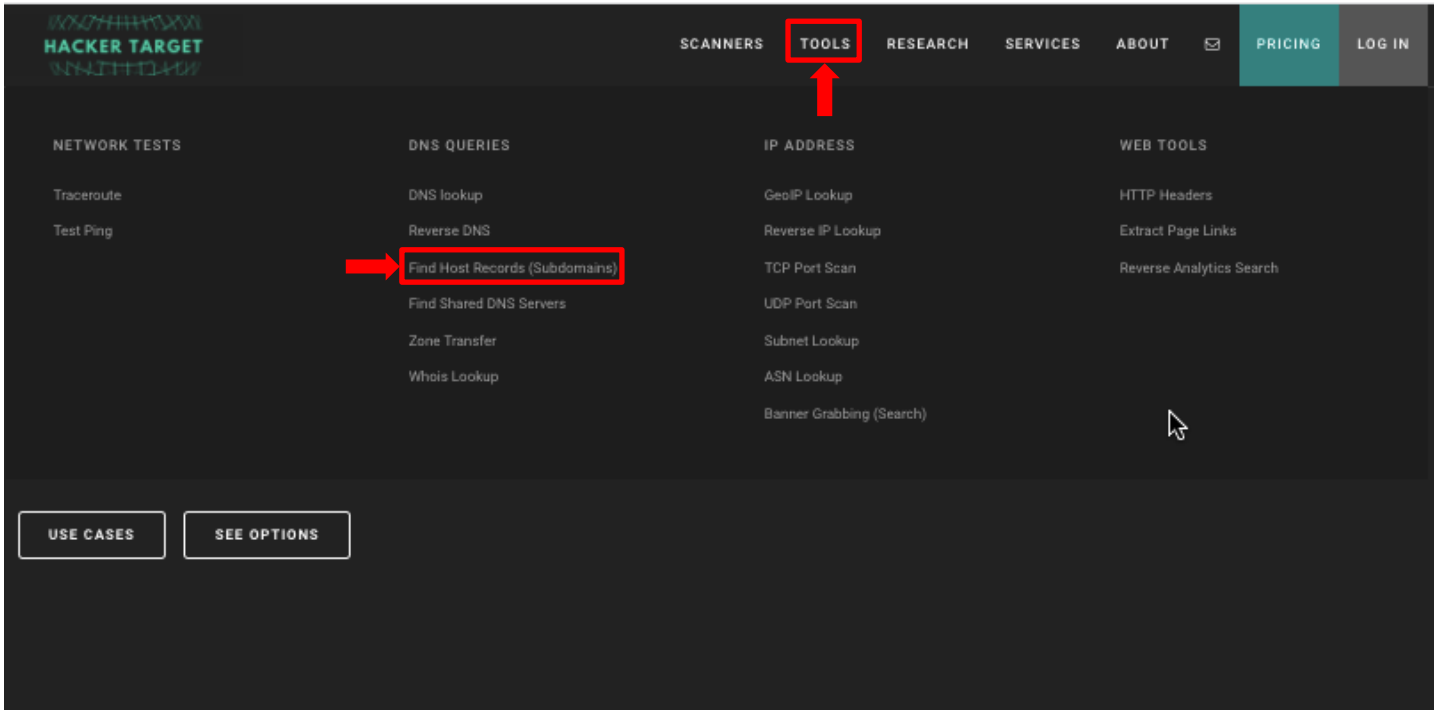
- https://hackertarget.com/
  - Permette di cercare informazioni riguardo domini e servizi di rete



Utilizzo di Risorse Web-Based

Asset Discovery – Hacker Target

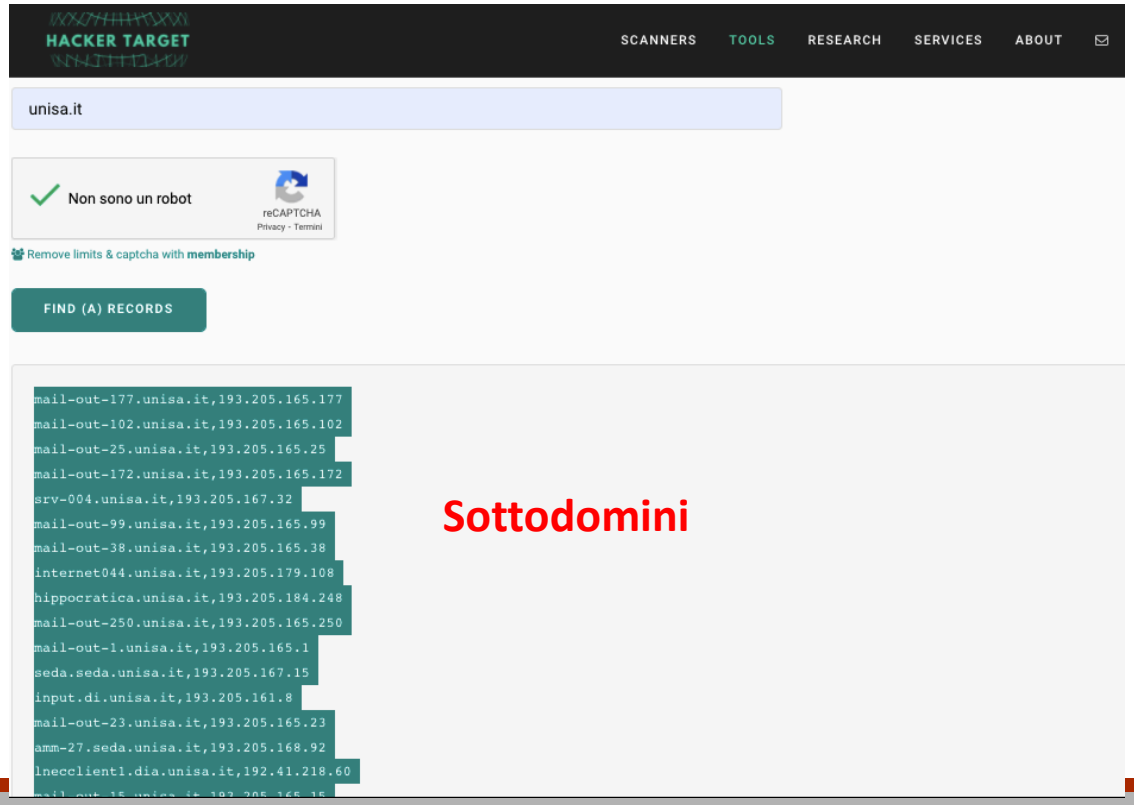
- https://hackertarget.com/
  - Permette di cercare informazioni riguardo domini e servizi di rete



Utilizzo di Risorse Web-Based

Asset Discovery – Hacker Target

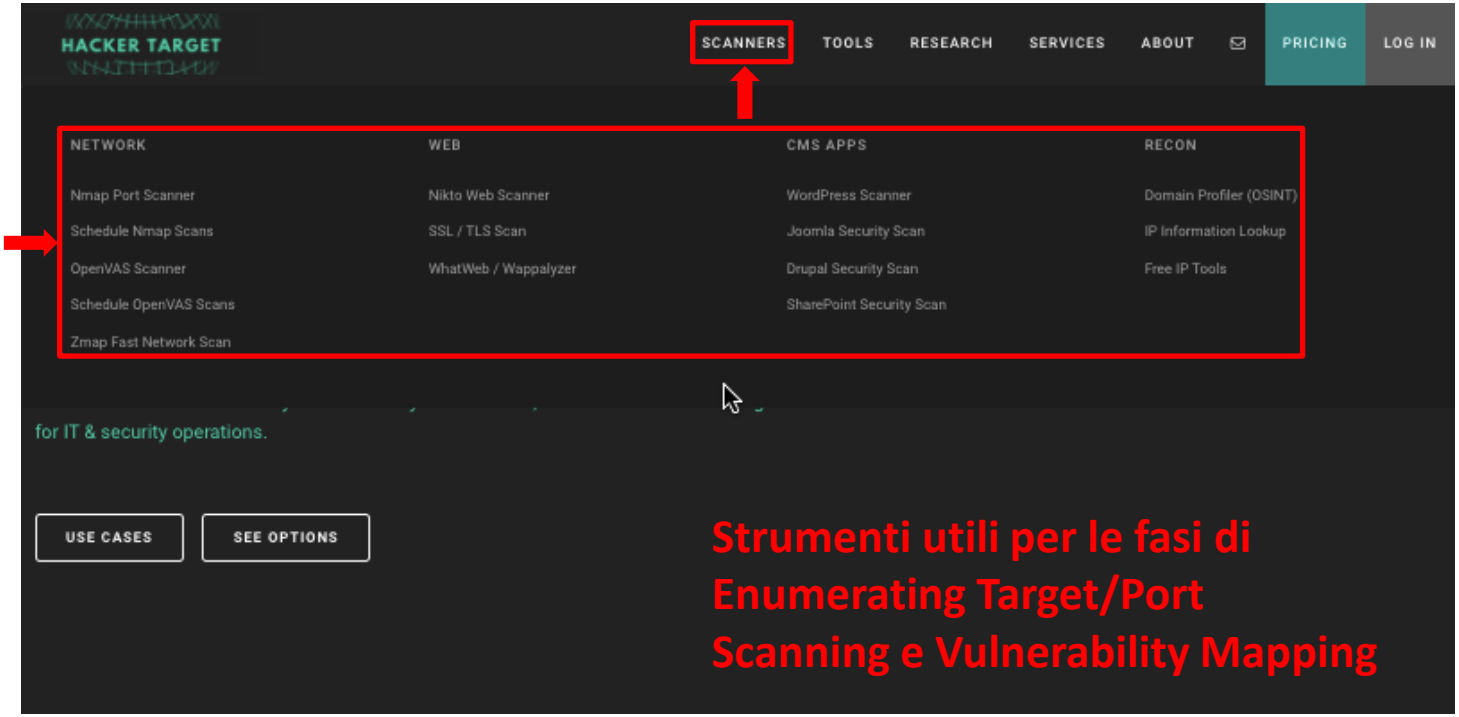
- https://hackertarget.com/
  - Permette di cercare informazioni riguardo domini e servizi di rete



Utilizzo di Risorse Web-Based

Asset Discovery – Hacker Target

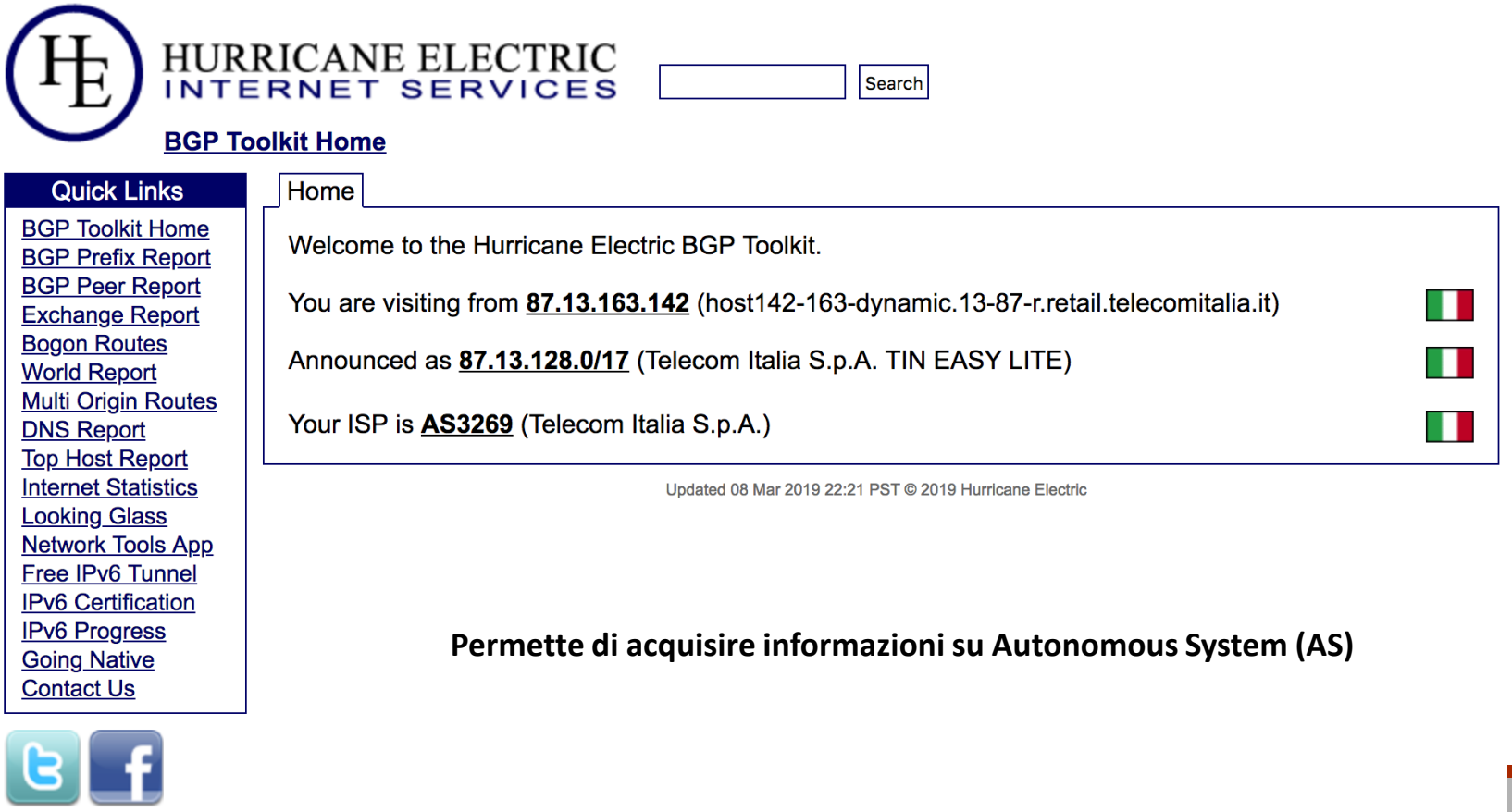
- https://hackertarget.com/
  - Permette di cercare informazioni riguardo domini e servizi di rete



Utilizzo di Risorse Web-Based

Asset Discovery – H. E. BGP Toolkit

- https://bgp.he.net/

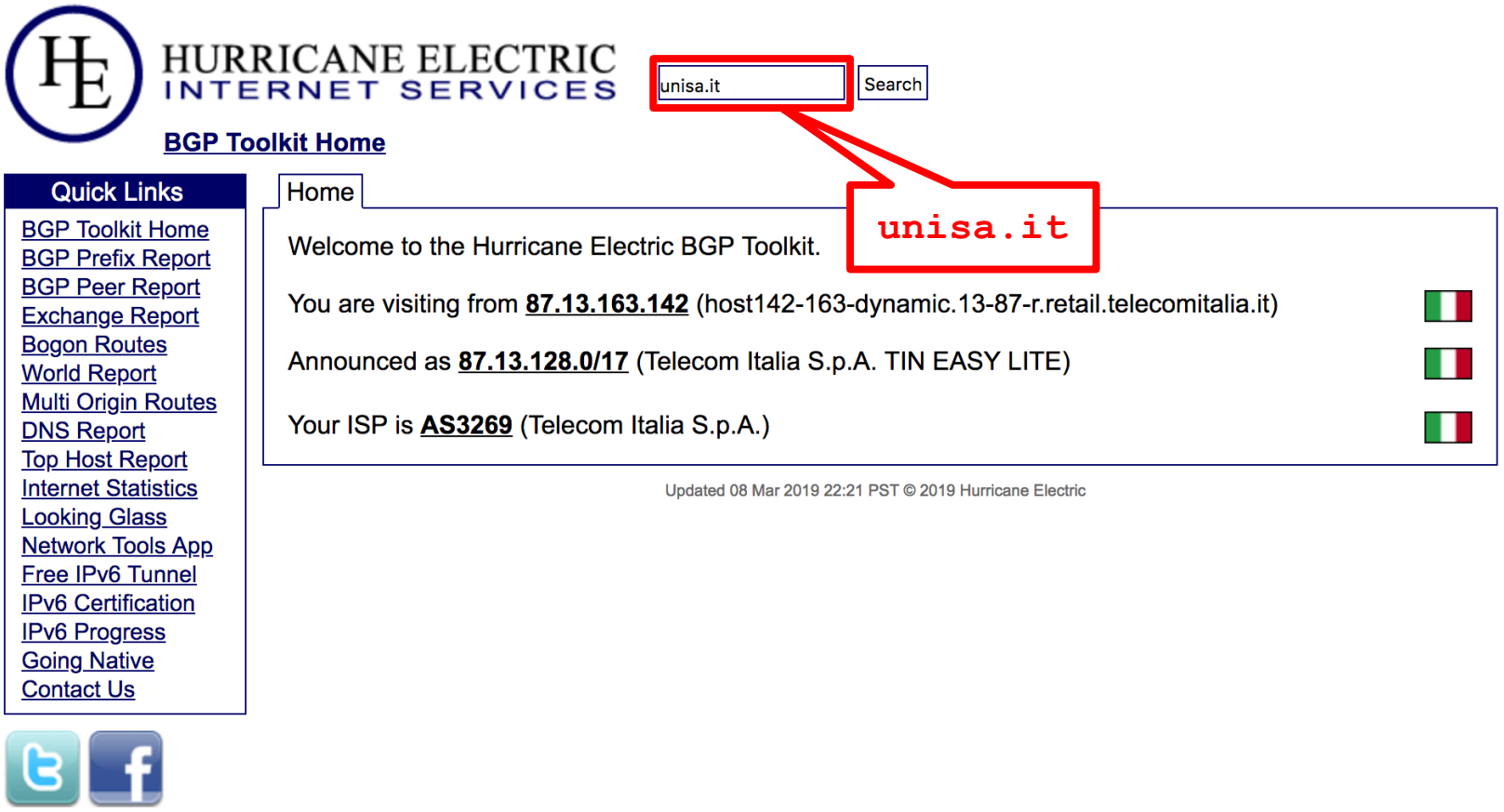


Permette di acquisire informazioni su Autonomous System (AS)

