



# 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

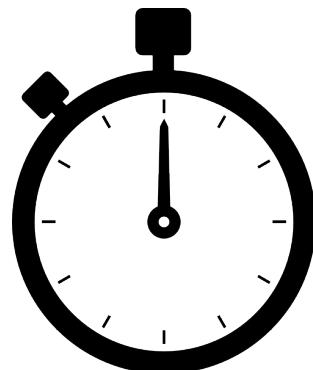
---

- 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 Open Source INTeelligence (**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

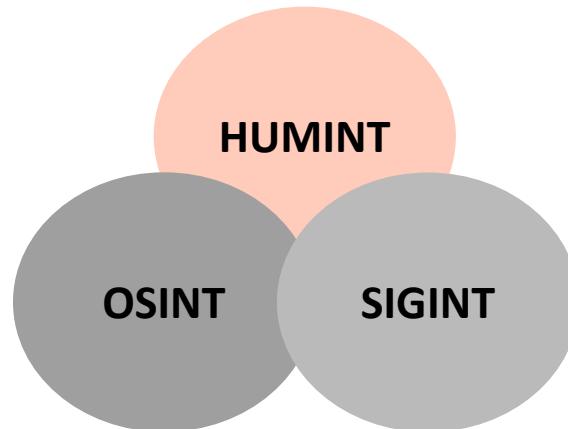


# Concetti Preliminari

## Open Source Intelligence

---

- Altre fonti di «intelligence»
  - Lo spionaggio che coinvolge l'interazione tra esseri umani viene definito come **HUMan INTelligence (HUMINT)**
  - La cattura di segnali radio con l'intento di violare la comunicazione prende il nome di **SIGnal INTelligence (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 «murate» 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**

The screenshot shows a Google search results page with the query "site:unisa.it" entered in the search bar. A red box highlights the search term "site:unisa.it". The results are filtered under the "Tutti" tab, showing approximately 272,000 results in 0.17 seconds. The first result is the official website of the University of Salerno (UNISA), which is highlighted with a red box. Other results include "Il Giornalista - Unisa", "PRIME 2017 - Giardini Naxos - Taormina, Italy - Home", "SMACD 2017 - Giardini Naxos - Taormina, Italy - Home", and "e-Lena: e-Learning & New Assessment".

site:unisa.it

Tutti Immagini Notizie Shopping Maps Altro Impostazioni Strumenti

Circa 272.000 risultati (0,17 secondi)

Prova la Google Search [www.google.com/webmasters/](https://www.google.com/webmasters/) Sei il proprietario di unisa.it? Ottieni informazioni su Google

**site:unisa.it**

**UNISA | Home**  
<https://www.unisa.it/>  
Università degli Studi di Salerno - Via Giovanni Paolo II, 132 - 84084 Fisciano (SA)

**Il Giornalista - Unisa**  
[www.ilgiornalista.unisa.it/](http://www.ilgiornalista.unisa.it/)  
Quotidiano della Scuola di Giornalismo dell'Università di Salerno.

**PRIME 2017 - Giardini Naxos - Taormina, Italy - Home**  
[prime2017.unisa.it/](http://prime2017.unisa.it/) Traduci questa pagina  
PRIME Conference 2017 - 12 - 15 June 2017, Giardini Naxos - Taormina, Italy - Home.

**SMACD 2017 - Giardini Naxos - Taormina, Italy - Home**  
[smacd2017.unisa.it/](http://smacd2017.unisa.it/) Traduci questa pagina  
SMACD Conference 2017 - 12 - 15 June 2017, Giardini Naxos - Taormina, Italy - Home.

**e-Lena: e-Learning & New Assessment**  
<https://www.elena.unisa.it/>  
e-Lena: e-Learning & New Assessment Piattaforma di e-Learning del Laboratorio Rimedi@DISUFF - Dipartimento di Scienze Umane, Filosofiche e della ...

# 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**

site:unisa.it sedute di laurea

Tutti Immagini Video Notizie Altro Impostazioni Strumenti

Circa 4.000 risultati (0)

Ingegneria Civile https://corsi.unisa.it/... 25 giu 2018 - N... Calendario sedute di Laurea dell'DIIn per gli anni Accademici 2018/2019 e 2019/2020. Il calendario delle sedute di Laurea dei Corsi di Laurea erogati presso l'Università degli Studi di Salerno 2018 a ...

**site:unisa.it sedute di laurea**

Economia | Esame Finale - UNISA | Corsi di Studio  
https://corsi.unisa.it/economia/didattica/esame-finale ▾  
Economia. CORSO DI LAUREA MAGISTRALE LM-56 ... Sedute di Laurea ... al sistema di gestione Tesi online gli studenti iscritti ai seguenti Corsi di Laurea: ...

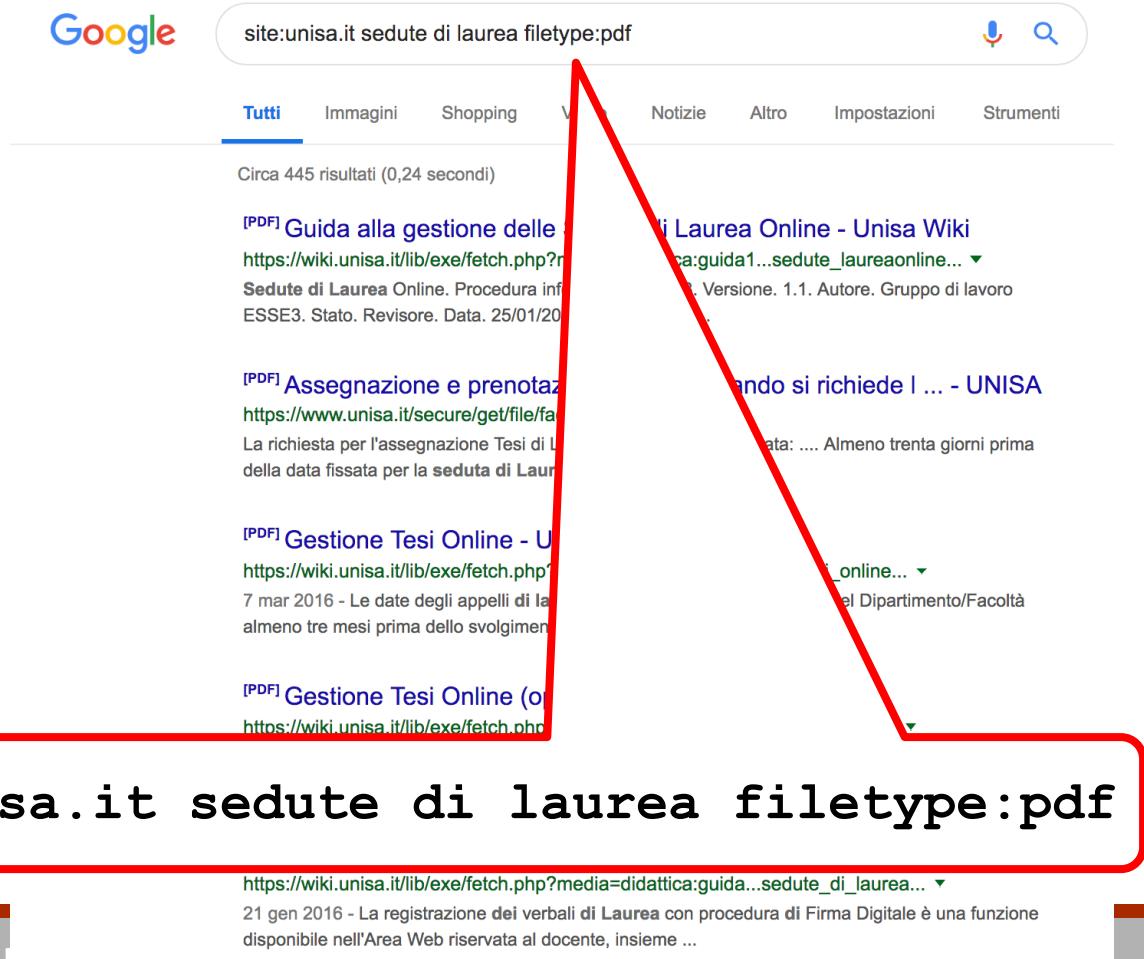
Matematica | Esame Finale - Piano - UNISA | Corsi di Studio  
https://corsi.unisa.it/mathematica/didattica/esame-finale ▾  
Matematica | Esame Finale. Matematica Esame Finale. Attivata, per le **sedute di Laurea**, da Maggio 2016 in poi, la nuova procedura di Gestione Tesi Online ...

Lettere | Esame Finale - UNISA | Corsi di Studio  
https://corsi.unisa.it/lettere/didattica/esame-finale ▾  
Lettere. CORSO DI LAUREA L-10. Toggle navigation. Menu ... Calendario **sedute di laurea** a.a. 2018/2019 ... Verbalizzazione Online - Esami di Laurea ...

# 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

All Images News Videos Maps More Settings Tools

About 131 results (24 seconds)

[PDF] Revisione verbale esame firmato digitalmente dal docente  
https://.../ib/exe/fetch.php?media...2.0\_esame... ▾ Translate this page  
Jan 27 del. 1. Matricola ...  
...rezione verbale esame firmato digitalmente dal docente  
ente che intende revocare un verbale errato, contatta l'Ufficio Didattica e Carriere  
nendo i seguenti dati: 1. Matricola ...

esame Prove Intercorso - UNISA  
...IAM%20-%20Modalità%20di%20esame.pdf ▾ Translate this page  
esame si svolgerà presso il laboratorio didattico multimediale della Facoltà di  
giorno fissato per l'appello e avrà inizio ...

me 25 Giugno 2013 - UNISA  
essori/rescigno/...esame/esame-25-6-13.pdf ▾ Translate this page  
anti. Tra le strutture di comunicazione a livello host, Pipe e Fifo offrono delle  
po avere dettagliatamente evidenziato le ...

Giugno 2016  
essori/rescigno/SO/...esame/esame-13-6-16.pdf ▾ Translate this page

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

[www.dl.unisa.it/ASD/12-0-15.pdf](http://www.dl.unisa.it/ASD/12-0-15.pdf) ▾ Translate this page

Jun 12, 2015 - 12 punti. Progettare una strategia efficiente per l'inserimento di un nuovo elemento in  
una lista semplice nei seguenti casi: 1. Nessun vincolo.

# 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**:

site:.gov filetype:sql

Tutti Immagini Notizie Shopping Maps Altro Impostazioni Strumenti

Circa 186 risultati (0,19 secondi)

UPDA... dggs.a... sonic\_data\_files SET filesize = 38, file\_size\_precision ...  
pubs/pdf\_update\_112718.sql - Traduci questa pagina

mai... http://.../fix\_cherenkov\_coef.s... - EICweb  
/whit/insane/.../fix\_cherenkov\_coef.s... ▾ Traduci questa pagina  
User Group Community.

**site:.gov filetype:sql**

https://www.douglasvillega.gov/25/Parks-Recreation/backup.sql ▾ Traduci questa pagina  
S, M, T, W, T, F, S, 24, 25, 26, 27, 28, 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 01, 02 ...

phpMyAdmin SQL Dump -- version 3.2.0.1 -- http://www.phpmyadmin ...  
https://www.arb.ca.gov/msprog/ordiesel/osm1085.sql ▾ Traduci questa pagina

Gen\_JN\_Triggers.sql  
ent-apps.fnal.gov/Journaling/Gen\_JN\_Triggers.sql - Traduci questa pagina

sql - NMFS InPort  
https://inport.nmfs.noaa.gov/inport/.../inport\_entity\_extract.sql ▾ Traduci questa pagina

create table dbo.PUBACC\_AC ( record\_type char(2) null ...  
wireless.fcc.gov/uls/data/documentation/pa\_ddef10.sql ▾ Traduci questa pagina

# 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**:

The screenshot shows a Google search results page with the following search parameters in the bar: `site:.gov intitle: "index of /"`. The results are filtered under the 'Tutti' tab. A red box highlights the search query in the search bar.

**Search Query:** site:.gov intitle: "index of /"

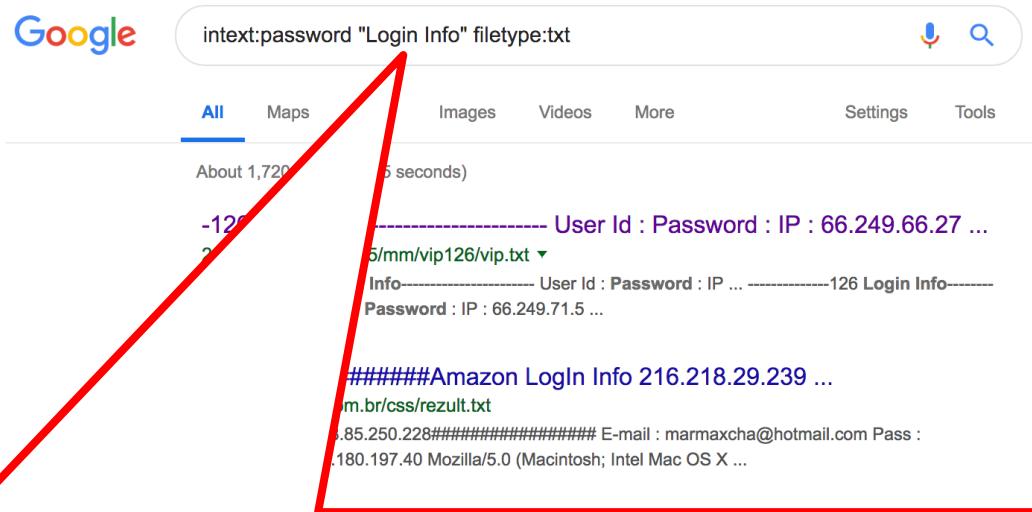
**Results:**

- Index of /ftp**  
https://idlastro.gsfc.nasa.gov/ftp/ ▾ Traduci questa pagina  
Index of /ftp. Name Last modified Size Description · Parent Directory - LICENSE 21-Jul-2014 13:09 1.3K aaareadme.txt 14-May-2015 14:18 4.6K astron.dir.tar.gz ...
- Index of /data - Aviation Weather Center**  
https://aviationweather.gov/data/ ▾ Traduci questa pagina  
Index of /data. Name · Last modified · Size · Parent Directory - .gis/, 01-Nov-2018 21:12, -.ifddp/, 06-Mar-2019 02:45, -.obs/, 06-Dec-2018 19:31, -.products ...
- Index of /ftp1 - NCI EVS**  
https://evs.nci.nih.gov/ftp1/ ▾ Traduci questa pagina  
Index of /ftp1. Name Last modified Size Description · Parent Directory - .bash\_history 2016-07-05 10:15 12 BiomedGT/ 2017-01-23 14:36 - CDISC/ 2018-12-10 ...

# 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



**intext:password "Login info" filetype:txt**

SPECIAL INTERNET CONNECTIONS: Last Update: 9/30/92 ...

[ccat.sas.upenn.edu/gopher/other/e-seminars/Internet/lrn/yanoff-list.txt](#) ▾

Sep 30, 1992 - (Login: genbank Password: 4nigm) -Genetics Bank mail .... Center telnet delocn.  
udel.edu or telnet 128.175.24.1 (Login: info) -Oracle mail ...

#@version 4.2.0;1249014846 #@admin add\_new\_author => Add ...

[zirkumflex.com/backup-site-v1/textpattern/lang/en-gb.txt](#) ▾

... Address change\_password => Change Your Password copy\_editor => Copy ... Your login info  
your\_login\_is => Your login is your\_new\_password => Your ...

# Utilizzo di Risorse Web-Based

## Google Hacking (o Google Dorking) – Esempio 8

➤ Operatori "" e +

The screenshot shows a Google search results page with the query **"index of /" +password**. The results are filtered under the **All** tab. A red box highlights the search term **"index of /" +password**.

Results:

- Index of /bonus/1**  
https://wikileaks.org/so...  
01-Jan-1970 00:01 34816  
Change password to acc...
- Index of /password/ - BeforeUs.com**  
www.beforeus.com/password/ ▾  
Index of /password/ ... 10.8K, application/x-httdp-php. password.inc.php, 2004-Jun-15 09:50:59, 3.7K, application/x-httdp-php. smtp.php, 2004-Jun-15 09:50:59 ...
- Index of /etc/passwd - Gray-World**  
gray-world.net/etc/passwd/ ▾  
master.passwd 31-Jul-2003 12:55 9k [ ] msadcs.dll 31-Jul-2003 12:55 63k [TXT] mysql.class 31-Jul-2003 12:55 1k [TXT] order.log 31-Jul-2003 12:55 3k [TXT] ...
- Index of /webapps/downloads/source/chap07/admin - cknuckles.com**  
www.cknuckles.com/webapps/downloads/source/chap07/admin/ ▾  
Index of /webapps/downloads/source/chap07/admin ... 2016-01-04 16:43, 15. [TXT], password.txt, 2016-01-04 16:43, 929. [DIR], states/, 2019-03-08 18:20, - ...

# 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)

The screenshot shows the 'Google Hacking Database' section of the Exploit Database website. The interface includes a sidebar with various icons for file types and search filters, a header with a logo and navigation links, and a main content area with a table of search results.