Utilizzo di Risorse Web-Based

Asset Discovery – H. E. BGP Toolkit

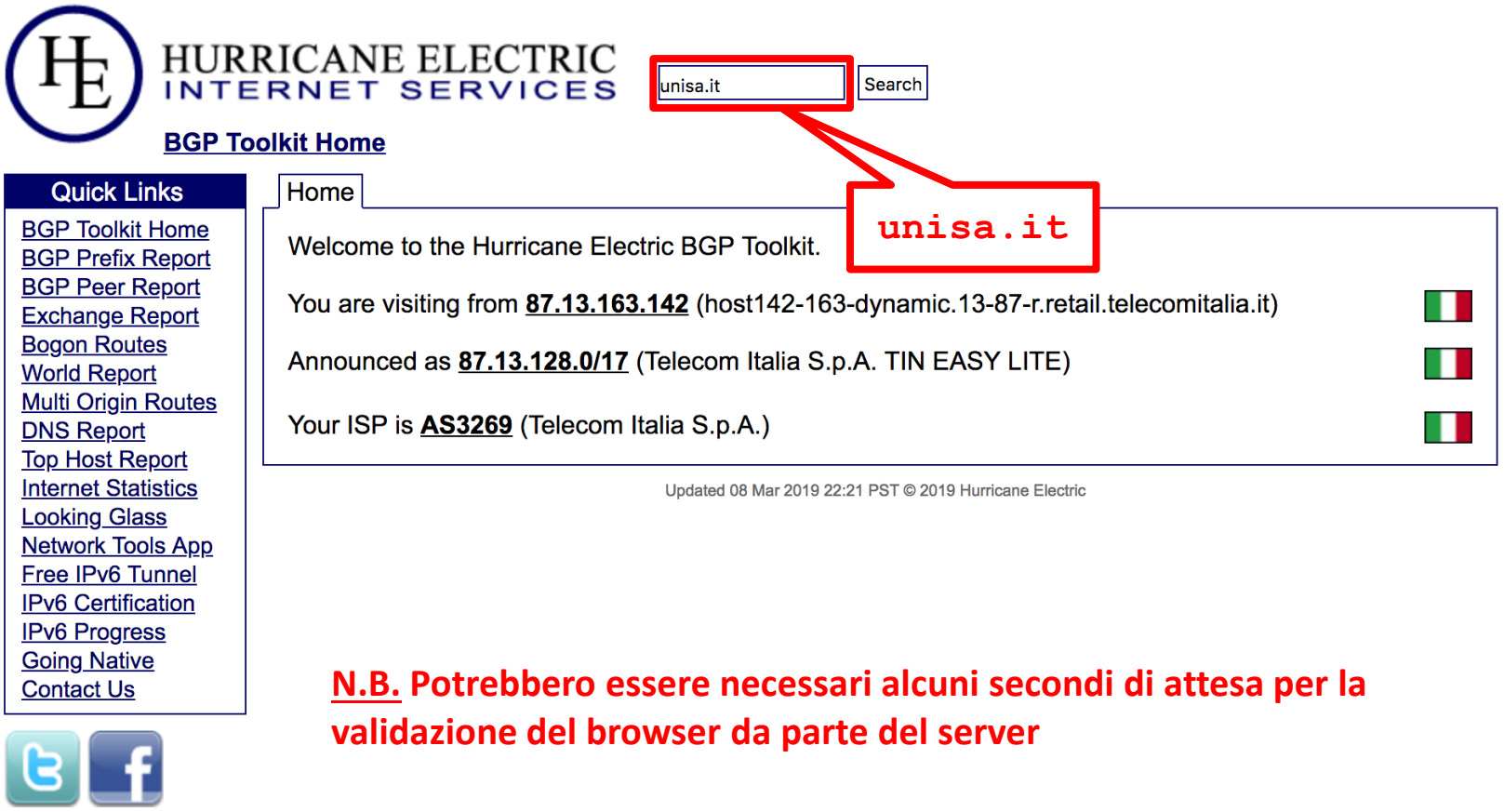
- https://bgp.he.net/



Utilizzo di Risorse Web-Based

Asset Discovery – H. E. BGP Toolkit

- https://bgp.he.net/

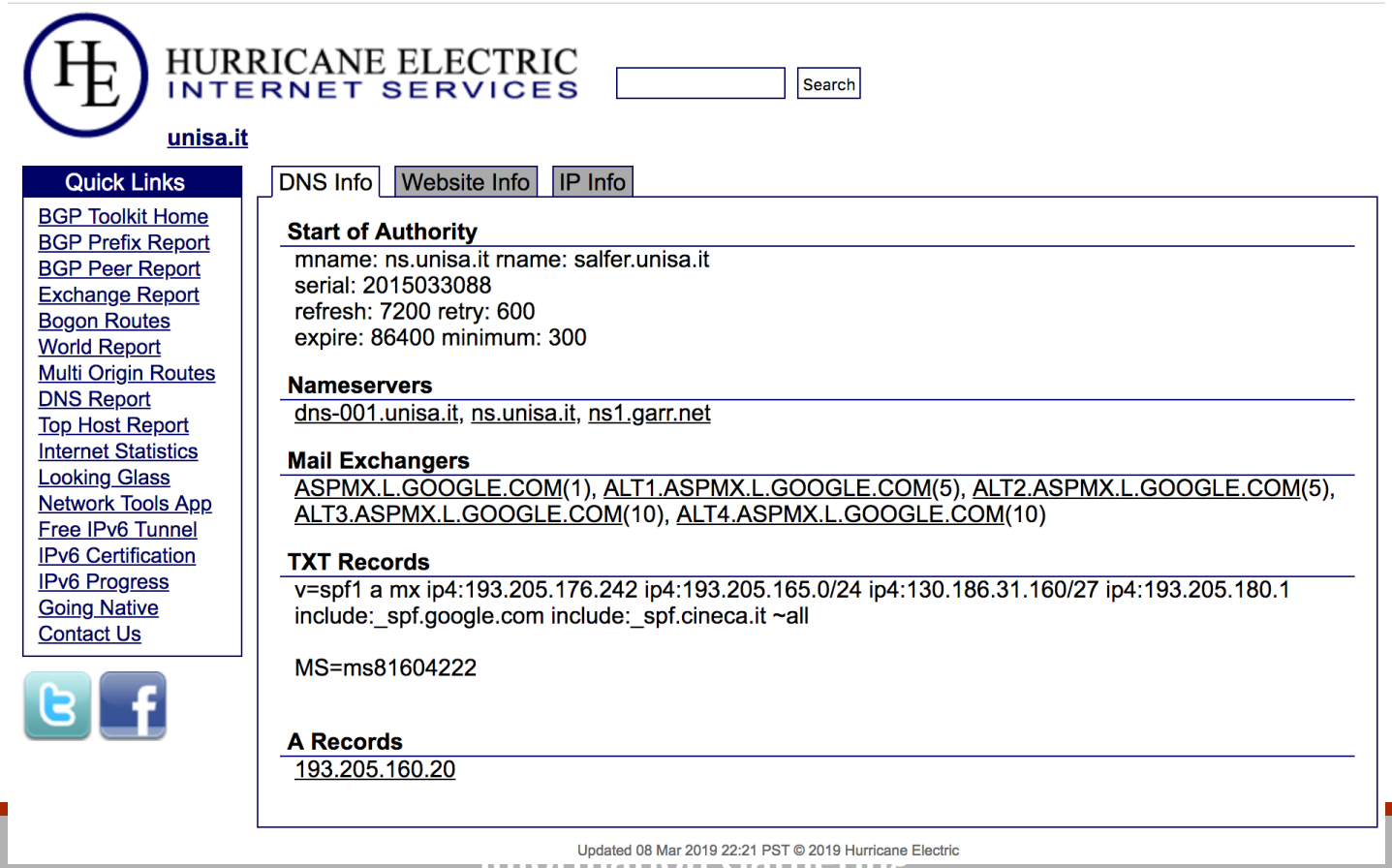


N.B. Potrebbero essere necessari alcuni secondi di attesa per la validazione del browser da parte del server

Utilizzo di Risorse Web-Based

Asset Discovery – H. E. BGP Toolkit

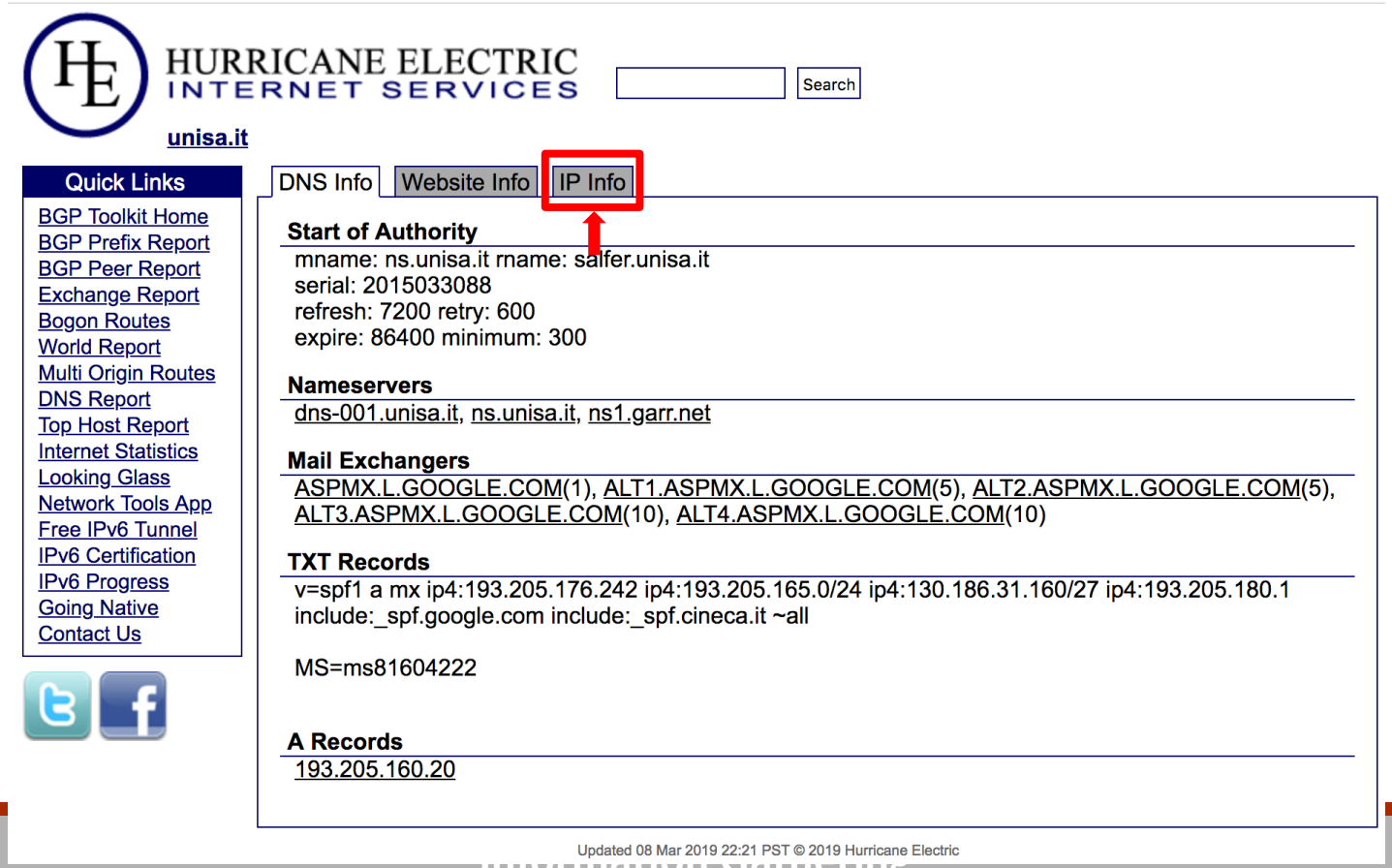
- https://bgp.he.net/



Utilizzo di Risorse Web-Based

Asset Discovery – H. E. BGP Toolkit

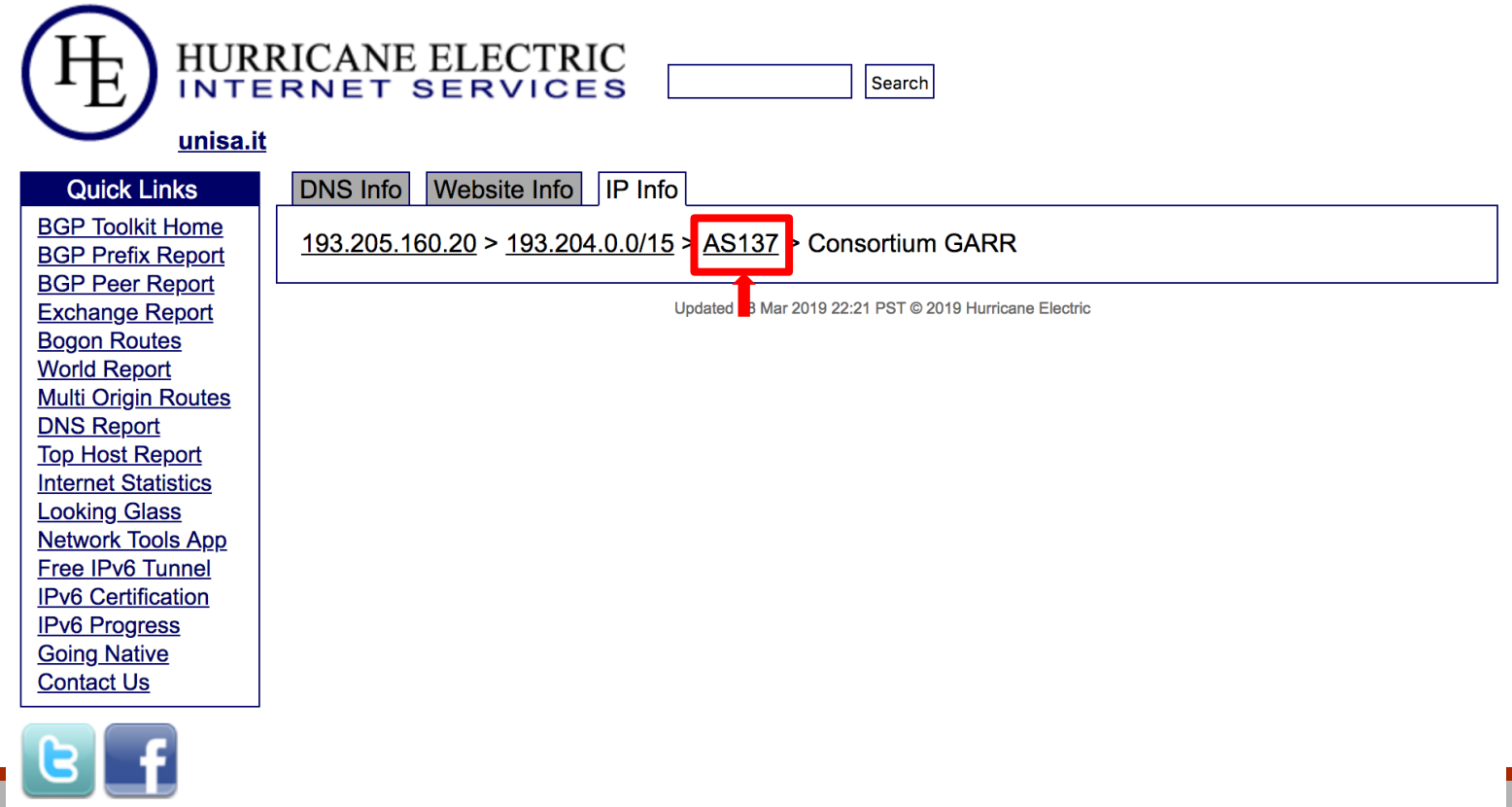
- https://bgp.he.net/



Utilizzo di Risorse Web-Based

Asset Discovery – H. E. BGP Toolkit

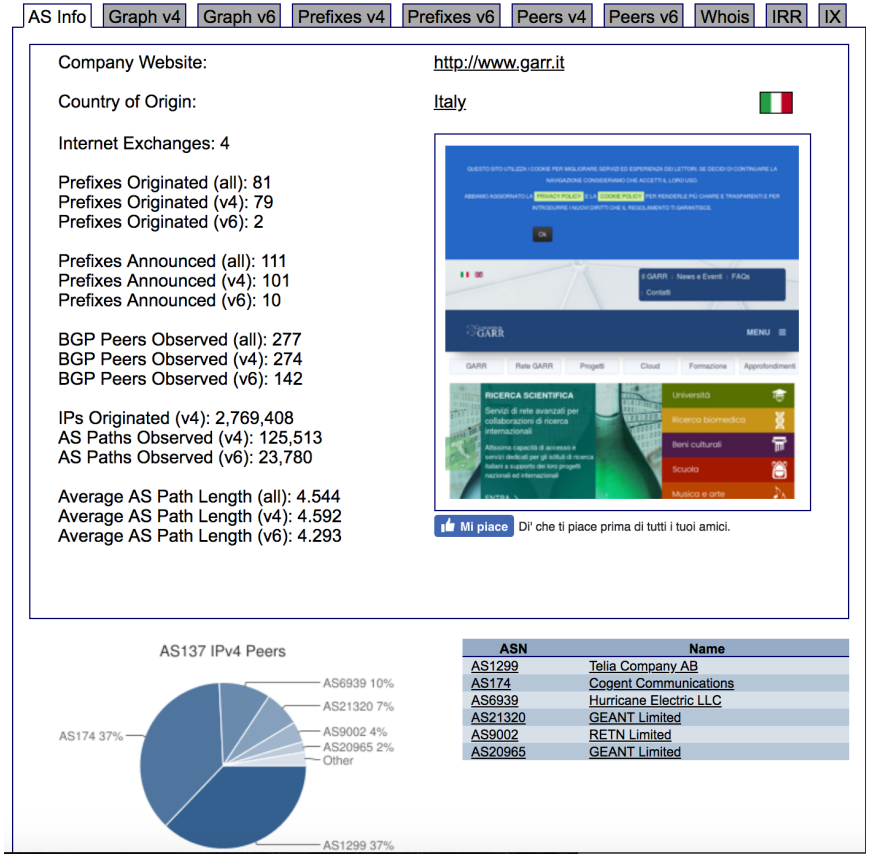
- https://bgp.he.net/



Utilizzo di Risorse Web-Based

Asset Discovery – H. E. BGP Toolkit

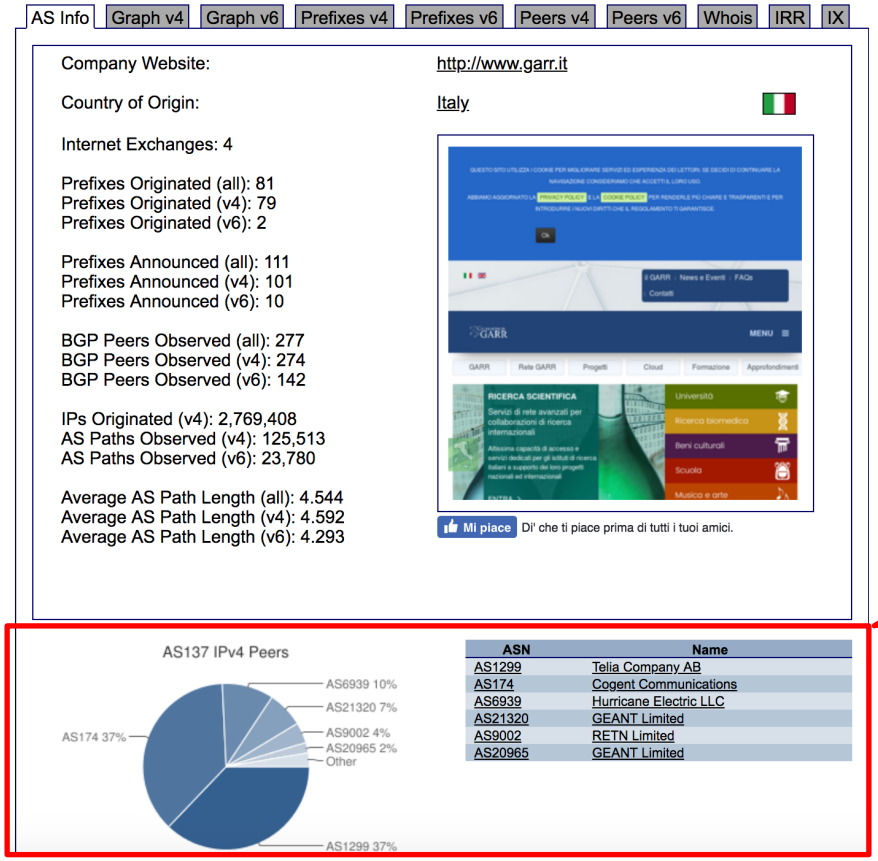
- https://bgp.he.net/



Utilizzo di Risorse Web-Based

Asset Discovery – H. E. BGP Toolkit

- https://bgp.he.net/



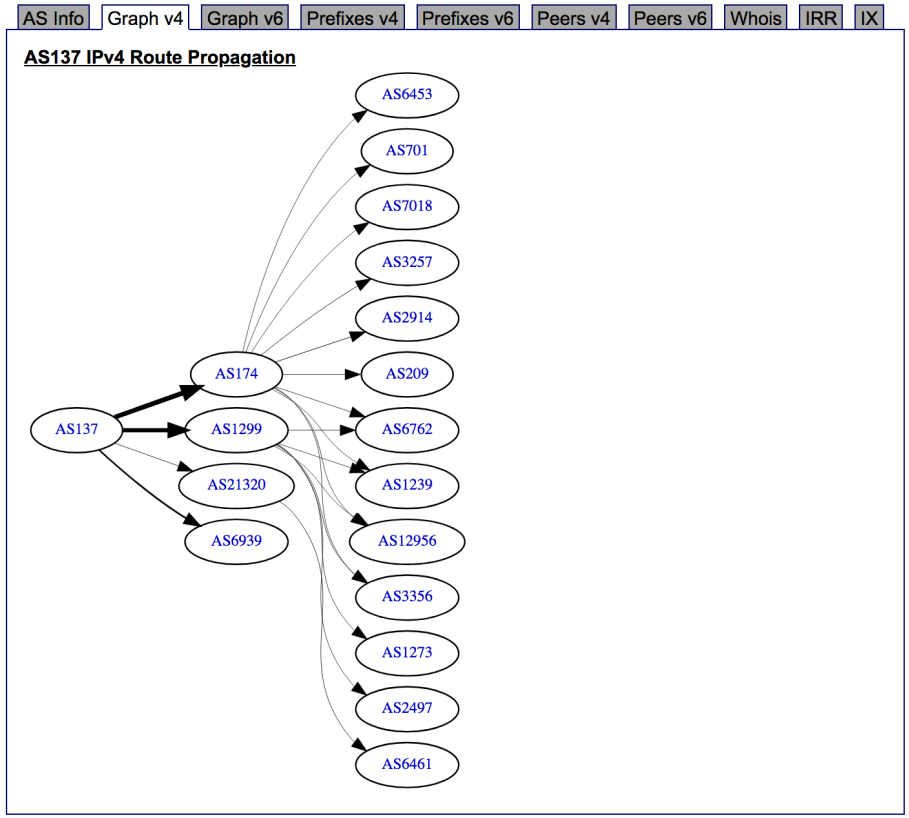
Peer con cui l'AS137 «interagisce» più frequentemente