**Google Hacking Database**

Show 15 ▾

Date Added Dork Category Author

Date Added	Dork	Category	Author
2022-01-12	site:vps*.vps.ovh.net	Web Server Detection	Chahine Boutighane
2022-01-12	inurl:adminpanel site:gov.*	Footholds	Asheet Tirkay
2021-11-19	site:gov.* intitle:"index of" *.csv	Files Containing Juicy Info	Midhun Mohanan
2021-11-19	site:papaly.com + keyword	Files Containing Juicy Info	Gabriel Tarsia
2021-11-19	Fwd: intitle:"Index of /" intext:"resource/"	Files Containing Juicy Info	Mugdha Bansode
2021-11-19	Google to wordpress	Files Containing Juicy Info	Aitor Herrero
2021-11-19	Fwd: intitle:"atvise - next generation"	Files Containing Juicy Info	Mugdha Bansode
2021-11-18	inurl:admin filetype:xlsx site:gov.*	Files Containing Juicy Info	Krishna Agarwal
2021-11-18	inurl:"*admin   login"   inurl:.php   .asp	Pages Containing Login Portals	Krishna Agarwal
2021-11-18	intitle:index of settings.py	Files Containing Juicy Info	Amit Adhikari
2021-11-18	inurl:/intranet/login.php	Pages Containing Login Portals	Diego Bardalez Plaza
2021-11-18	inurl: /wp-content/uploads/ inurl:"robots.txt" "Disallow:" filetype:txt	Files Containing Juicy Info	Ritwick Dadhich
2021-11-18	site:postman.com + keyword	Files Containing Juicy Info	Gabriel Tarsia
2021-11-18	site:pastebin.com intitle:"cpanel"	Files Containing Juicy Info	Ishani Dhar
2021-11-18	inurl:admin filetype:xls	Files Containing Juicy Info	Ritwick Dadhich

Showing 1 to 15 of 7,341 entries

FIRST PREVIOUS 1 2 3 4 5 ... 490 NEXT LAST

# Utilizzo di Risorse Web-Based

## Google Hacking Database (GHDB)

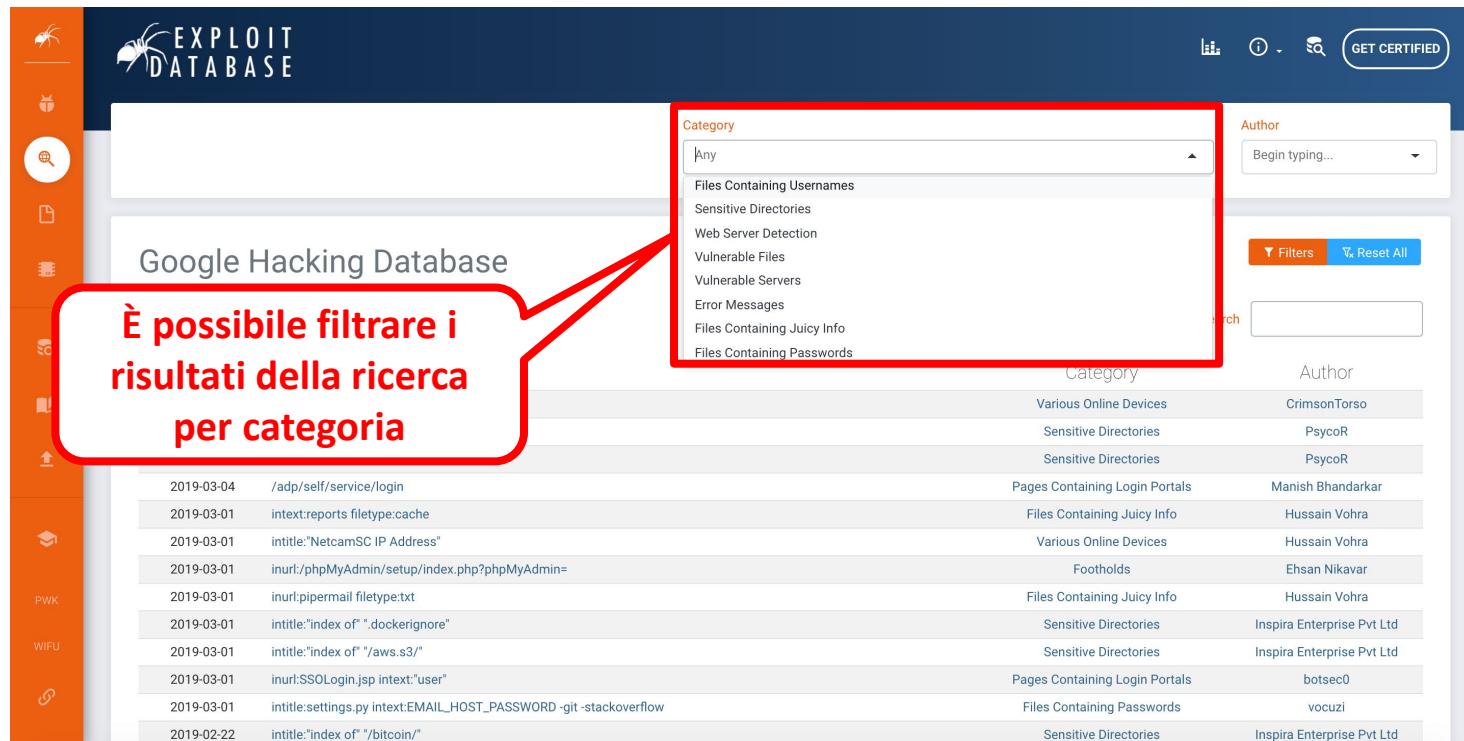
È possibile filtrare i risultati della ricerca

The screenshot shows the Exploit Database interface with the following details:

- Left Sidebar:** Contains icons for various tools: Spider (Exploit Database), Bug (Vulnerabilities), Magnifying Glass (Search), Document (Downloads), Folders (Projects), Database (Database), Up Arrow (Upload), Graduation Cap (Education), PWK (Penetration Testing), WIFU (Wireless Fuzzing), and a circular arrow (Automation).
- Header:** Includes the Exploit Database logo, search bar, and "GET CERTIFIED" button.
- Main Content:** Title "Google Hacking Database".
  - Show dropdown set to 15.
  - Date Added filter set to Dork.
  - Author column header.
  - Table of results:
    - 2019-03-07 /1000/system\_information.asp Author: CrimsonTorso
    - 2019-03-04 inurl:typo3conf/l10n/ Sensitive Directories Author: PsycoR
    - 2019-03-04 inurl:/files/contao Sensitive Directories Author: PsycoR
    - 2019-03-04 /adp/self/service/login Pages Containing Login Portals Author: Manish Bhandarkar
    - 2019-03-01 intext:reports filetype:cache Files Containing Juicy Info Author: Hussain Vohra
    - 2019-03-01 intitle:"NetcamSC IP Address" Various Online Devices Author: Hussain Vohra
    - 2019-03-01 inurl:/phpMyAdmin/setup/index.php?phpMyAdmin= Footholds Author: Ehsan Nikavar
    - 2019-03-01 inurl:pipermail filetype:txt Files Containing Juicy Info Author: Hussain Vohra
    - 2019-03-01 intitle:"index of" ".dockergignore" Sensitive Directories Author: Inspira Enterprise Pvt Ltd
    - 2019-03-01 intitle:"index of" "/aws.s3/" Sensitive Directories Author: Inspira Enterprise Pvt Ltd
    - 2019-03-01 inurl:SSOLogin.jsp intext:"user" Pages Containing Login Portals Author: botsec0
    - 2019-03-01 intitle:settings.py intext:EMAIL\_HOST\_PASSWORD -git -stackoverflow Files Containing Passwords Author: vocuzi
    - 2019-02-22 intitle:"index of" "/bitcoin/" Sensitive Directories Author: Inspira Enterprise Pvt Ltd
    - 2019-02-22 intitle:"index of" ".pem" Sensitive Directories Author: Inspira Enterprise Pvt Ltd
    - 2019-02-20 allinurl:asdm.jnlp Various Online Devices Author: Kevin Randall
  - Pagination:** FIRST, PREVIOUS, 1 (highlighted in orange), 2, 3, 4, 5, ..., 311, NEXT, LAST.

# Utilizzo di Risorse Web-Based

## Google Hacking Database (GHDB)



È possibile filtrare i risultati della ricerca per categoria

Category	Author
Any	Begin typing...
Files Containing Usernames	
Sensitive Directories	
Web Server Detection	
Vulnerable Files	
Vulnerable Servers	
Error Messages	
Files Containing Juicy Info	
Files Containing Passwords	
Category	Author
Various Online Devices	CrimsonTorso
Sensitive Directories	PsycoR
Sensitive Directories	PsycoR
Pages Containing Login Portals	Manish Bhandarkar
Files Containing Juicy Info	Hussain Vohra
Various Online Devices	Hussain Vohra
Footholds	Ehsan Nikavar
Files Containing Juicy Info	Hussain Vohra
Sensitive Directories	Inspira Enterprise Pvt Ltd
Sensitive Directories	Inspira Enterprise Pvt Ltd
Pages Containing Login Portals	botsec0
Files Containing Passwords	vocuzi
Sensitive Directories	Inspira Enterprise Pvt Ltd

# Utilizzo di Risorse Web-Based

## Google Hacking Database (GHDB)

The screenshot shows the Exploit Database interface with the "Google Hacking Database" section selected. The left sidebar has icons for various tools like Nmap, Metasploit, and Shodan. The main area displays a table of search queries with columns for Date Added, Category, and Author. A red arrow points to the second result in the table, which is highlighted with a red border.

Date Added	Dork	Category	Author
2019-03-07	"/1000/system_information.asp"	Various Online Devices	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" ".dockergignore"	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

# 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)

intitle:settings.py intext:EMAIL\_HOST\_PASSWORD -git -stackoverflow

<b>GHDB-ID:</b> 5141	<b>Author:</b> VOCUZI	<b>Google Dork Description:</b> intitle:settings.py intext:EMAIL_HOST_PASSWORD -git -stackoverflow
<b>Published:</b> 2019-03-01		<b>Google Search:</b> <a href="#">intitle:settings.py intext:EMAIL_HOST_PASSWORD -git -stackoverflow</a>

← →

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

Dork :  
intitle:settings.py intext:EMAIL\_HOST\_PASSWORD -git -stackoverflow

Author :  
Vipin Joshi (@vocuzi)

**Cliccando sul link è possibile effettuare direttamente la query tramite Google**

# Utilizzo di Risorse Web-Based

## Google Advanced Search

➤ [https://www.google.com/advanced\\_search](https://www.google.com/advanced_search)

### Advanced Search

Find pages with...

all these words:

To do this in the search box.

Type the important words: tri-colour rat terrier

this exact word or phrase:

Put exact words in quotes: "rat terrier"

any of these words:

Type OR between all the words you want: miniature OR standard

none of these words:

Put a minus sign just before words that you don't want:  
-rodent, -"Jack Russell"

numbers ranging from:

 to 

Put two full stops between the numbers and add a unit of measurement:  
10..35 kg, £300..£500, 2010..2011

Then narrow your results  
by...

language:

 any language

Find pages in the language that you select.

region:

 any region

Find pages published in a particular region.

last update:

 anytime

Find pages updated within the time that you specify.

site or domain:

Search one site (like wikipedia.org) or limit your results to a domain like .edu, .org or .gov

terms appearing:

 anywhere in the page

Search for terms in the whole page, page title or web address, or links to the page you're looking for.

SafeSearch:

 Show explicit results

Tell SafeSearch whether to filter sexually explicit content.

file type:

 any format

Find pages in the format that you prefer.

usage rights:

 not filtered by licence

Find pages that you are free to use yourself.

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

The screenshot shows the SecurityTrails dashboard. At the top left is the company logo "SecurityTrails A Recorded Future Company". To its right is a search bar with the placeholder "Enter a Domain, IP, Keyword, or Hostname" and a magnifying glass icon. On the far right are "Support" and a user profile icon. Below the header, a red arrow points to the search bar, and another red arrow points to the "Dashboard" link in the navigation menu.

**Navigation Menu:**

- Get SurfaceBrowser™
- Dashboard** (highlighted with a red box and arrow)
- API
- Feeds
- Account

**Dashboard Section:**

Hi, you can access our data with your browser (search field in navigation bar) or by using our API.

**Daily API Requests Overview:** A chart showing 0 requests on Mar 22 Coordinated Universal Time (UTC). Buttons include "More Stats" and "Manage plan >".

**Subscription:** Current Plan **Free**. Buttons include "Manage plan >" and "Upgrade".

**Quota usage Mar 2023:** 0 of 50 (0%)

**Choose a plan that's right for your business:** A call-to-action button labeled "Upgrade now".

## Dashboard

# Utilizzo di Risorse Web-Based

## Asset Discovery – SecurityTrails – Esempio

The screenshot shows the SecurityTrails dashboard. At the top left is the company logo "SecurityTrails A Recorded Future Company". To its right is a search bar with the placeholder "Enter a Domain, IP, Keyword, or Hostname" and a magnifying glass icon. A red box highlights this search bar, and a red arrow points from it to the search term "unisa.it" which is also highlighted with a red box. In the top right corner are "Support" and a user profile icon. Below the header is a navigation menu with "Get SurfaceBrowser™" and "Dashboard" (which is highlighted with a red box and has a red arrow pointing to it). Other menu items include "API", "Feeds", and "Account". On the left, there's a sidebar with the text "Choose a plan that's right for your business" and a blue "Upgrade now" button. The main dashboard area features a "Daily API Requests Overview" chart (0 requests on Mar 22 UTC), a "Subscription" section showing "Current Plan Free" with a "Manage plan >" link, and a "Quota usage Mar 2023" section showing 0 of 50 (0%) with an "Upgrade" link.

## Dashboard

# Utilizzo di Risorse Web-Based

## Asset Discovery – SecurityTrails – Esempio

The screenshot shows the SecurityTrails interface for the domain `unisa.it`. A red arrow points to the `DNS Records` button in the top navigation bar. The main content area displays the following sections:

- A records:** Consortium GARR, IP `193.205.185.20`, 238 entries.
- AAAA records:** NO RECORDS
- MX records:** Google LLC, entries:
  - 1 `aspmx.l.google.com` (15,185,518)
  - 10 `alt4.aspmx.l.google.com` (10,826,645)
  - 10 `alt3.aspmx.l.google.com` (10,684,469)
  - 5 `alt2.aspmx.l.google.com` (14,885,038)
  - 5 `alt1.aspmx.l.google.com` (14,958,308)
- NS records:** Consortium GARR, `ns1.garr.net`, `ns.unisa.it`, `dns-001.unisa.it`.
- SOA records:** TTL: 7200, Email: `salfer.unisa.it`, 15 entries.
- TXT records:** `v=spf1 a mx ip4:193.205.176.242 ip4:193.205.165.0/24 ip4:130.186.31.160/27 ip4:193.205.180.1 include:_spf.google.com include:_spf.cineca.it -all`, `MS=ms81604222`.

# Utilizzo di Risorse Web-Based

## Asset Discovery – SecurityTrails – Esempio

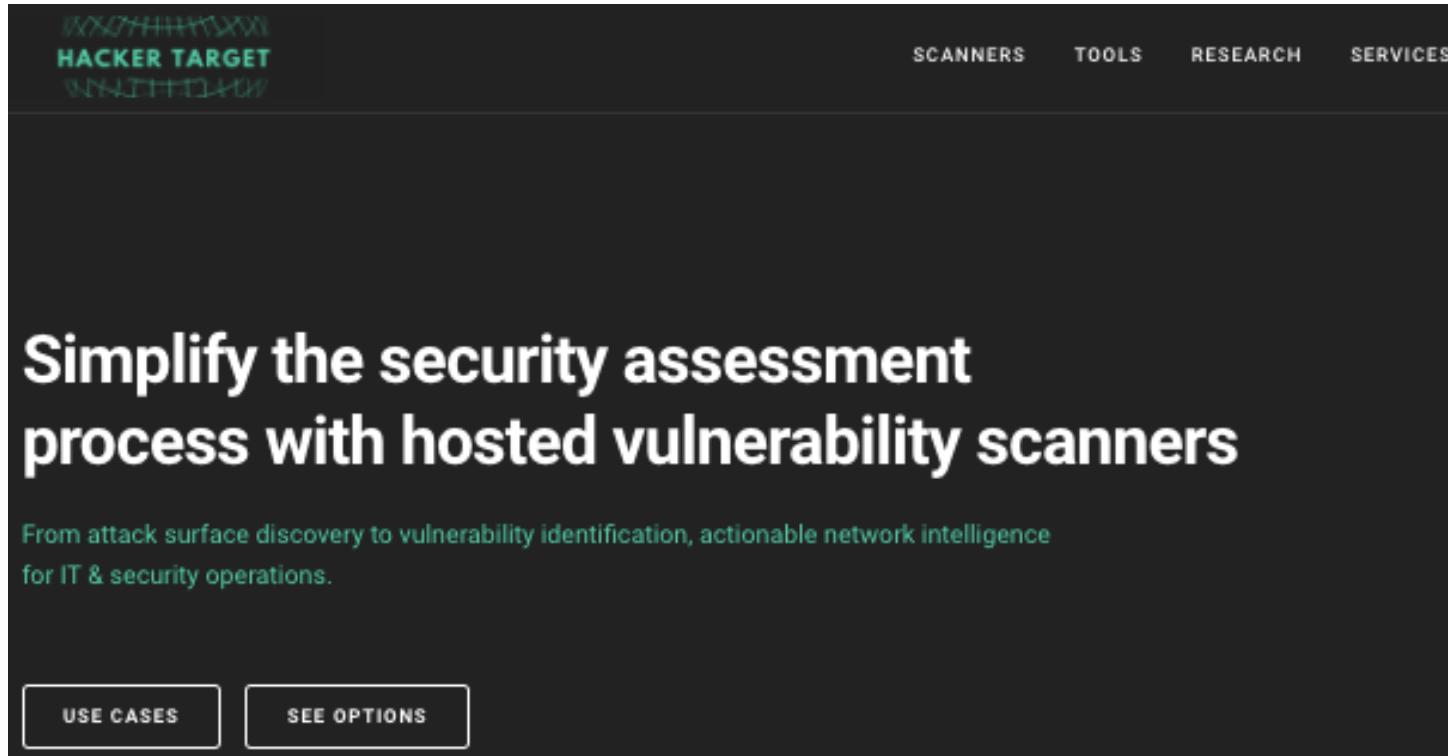
The screenshot shows the SecurityTrails interface for the domain `unisa.it`. On the left, there's a sidebar with options like DOMAIN, DNS Records, and Historical Data. A red arrow points to the "Subdomains" button, which is highlighted with a red border and shows the number 3,494. Below this is a promotional banner for choosing a plan and an "Upgrade now" button. The main content area is titled "unisa.it subdomains" and contains a search bar. It displays a table of 3,494 results, with the first few rows shown:

Domain	Rank	Hosting Provider	Mail Provider
unisa.it	160,674	Consortium GARR	Google LLC
diciv.unisa.it	641,977	-	-
libeccio.di.unisa.it	867,180	Consortium GARR	-
dia.unisa.it	1,401,570	Consortium GARR	-
dipmat2.unisa.it	1,412,604	Consortium GARR	-
dipmat.unisa.it	1,448,026	-	-
sirocco2013.di.unisa.it	1,471,654	Consortium GARR	-
gpc2017.di.unisa.it	1,476,951	Consortium GARR	-
cpm2015.di.unisa.it	1,479,261	Consortium GARR	-

# Utilizzo di Risorse Web-Based

## Asset Discovery – Hacker Target

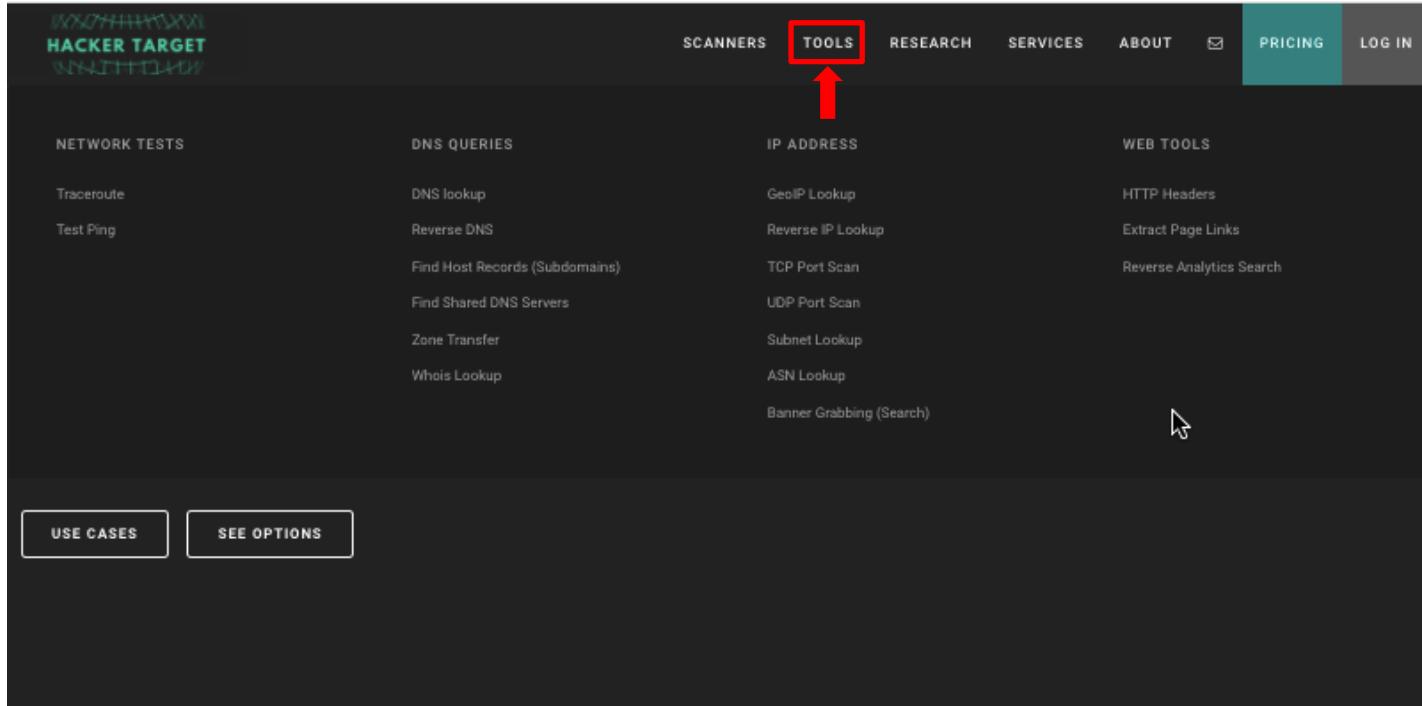
- <https://hackertarget.com/>
- Permette di cercare informazioni riguardo domini e servizi di rete



# Utilizzo di Risorse Web-Based

## Asset Discovery – Hacker Target

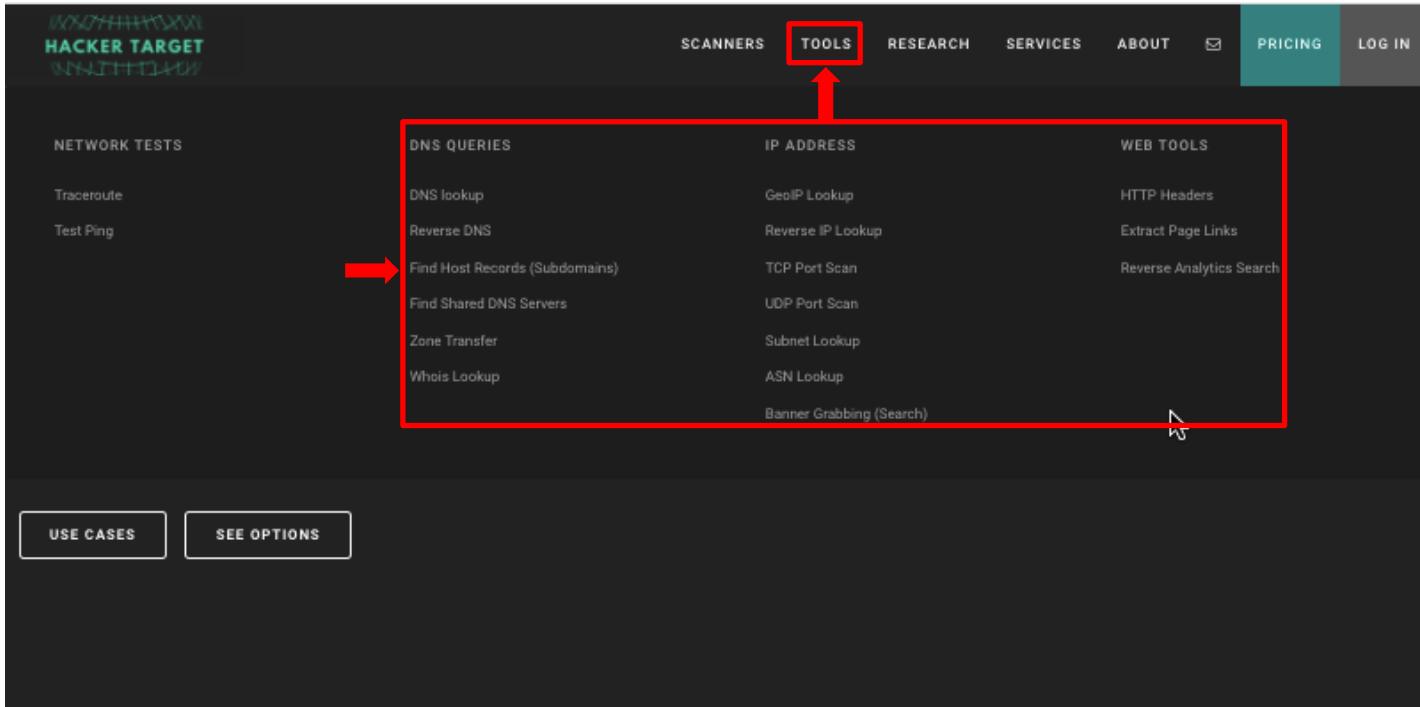
- <https://hackertarget.com/>
- Permette di cercare informazioni riguardo domini e servizi di rete



# Utilizzo di Risorse Web-Based

## Asset Discovery – Hacker Target

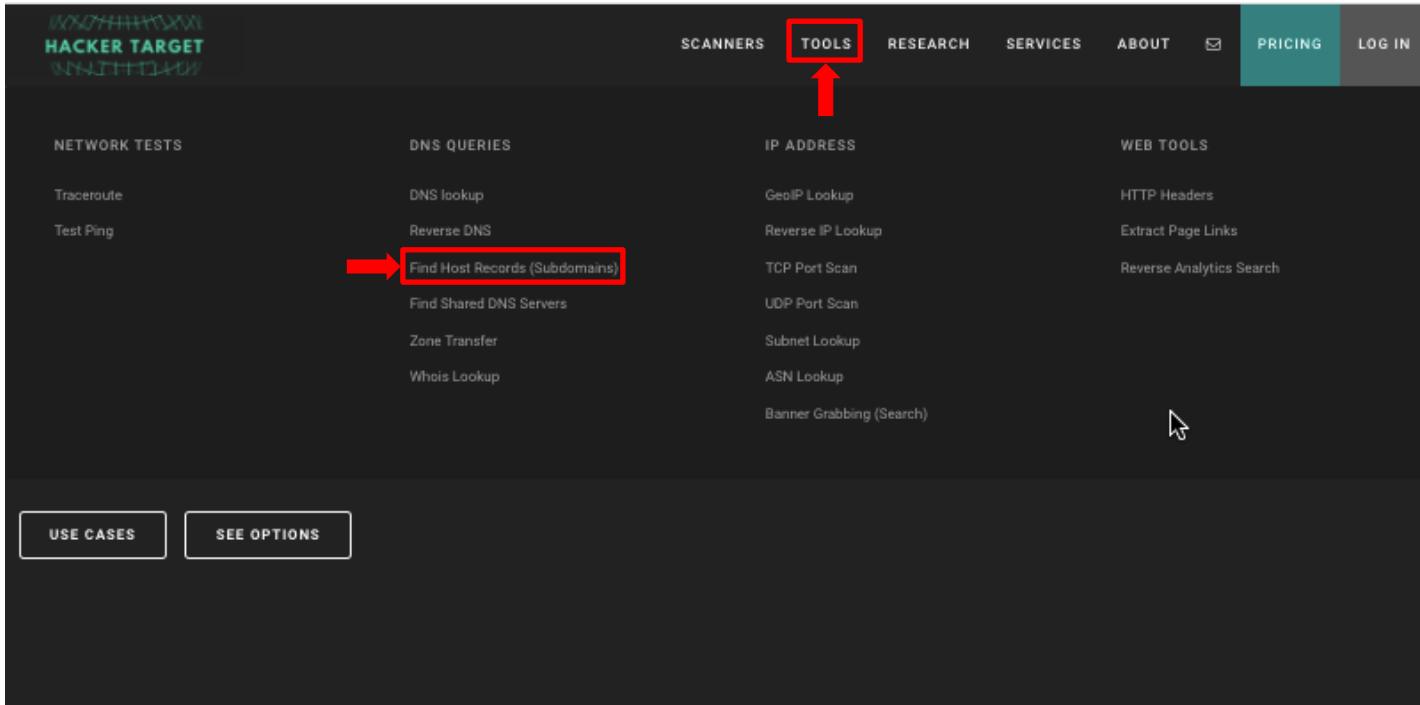
- <https://hackertarget.com/>
- Permette di cercare informazioni riguardo domini e servizi di rete



# 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

The screenshot shows the Hackertarget.com homepage. At the top, there is a navigation bar with links for SCANNERS, TOOLS, RESEARCH, SERVICES, ABOUT, and a mail icon. Below the navigation bar, a search bar contains the domain "unisa.it". Underneath the search bar, there is a CAPTCHA section with a green checkmark indicating "Non sono un robot" and a reCAPTCHA logo. A link to "Remove limits & captcha with membership" is also present. Below the CAPTCHA, a large green button says "FIND (A) RECORDS". To the right of this button, the text "Sottodomini" is highlighted in red. A list of subdomains is displayed in a table format, with the first few entries being: mail-out-177.unisa.it, 193.205.165.177; mail-out-102.unisa.it, 193.205.165.102; mail-out-25.unisa.it, 193.205.165.25; mail-out-172.unisa.it, 193.205.165.172; srv-004.unisa.it, 193.205.167.32; mail-out-99.unisa.it, 193.205.165.99; mail-out-38.unisa.it, 193.205.165.38; internet044.unisa.it, 193.205.179.108; hippocistica.unisa.it, 193.205.184.248; mail-out-250.unisa.it, 193.205.165.250; mail-out-1.unisa.it, 193.205.165.1; seda.seda.unisa.it, 193.205.167.15; input.di.unisa.it, 193.205.161.8; mail-out-23.unisa.it, 193.205.165.23; amm-27.seda.unisa.it, 193.205.168.92; lnecclient1.dia.unisa.it, 192.41.218.60.

Information Gathering

# Utilizzo di Risorse Web-Based

## Asset Discovery – Hacker Target

➤ <https://hackertarget.com/>

➤ Permette di cercare informazioni riguardo domini e servizi di rete

The screenshot shows the homepage of [Hackertarget.com](https://hackertarget.com/). At the top, there is a navigation bar with links for SCANNERS, TOOLS, RESEARCH, SERVICES, ABOUT, PRICING, and LOG IN. A red box highlights the 'SCANNERS' link, and a red arrow points upwards from the bottom of the page towards it. Below the navigation bar, there is a grid of tools categorized into four sections: NETWORK, WEB, CMS APPS, and RECON. A red box surrounds the entire grid. Another red arrow points to the left side of the 'NETWORK' section. The 'NETWORK' section contains links for Nmap Port Scanner, Schedule Nmap Scans, OpenVAS Scanner, Schedule OpenVAS Scans, and Zmap Fast Network Scan. The 'WEB' section contains links for Nikto Web Scanner, SSL / TLS Scan, and WhatWeb / Wappalyzer. The 'CMS APPS' section contains links for WordPress Scanner, Joomla Security Scan, Drupal Security Scan, and SharePoint Security Scan. The 'RECON' section contains links for Domain Profiler (OSINT), IP Information Lookup, and Free IP Tools. At the bottom left, there are two buttons: 'USE CASES' and 'SEE OPTIONS'. At the bottom right, there is a large red text overlay that reads: 'Strumenti utili per le fasi di Enumerating Target/Port Scanning e Vulnerability Mapping'.

NETWORK	WEB	CMS APPS	RECON
Nmap Port Scanner	Nikto Web Scanner	WordPress Scanner	Domain Profiler (OSINT)
Schedule Nmap Scans	SSL / TLS Scan	Joomla Security Scan	IP Information Lookup
OpenVAS Scanner	WhatWeb / Wappalyzer	Drupal Security Scan	Free IP Tools
Schedule OpenVAS Scans		SharePoint Security Scan	
Zmap Fast Network Scan			

for IT & security operations.

USE CASES SEE OPTIONS

Strumenti utili per le fasi di  
Enumerating Target/Port  
Scanning e Vulnerability Mapping

# Utilizzo di Risorse Web-Based

## Asset Discovery – H. E. BGP Toolkit

➤ <https://bgp.he.net/>

The screenshot shows the Hurricane Electric BGP Toolkit Home page. At the top left is the HE logo and the text "HURRICANE ELECTRIC INTERNET SERVICES". To the right is a search bar with a "Search" button. Below the header, a "Quick Links" sidebar on the left lists various tools: BGP Toolkit Home, BGP Prefix Report, BGP Peer Report, Exchange Report, Bogon Routes, World Report, Multi Origin Routes, DNS Report, Top Host Report, Internet Statistics, Looking Glass, Network Tools App, Free IPv6 Tunnel, IPv6 Certification, IPv6 Progress, Going Native, and Contact Us. The main content area has a "Home" tab selected. It displays a welcome message, the visitor's IP address (87.13.163.142) with a Telecom Italia flag, the announced network (87.13.128.0/17) with a Telecom Italia flag, and the ISP (AS3269) with a Telecom Italia flag. At the bottom, it says "Updated 08 Mar 2019 22:21 PST © 2019 Hurricane Electric". A red banner at the very bottom contains social media icons for Twitter and Facebook, and the text "Information Gathering".