Utilizzo di Risorse Web-Based

Asset Discovery – H. E. BGP Toolkit

- https://bgp.he.net/

Accordi di Peering



Utilizzo di Risorse Web-Based

Asset Discovery – DNSdumpster

- https://dnsdumpster.com

- Strumento per condurre attività di Information Gathering, prevalentemente basate su OSINT

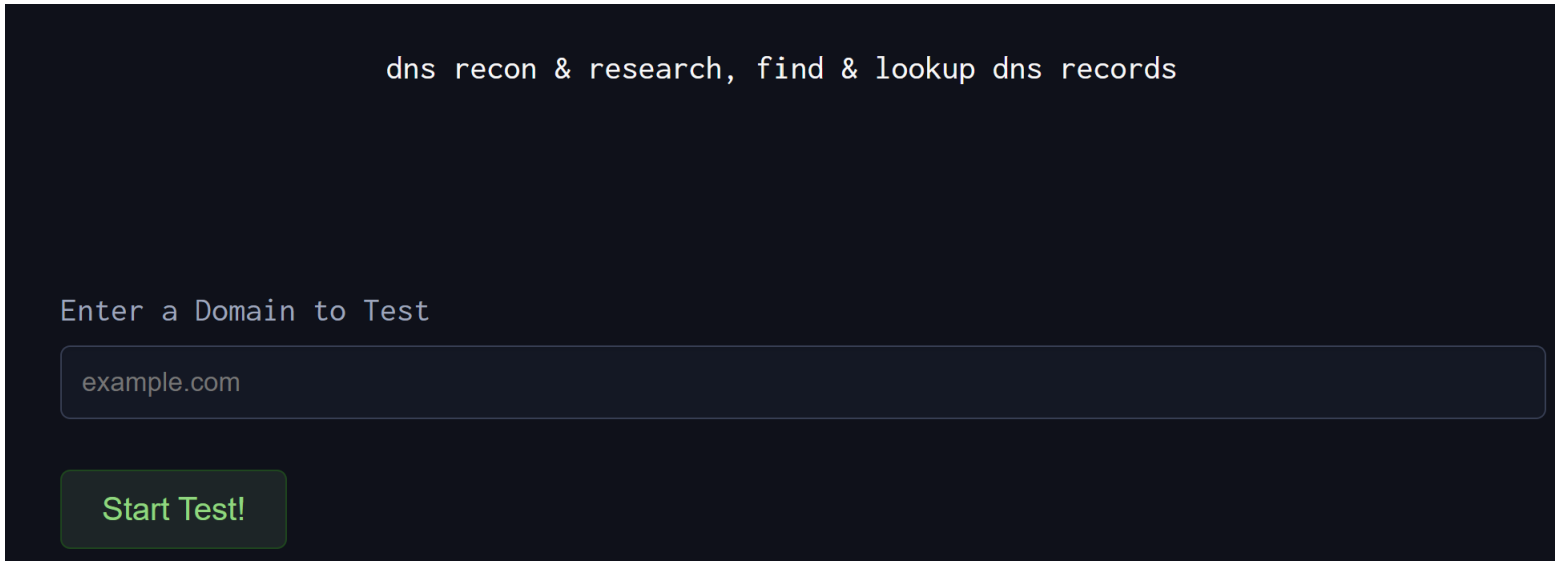
- Permette di
  - Cercare informazioni su domini e servizi di rete
  - Rappresentare in modalità grafica le informazioni ottenute

- Disponibile sia in versione Web-based che tramite API

Utilizzo di Risorse Web-Based

Asset Discovery – DNSdumpster

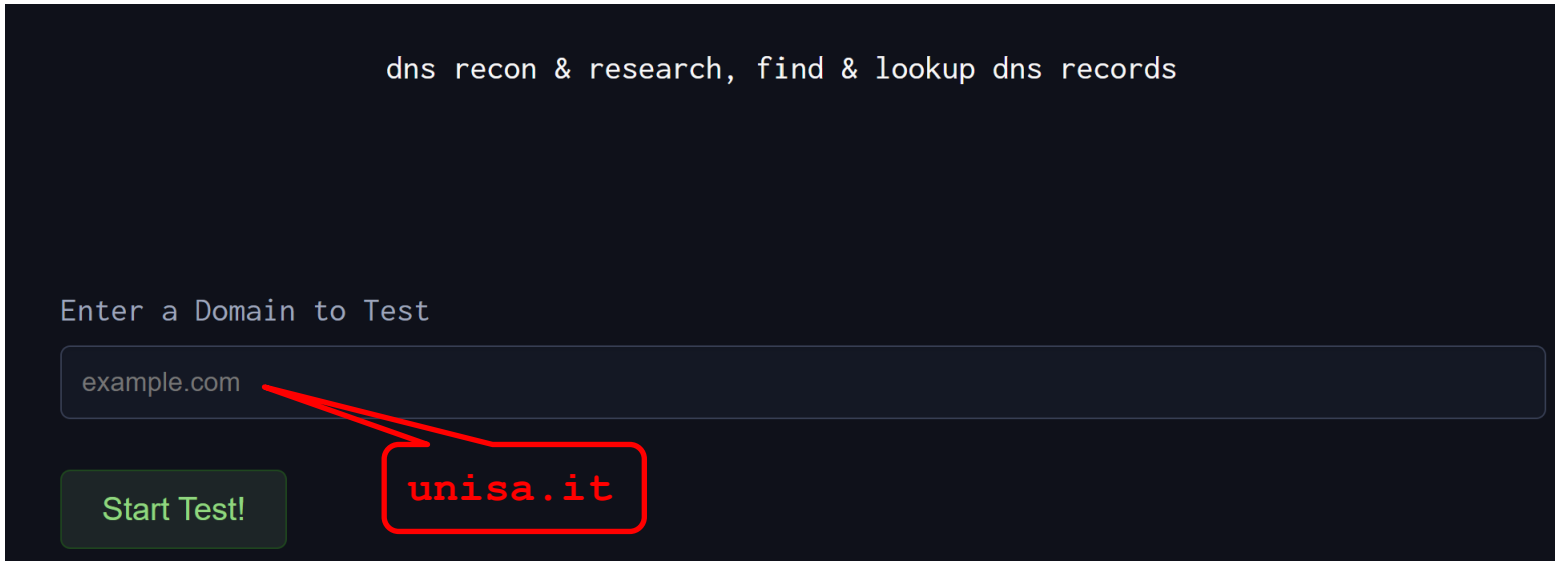
- Lo strumento richiede soltanto l'inserimento di un dominio



Utilizzo di Risorse Web-Based

Asset Discovery – DNSdumpster

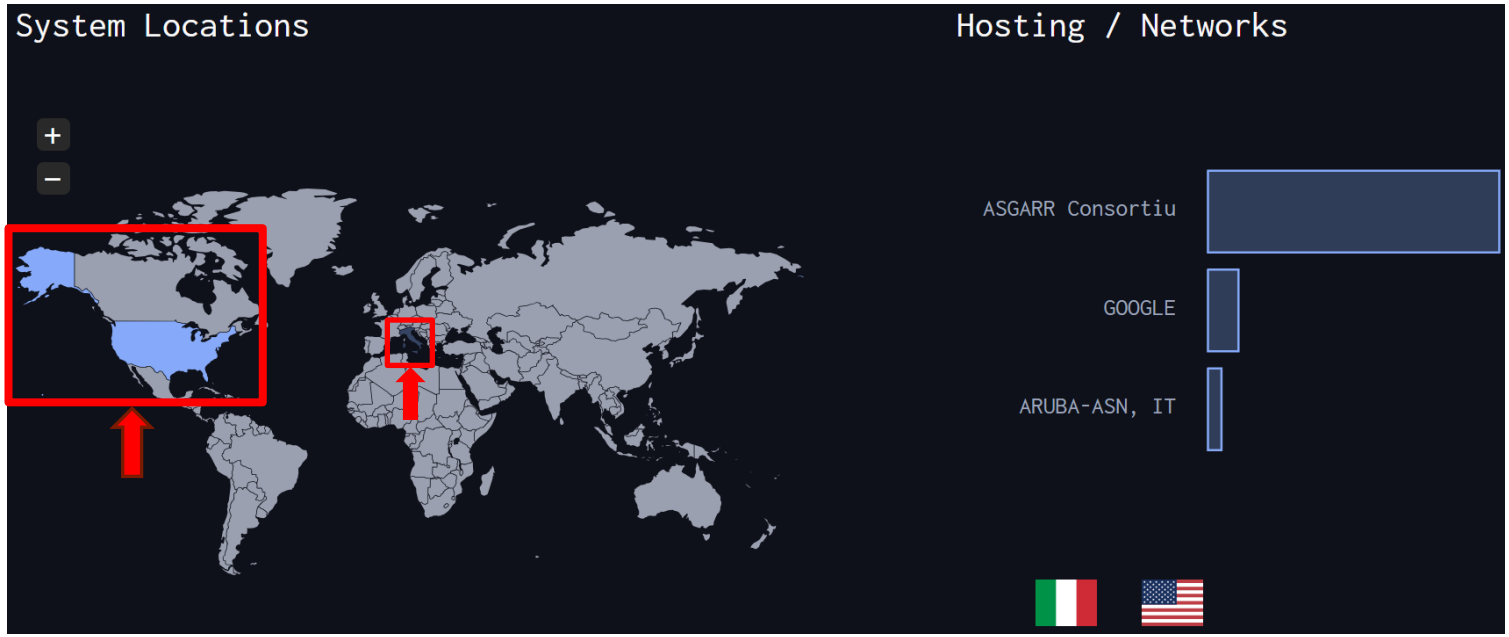
- Lo strumento richiede soltanto l'inserimento di un dominio



Utilizzo di Risorse Web-Based

Asset Discovery – DNSdumpster

- Lo strumento mostra innanzitutto informazioni di tipo geografico



Utilizzo di Risorse Web-Based

Asset Discovery – DNSdumpster

- Successivamente, lo strumento mostra informazioni relative ai sottodomini rilevati

A Records (subdomains from dataset)

Host	IP	ASN	ASN Name
unisamx.1.unisa.it	193.205.160.9 esa-mx-1.unisa.it	ASN:137 193.204.0.0/15	ASGARR Consortium GARR, IT Italy
unisamx.2.unisa.it	193.205.160.11 esa-mx-2.unisa.it	ASN:137 193.204.0.0/15	ASGARR Consortium GARR, IT Italy
6000r.unisa.it	193.205.160.190 6000r.unisa.it	ASN:137 193.204.0.0/15	ASGARR Consortium GARR, IT Italy
adisu-sistemi.unisa.it	193.205.185.17 adisu-sistemi.unisa.it	ASN:137 193.204.0.0/15	ASGARR Consortium GARR, IT Italy

Utilizzo di Risorse Web-Based

Asset Discovery – DNSdumpster

- Per ciascun sottodominio rilevato, lo strumento consente di effettuare varie operazioni

A Records (subdomains from dataset)

Host	IP	ASN	ASN Name
unisamx.1.unisa.it	193.205.160.9 esa-mx-1.unisa.it	ASN:137 193.204.0.0/15	ASGARR Consortium GARR, IT Italy
unisamx.2.unisa.it	193.205.160.11 esa-mx-2.unisa.it	ASN:137 193.204.0.0/15	ASGARR Consortium GARR, IT Italy
6000r.unisa.it	193.205.160.190 6000r.unisa.it	ASN:137 193.204.0.0/15	ASGARR Consortium GARR, IT Italy
adisu-sistemi.unisa.it	193.205.185.17 adisu-sistemi.unisa.it	ASN:137 193.204.0.0/15	ASGARR Consortium GARR, IT Italy

Utilizzo di Risorse Web-Based

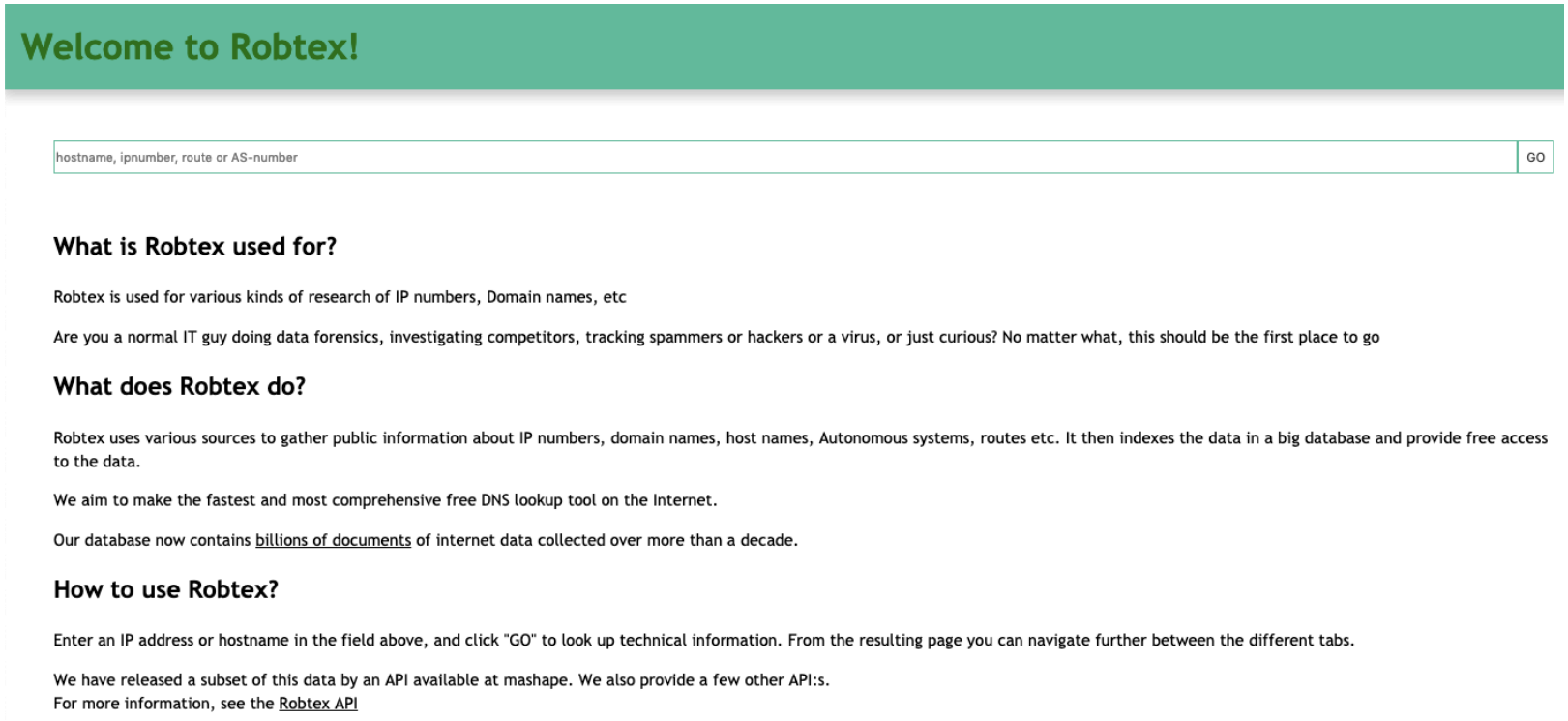
Asset Discovery – DNSdumpster

- Per ciascun sottodominio rilevato, lo strumento consente di effettuare varie operazioni, tra le quali
  - DNS Lookup
  - ASN Lookup
  - Subnet Lookup
  - Reverse IP

Utilizzo di Risorse Web-Based

Asset Discovery – Robtex

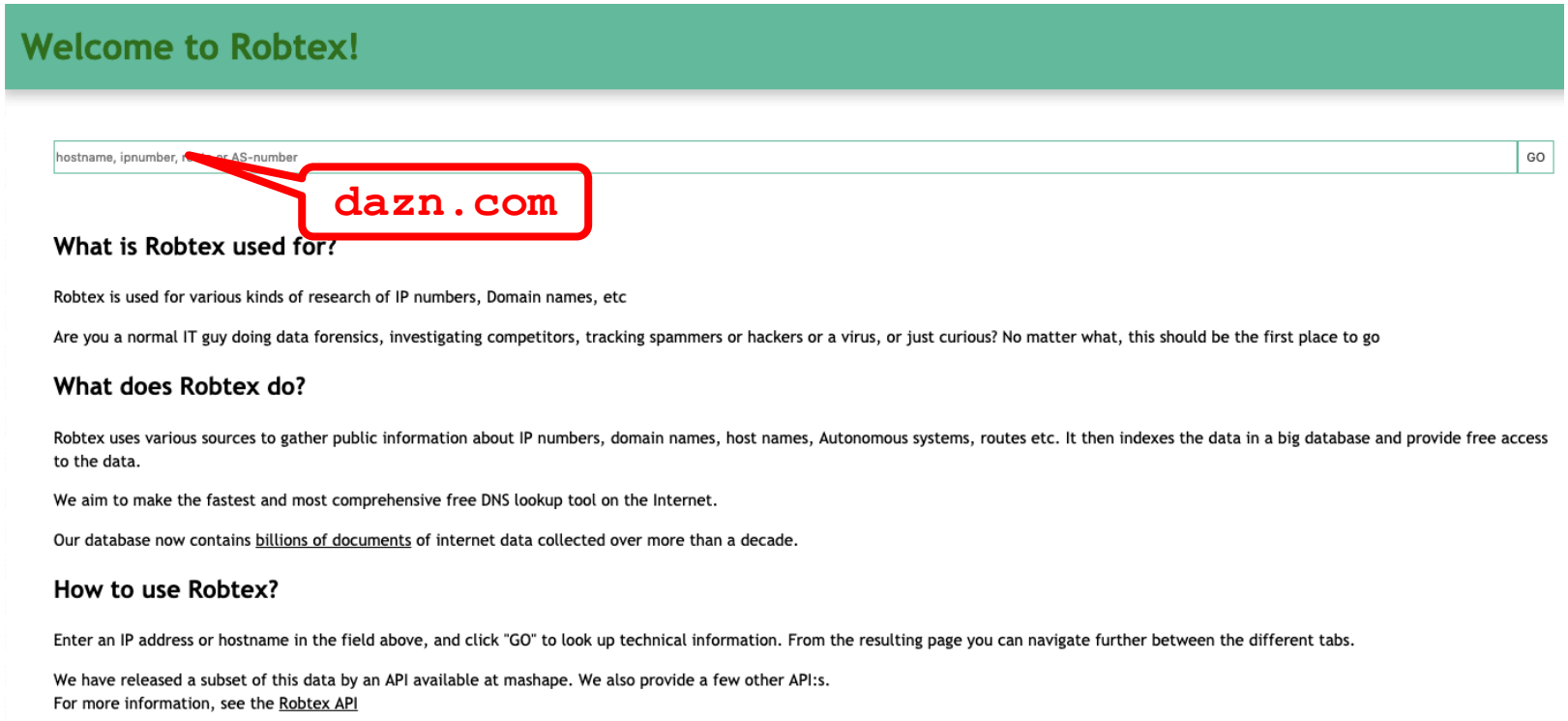
- https://www.robtex.com/
  - Permette di cercare informazioni riguardo domini e servizi di rete

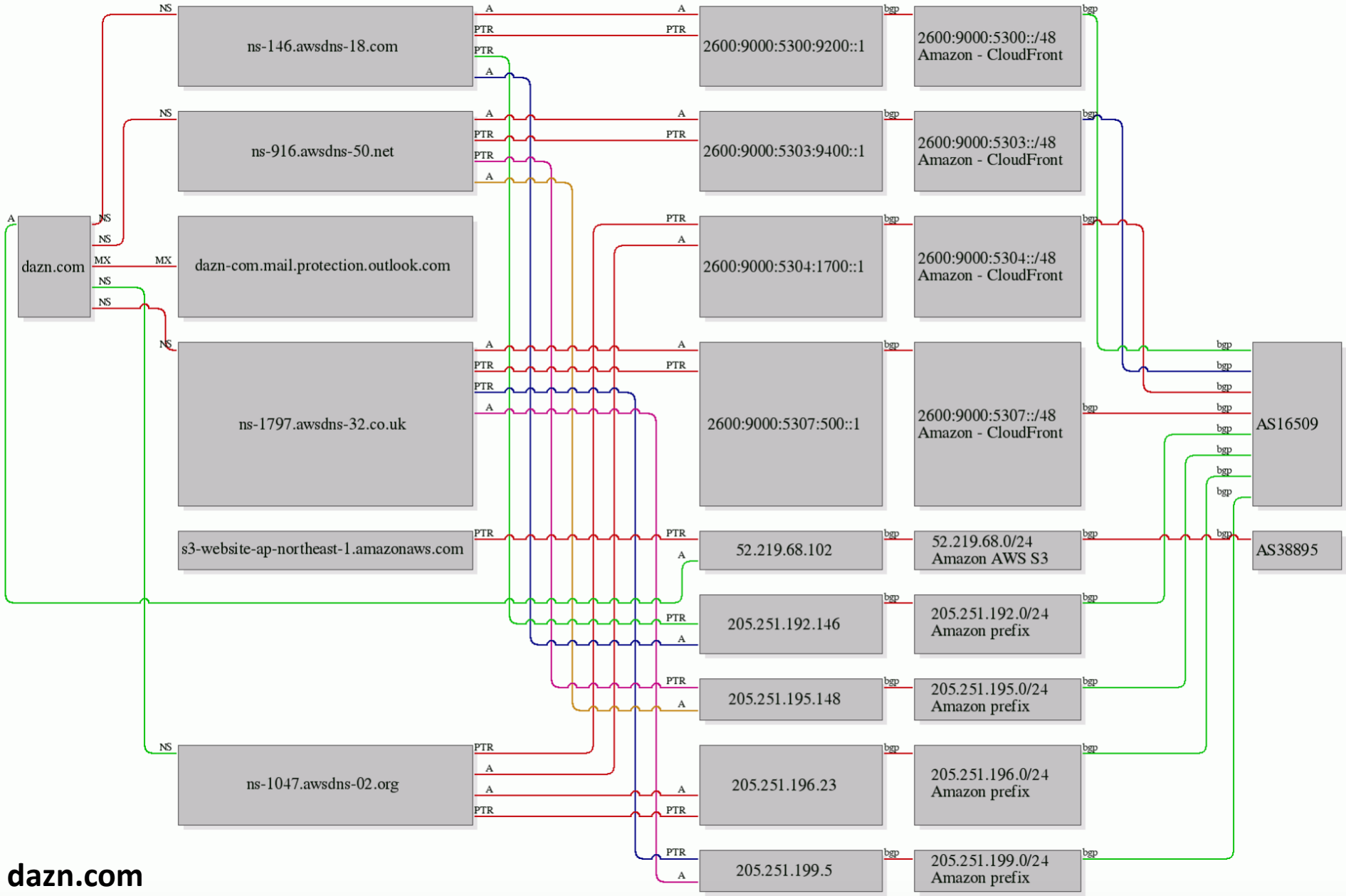


Utilizzo di Risorse Web-Based

Asset Discovery – Robtex

- https://www.robtex.com/
  - Permette di cercare informazioni riguardo domini e servizi di rete




dazn.com
ns-146.awsdns-18.com
ns-916.awsdns-50.net
dazn-com.mail.protection.outlook.com
ns-1797.awsdns-32.co.uk
s3-website-ap-northeast-1.amazonaws.com
ns-1047.awsdns-02.org
2600:9000:5300:9200::1
2600:9000:5303:9400::1
2600:9000:5304:1700::1
2600:9000:5307:500::1
52.219.68.102
205.251.192.146
205.251.195.148
205.251.196.23
205.251.199.5
2600:9000:5300::/48
Amazon - CloudFront
2600:9000:5303::/48
Amazon - CloudFront
2600:9000:5304::/48
Amazon - CloudFront
2600:9000:5307::/48
Amazon - CloudFront
52.219.68.0/24
Amazon AWS S3
205.251.192.0/24
Amazon prefix
205.251.195.0/24
Amazon prefix
205.251.196.0/24
Amazon prefix
205.251.199.0/24
Amazon prefix
AS16509
AS38895

dazn.com

Utilizzo di Risorse Web-Based

Web Archiving

- Raccolta di «parti» del World Wide Web (WWW) per garantire che le informazioni siano conservate in un archivio per scopi/usi futuri

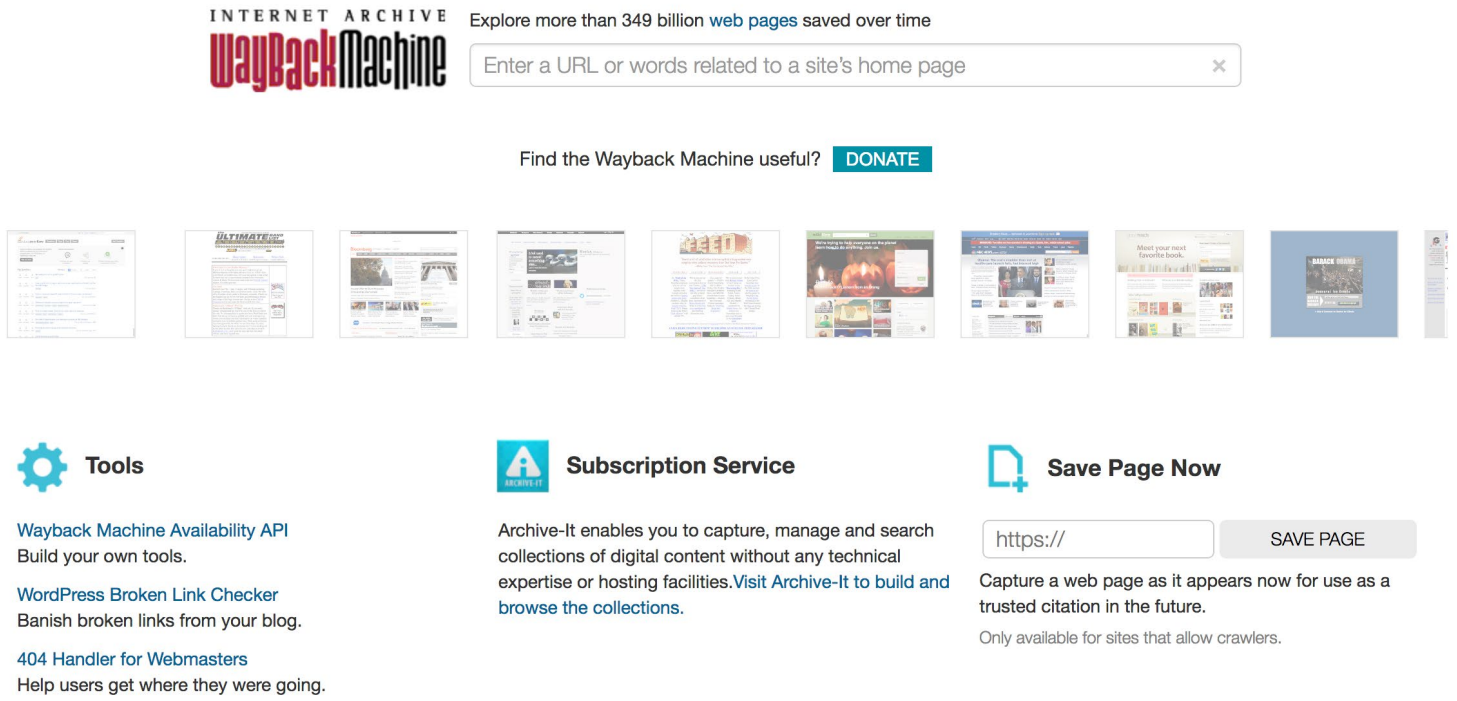
- Utilizzo di *Web Crawler* per raccogliere enormi quantità di informazioni
  - Heritrix
  - HTTrack
  - Etc

- Estremamente **utile per capire la periodicità di aggiornamento di un determinato sito Web**

Utilizzo di Risorse Web-Based

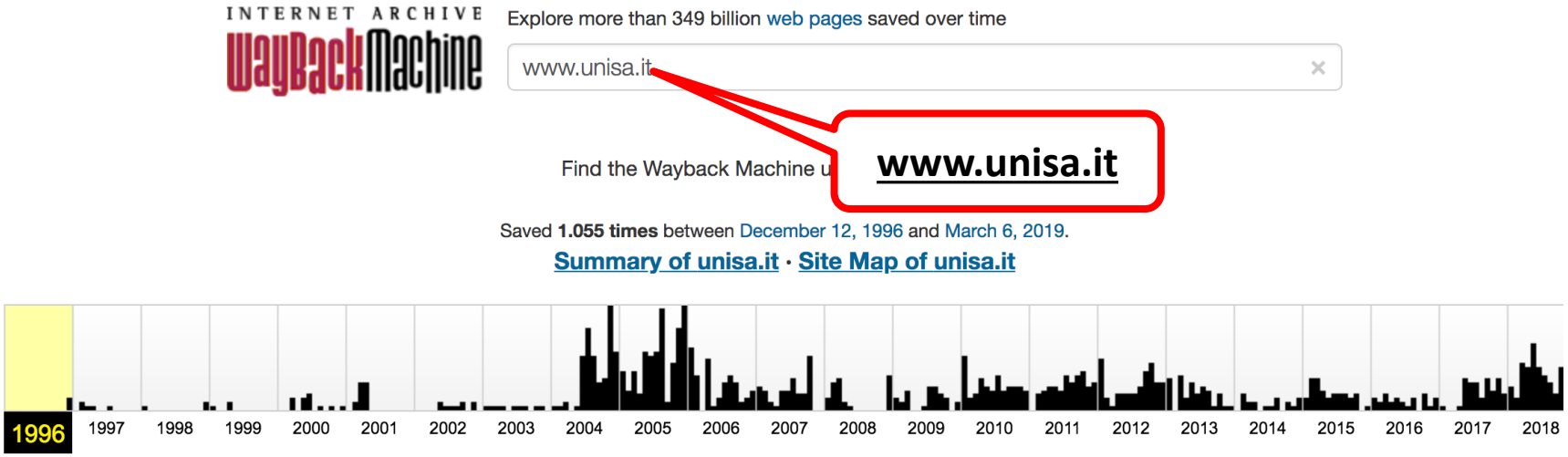
Web Archiving – Wayback Machine

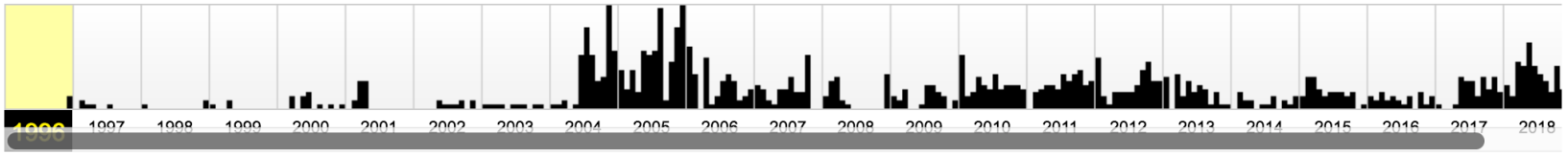
- http://web.archive.org
  - Contiene un archivio delle pagine Web presenti sulla rete Internet



Utilizzo di Risorse Web-Based

Web Archiving – Wayback Machine – Esempio 1





JAN

	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

FEB

				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29		

MAR

					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

APR

	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

MAY

			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

JUN

						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22

JUL

	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27

AUG

				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
28	29	30	31			

SEP

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

OCT

6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

NOV

3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

DEC

			4	5	6	7
8	9	10	11	**12**	13	14
15	16	17	18	19	20	21
22	23	24	25	26	**27**	28
29	30	31				

Il primo snapshot di www.unisa.it risale al 12 dicembre 1996

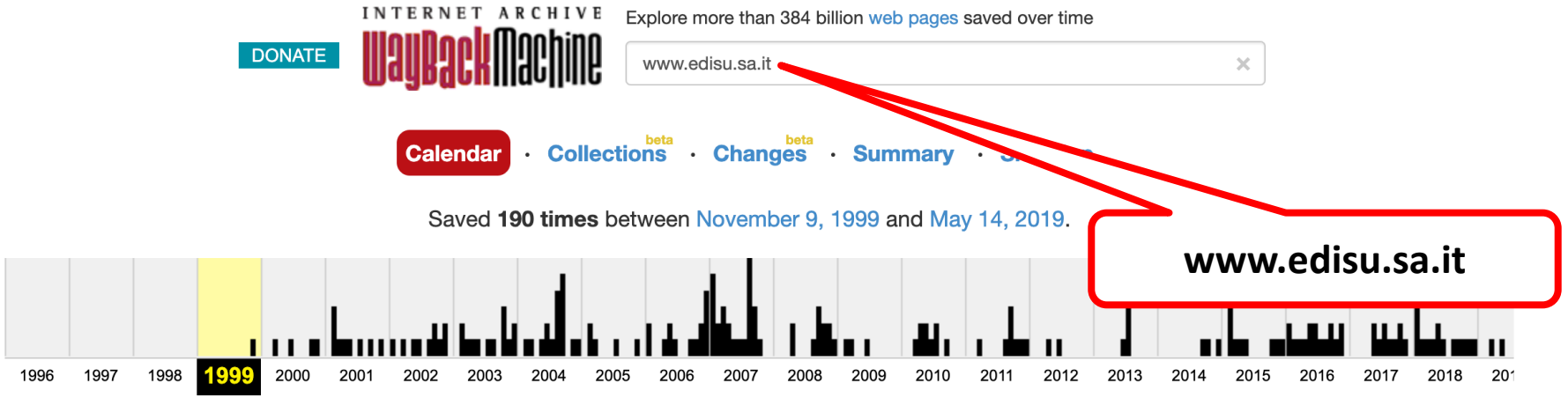
Utilizzo di Risorse Web-Based

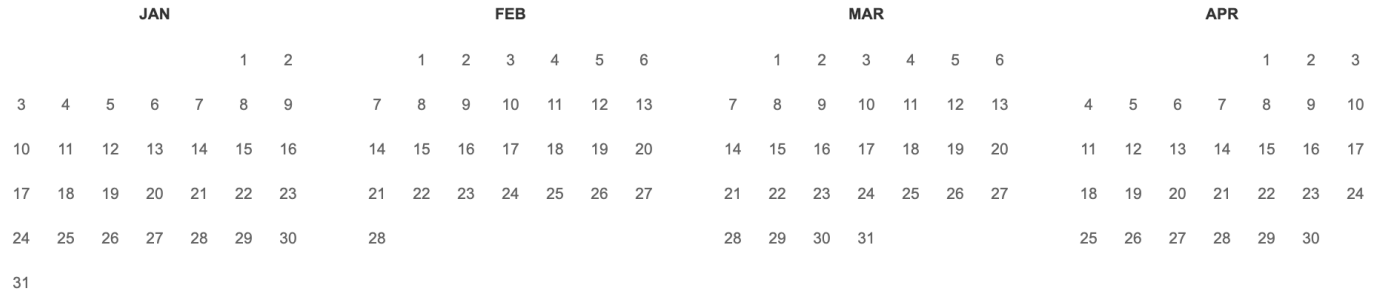
Web Archiving – Wayback Machine – Esempio 1

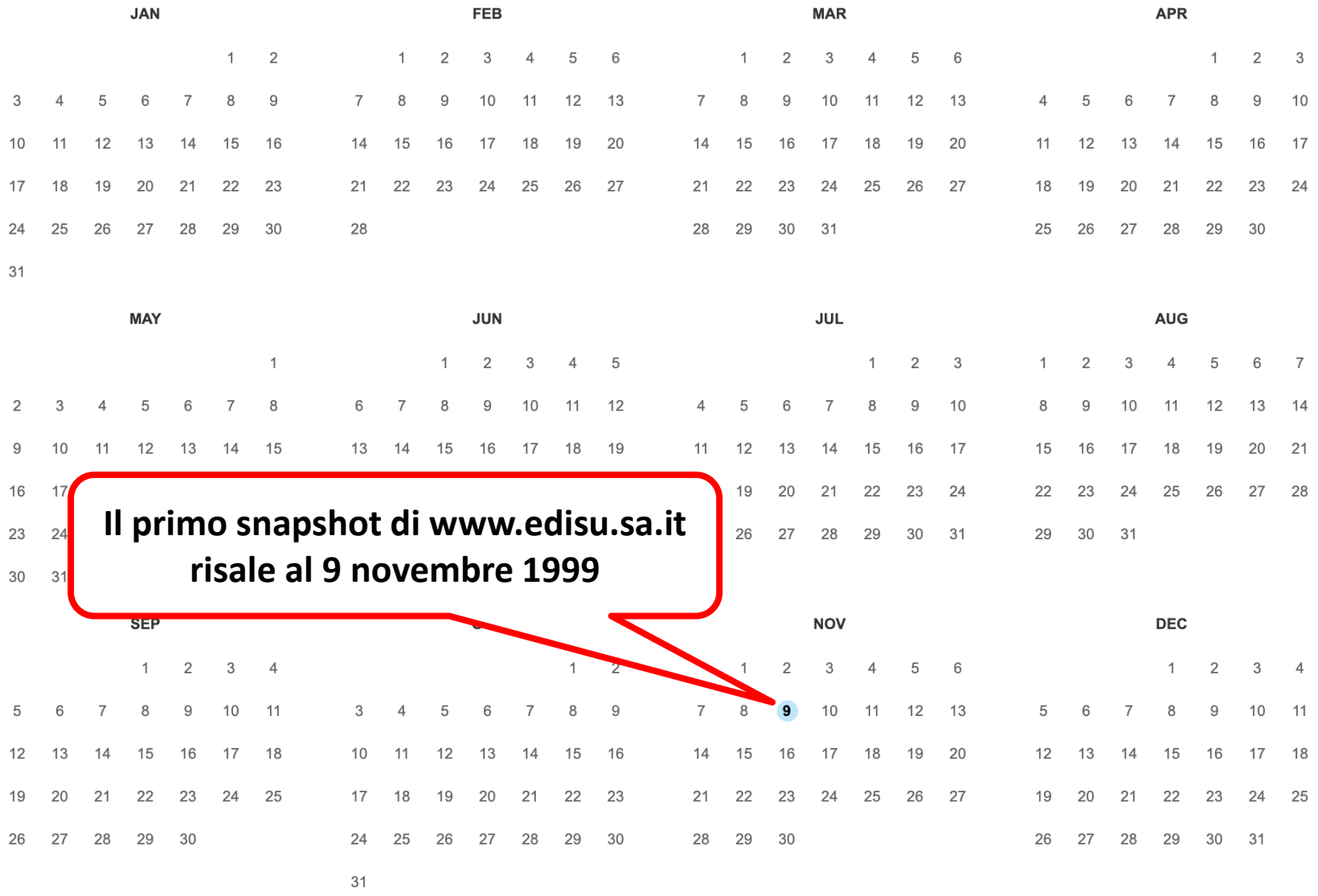
Primo sito Web dell'Università degli Studi di Salerno

Utilizzo di Risorse Web-Based

Web Archiving – Wayback Machine – Esempio 2






JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
NOV
DEC
Il primo snapshot di www.edisu.sa.it risale al 9 novembre 1999

Utilizzo di Risorse Web-Based

Web Archiving – Wayback Machine – Esempio 2

Primo sito Web dell'E.DI.S.U.