**HURRICANE ELECTRIC  
INTERNET SERVICES**

[BGP Toolkit Home](#)

**Quick Links**

- [BGP Toolkit Home](#)
- [BGP Prefix Report](#)
- [BGP Peer Report](#)
- [Exchange Report](#)
- [Bogon Routes](#)
- [World Report](#)
- [Multi Origin Routes](#)
- [DNS Report](#)
- [Top Host Report](#)
- [Internet Statistics](#)
- [Looking Glass](#)
- [Network Tools App](#)
- [Free IPv6 Tunnel](#)
- [IPv6 Certification](#)
- [IPv6 Progress](#)
- [Going Native](#)
- [Contact Us](#)

**Home**

Welcome to the Hurricane Electric BGP Toolkit.

You are visiting from **87.13.163.142** (host142-163-dynamic.13-87-r.retail.telecomitalia.it)

Announced as **87.13.128.0/17** (Telecom Italia S.p.A. TIN EASY LITE)

Your ISP is **AS3269** (Telecom Italia S.p.A.)

Updated 08 Mar 2019 22:21 PST © 2019 Hurricane Electric

**Permette di acquisire informazioni su Autonomous System (AS)**

Information Gathering

# Utilizzo di Risorse Web-Based

## Asset Discovery – H. E. BGP Toolkit

➤ <https://bgp.he.net/>

The screenshot shows the Hurricane Electric BGP Toolkit Home page. At the top, there is a logo consisting of a blue circle with 'HE' in white, followed by the text 'HURRICANE ELECTRIC INTERNET SERVICES'. Below the logo is a search bar with the input 'unisa.it' and a 'Search' button. A red box highlights the search input field, and another red box highlights the search result 'unisa.it' in the main content area. The main content area includes a 'Home' link, a welcome message, information about the visitor's IP address and ISP, and links to various network tools.

**Quick Links**

- [BGP Toolkit Home](#)
- [BGP Prefix Report](#)
- [BGP Peer Report](#)
- [Exchange Report](#)
- [Bogon Routes](#)
- [World Report](#)
- [Multi Origin Routes](#)
- [DNS Report](#)
- [Top Host Report](#)
- [Internet Statistics](#)
- [Looking Glass](#)
- [Network Tools App](#)
- [Free IPv6 Tunnel](#)
- [IPv6 Certification](#)
- [IPv6 Progress](#)
- [Going Native](#)
- [Contact Us](#)

**unisa.it**

Welcome to the Hurricane Electric BGP Toolkit.

You are visiting from **87.13.163.142** (host142-163-dynamic.13-87-r.retail.telecomitalia.it)

Announced as **87.13.128.0/17** (Telecom Italia S.p.A. TIN EASY LITE)

Your ISP is **AS3269** (Telecom Italia S.p.A.)

Updated 08 Mar 2019 22:21 PST © 2019 Hurricane Electric



# Utilizzo di Risorse Web-Based

## Asset Discovery – H. E. BGP Toolkit

➤ <https://bgp.he.net/>

The screenshot shows the Hurricane Electric BGP Toolkit homepage. At the top, there is a logo consisting of a blue circle with 'HE' in white, followed by the text 'HURRICANE ELECTRIC INTERNET SERVICES'. Below the logo is a search bar with the input 'unisa.it' and a 'Search' button. A red box highlights the search term 'unisa.it' in the search bar, and another red box highlights the result 'unisa.it' in the search results area. The search results area contains the following information:

- Welcome to the Hurricane Electric BGP Toolkit.
- You are visiting from [87.13.163.142](#) (host142-163-dynamic.13-87-r.retail.telecomitalia.it)
- Announced as [87.13.128.0/17](#) (Telecom Italia S.p.A. TIN EASY LITE)
- Your ISP is [AS3269](#) (Telecom Italia S.p.A.)

At the bottom of the search results area, it says 'Updated 08 Mar 2019 22:21 PST © 2019 Hurricane Electric'.

**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/>

 **HURRICANE ELECTRIC  
INTERNET SERVICES**

[unisa.it](#)

**Quick Links**

[BGP Toolkit Home](#)  
[BGP Prefix Report](#)  
[BGP Peer Report](#)  
[Exchange Report](#)  
[Bogon Routes](#)  
[World Report](#)  
[Multi Origin Routes](#)  
[DNS Report](#)  
[Top Host Report](#)  
[Internet Statistics](#)  
[Looking Glass](#)  
[Network Tools App](#)  
[Free IPv6 Tunnel](#)  
[IPv6 Certification](#)  
[IPv6 Progress](#)  
[Going Native](#)  
[Contact Us](#)

[!\[\]\(04f079d792c65fca73a2705e3ffd94ce\_img.jpg\)](#) [!\[\]\(d0d6c70cd2b091e40e3612391b2e7f96\_img.jpg\)](#)

[DNS Info](#) [Website Info](#) [IP Info](#)

**Start of Authority**

mname: ns.unisa.it rname: salfer.unisa.it  
serial: 2015033088  
refresh: 7200 retry: 600  
expire: 86400 minimum: 300

**Nameservers**

[dns-001.unisa.it](#), [ns.unisa.it](#), [ns1.garr.net](#)

**Mail Exchangers**

[ASPMX.L.GOOGLE.COM\(1\)](#), [ALT1.ASPMX.L.GOOGLE.COM\(5\)](#), [ALT2.ASPMX.L.GOOGLE.COM\(5\)](#),  
[ALT3.ASPMX.L.GOOGLE.COM\(10\)](#), [ALT4.ASPMX.L.GOOGLE.COM\(10\)](#)

**TXT Records**

v=spf1 a mx ip4:193.205.176.242 ip4:193.205.165.0/24 ip4:130.186.31.160/27 ip4:193.205.180.1  
include:\_spf.google.com include:\_spf.cineca.it ~all

MS=ms81604222

**A Records**

[193.205.160.20](#)

Updated 08 Mar 2019 22:21 PST © 2019 Hurricane Electric

# Utilizzo di Risorse Web-Based

## Asset Discovery – H. E. BGP Toolkit

➤ <https://bgp.he.net/>

The screenshot shows the Hurricane Electric BGP Toolkit homepage. At the top left is the HE logo and the text "HURRICANE ELECTRIC INTERNET SERVICES". Below the logo is the URL "unisa.it". A search bar is present at the top right. On the left, a sidebar titled "Quick Links" lists various tools: BGP Toolkit Home, BGP Prefix Report, BGP Peer Report, Exchange Report, Bogon Routes, World Report, Multi Origin Routes, DNS Report, Top Host Report, Internet Statistics, Looking Glass, Network Tools App, Free IPv6 Tunnel, IPv6 Certification, IPv6 Progress, Going Native, and Contact Us. Below the sidebar are social media icons for Twitter and Facebook. The main content area has tabs for "DNS Info", "Website Info", and "IP Info", with "IP Info" highlighted by a red box and an arrow pointing to it from below. The "IP Info" section contains sections for "Start of Authority", "Nameservers", "Mail Exchangers", "TXT Records", and "A Records". The "Start of Authority" section shows mname: ns.unisa.it rname: safer.unisa.it, serial: 2015033088, refresh: 7200, retry: 600, expire: 86400, and minimum: 300. The "Nameservers" section lists dns-001.unisa.it, ns.unisa.it, and ns1.garr.net. The "Mail Exchangers" section lists several Google servers. The "TXT Records" section shows a SPF record: v=spf1 a mx ip4:193.205.176.242 ip4:193.205.165.0/24 ip4:130.186.31.160/27 ip4:193.205.180.1 include:\_spf.google.com include:\_spf.cineca.it ~all. The "A Records" section lists the IP address 193.205.160.20. At the bottom, a footer states "Updated 08 Mar 2019 22:21 PST © 2019 Hurricane Electric".

# Utilizzo di Risorse Web-Based

## Asset Discovery – H. E. BGP Toolkit

➤ <https://bgp.he.net/>

The screenshot shows the Hurricane Electric BGP Toolkit homepage. At the top left is the HE logo and the text "HURRICANE ELECTRIC INTERNET SERVICES". To the right is a search bar with a "Search" button. Below the header is a "Quick Links" sidebar containing various links such as BGP Toolkit Home, BGP Prefix Report, BGP Peer Report, Exchange Report, Bogon Routes, World Report, Multi Origin Routes, DNS Report, Top Host Report, Internet Statistics, Looking Glass, Network Tools App, Free IPv6 Tunnel, IPv6 Certification, IPv6 Progress, Going Native, and Contact Us. The main content area features three tabs: DNS Info, Website Info, and IP Info. The IP Info tab is active, displaying a network path: "193.205.160.20 > 193.204.0.0/15 > **AS137** > Consortium GARR". A red box highlights the AS137 entry in the path. An arrow points from this red box down to a timestamp at the bottom of the IP Info box: "Updated 18 Mar 2019 22:21 PST © 2019 Hurricane Electric". At the bottom left are social media icons for Twitter and Facebook. The footer contains the text "Information Gathering".

# Utilizzo di Risorse Web-Based

## Asset Discovery – H. E. BGP Toolkit

➤ <https://bgp.he.net/>

AS Info Graph v4 Graph v6 Prefixes v4 Prefixes v6 Peers v4 Peers v6 Whois IRR IX

Company Website: <http://www.garr.it>

Country of Origin: Italy 

Internet Exchanges: 4

Prefixes Originated (all): 81  
Prefixes Originated (v4): 79  
Prefixes Originated (v6): 2

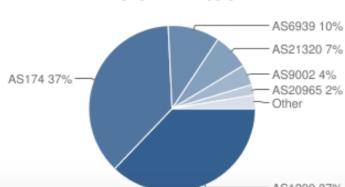
Prefixes Announced (all): 111  
Prefixes Announced (v4): 101  
Prefixes Announced (v6): 10

BGP Peers Observed (all): 277  
BGP Peers Observed (v4): 274  
BGP Peers Observed (v6): 142

IPs Originated (v4): 2,769,408  
AS Paths Observed (v4): 125,513  
AS Paths Observed (v6): 23,780

Average AS Path Length (all): 4.544  
Average AS Path Length (v4): 4.592  
Average AS Path Length (v6): 4.293

AS137 IPv4 Peers



ASN	Name
AS1299	Telia Company AB
AS174	Cogent Communications
AS6939	Hurricane Electric LLC
AS21320	GEANT Limited
AS9002	RETN Limited
AS20965	GEANT Limited

# Utilizzo di Risorse Web-Based

## Asset Discovery – H. E. BGP Toolkit

➤ <https://bgp.he.net/>

The screenshot shows the H. E. BGP Toolkit interface with the 'AS Info' tab selected. The main panel displays various network statistics for AS137:

- Company Website: <http://www.garr.it>
- Country of Origin: Italy (with flag)
- Internet Exchanges: 4
- Prefixes Originated (all): 81
- Prefixes Originated (v4): 79
- Prefixes Originated (v6): 2
- Prefixes Announced (all): 111
- Prefixes Announced (v4): 101
- Prefixes Announced (v6): 10
- BGP Peers Observed (all): 277
- BGP Peers Observed (v4): 274
- BGP Peers Observed (v6): 142
- IPs Originated (v4): 2,769,408
- AS Paths Observed (v4): 125,513
- AS Paths Observed (v6): 23,780
- Average AS Path Length (all): 4.544
- Average AS Path Length (v4): 4.592
- Average AS Path Length (v6): 4.293

Below this, a pie chart titled "AS137 IPv4 Peers" shows the distribution of peers:

ASN	Name
AS1299	Telia Company AB
AS174	Cogent Communications
AS6939	Hurricane Electric LLC
AS21320	GEANT Limited
AS9002	RETN Limited
AS20965	GEANT Limited

A red box highlights the pie chart and the table, and a red callout points from it to the text "Peer con cui l'AS137 «interagisce» più frequentemente".

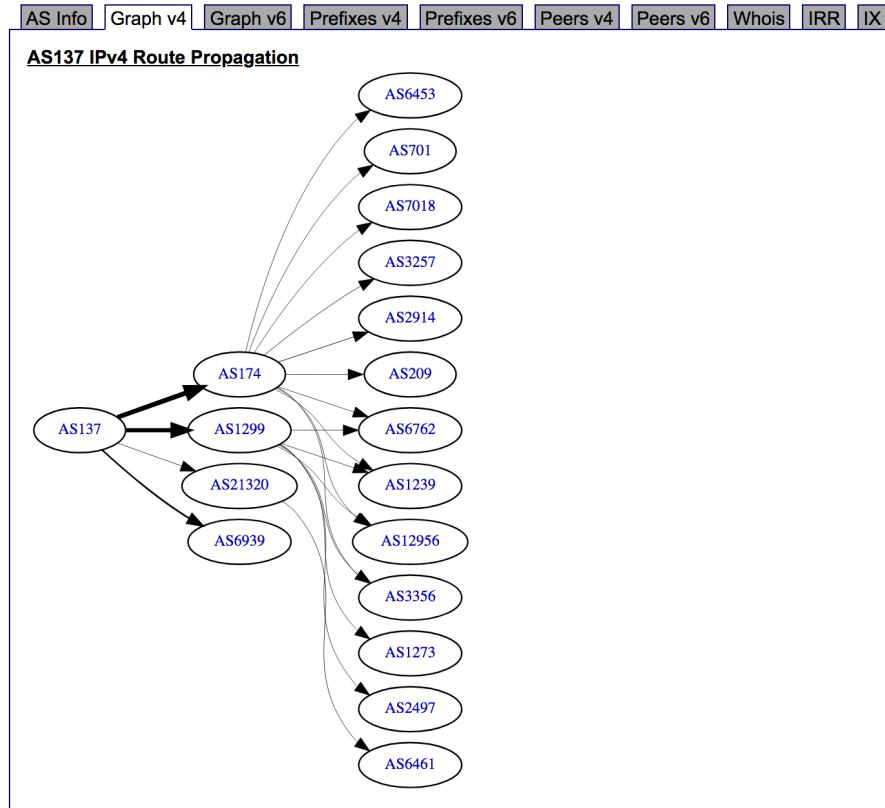
Peer con cui l'AS137  
«interagisce» più  
frequentemente

# 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

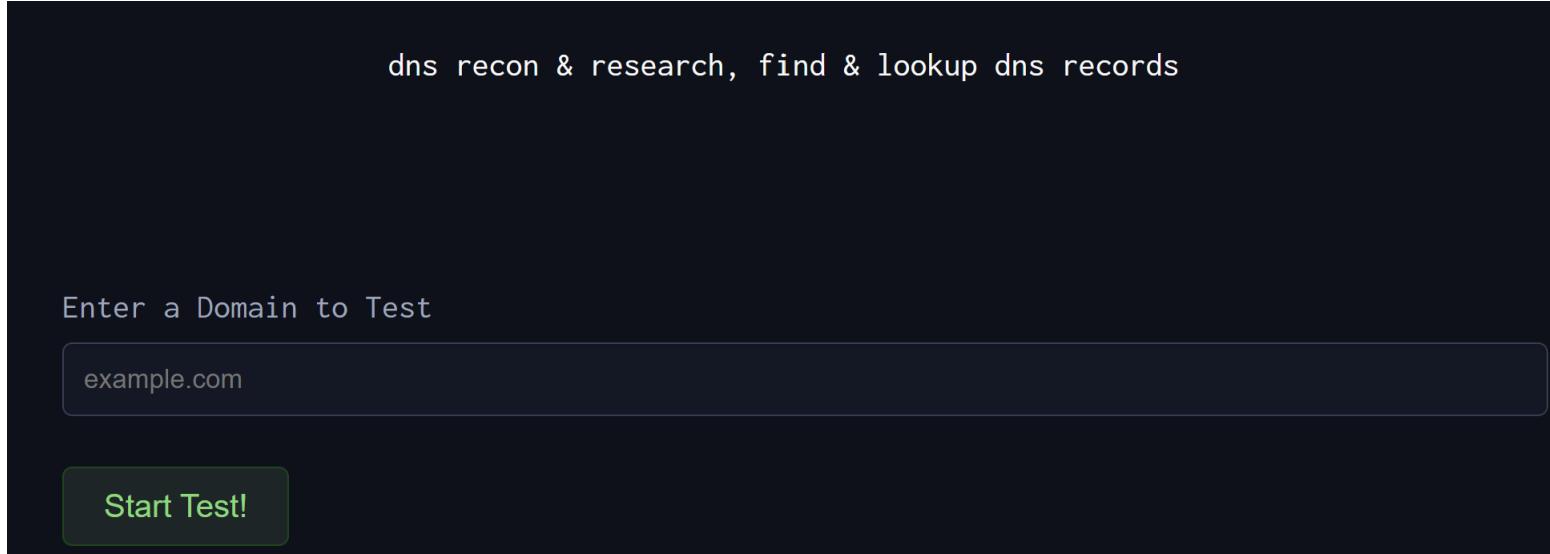
---

- <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

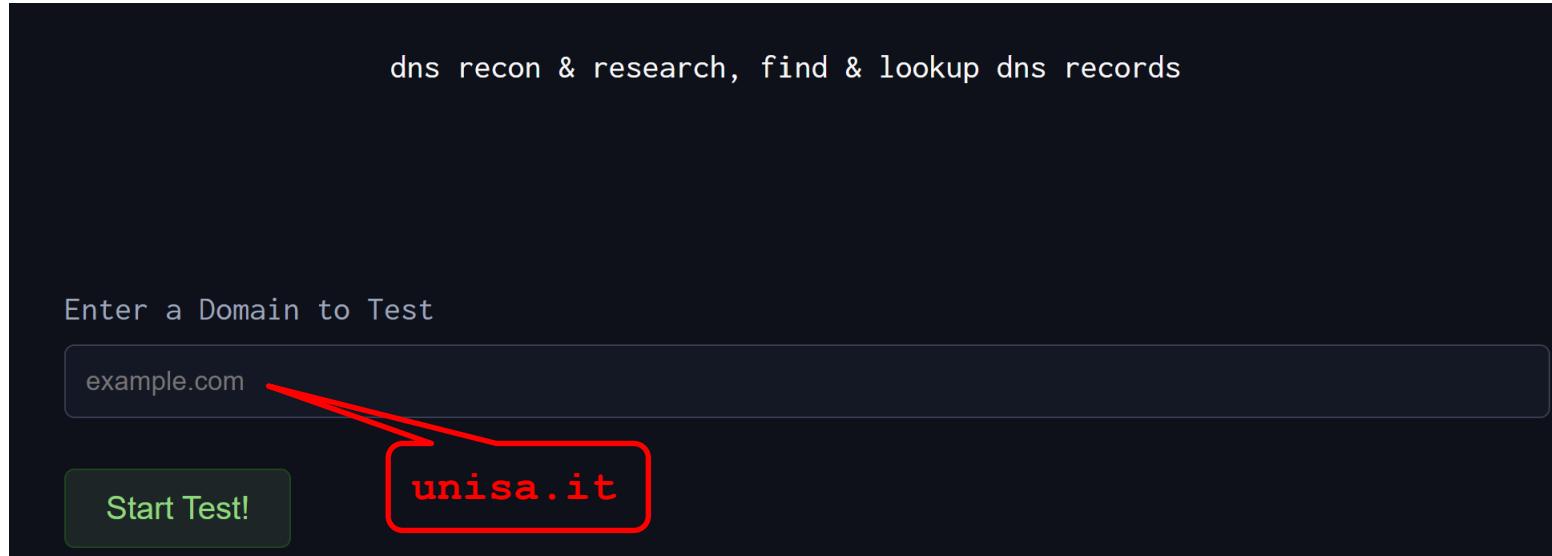
- Lo strumento richiede soltanto l'inserimento di un dominio



# Utilizzo di Risorse Web-Based

## Asset Discovery – DNSdumpster

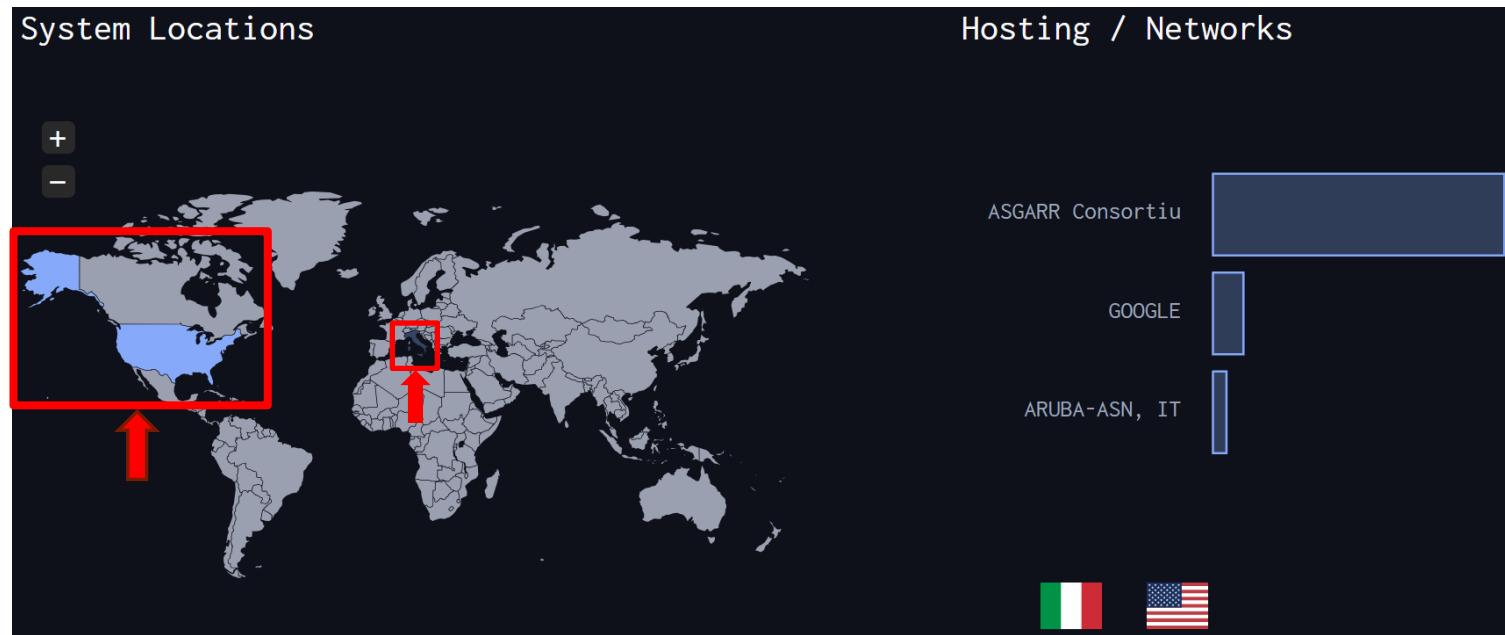
- Lo strumento richiede soltanto l'inserimento di un dominio



# 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	<a href="#">ASN: 137</a>	ASGARR Consortium GARR, IT
	esa-mx-1.unisa.it	193.204.0.0/15	Italy
unisamx.2.unisa.it	193.205.160.11	<a href="#">ASN: 137</a>	ASGARR Consortium GARR, IT
	esa-mx-2.unisa.it	193.204.0.0/15	Italy
6000r.unisa.it	193.205.160.190	<a href="#">ASN: 137</a>	ASGARR Consortium GARR, IT
	6000r.unisa.it	193.204.0.0/15	Italy
adisu-sistemi.unisa.it	193.205.185.17	<a href="#">ASN: 137</a>	ASGARR Consortium GARR, IT
	adisu-sistemi.unisa.it	193.204.0.0/15	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	ASN:137	ASGARR Consortium GARR, IT
	esa-mx-1.unisa.it	193.204.0.0/15	Italy
unisamx.2.unisa.it	193.205.160.11	ASN:137	ASGARR Consortium GARR, IT
	esa-mx-2.unisa.it	193.204.0.0/15	Italy
6000r.unisa.it	193.205.160.190	ASN:137	ASGARR Consortium GARR, IT
	6000r.unisa.it	193.204.0.0/15	Italy
adisu-sistemi.unisa.it	193.205.185.17	ASN:137	ASGARR Consortium GARR, IT
	adisu-sistemi.unisa.it	193.204.0.0/15	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

### Welcome to Robtex!

hostname, ipnumber, route or AS-number

GO

#### What is Robtex used for?

Robtex is used for various kinds of research of IP numbers, Domain names, etc

Are you a normal IT guy doing data forensics, investigating competitors, tracking spammers or hackers or a virus, or just curious? No matter what, this should be the first place to go

#### What does Robtex do?

Robtex uses various sources to gather public information about IP numbers, domain names, host names, Autonomous systems, routes etc. It then indexes the data in a big database and provide free access to the data.

We aim to make the fastest and most comprehensive free DNS lookup tool on the Internet.

Our database now contains [billions of documents](#) of internet data collected over more than a decade.

#### How to use Robtex?

Enter an IP address or hostname in the field above, and click "GO" to look up technical information. From the resulting page you can navigate further between the different tabs.

We have released a subset of this data by an API available at [mashape](#). We also provide a few other APIs:

For more information, see the [Robtex API](#)

# Utilizzo di Risorse Web-Based

## Asset Discovery – Robtex

➤ <https://www.robtex.com/>

➤ Permette di cercare informazioni riguardo domini e servizi di rete



Welcome to Robtex!

hostname, ipnumber, route or AS-number  GO

**What is Robtex used for?**

Robtex is used for various kinds of research of IP numbers, Domain names, etc

Are you a normal IT guy doing data forensics, investigating competitors, tracking spammers or hackers or a virus, or just curious? No matter what, this should be the first place to go

**What does Robtex do?**

Robtex uses various sources to gather public information about IP numbers, domain names, host names, Autonomous systems, routes etc. It then indexes the data in a big database and provide free access to the data.

We aim to make the fastest and most comprehensive free DNS lookup tool on the Internet.

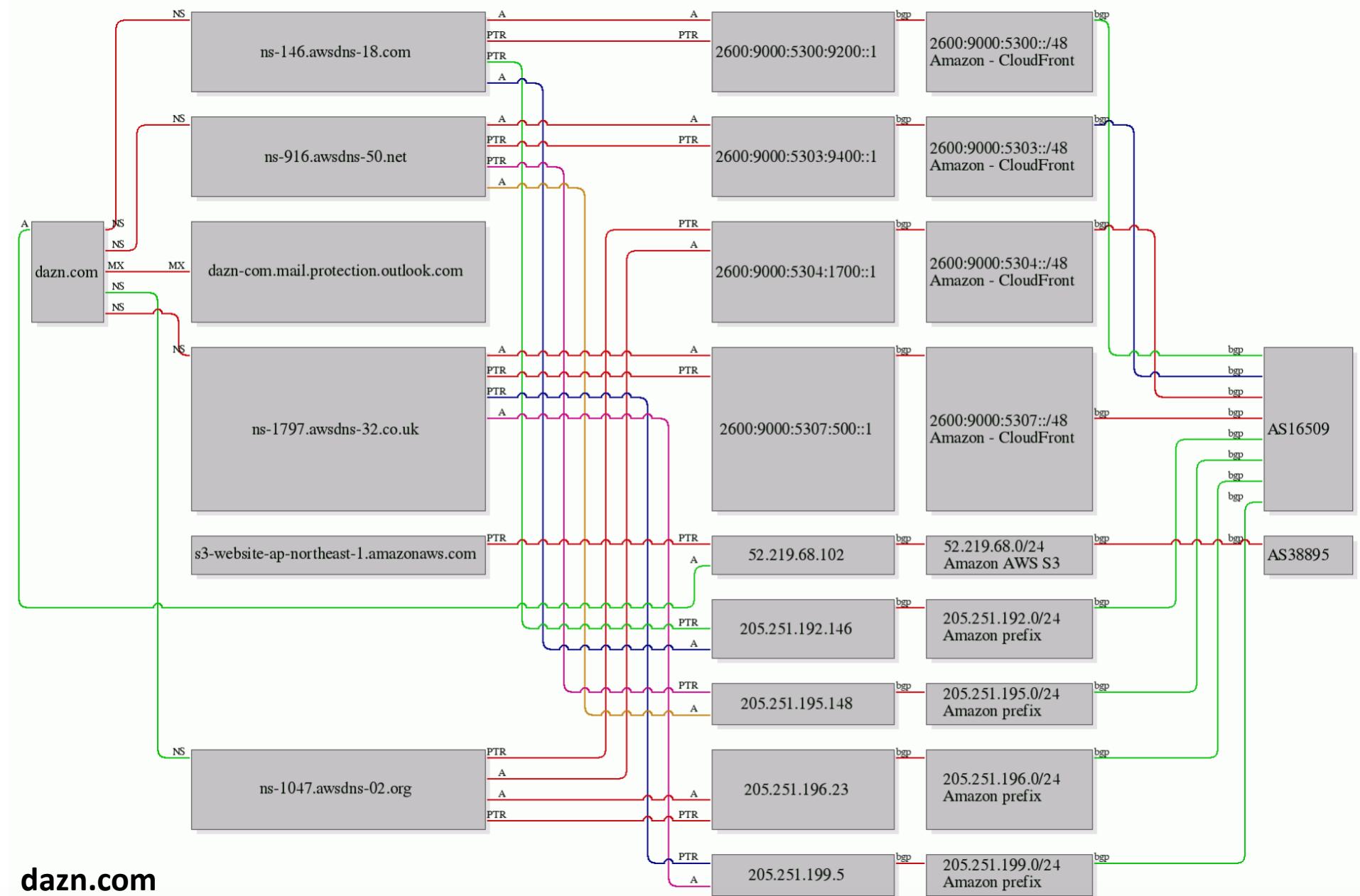
Our database now contains billions of documents of internet data collected over more than a decade.

**How to use Robtex?**

Enter an IP address or hostname in the field above, and click "GO" to look up technical information. From the resulting page you can navigate further between the different tabs.

We have released a subset of this data by an API available at [mashape](#). We also provide a few other APIs.

For more information, see the [Robtex API](#)



## Information Gathering

# Utilizzo di Risorse Web-Based

## Web Archiving

---

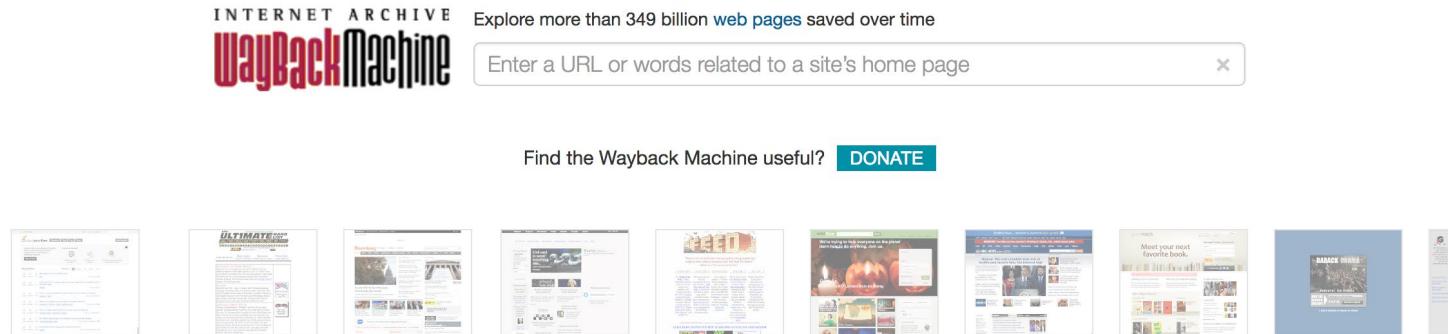
- Raccolta di «parti» del World Wide Web (WWW) per garantire che le informazioni siano conservate in un archivio per scopi/usi futuri
  
- Utilizzo di *Web Crawler* per raccogliere enormi quantità di informazioni
  - Heritrix
  - HTrack
  - Etc
  
- Estremamente utile per capire la periodicità di aggiornamento 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



[Wayback Machine Availability API](#)  
Build your own tools.

[WordPress Broken Link Checker](#)  
Banish broken links from your blog.

[404 Handler for Webmasters](#)  
Help users get where they were going.



### Subscription Service

Archive-It enables you to capture, manage and search collections of digital content without any technical expertise or hosting facilities. [Visit Archive-It to build and browse the collections.](#)

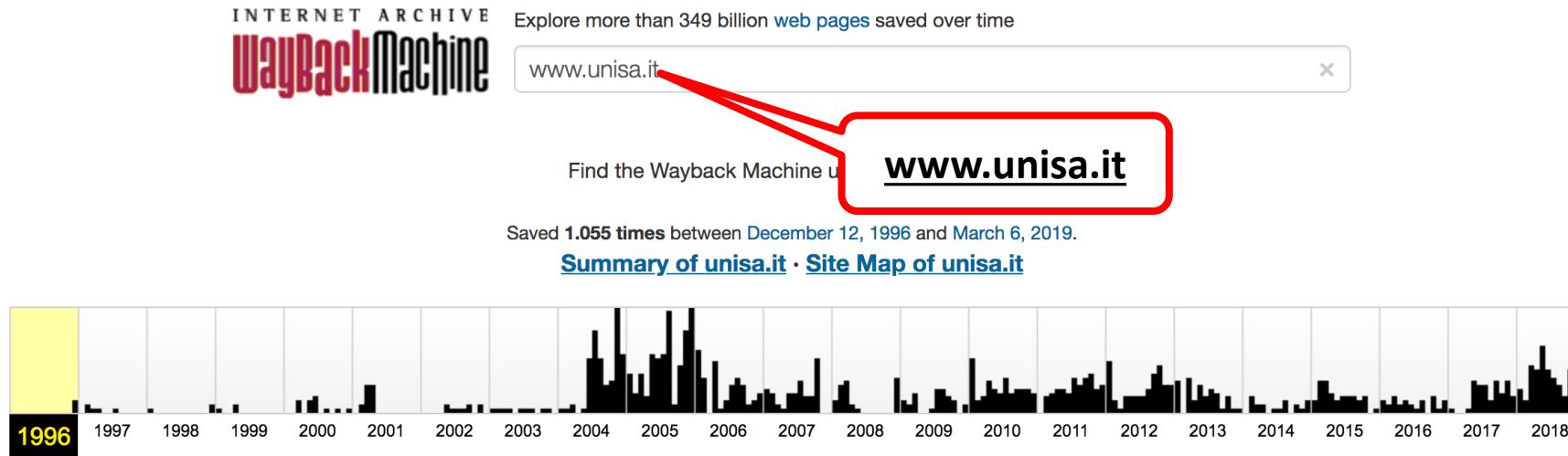


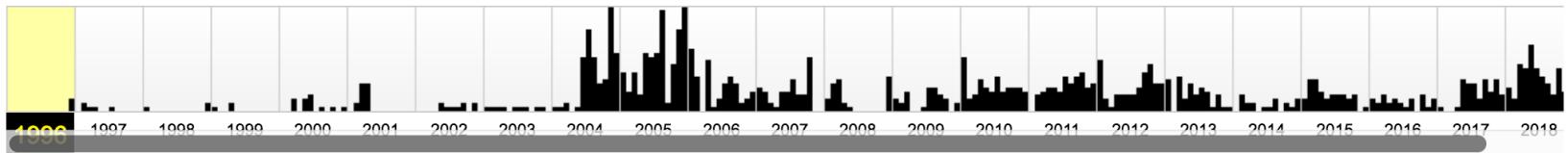
### Save Page Now

[SAVE PAGE](#)  
Capture a web page as it appears now for use as a trusted citation in the future.  
Only available for sites that allow crawlers.