Utilizzo di Risorse Web-Based

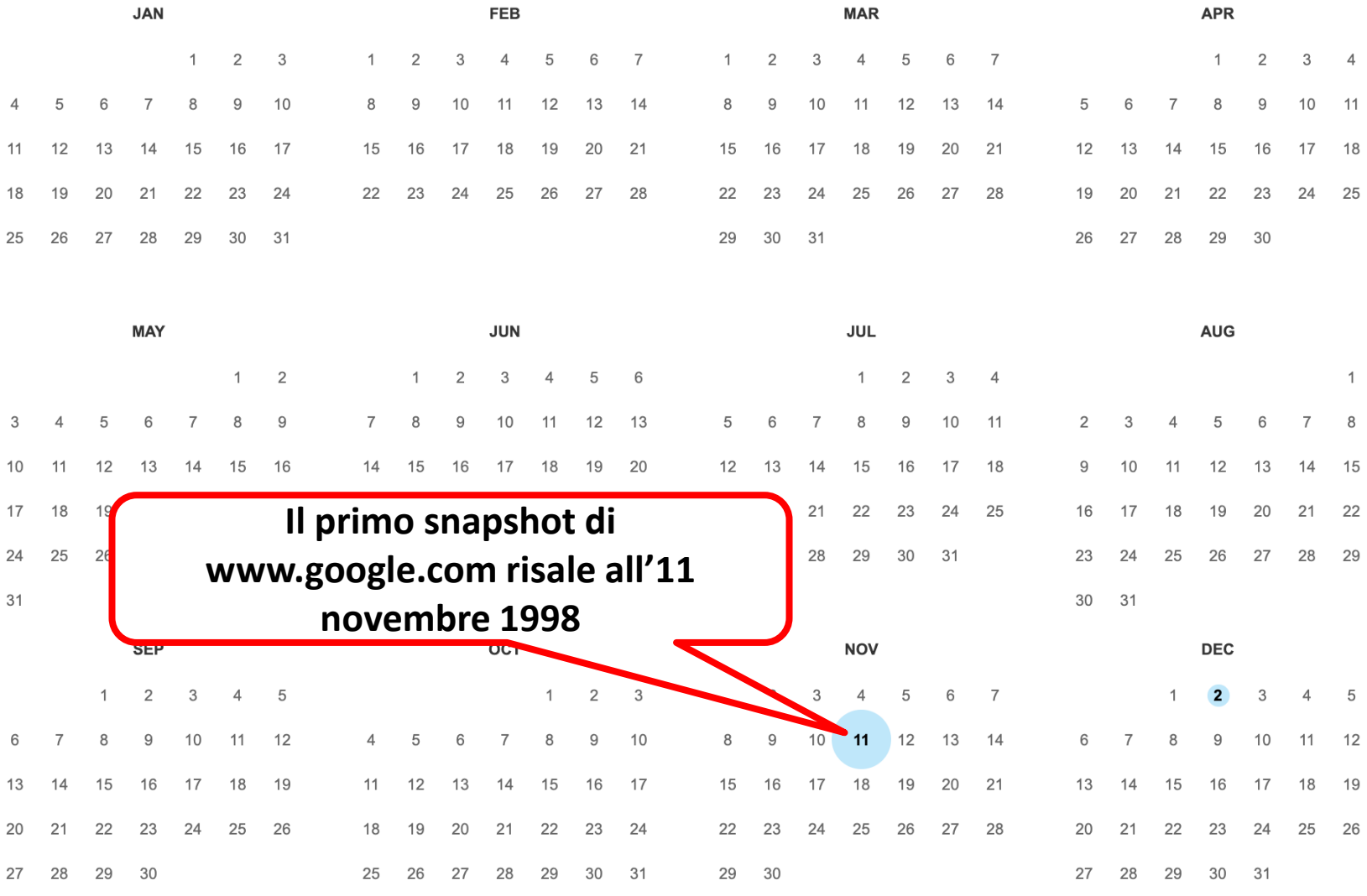
Web Archiving – Wayback Machine – Esempio 3

JAN						
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

FEB						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

MAR						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

APR						
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		


JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
Il primo snapshot di www.google.com risale all'11 novembre 1998

Utilizzo di Risorse Web-Based

Web Archiving – Wayback Machine – Esempio 3

Primo sito Web di Google

Utilizzo di Risorse Web-Based

Web Archiving – Wayback Machine – Esempio 3

Search the web using Google!

10 results | Google Search | I'm feeling lucky

Index contains ~25 million pages (soon to be much bigger)

About Google!

Stanford Search Linux Search

Get Google! updates monthly!

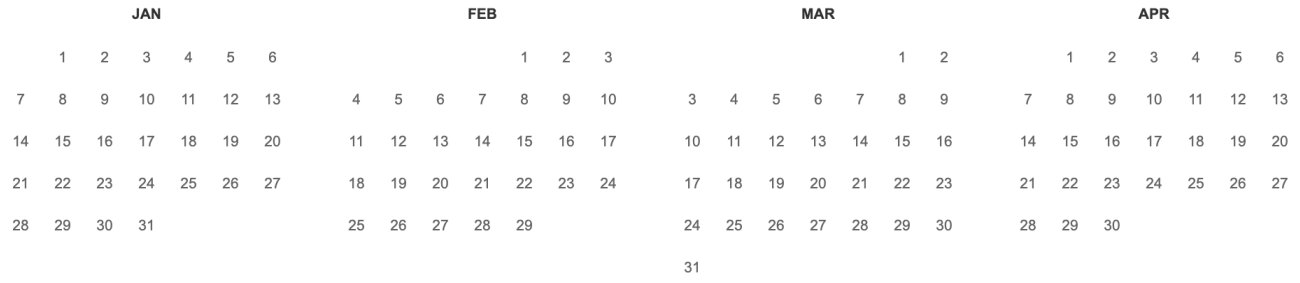
your e-mail | Subscribe | Archive

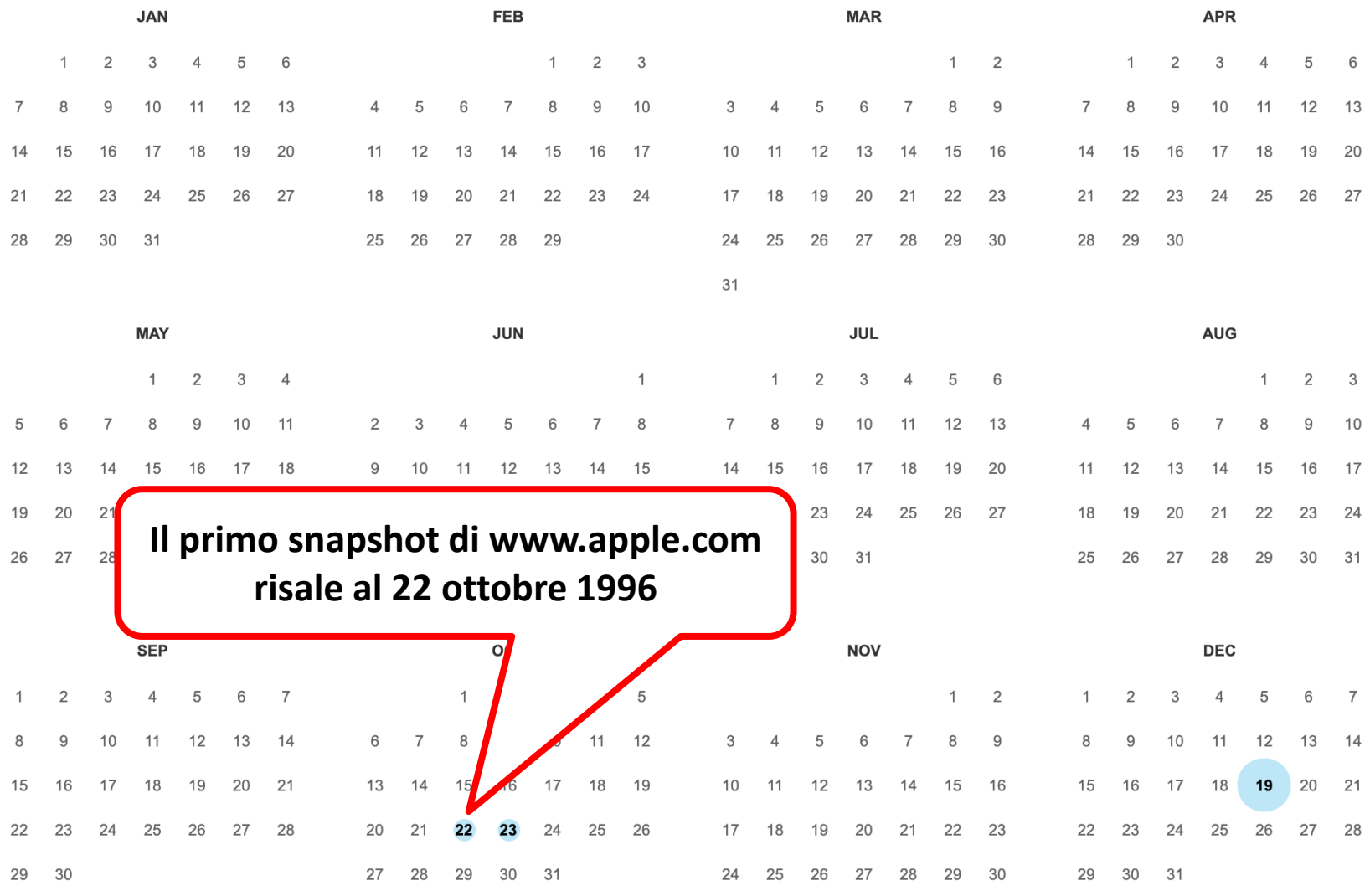
Copyright ©1997-8 Stanford University

Primo sito Web di Google

Utilizzo di Risorse Web-Based

Web Archiving – Wayback Machine – Esempio 4




JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
Il primo snapshot di www.apple.com risale al 22 ottobre 1996

Utilizzo di Risorse Web-Based

Web Archiving – Wayback Machine – Esempio 4

Primo sito Web di Apple

Utilizzo di Risorse Web-Based

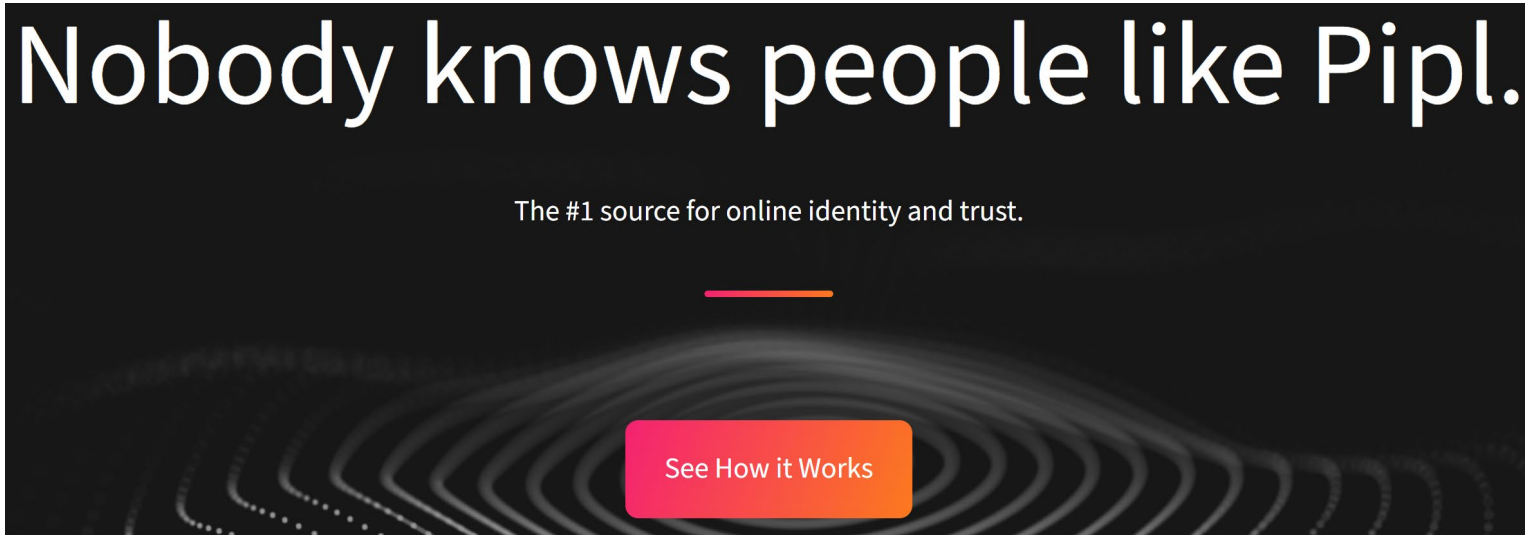
Ricerca Informazioni Personali – Social Network

Social Network	Type	Scope	Main potential for OSINT
4chan	Online community	Worldwide	Users interested in illicit activities
Badoo	Dating	Worldwide	Intimate and personal details
Cloob	Social connections	Iran	Personal profile, posting and community membership
Draugiem	Social connections	Latvia	Personal profile, publications in blogs, group membership
Facebook	Social connections	Worldwide	Personal profile, preferences and places visited
Facenama	Social connections	Iran	Personal profile, publications, photos and videos
Flickr	Photo-sharing	Worldwide	Activities, hobbies, places and personal relationships
Instagram	Social connections	Worldwide	Habits, locations and personal relationships
LinkedIn	Business	Worldwide	Professional profile, education, skills and languages
Mixi	Social connections	Japan	Personal profile, interests and opinions
Odnoklassniki	Social connections	Mainly Russia	Personal profile of adults, past and present friendships
Qzone	Social connections	Mainly China	Personal profile, preferences, habits
Reddit	Online community	Worldwide	Users trends, behaviors, and publications
Renren	Social connections	Mainly China	Personal profile of students, friendships and discussions
Taringa!	Social connections	Mainly Latin America	Personal profile, publications and community membership
Tinder	Dating	Worldwide	Intimate and personal details
Tumblr	Photo-sharing	Worldwide	Activities, hobbies, places and personal relationships
Twitter	Social connections	Worldwide	Personal profile, opinions and publications
VKontakte (VK)	Social connections	Mainly Russia	Personal profile, preferences and publications
Weibo	Social connections	Mainly China	Personal profile, opinions and publications

Utilizzo di Risorse Web-Based

Ricerca Informazioni Personali – Pipl

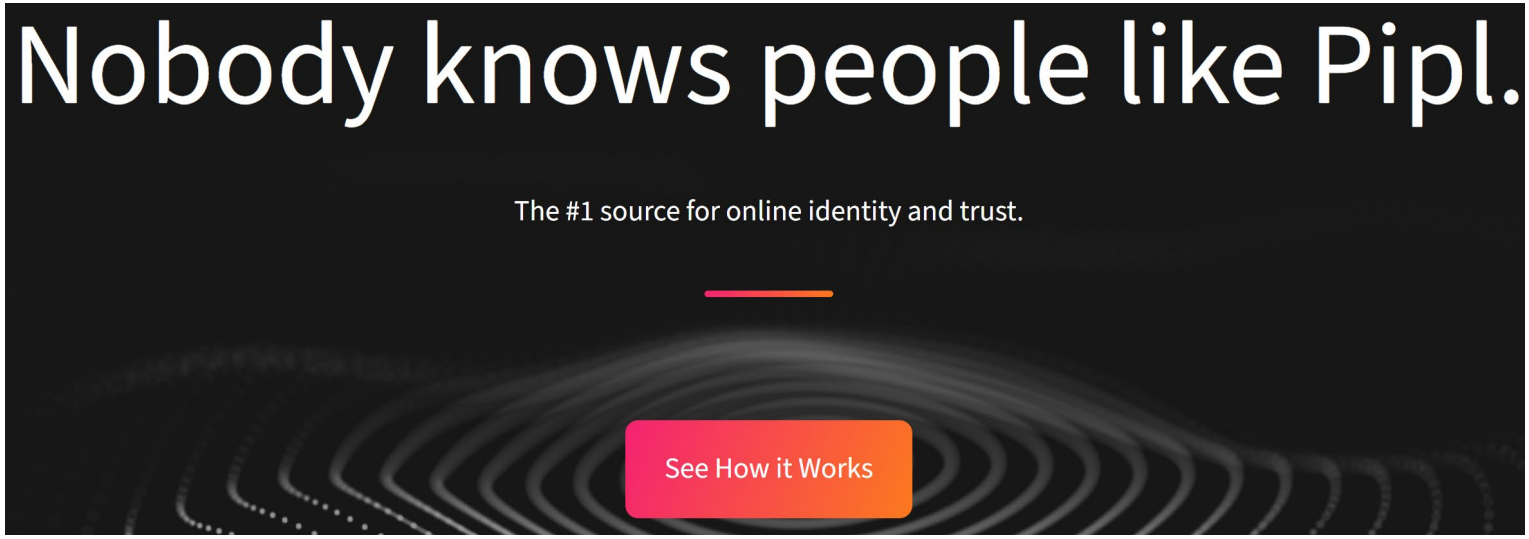
- http://www.pipl.com
  - Permette di cercare informazioni su persone in base al loro nome e cognome, città, stato, paese, numero telefonico, etc



Utilizzo di Risorse Web-Based

Ricerca Informazioni Personali – Pipl

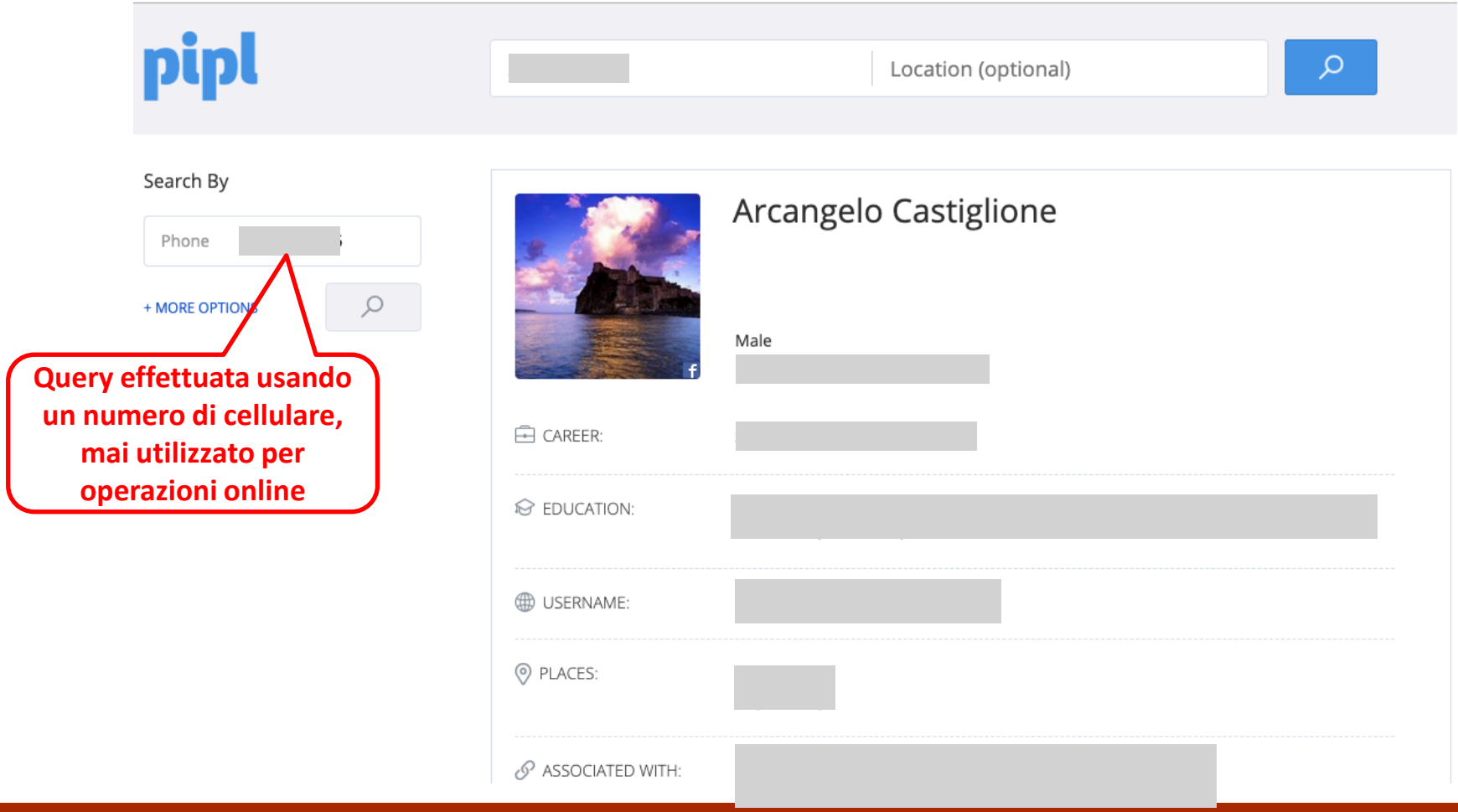
- http://www.pipl.com
  - Permette di cercare informazioni su persone in base al loro nome e cognome, città, stato, paese, numero telefonico, etc



Tale servizio, in origine utilizzabile gratuitamente, è stato poi reso a pagamento

Utilizzo di Risorse Web-Based

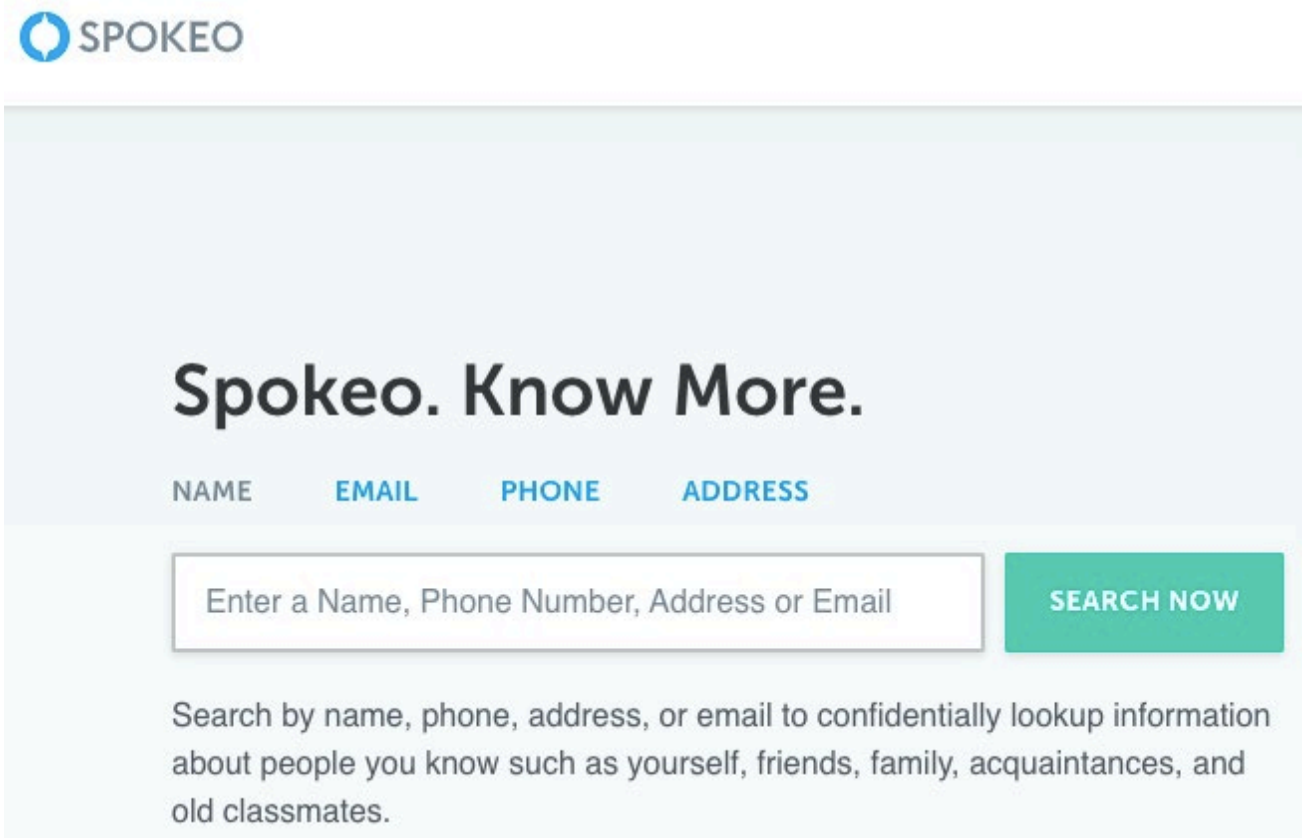
Ricerca Informazioni Personali – Pipl – Esempio