# Utilizzo di Risorse Web-Based

## Web Archiving – Wayback Machine – Esempio 1





## Information Gathering

# Utilizzo di Risorse Web-Based

## Web Archiving – Wayback Machine – Esempio 1

---

*Benvenuti sul Web Server dell' Università degli Studi di Salerno*



Università degli Studi di Salerno

- [INFORMAZIONI GENERALI](#)
- [FACOLTÀ](#)
- [DIPARTIMENTI ed ISTITUTI](#)
- [CENTRI BIBLIOTECARI](#)

- [GUIDA DELLO STUDENTE](#)
- [Programma SOCRATES/ERASMUS](#)
- [INIZIATIVE CULTURALI](#)
- [Storia dell'Ateneo](#)



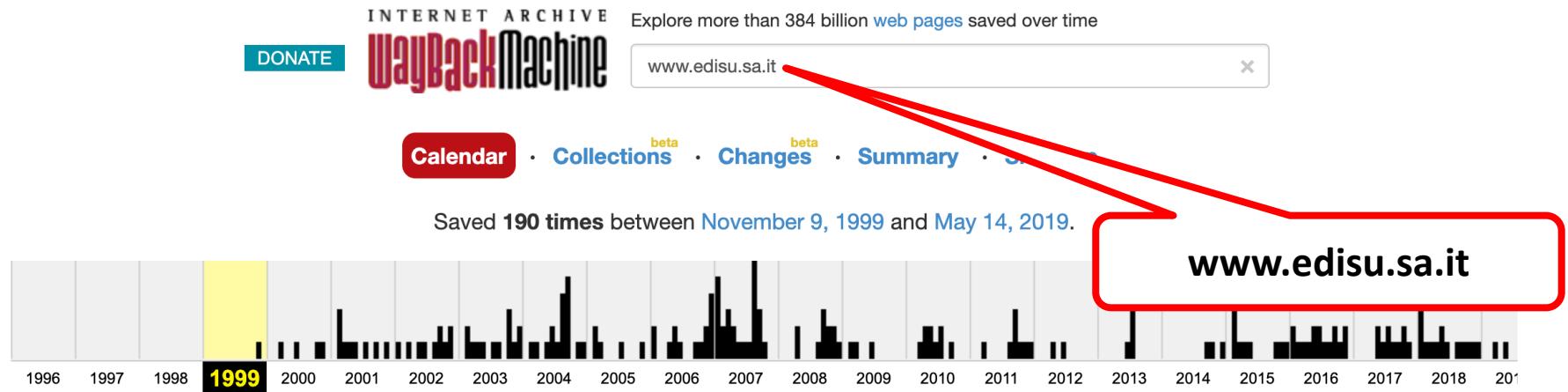
LAST UPDATE 12 Jun 1996

DIA Dipartimento di Informatica ed Applicazioni / [webmaster@dia.unisa.it](mailto:webmaster@dia.unisa.it)

**Primo sito Web dell'Università degli Studi di Salerno**

# Utilizzo di Risorse Web-Based

## Web Archiving – Wayback Machine – Esempio 2



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

31

JAN					FEB						MAR						APR											
					1	2		1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3
3	4	5	6	7	8	9		7	8	9	10	11	12	13	7	8	9	10	11	12	13	4	5	6	7	8	9	10
10	11	12	13	14	15	16		14	15	16	17	18	19	20	14	15	16	17	18	19	20	11	12	13	14	15	16	17
17	18	19	20	21	22	23		21	22	23	24	25	26	27	21	22	23	24	25	26	27	18	19	20	21	22	23	24
24	25	26	27	28	29	30		28							28	29	30	31				25	26	27	28	29	30	
31																												
MAY					JUN						JUL						AUG											
					1			1	2	3	4	5				1	2	3				1	2	3	4	5	6	7
2	3	4	5	6	7	8		6	7	8	9	10	11	12	4	5	6	7	8	9	10	8	9	10	11	12	13	14
9	10	11	12	13	14	15		13	14	15	16	17	18	19	11	12	13	14	15	16	17	15	16	17	18	19	20	21
16	17														19	20	21	22	23	24		22	23	24	25	26	27	28
23	24														26	27	28	29	30	31		29	30	31				
30	31																											
SEP					OCT						NOV						DEC											
					1	2	3	4			1	2			1	2	3	4	5	6		1	2	3	4			
5	6	7	8	9	10	11		3	4	5	6	7	8	9	7	8	9	10	11	12	13	5	6	7	8	9	10	11
12	13	14	15	16	17	18		10	11	12	13	14	15	16	14	15	16	17	18	19	20	12	13	14	15	16	17	18
19	20	21	22	23	24	25		17	18	19	20	21	22	23	21	22	23	24	25	26	27	19	20	21	22	23	24	25
26	27	28	29	30				24	25	26	27	28	29	30	28	29	30					26	27	28	29	30	31	
								31																				

# Utilizzo di Risorse Web-Based

## Web Archiving – Wayback Machine – Esempio 2



[Regione Campania](#)

### E.D.I.S.U.

Ente per il Diritto allo Studio Universitario [Università di Salerno](#)  
Salerno

[Menu' Principale](#)

- [Chi Siamo](#)
- [Dove Siamo](#)
- [Numeri Telefonici](#)
- [Ulteriori Informazioni](#)
- [Links](#)

[Download](#)

- [Bando Borsa di Studio 1998/99](#)
- [Bando Posto Alloggio 1998/99](#)
- [Bando Tessineri Mensa](#)
- [Bando Ricerca Tesi](#)
- [Bando Contributi Integrativi Erasmus](#)

[Primi Anni](#)

- [Primi Anni \(definitive\)](#)
- [Ammessi](#)
- [Concessioni](#)
- [Mancate concessioni](#)
- [Esclusi](#)

[Anni Successivi](#)

- [Anni Successivi \(definitive\)](#)
- [Ammessi](#)
- [Concessioni](#)
- [Mancate Concessioni](#)
- [Esclusi](#)

[Posti Alloggio](#)

- [\(Graduatorie Definitive\)](#)
- [Concessioni](#)
- [Esclusioni](#)
- [Mancate Concessioni](#)
- [Idoneo](#)

**Primo sito Web dell'E.D.I.S.U.**

# Utilizzo di Risorse Web-Based

## Web Archiving – Wayback Machine – Esempio 3



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

JAN					FEB							MAR							APR								
		1	2	3	1	2	3	4	5	6	7	1	2	3	4	5	6	7	1	2	3	4					
4	5	6	7	8	9	10	8	9	10	11	12	13	14	8	9	10	11	12	13	14	5	6	7	8	9	10	11
11	12	13	14	15	16	17	15	16	17	18	19	20	21	15	16	17	18	19	20	21	12	13	14	15	16	17	18
18	19	20	21	22	23	24	22	23	24	25	26	27	28	22	23	24	25	26	27	28	19	20	21	22	23	24	25
25	26	27	28	29	30	31								29	30	31					26	27	28	29	30		
MAY					JUN							JUL							AUG								
		1	2		1	2	3	4	5	6		1	2	3	4									1			
3	4	5	6	7	8	9	7	8	9	10	11	12	13	5	6	7	8	9	10	11	2	3	4	5	6	7	8
10	11	12	13	14	15	16	14	15	16	17	18	19	20	12	13	14	15	16	17	18	9	10	11	12	13	14	15
17	18	19												21	22	23	24	25			16	17	18	19	20	21	22
24	25	26												28	29	30	31				23	24	25	26	27	28	29
31																				30	31						
SEP					OCT							NOV							DEC								
	1	2	3	4	5		1	2	3	4	5	6	7	3	4	5	6	7	1	2	3	4	5				
6	7	8	9	10	11	12	4	5	6	7	8	9	10	8	9	10	11	12	13	14	6	7	8	9	10	11	12
13	14	15	16	17	18	19	11	12	13	14	15	16	17	15	16	17	18	19	20	21	13	14	15	16	17	18	19
20	21	22	23	24	25	26	18	19	20	21	22	23	24	22	23	24	25	26	27	28	20	21	22	23	24	25	26
27	28	29	30				25	26	27	28	29	30	31	29	30						27	28	29	30	31		

**Il primo snapshot di  
www.google.com risale all'11  
novembre 1998**

# Utilizzo di Risorse Web-Based

## Web Archiving – Wayback Machine – Esempio 3

---

### Welcome to Google

[Google Search Engine Prototype](#)

[Might-work-some-of-the-time-prototype that is much more up to date.](#)

**Primo sito Web di Google**

# Utilizzo di Risorse Web-Based

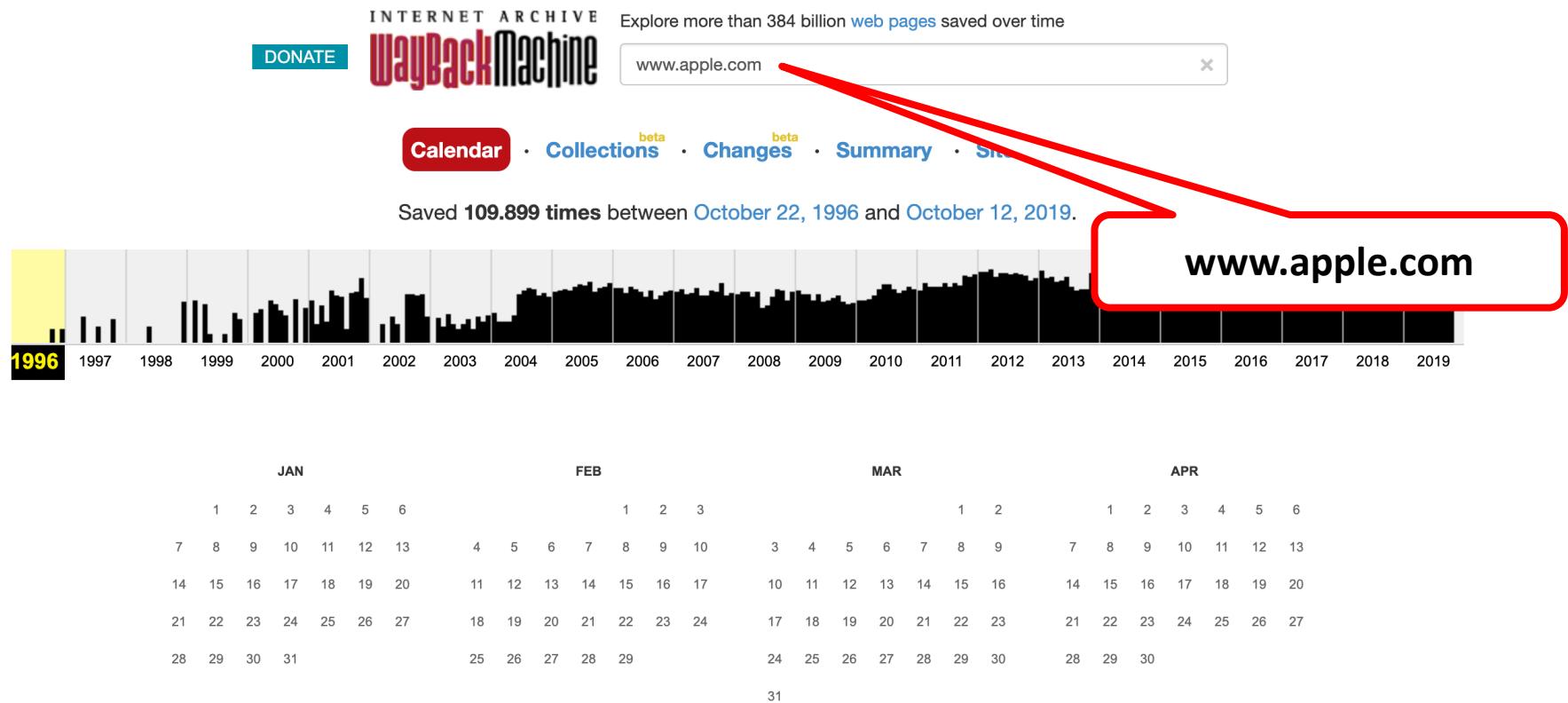
## Web Archiving – Wayback Machine – Esempio 3



Primo sito Web di Google

# Utilizzo di Risorse Web-Based

## Web Archiving – Wayback Machine – Esempio 4



JAN						FEB						MAR						APR									
1	2	3	4	5	6		1	2	3			1	2		1	2		1	2		1	2	3	4	5	6	
7	8	9	10	11	12	13	4	5	6	7	8	9	10	3	4	5	6	7	8	9	7	8	9	10	11	12	13
14	15	16	17	18	19	20	11	12	13	14	15	16	17	10	11	12	13	14	15	16	14	15	16	17	18	19	20
21	22	23	24	25	26	27	18	19	20	21	22	23	24	17	18	19	20	21	22	23	21	22	23	24	25	26	27
28	29	30	31				25	26	27	28	29			24	25	26	27	28	29	30	28	29	30				
														31													
MAY						JUN						JUL						AUG									
		1	2	3	4			1				1	2	3	4	5	6				1	2	3				
5	6	7	8	9	10	11	2	3	4	5	6	7	8	7	8	9	10	11	12	13	4	5	6	7	8	9	10
12	13	14	15	16	17	18	9	10	11	12	13	14	15	14	15	16	17	18	19	20	11	12	13	14	15	16	17
19	20	21												23	24	25	26	27			18	19	20	21	22	23	24
26	27	28												30	31						25	26	27	28	29	30	31
SEP						O	NOV						DEC														
1	2	3	4	5	6	7	1						1	2		1	2		1	2	3	4	5	6	7		
8	9	10	11	12	13	14	6	7	8	9	10	11	12	3	4	5	6	7	8	9	8	9	10	11	12	13	14
15	16	17	18	19	20	21	13	14	15	16	17	18	19	10	11	12	13	14	15	16	15	16	17	18	19	20	21
22	23	24	25	26	27	28	20	21	22	23	24	25	26	17	18	19	20	21	22	23	22	23	24	25	26	27	28
29	30						27	28	29	30	31			24	25	26	27	28	29	30	29	30	31				

Il primo snapshot di [www.apple.com](http://www.apple.com)  
risale al 22 ottobre 1996

# Utilizzo di Risorse Web-Based

## Web Archiving – Wayback Machine – Esempio 4

The screenshot shows the homepage of the first Apple website, which was a single page with a white background and black text. At the top, there's a navigation bar with links for "Find It", "Product Information", "Customer Support", "Technology & Research", "Developer World", "Groups & Interests", "Resources Online", and "About Apple". Below the navigation, there's a section titled "Welcome to Apple" with three links: "POWERBOOK & CD-ROM: Cool New Ways to Go Mobile", "FOCUS: Bring Learning Home - Classrooms of Tomorrow", and "QUARTERLY RESULTS: Apple Scores Profit". A sidebar on the left is titled "Apple Sites" and lists regional sites for Asia, Australia, Belgium, Canada, Chile, and Denmark. Another sidebar at the bottom left is titled "Where to Buy". The main content area contains several news items: "New PowerBook Family" (about the 1400 series), "Faster GeoPort" (about the new version of the GeoPort adapter), "New Color Solutions" (about the Color LaserWriter 12/660 PS and PhotoGrade Print Kit), and "Performa News" (about the Performa 6360 and 6400/200 Video Editing Edition). There's also a section titled "Chat with Guy" featuring an interview with Steve Jobs.

Primo sito Web di Apple

# Utilizzo di Risorse Web-Based

## Ricerca Informazioni Personali – Social Network

---

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

# Nobody knows people like Pipl.

The #1 source for online identity and trust.