Utilizzo di Risorse Web-Based

Ricerca Informazioni Personali – SPOKEO

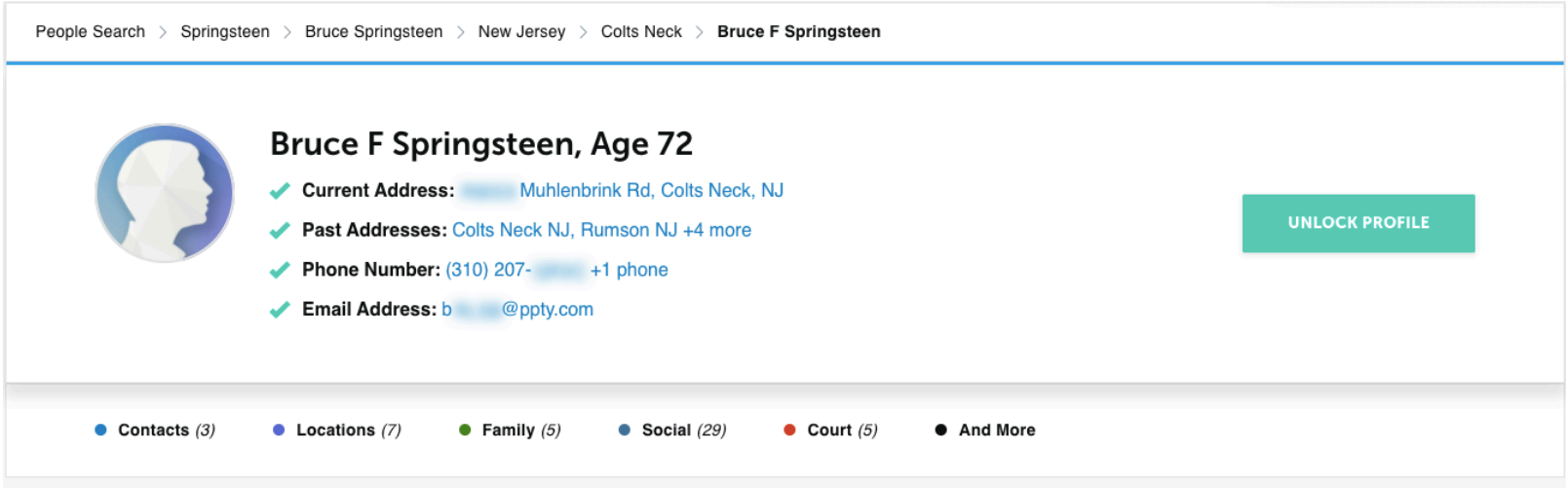
- https://www.spokeo.com/



Utilizzo di Risorse Web-Based

Ricerca Informazioni Personali – SPOKEO – Esempio

- https://www.spokeo.com/



Utilizzo di Risorse Web-Based

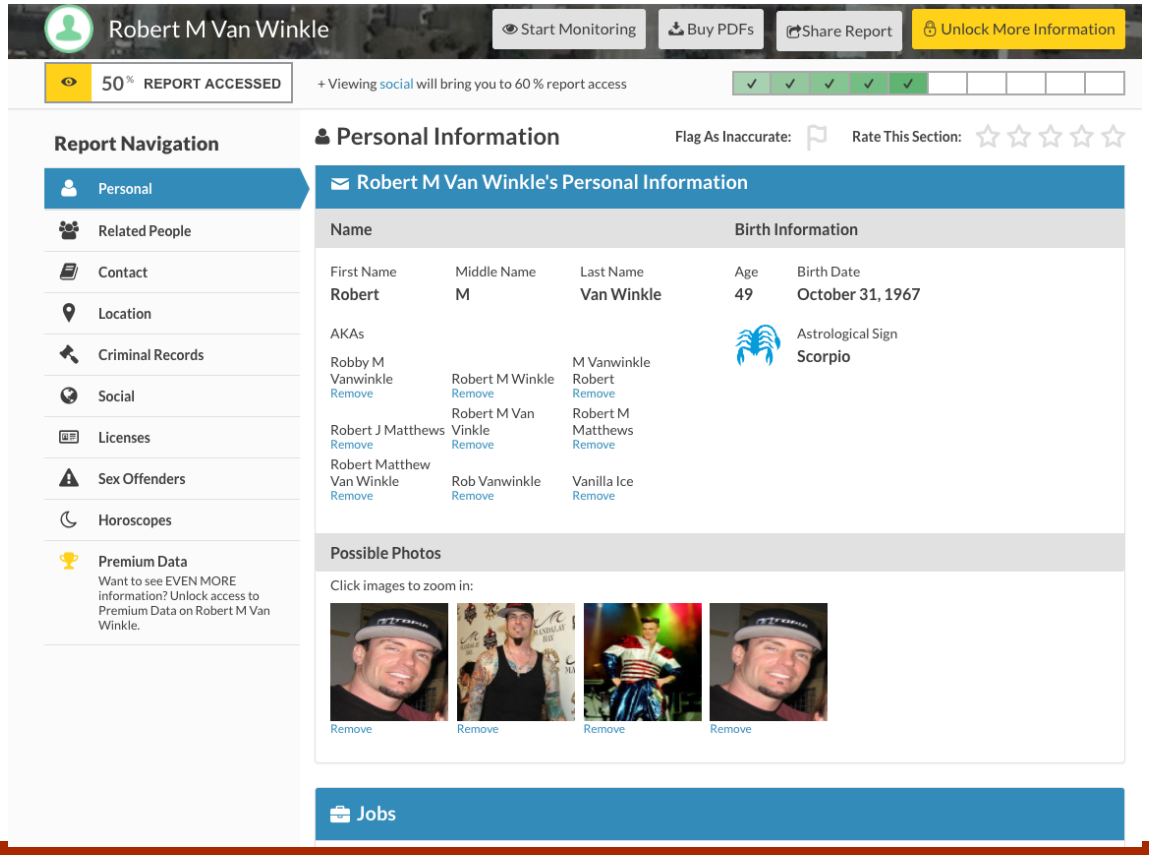
Ricerca Informazioni Personali

- https://www.instantcheckmate.com/

Utilizzo di Risorse Web-Based

Ricerca Informazioni Personali

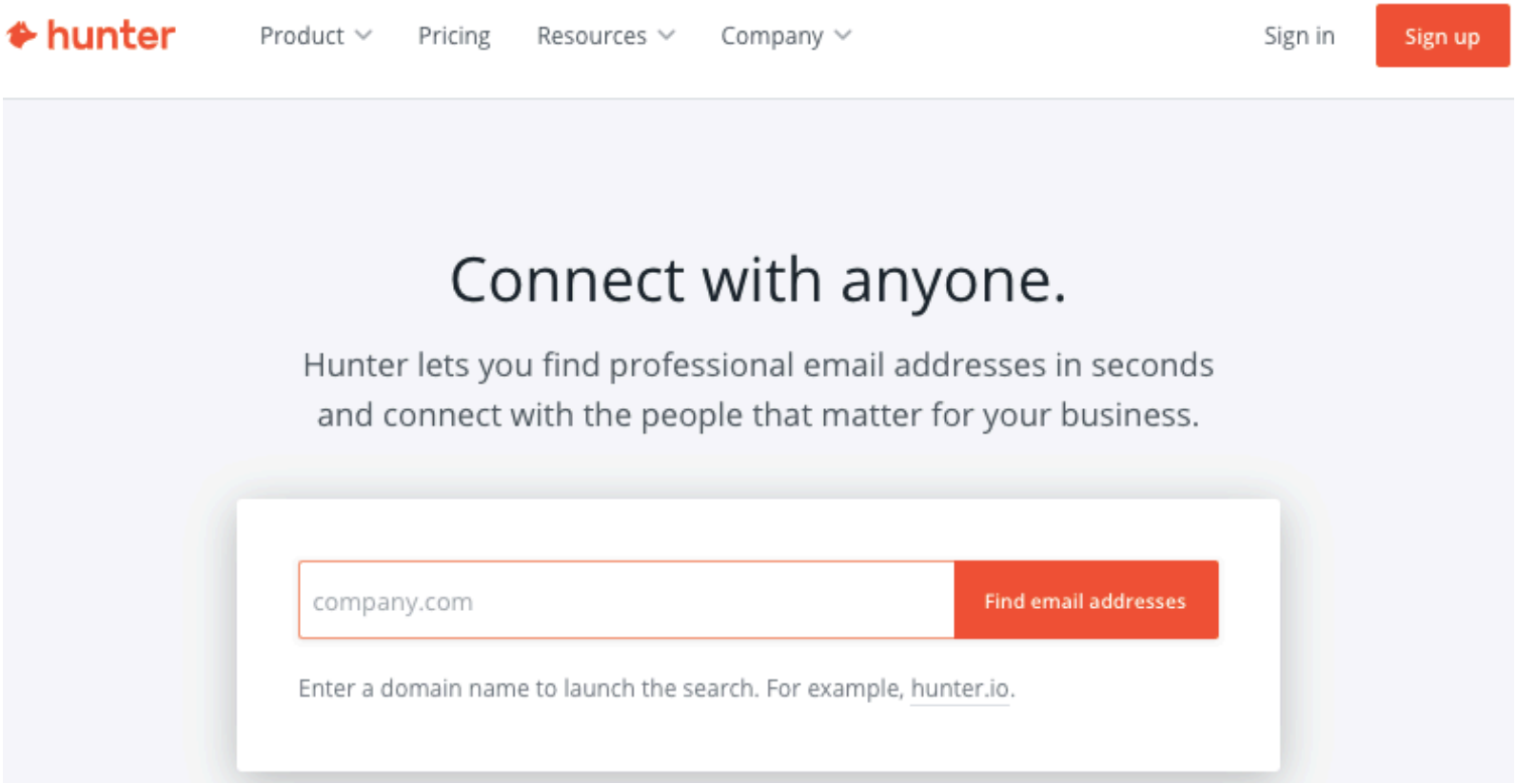
- https://www.instantcheckmate.com/



Utilizzo di Risorse Web-Based

Ricerca Indirizzi E-mail

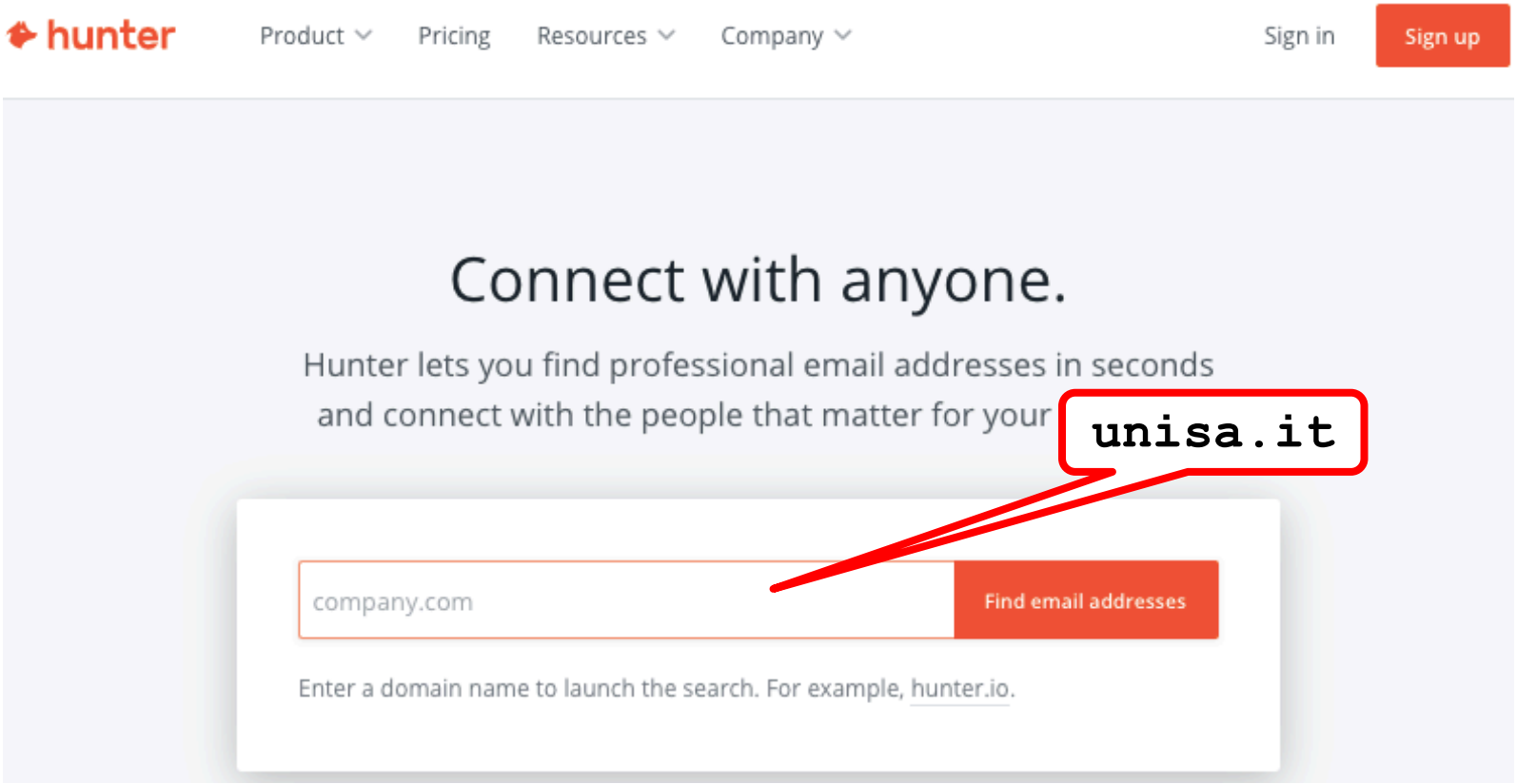
- https://hunter.io



Utilizzo di Risorse Web-Based

Ricerca Indirizzi E-mail

- https://hunter.io

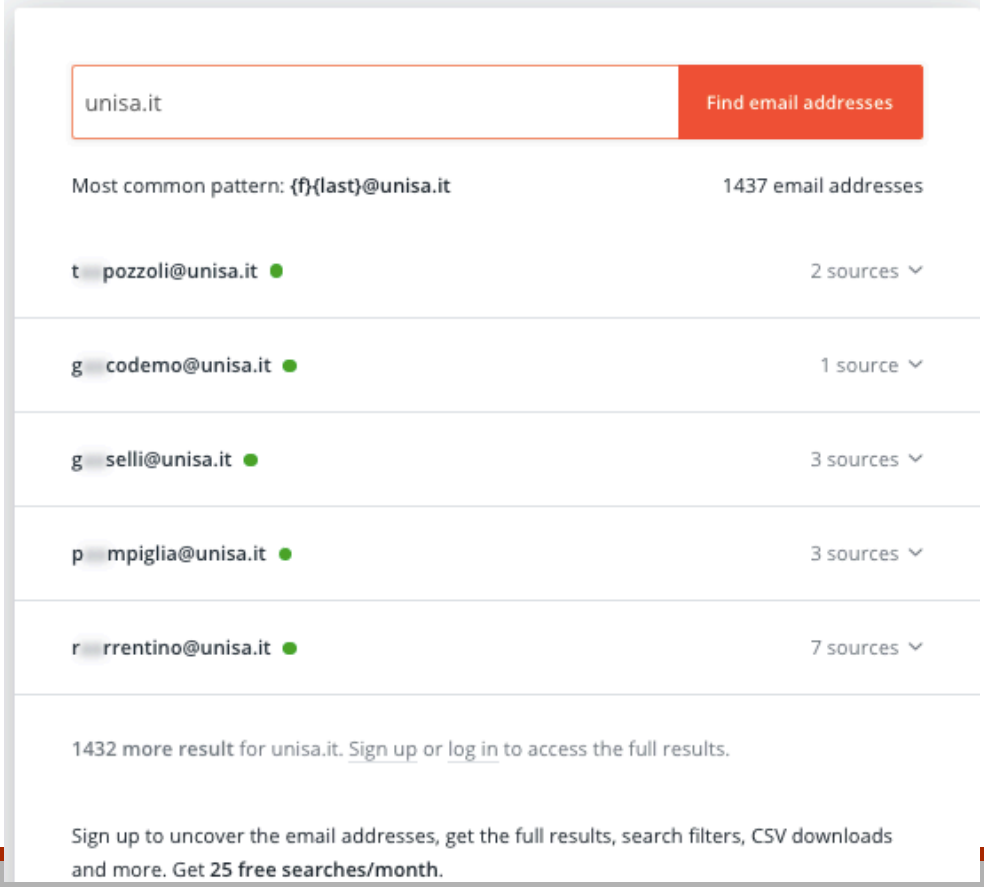


Utilizzo di Risorse Web-Based

Ricerca Indirizzi E-mail

- https://hunter.io

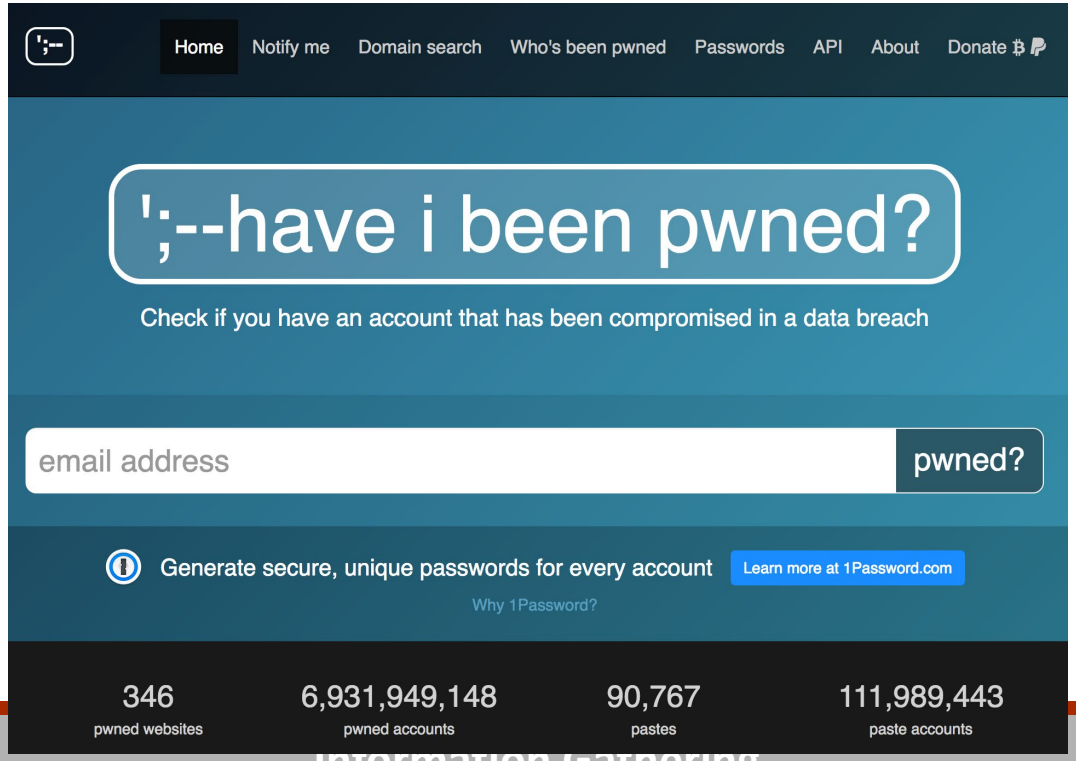
E-mail relative ad unisa.it



Utilizzo di Risorse Web-Based

Ricerca su Data Breach

- haveibeenpwned.com
  - Permette di controllare se una determinata e-mail è stata coinvolta in data breach



Utilizzo di Risorse Web-Based

Ricerca su Data Breach

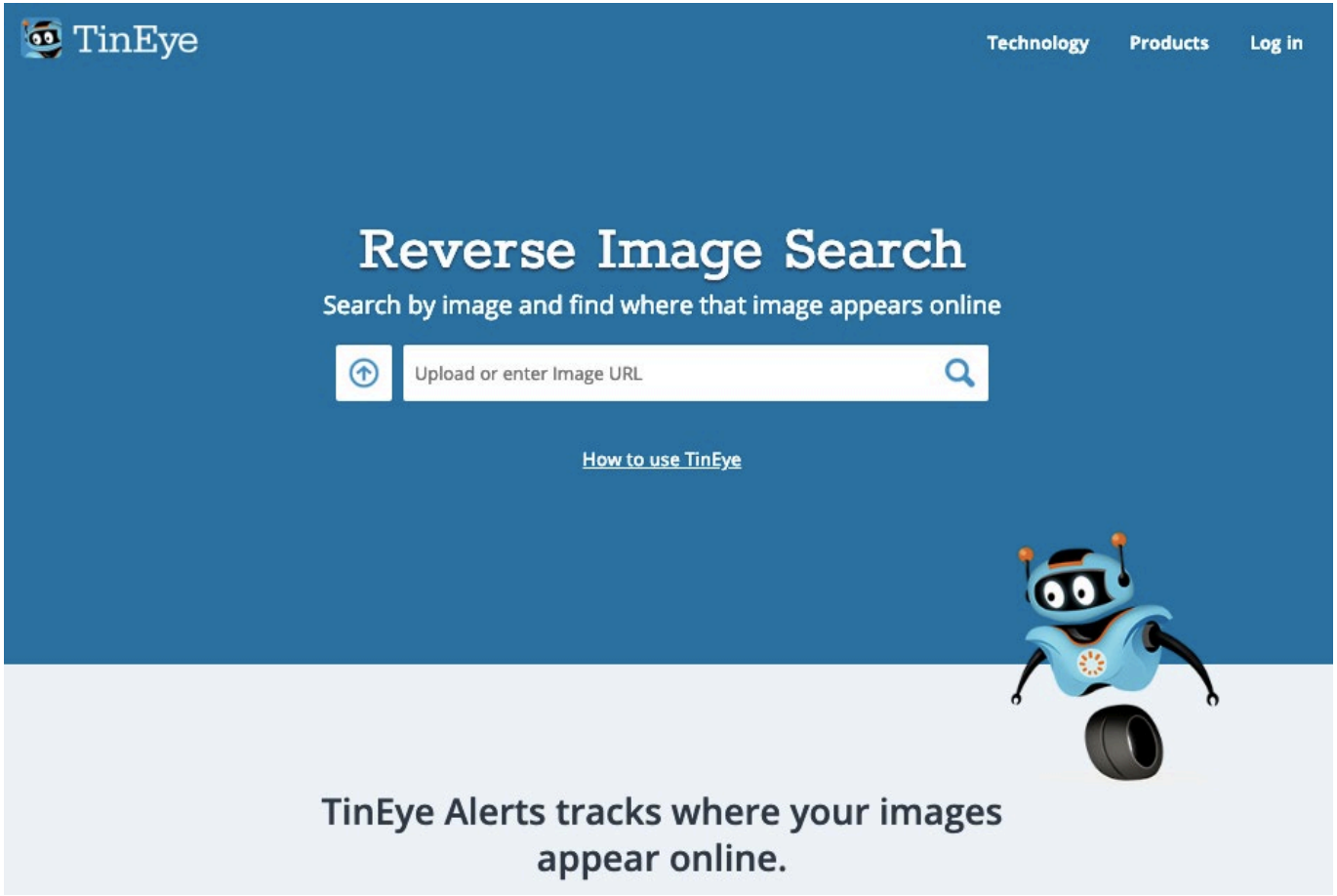
Utilizzo di Risorse Web-Based

Reverse Image Search – TinEye

- http://www.tineye.com
  - Reverse Image Search Engine
  - Permette di
    - Scoprire
      - Da dove proviene un'immagine
      - Come viene usata
      - Se esistono versioni modificate dell'immagine
    - Trovare versioni dell'immagine con risoluzione più elevata
    - Etc

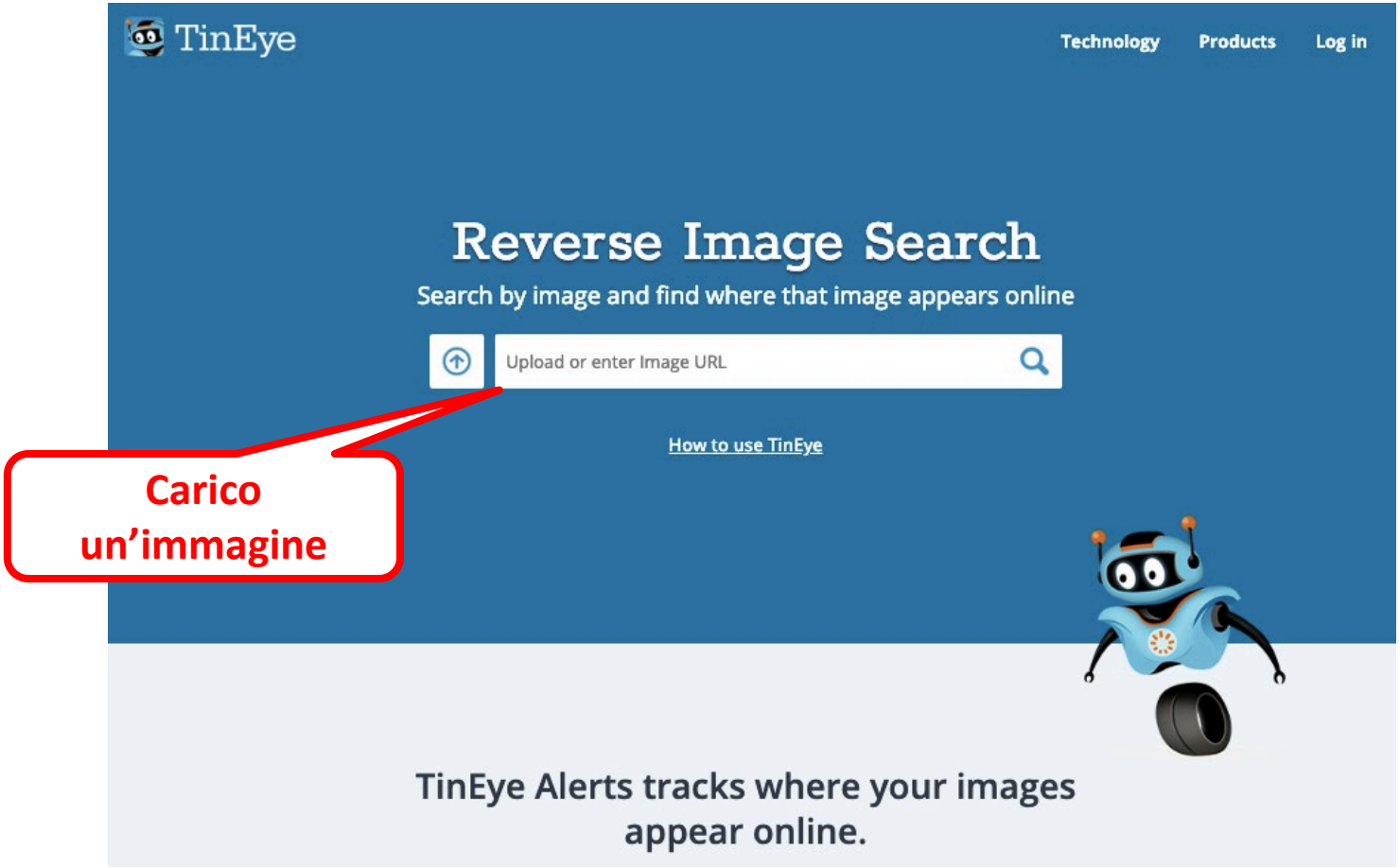
Utilizzo di Risorse Web-Based

Reverse Image Search – TinEye



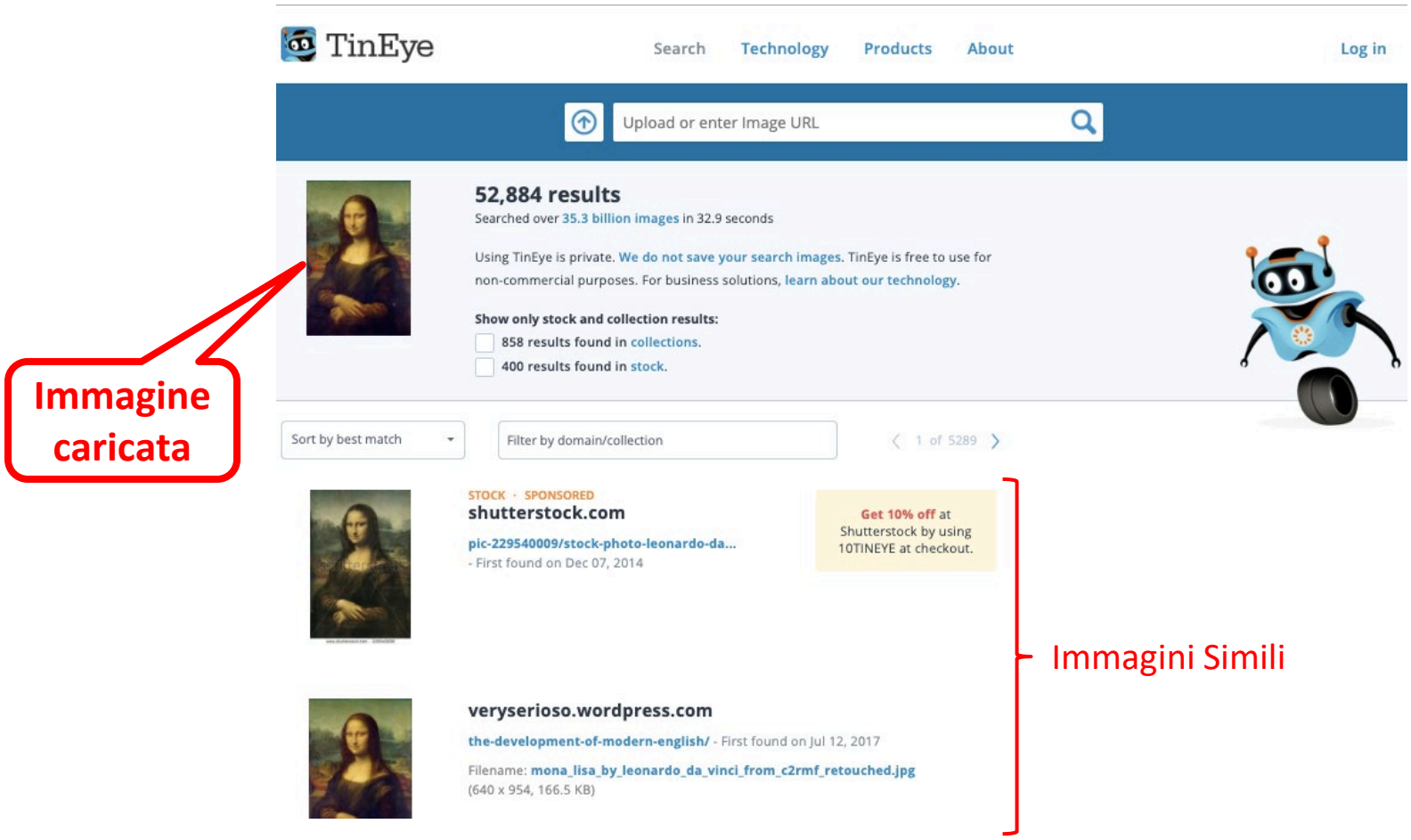
Utilizzo di Risorse Web-Based

Reverse Image Search – TinEye – Esempio 1



Utilizzo di Risorse Web-Based

Reverse Image Search – TinEye – Esempio 1



Utilizzo di Risorse Web-Based

Reverse Image Search – TinEye – Esempio 2

- TinEye fornisce un'estensione per alcuni tra i browser più comuni
  - Chrome, Firefox, Edge, etc

Firefox Chrome Opera

TinEye for Firefox

Install the TinEye extension for Firefox

How to install

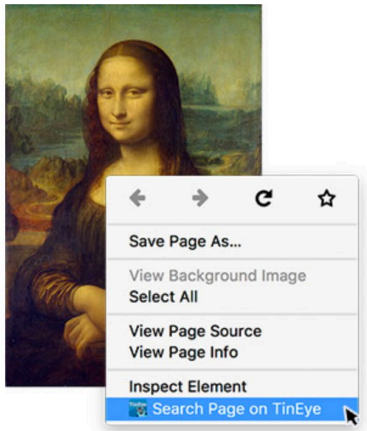
Visit the **Firefox Add-ons page** to install the free TinEye browser extension.

How to use

Right-click on any web image and select *Search Image on TinEye* from the context menu. Results are displayed for you at tineye.com.

Configuration

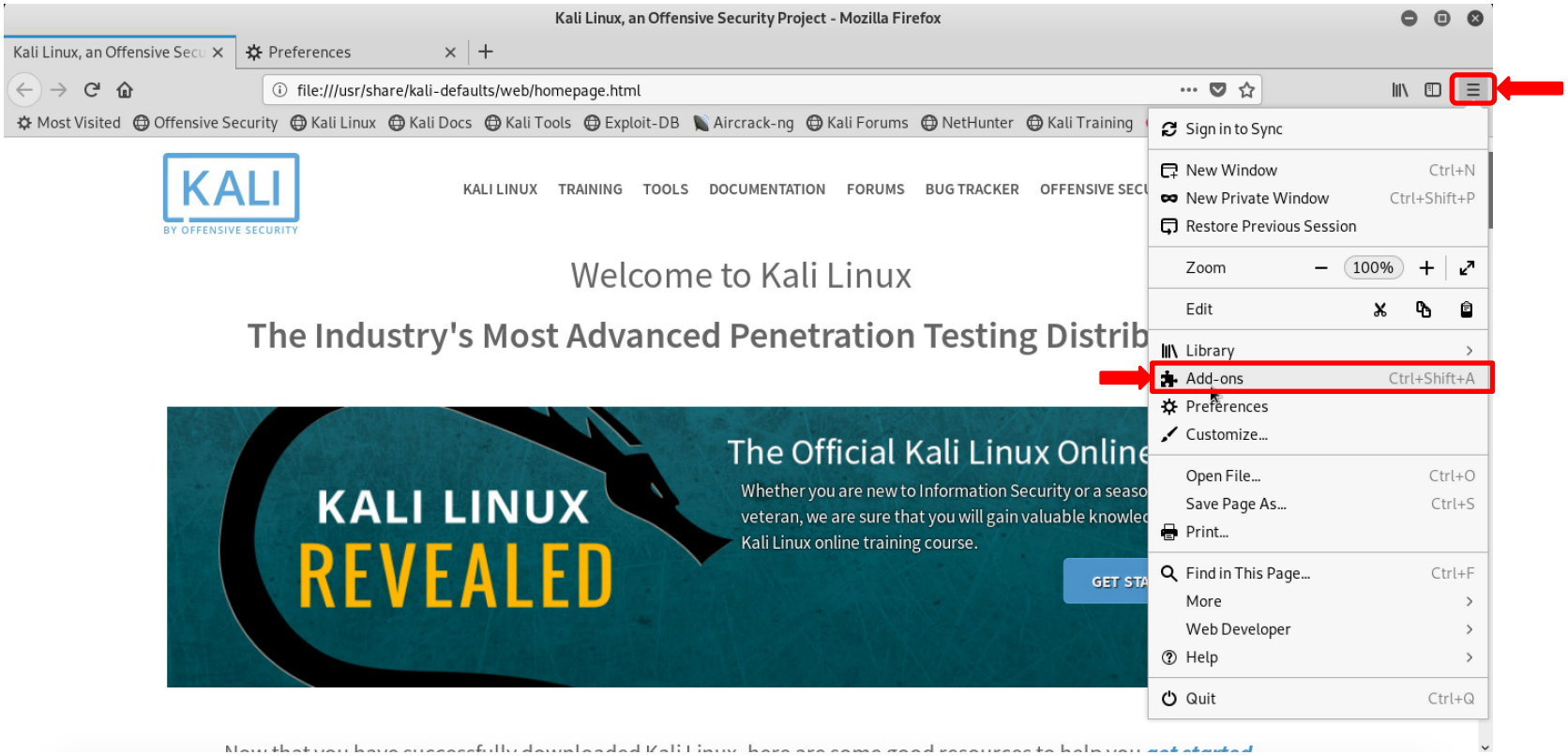
You can choose whether TinEye.com opens in the current tab, in a new tab in the foreground or in a new tab in the background and select the order in which your results will