See How it Works

# 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

The screenshot shows the Pipl search interface. At the top, there's a search bar with a placeholder 'Search for people' and a 'Location (optional)' field. Below the search bar, the Pipl logo is on the left, and a search button with a magnifying glass icon is on the right. The main content area displays a profile for 'Arcangelo Castiglione'. It includes a thumbnail image of a castle at sunset, the name 'Arcangelo Castiglione' in bold, and the gender 'Male'. Below the name, there are sections for 'CAREER', 'EDUCATION', 'USERNAME', 'PLACES', and 'ASSOCIATED WITH', each with a corresponding icon and a redacted value. A red callout box on the left side of the screen highlights the search input field and the 'MORE OPTIONS' link, with the text: 'Query effettuata usando un numero di cellulare, mai utilizzato per operazioni online'.

Query effettuata usando  
un numero di cellulare,  
mai utilizzato per  
operazioni online

pipl

Search By

Phone  + MORE OPTIONS

Location (optional)

Arcangelo Castiglione

Male

CAREER:

EDUCATION:

USERNAME:

PLACES:

ASSOCIATED WITH:

# Utilizzo di Risorse Web-Based

## Ricerca Informazioni Personali – SPOKEO

➤ <https://www.spokeo.com/>

The screenshot shows the Spokeo search interface. At the top left is the Spokeo logo. Below it is a large search bar with the placeholder text "Enter a Name, Phone Number, Address or Email". To the right of the search bar is a green button labeled "SEARCH NOW". Above the search bar, there are four input fields with labels: "NAME", "EMAIL", "PHONE", and "ADDRESS". Below the search bar, a descriptive text reads: "Search by name, phone, address, or email to confidentially lookup information about people you know such as yourself, friends, family, acquaintances, and old classmates.".

# Utilizzo di Risorse Web-Based

## Ricerca Informazioni Personali – SPOKEO – Esempio

➤ <https://www.spokeo.com/>

People Search > Springsteen > Bruce Springsteen > New Jersey > Colts Neck > **Bruce F Springsteen**



### Bruce F Springsteen, Age 72

- ✓ Current Address: Muhlenbrink Rd, Colts Neck, NJ
- ✓ Past Addresses: Colts Neck NJ, Rumson NJ +4 more
- ✓ Phone Number: (310) 207- [REDACTED] +1 phone
- ✓ Email Address: b [REDACTED] @pty.com

**UNLOCK PROFILE**

● Contacts (3)   ● Locations (7)   ● Family (5)   ● Social (29)   ● Court (5)   ● And More

# Utilizzo di Risorse Web-Based

## Ricerca Informazioni Personali

➤ <https://www.instantcheckmate.com/>

The screenshot shows the homepage of InstantCheckmate. At the top, there's a navigation bar with links for People Search, Reverse Phone Lookup, Criminal Records, Inmate Search, Contact, and a green LOGIN button. To the left of the main content area is the InstantCheckmate logo and a yellow badge from the BBB rating A+. In the center, there's a testimonial bubble with a thumbs-up icon and the text "I am amazed by the results!" followed by "- David F., Real User". Below this, the main heading reads "Public Records Search Service" in large, bold letters. Underneath, a sub-headline says "Find Contact Information, Location Data, Criminal Records, Phone Numbers, Social Media Profiles, Death Records and Much More!". A blue call-to-action button at the bottom left says "START HERE - Try searching a friend, relative, yourself, old schoolmates or someone else you might know...". Below this are four input fields: "First Name" (placeholder "e.g. John"), "Last Name" (placeholder "e.g. Smith"), "City" (placeholder "e.g. Chicago"), and "Location" (dropdown menu showing "All States" with a dropdown arrow). To the right of these fields is a checkbox labeled "This is me" and a large green "SEARCH" button.

Information Gathering

# Utilizzo di Risorse Web-Based

## Ricerca Informazioni Personali

➤ <https://www.instantcheckmate.com/>

Robert M Van Winkle

Start Monitoring Buy PDFs Share Report Unlock More Information

50% REPORT ACCESSED Viewing social will bring you to 60% report access

Report Navigation

- Personal
- Related People
- Contact
- Location
- Criminal Records
- Social
- Licenses
- Sex Offenders
- Horoscopes

Premium Data Want to see EVEN MORE information? Unlock access to Premium Data on Robert M Van Winkle.

Personal Information

Flag As Inaccurate: Rate This Section:

Robert M Van Winkle's Personal Information

Name	Birth Information			
First Name Robert	Middle Name M	Last Name Van Winkle	Age 49	Birth Date October 31, 1967
AKAs				
Robby M Vanwinkle <a href="#">Remove</a>	Robert M Winkle <a href="#">Remove</a>	M Vanwinkle Robert <a href="#">Remove</a>	Astrological Sign Scorpio	
Robert J Matthews <a href="#">Remove</a>	Robert M Van Vinkle <a href="#">Remove</a>	Robert M Matthews <a href="#">Remove</a>		
Robert Matthew Van Winkle <a href="#">Remove</a>	Rob Vanwinkle <a href="#">Remove</a>	Vanilla Ice <a href="#">Remove</a>		

Possible Photos

Click images to zoom in:

Remove Remove Remove Remove

Jobs

# Utilizzo di Risorse Web-Based

## Ricerca Indirizzi E-mail

➤ <https://hunter.io>

The screenshot shows the homepage of hunter.io. At the top, there is a navigation bar with the logo 'hunter' (a red icon of a person with a bow), 'Product', 'Pricing', 'Resources', 'Company', 'Sign in', and a red 'Sign up' button. Below the navigation bar, the main headline reads 'Connect with anyone.' followed by the subtext 'Hunter lets you find professional email addresses in seconds and connect with the people that matter for your business.' A large search bar at the bottom contains the placeholder 'company.com' and a red 'Find email addresses' button. Below the search bar, a note says 'Enter a domain name to launch the search. For example, [hunter.io](#)'.

# Utilizzo di Risorse Web-Based

## Ricerca Indirizzi E-mail

➤ <https://hunter.io>

The screenshot shows the homepage of hunter.io. At the top, there is a navigation bar with the logo 'hunter' (a red arrow icon followed by the word 'hunter' in red), 'Product' (with a dropdown arrow), 'Pricing', 'Resources' (with a dropdown arrow), 'Company' (with a dropdown arrow), 'Sign in' (in grey), and a red 'Sign up' button. Below the navigation bar, the main headline reads 'Connect with anyone.' in large, bold, black font. A subtext below it says 'Hunter lets you find professional email addresses in seconds and connect with the people that matter for your'. A red callout bubble points from the word 'unisa.it' in the subtext towards the search bar. The search bar itself has a placeholder 'company.com' and a red 'Find email addresses' button. Below the search bar, there is a text input field with the placeholder 'Enter a domain name to launch the search. For example, [hunter.io](#)'.

# Utilizzo di Risorse Web-Based

## Ricerca Indirizzi E-mail

➤ <https://hunter.io>

E-mail relative ad  
unisa.it

unisa.it

Find email addresses

Most common pattern: {f}{last}@unisa.it

1437 email addresses

t pozzoli@unisa.it 2 sources

g codemo@unisa.it 1 source

g selli@unisa.it 3 sources

p mpiglia@unisa.it 3 sources

r rrentino@unisa.it 7 sources

1432 more result for unisa.it. [Sign up](#) or [log in](#) to access the full results.

Sign up to uncover the email addresses, get the full results, search filters, CSV downloads and more. Get 25 free searches/month.

# Utilizzo di Risorse Web-Based

## Ricerca su Data Breach

➤ [haveibeenpwned.com](https://haveibeenpwned.com)

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

The screenshot shows the homepage of haveibeenpwned.com. At the top, there is a navigation bar with links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main feature is a large button with the text '';--have i been pwned?'. Below it, a subtext reads 'Check if you have an account that has been compromised in a data breach'. There is a form with an 'email address' input field and a 'pwned?' button. At the bottom, there is a call-to-action button for 'Generate secure, unique passwords for every account' and a link to 'Learn more at 1Password.com'. Below that, there is a 'Why 1Password?' link. The footer contains four pieces of information: '346 pwned websites', '6,931,949,148 pwned accounts', '90,767 pastes', and '111,989,443 paste accounts'. The word 'Information Gathering' is visible at the very bottom.

email address **pwned?**

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

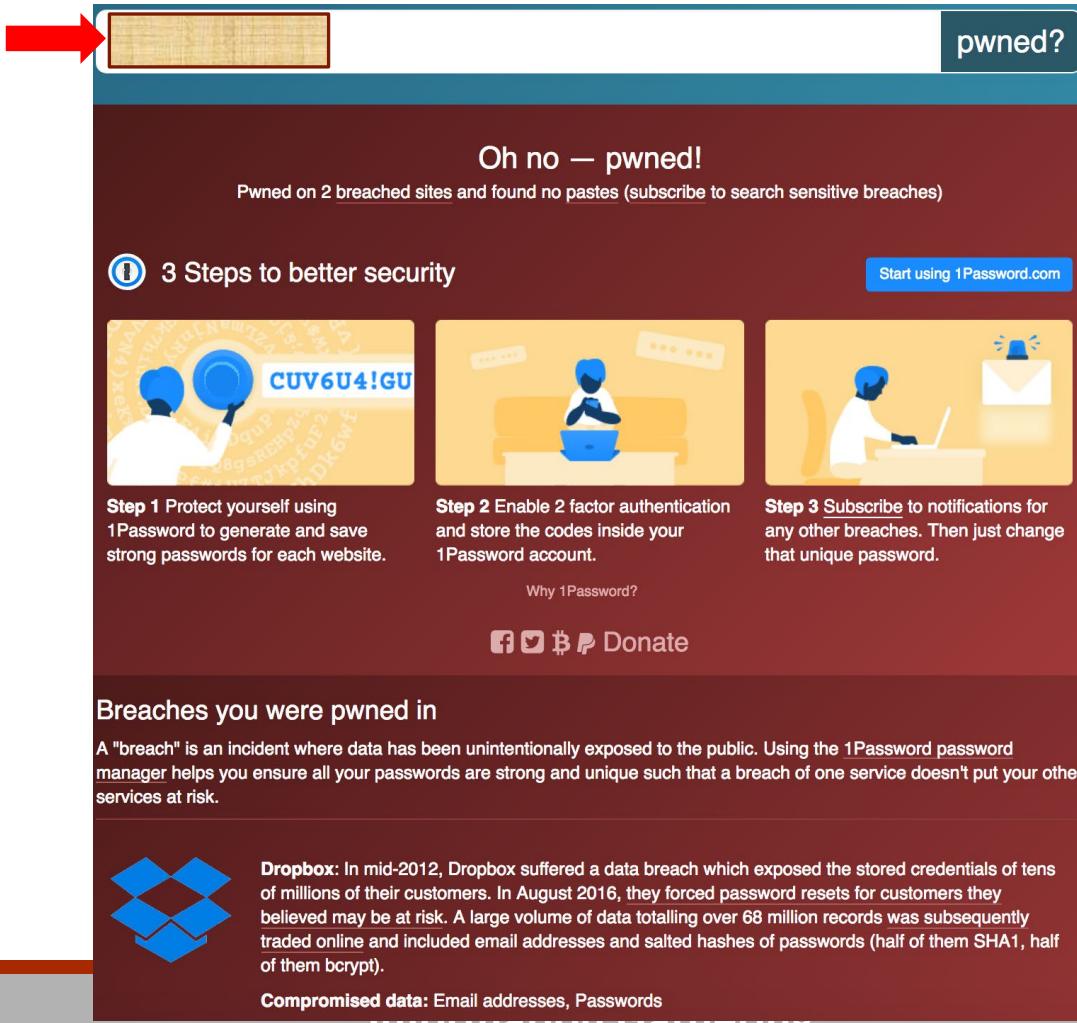
Why 1Password?

346 pwned websites    6,931,949,148 pwned accounts    90,767 pastes    111,989,443 paste accounts

Information Gathering

# Utilizzo di Risorse Web-Based

## Ricerca su Data Breach



A screenshot of the 1Password "pwned?" service interface. At the top, there is a search bar with a red arrow pointing to it, containing the text "pwned?". To the right of the search bar is a button labeled "pwned?". Below the search bar, the text "Oh no — pwned!" is displayed in large white letters on a dark background. A subtext below it says "Pwned on 2 breached sites and found no pastes (subscribe to search sensitive breaches)".

**3 Steps to better security**

- Step 1** Protect yourself using 1Password to generate and save strong passwords for each website.
- Step 2** Enable 2 factor authentication and store the codes inside your 1Password account.
- Step 3** Subscribe to notifications for any other breaches. Then just change that unique password.

[Start using 1Password.com](#)

**Breaches you were pwned in**

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

 **Dropbox:** In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

**Compromised data:** Email addresses, Passwords

# Utilizzo di Risorse Web-Based

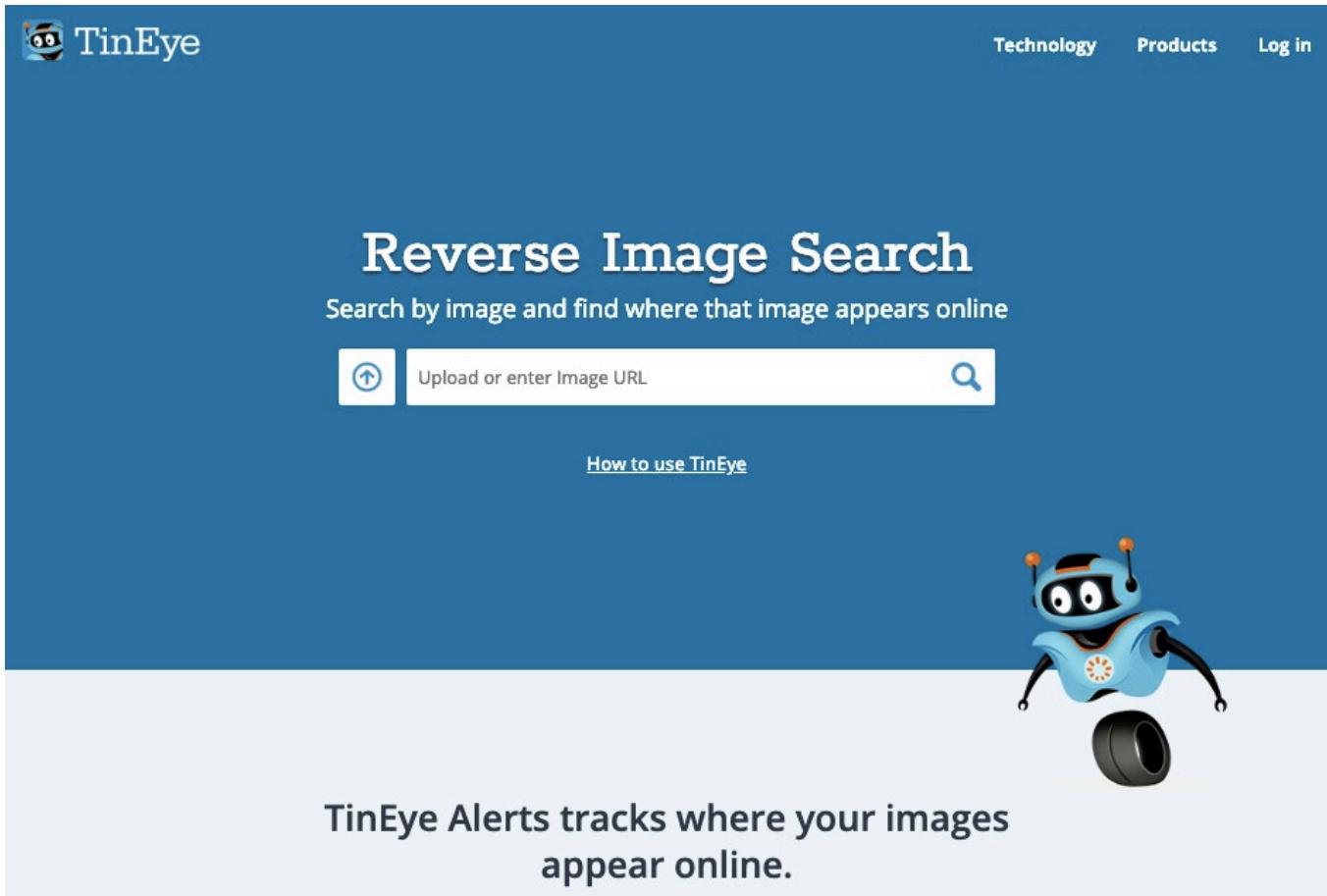
## Reverse Image Search – TinEye

---

- <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



The screenshot shows the TinEye homepage with a blue header and a white main content area. The header features the TinEye logo (a cartoon eye icon) and the word "TinEye". On the right side of the header are links for "Technology", "Products", and "Log in". The main title "Reverse Image Search" is prominently displayed in large, bold, white font. Below it, a subtitle reads "Search by image and find where that image appears online". There is a file upload input field with an "Upload or enter Image URL" placeholder and a magnifying glass search icon. A "How to use TinEye" link is located below the search bar. In the bottom right corner of the main area, there is a cartoon illustration of a blue robot with a single large eye, two antennae, and a small propeller on its back. The bottom section of the page has a light gray background with the text "TinEye Alerts tracks where your images appear online." centered.

TinEye Alerts tracks where your images appear online.

# Utilizzo di Risorse Web-Based

## Reverse Image Search – TinEye – Esempio 1

The screenshot shows the TinEye homepage with a blue header. The header includes the TinEye logo, navigation links for 'Technology', 'Products', and 'Log in', and a search bar. Below the header, the main title 'Reverse Image Search' is displayed in large white text, followed by the subtitle 'Search by image and find where that image appears online'. There is an input field with a file upload icon and a search button. A red callout box with the text 'Carico un\'immagine' (Load an image) points to the input field. A small robot character is on the right. A banner at the bottom states 'TinEye Alerts tracks where your images appear online.'

Carico  
un'immagine

Technology Products Log in

## Reverse Image Search

Search by image and find where that image appears online

Upload or enter Image URL

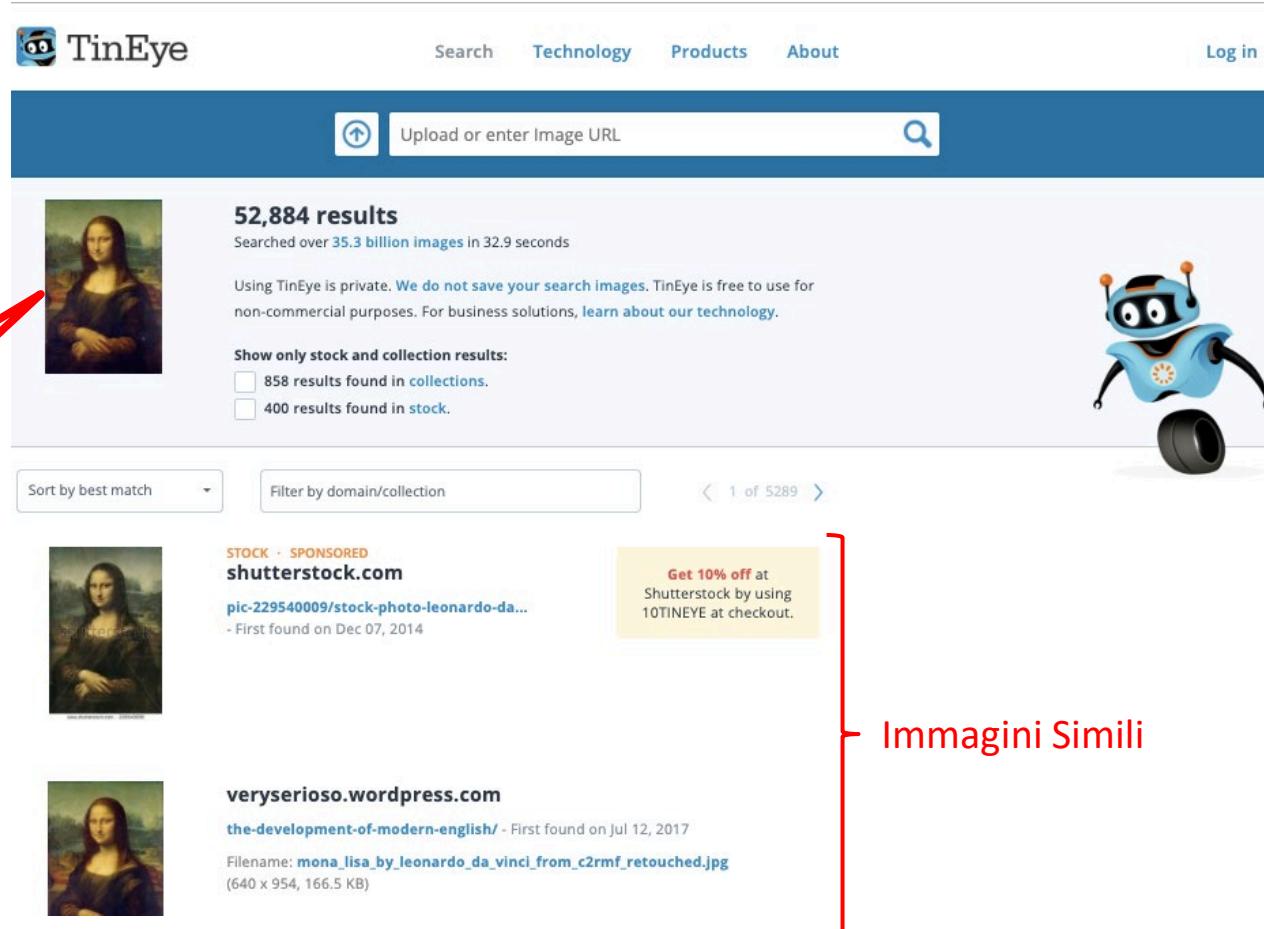
How to use TinEye

TinEye Alerts tracks where your images appear online.

# Utilizzo di Risorse Web-Based

## Reverse Image Search – TinEye – Esempio 1

**Immagine caricata**



The screenshot shows the TinEye search interface. A red box highlights the uploaded image of the Mona Lisa. The search bar contains the text "Upload or enter Image URL". The results summary is "52,884 results" found over 35.3 billion images in 32.9 seconds. A note states that TinEye is private and does not save search images. It offers filters for "stock and collection" results (858 collections, 400 stock). Below the search bar, there are dropdown menus for sorting and filtering, and a page navigation indicator showing 1 of 5289. The search results list includes a sponsored result from shutterstock.com for a photo of the Mona Lisa, and another result from veryserioso.wordpress.com featuring the same painting. A promotional box for Shutterstock offers a 10% discount. A cartoon robot character is visible on the right.

**Immagini Simili**

STOCK · SPONSORED  
[shutterstock.com](#)  
pic-229540009/stock-photo-leonardo-da-vinci-mon...  
- First found on Dec 07, 2014

Get 10% off at  
Shutterstock by using  
10TINEYE at checkout.

[veryserioso.wordpress.com](#)  
[the-development-of-modern-english/](#) - First found on Jul 12, 2017  
Filename: [mona\\_lisa\\_by\\_leonardo\\_da\\_vinci\\_from\\_c2rmf\\_retouch...jpg](#)  
(640 x 954, 166.5 KB)

# 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

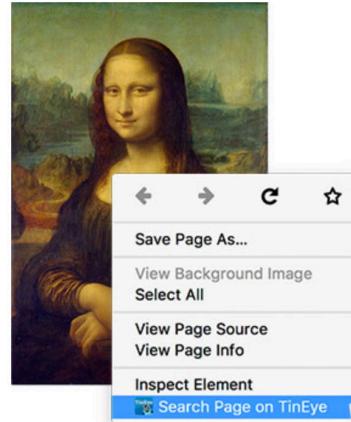
Visit the [Firefox Add-ons page](#) to install the free TinEye browser extension.

## 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](http://tineye.com).

## Configuration

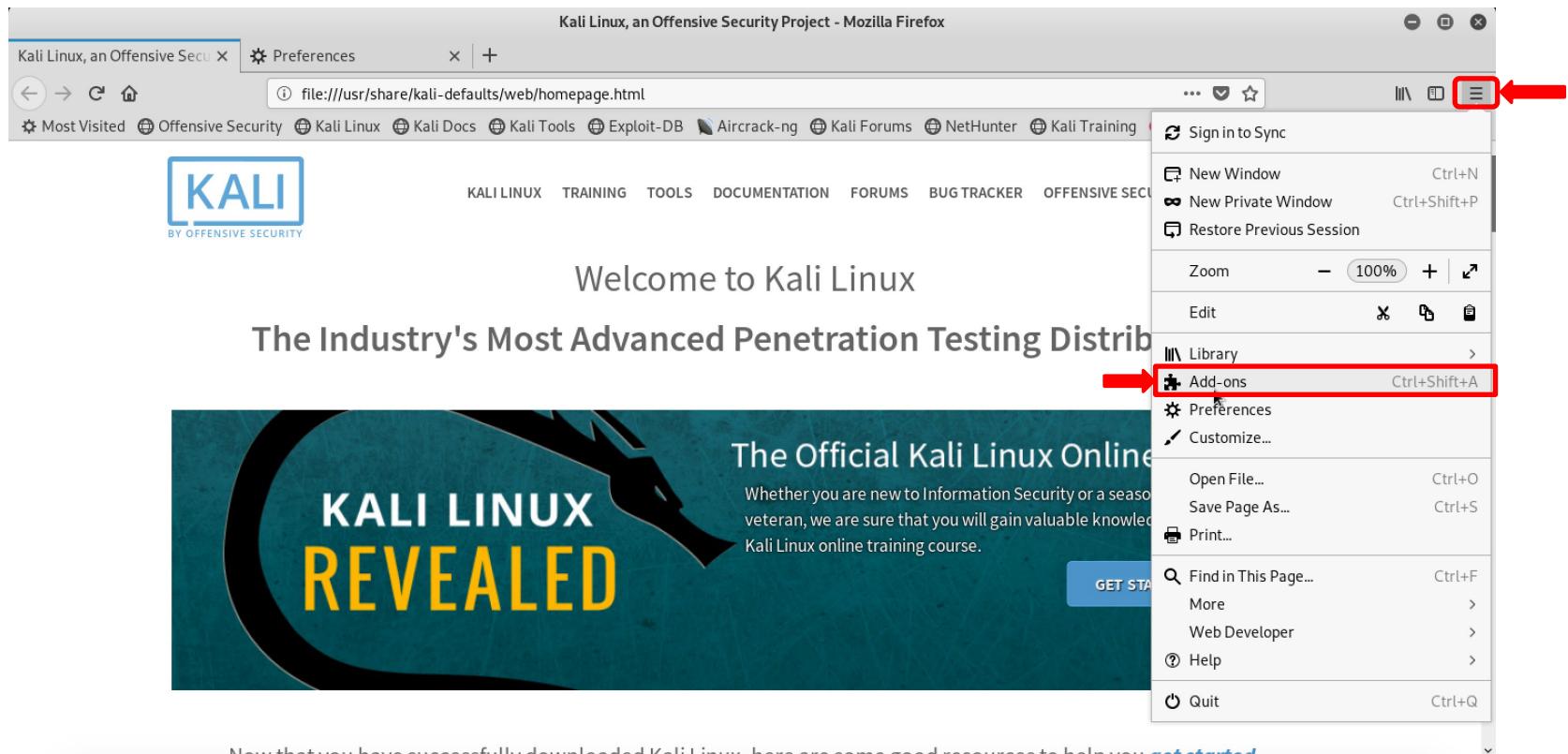
You can choose whether TinEye.com opens in the current tab, in a new tab in the foreground or in a new tab in the background and select the order in which your results will



# Utilizzo di Risorse Web-Based

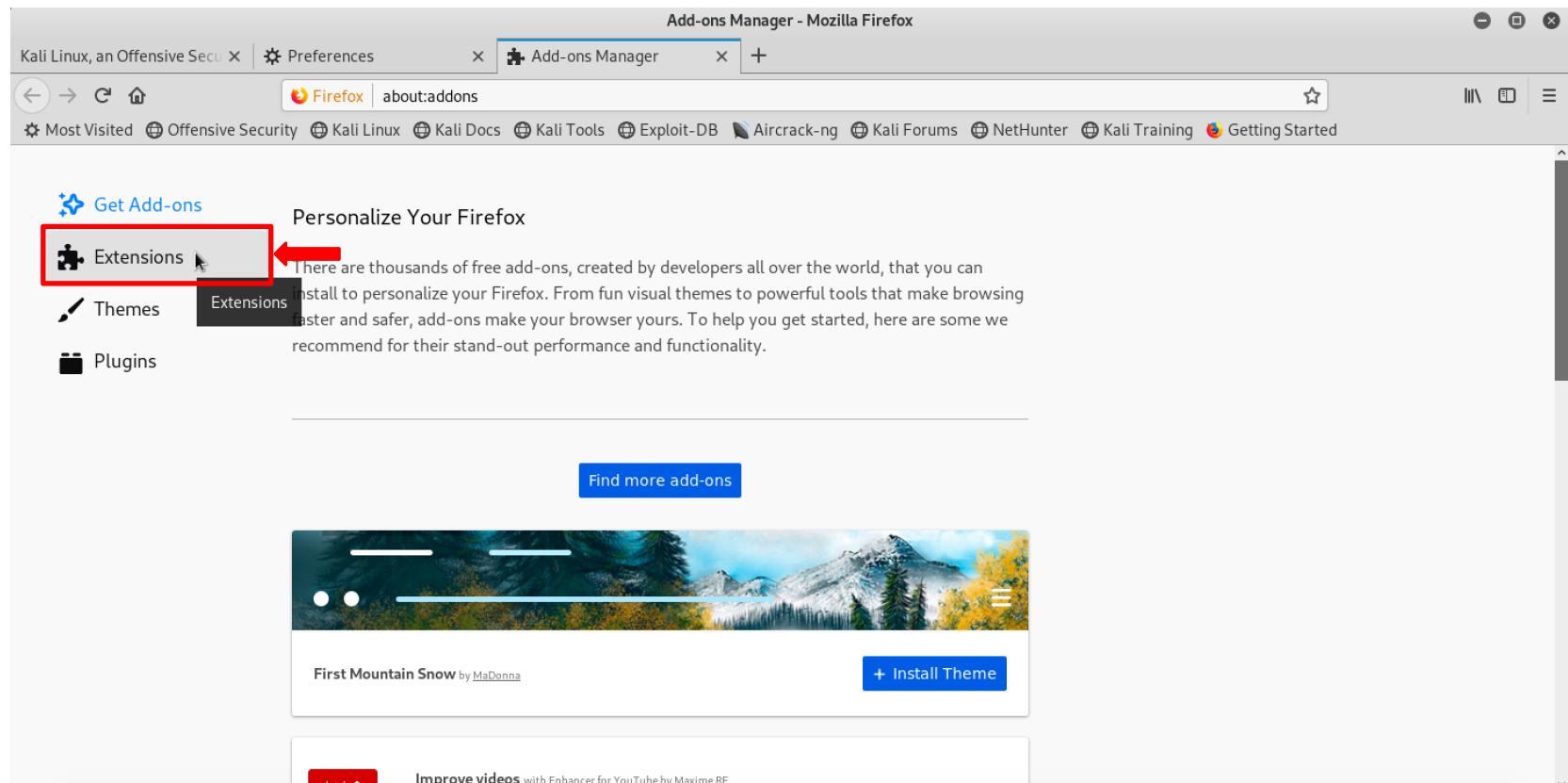
## Reverse Image Search – TinEye – Esempio 2

- 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

The screenshot shows the Mozilla Firefox Add-ons search results page for the query "tineye". The search bar at the top contains "tineye". The main heading says "1,435 results found for 'tineye'". On the left, there is a "Filter results" sidebar with dropdowns for "Sort by" (set to "Relevance"), "Add-on Type" (set to "All"), and "Operating System" (set to "All"). There is also a checkbox for "Recommended add-ons only" which is unchecked. The main area displays a list of search results:

- TinEye Reverse Image Search** (Recommended) - Click on any image on the web to search for it on TinEye. Recommended by Firefox! Discover where an image came from, see how it is being used, check if modified versions exist or locate high resolution versions. Made with love by the TinEye team.  
60,447 users
- Image Search for Tineye** - Image Search for Tineye. Right click image and search image copies for Tineye.  
1,105 users
- TinEye Commercial API Search** - Adds TinEye Commercial API search context menu item for images.  
132 users
- Buscar imagen en TinEYE** - Agrega la opción buscar imagen en TinEYE en el menú contextual  
20 users
- Search by Image** (Recommended) - Reverse image search using various search engines, such as Google, Bing, Yandex, Baidu and TinEye.  
83,788 users
- Reverse Image Search** - Capture, Reverse Image Search is a powerful capturing reverse image search tool built on top of TinEye engine.  
6,484 users
- Fast Image Research** - Right click any image to instantly get reverse image search results from Grindex  
1,166 users

A red arrow points to the first result, "TinEye Reverse Image Search".

# Utilizzo di Risorse Web-Based

## Reverse Image Search – TinEye – Esempio 2

Dopo aver installato l'estensione, per utilizzarla è sufficiente cliccare con il tasto destro sull'immagine che si intende ricercare



# 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

Technical Contacts	
Name:	Salvatore Ferrandino
Address:	Universita\' di Salerno Fisciano 84084 SA IT
Created:	2000-06-21 00:00:00
Last Update:	2012-11-29 12:30:07
Name:	Vittorio Galdi
Address:	Centro Elaborazione Dati Via Ponte Don Melillo Fisciano 84084 SA IT
Created:	2000-06-21 00:00:00
Last Update:	2011-03-24 11:01:09

Responsabili tecnici del dominio

# Informazioni di Registrazione

## Whois – Esempio 1

```
Registrar
Organization: Consortium GARR
Name: GARR-REG
Web: http://www.garr.it
DNSSEC: no

Nameservers
ns.unisa.it
dns-001.unisa.it
ns1.garr.net
```

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#clientTransferProhibited
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@markmonit...
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#cl...
Domain Status: clientTransferProhibited https://icann.org/epp#cl...
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)