Utilizzo di Risorse Web-Based

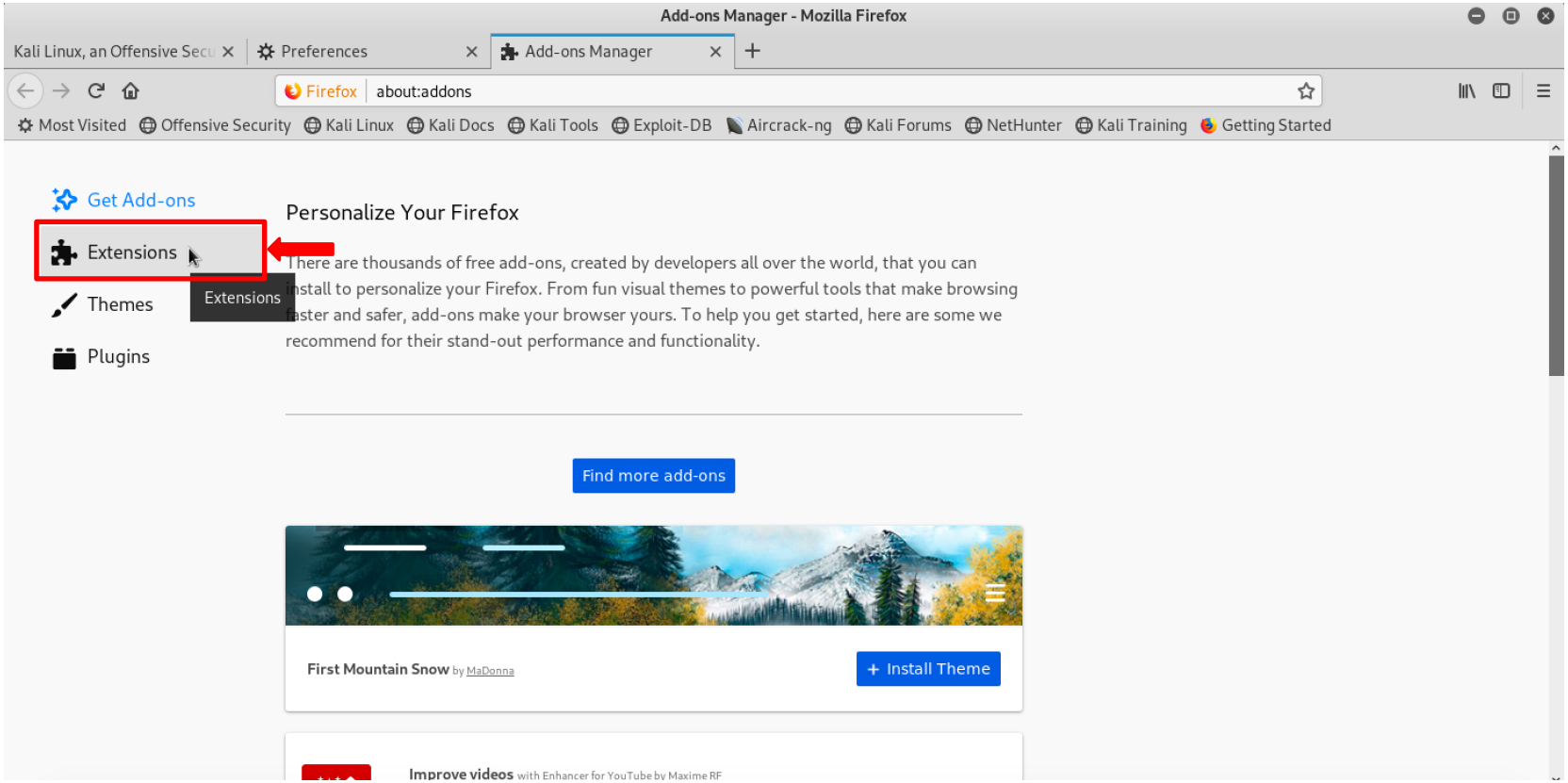
Reverse Image Search – TinEye – Esempio 2

- Installiamo l'estensione per Firefox



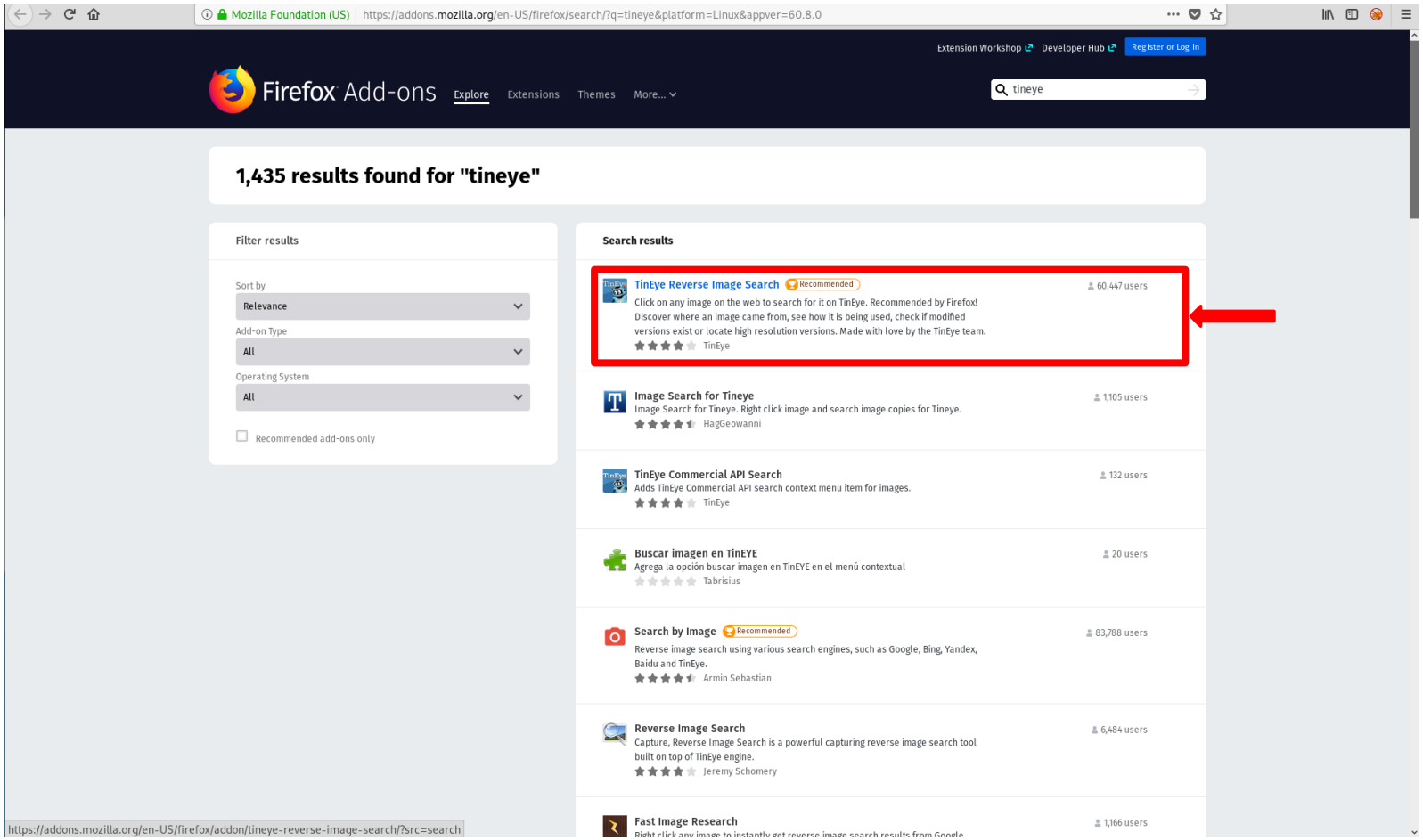
Utilizzo di Risorse Web-Based

Reverse Image Search – TinEye – Esempio 2



Utilizzo di Risorse Web-Based

Reverse Image Search – TinEye – Esempio 2



Utilizzo di Risorse Web-Based

Reverse Image Search – TinEye – Esempio 2

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

Informazioni di Registrazione
Whois

- WHOIS
  - Protocollo definito dall'RFC 3912
  - Strumento (comando) disponibile in molti sistemi operativi

Informazioni di Registrazione
Whois

- Mediante il WHOIS è possibile ottenere informazioni di registrazione su un determinato nome di dominio (o indirizzo IP)
  - E-mail
  - Numeri di telefono
  - Indirizzi
  - Etc

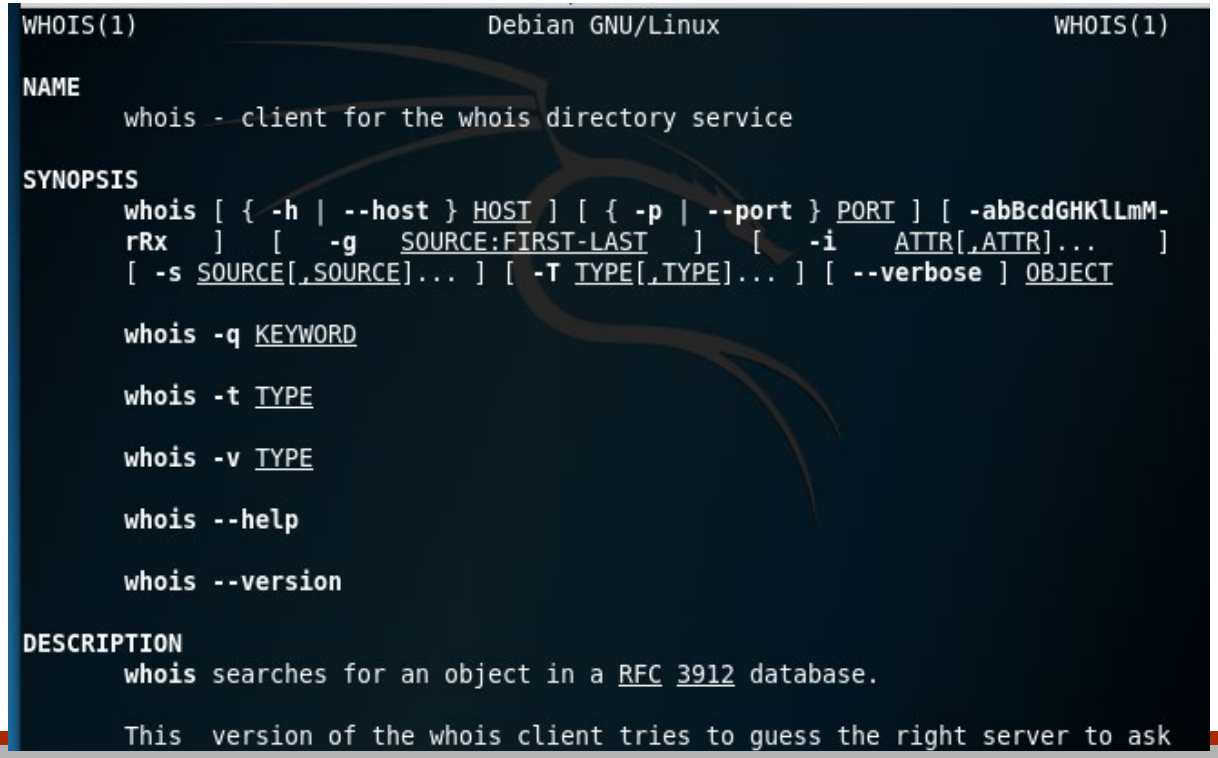
Informazioni di Registrazione
Whois

- Mediante il comando **`whois`** è possibile accedere a tutte le funzionalità fornite dal protocollo WHOIS

- Oltre al comando **`whois`**, il protocollo WHOIS può essere acceduto mediante alcuni servizi Web-based
  - https://www.whois.com/whois/
  - https://whois.domaintools.com
  - Etc

Informazioni di Registrazione
Whois

- Per maggiori informazioni sul comando **`whois`**
  - **`man whois`**



```
WHOIS(1)                        Debian GNU/Linux                        WHOIS(1)

NAME
       whois - client for the whois directory service

SYNOPSIS
       whois [ { -h | --host } HOST ] [ { -p | --port } PORT ] [ -abBcdGHKlLmM-
       rRx   ]   [   -g   SOURCE:FIRST-LAST   ]   [   -i   ATTR[,ATTR]...   ]
       [ -s SOURCE[,SOURCE]... ] [ -T TYPE[,TYPE]... ] [ --verbose ] OBJECT

       whois -q KEYWORD

       whois -t TYPE

       whois -v TYPE

       whois --help

       whois --version

DESCRIPTION
       whois searches for an object in a RFC 3912 database.

       This  version of the whois client tries to guess the right server to ask
```

Informazioni di Registrazione

Whois – Esempio 1

- **whois unisa.it**

```
root@kali:~# whois unisa.it

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

Domain:                 unisa.it
Status:                 ok
Signed:                 no
Created:                1996-01-29 00:00:00
Last Update:            2019-02-14 00:59:04
Expire Date:            2020-01-29
```

Informazioni sulle date di creazione e registrazione del dominio

Informazioni di Registrazione

Whois – Esempio 1

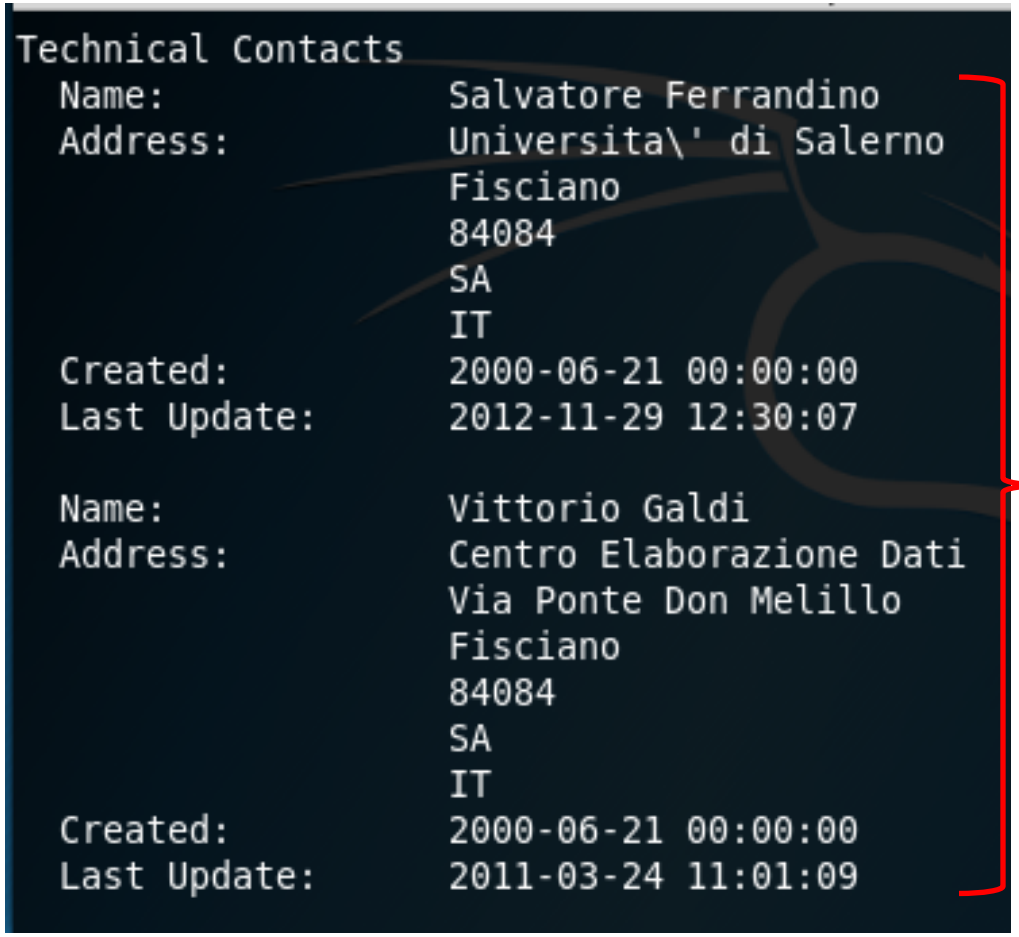
```
Registrant
  Organization:     Universita' di Salerno
  Address:          Universita' di Salerno
                    Baronissi
                    84081
                    SA
                    IT
  Created:          2007-03-01 10:47:03
  Last Update:      2011-03-24 11:01:07

Admin Contact
  Name:             Giuseppe Cattaneo
  Address:          Universita' di Salerno
                    Baronissi
                    84081
                    SA
                    IT
  Created:          1994-11-12 00:00:00
  Last Update:      2011-03-24 11:01:08
```

Organizzazione a cui appartiene il dominio

Responsabile amministrativo del dominio

Informazioni di Registrazione

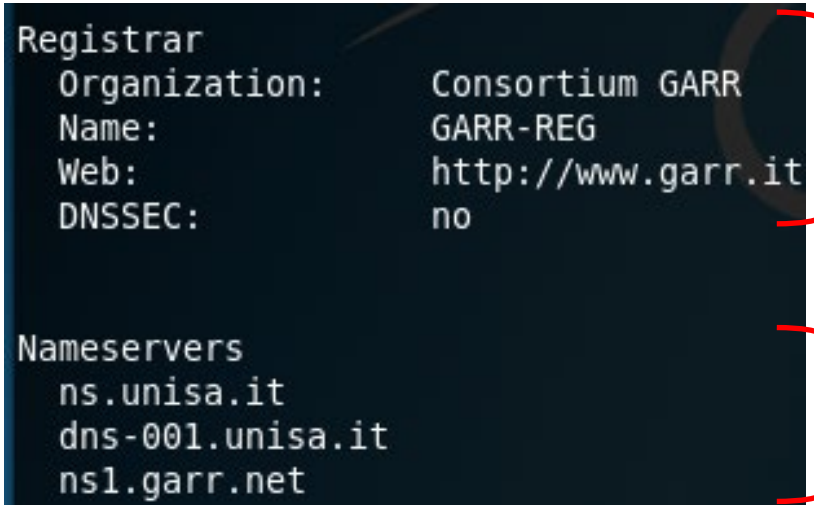
Whois – Esempio 1



Responsabili tecnici del dominio

Informazioni di Registrazione

Whois – Esempio 1



Organizzazione presso cui è registrato il dominio

DNS associati al dominio

Informazioni di Registrazione

Whois – Esempio 2

- **`whois github.com`**

Output parziale

```
root@kali:~# whois github.com
   Domain Name: GITHUB.COM
   Registry Domain ID: 1264983250_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2017-06-26T16:02:39Z
   Creation Date: 2007-10-09T18:20:50Z
   Registry Expiry Date: 2020-10-09T18:20:50Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhib
ited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS-1283.AWSDNS-32.ORG
   Name Server: NS-1707.AWSDNS-21.CO.UK
   Name Server: NS-421.AWSDNS-52.COM
```

Informazioni di Registrazione

Whois – Esempio 2

- **`whois github.com`**

Output parziale

```
root@kali:~# whois github.com
   Domain Name: GITHUB.COM
   Registry Domain ID: 1264983250_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2017-06-26T16:02:39Z
   Creation Date: 2007-10-09T18:20:50Z
   Registry Expiry Date: 2020-10-09T18:20:50Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://i
   Domain Status: clientTransferProhibited https:/
ited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS-1283.AWSDNS-32.ORG
   Name Server: NS-1707.AWSDNS-21.CO.UK
   Name Server: NS-421.AWSDNS-52.COM
```

github.com utilizza servizi cloud (Amazon Web Services)