

Un elenco telefonico del web: ‘whois’

1 Durata

5 minuti

2 Livello arcobaleno

L_1 - Servizi

3 Difficoltà

Facile

4 Esempi pronti

```
grafchi@DESKTOP-6FDPVTU:/mnt/c/WINDOWS/system32$ whois poste.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:               poste.it
Status:               ok
Signed:               no
Created:              2000-05-29 00:00:00
Last Update:          2021-05-10 00:50:59
Expire Date:          2022-04-24

Registrant
  Organization:       Poste Italiane spa
  Address:             Viale Europa, 190
                     Roma
                     00144
                     RM
                     IT
  Created:             2019-04-24 01:10:34
  Last Update:         2019-04-24 01:10:34

Admin Contact
  Name:               CANDIDO ARMANDO
  Organization:        POSTE ITALIANE S.p.A
  Address:             VIALE EUROPA 175
                     ROMA
                     00144
                     RM
                     IT
  Created:             2019-04-24 01:10:34
  Last Update:         2019-04-24 01:10:34

Technical Contacts
  Name:               Poste Italiane spa
  Organization:        Poste Italiane spa
  Address:             Viale Europa, 190
                     Roma
                     00144
                     RM
                     IT
  Created:             2019-04-24 01:10:34
  Last Update:         2019-04-24 01:10:34

Registrar
  Organization:        Register S.p.a.
  Name:               REGISTER-REG
  Web:                 https://www.register.it
  DNSSEC:              no

Nameservers
  dns.poste.it
  dns1.poste.it
  dns2.poste.it
```

(a) Ambiente Linux

```
*****
* 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:               poste.it
Status:               ok
Signed:               no
Created:              2000-05-29 00:00:00
Last Update:          2021-05-10 00:50:59
Expire Date:          2022-04-24

Registrant
  Organization:       Poste Italiane spa
  Address:             Viale Europa, 190
                     Roma
                     00144
                     RM
                     IT
  Created:             2019-04-24 01:10:34
  Last Update:         2019-04-24 01:10:34

Admin Contact
  Name:               CANDIDO ARMANDO
  Organization:        POSTE ITALIANE S.p.A
  Address:             VIALE EUROPA 175
                     ROMA
                     00144
                     RM
                     IT
  Created:             2019-04-24 01:10:34
  Last Update:         2019-04-24 01:10:34

Technical Contacts
  Name:               Poste Italiane spa
  Organization:        Poste Italiane spa
  Address:             Viale Europa, 190
                     Roma
                     00144
                     RM
                     IT
  Created:             2019-04-24 01:10:34
  Last Update:         2019-04-24 01:10:34

Registrar
  Organization:        Register S.p.a.
  Name:               REGISTER-REG
  Web:                 https://www.register.it
  DNSSEC:              no

Nameservers
  dns.poste.it
  dns1.poste.it
  dns2.poste.it
```

(b) Browser web

Figura 1: Esempi dell'utilizzo di `whois` per il dominio `poste.it`

```

gfacchi@DESKTOP-6FDPVTU:/mnt/c/WINDOWS/system32$ whois unimi.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:                unimi.it
Status:                ok
Signed:                no
Created:               1996-01-29 00:00:00
Last Update:          2021-02-14 00:56:45
Expire Date:           2022-01-29

Registrant
  Organization:        Universita' degli Studi di Milano
  Address:              Via G. Colombo 46
                      Milano
                      20133
                      MI
                      IT
  Created:              2007-03-01 10:35:42
  Last Update:          2011-03-24 11:01:07

Admin Contact
  Name:                Pasquinelli Yuri Benvenuto
  Organization:         Università degli Studi di Milano
  Address:              Via Giuseppe Colombo, 46
                      Milano
                      20133
                      MI
                      IT
  Created:              2020-05-08 09:23:58
  Last Update:          2020-05-08 09:23:58

Technical Contacts
  Name:                Antonio Rossello
  Address:              Università degli Studi di Milano
                      Via G. Colombo 46
                      Milano
                      20133
                      MI
                      IT
  Created:              1999-09-08 00:00:00
  Last Update:          2011-03-24 11:01:09

  Name:                Giancarlo Galluzzi
  Address:              Università degli Studi di Milano
                      Via G. Colombo 46
                      Milano
                      20133
                      MI
                      IT
  Created:              1999-09-08 00:00:00
  Last Update:          2011-03-24 11:01:09

Registrar
  Organization:         Consortium GARR

```

Figura 2: Utilizzo del comando whois per il dominio unimi.it

5 Strumenti necessari

Sistema Operativo Qualsiasi

- Connessione internet

- Command Prompt, in alternativa un browser web

6 Costi

Gratuito

7 Istruzioni dettagliate

Linux

1. Aprire il terminale
2. Eseguire il comando `sudo apt install whois`
3. Inserire eventuale password se richiesta
4. Eseguire il comando `whois poste.it`

Windows

1. Scaricare il tool nmap dal seguente link <https://nmap.org/dist/nmap-7.92-setup.exe>
2. Installare il file scaricato
3. Premere contemporaneamente WIN + R, oppure selezionare Esegui dal menù Start
4. Digitare `cmd` e premere invio
5. Eseguire il comando `nmap --script whois-domain.nse poste.it`

Browser Web

1. Navigare all'indirizzo <https://www.whois.com/whois>
2. Digitare nell'apposita sezione il dominio `poste.it`
3. Premere sul pulsante Search

8 Suggerimenti per variazioni

- Provare cercando un `whois` record di un dominio diverso

9 Risultati attesi

Il risultato dell'esecuzione del comando `whois` comprende diverse informazioni:

Attributo	Significato
Registrant	<i>Persona fisica o giuridica che ha registrato il dominio</i>
Admin Contact	<i>Informazioni e contatti relativi alla persona fisica/giuridica che amministra il dominio</i>
Technical Contact	<i>Informazioni e contatti relativi alla persona fisica/giuridica che mantiene il dominio</i>
Registrar	<i>Figura che, in base ad un contratto con il registro di uno dei domini di primo livello, può gestirli per conto degli utenti finali, cosa di cui il registro stesso non si occupa</i>
Nameservers	<i>Le componenti "server" del DNS</i>

10 Obiettivi raggiunti

Come interrogare un host per ricevere informazioni riguardo dominio, intestatario, gestore e altro.

11 Lezioni imparate

- Consapevolezza di avere la possibilità di sapere chi gestisce un dominio web
- Risalire a informazioni cruciali sui gestori di siti web che trattano temi critici

12 Proseguì con

Traceroute, Nslookup

13 Note

L'idea che ha spinto la stesura di questo esercizio è nata da un servizio giornalistico d'inchiesta su correlazioni tra proprietà di domini collegati a profili politici diametralmente opposti, ma che fanno riferimento allo stesso proprietario. Nello specifico, Gianluigi Paragone (politico, conduttore televisivo e giornalista italiano, senatore della Repubblica dal 2018) lanciava il partito Italexit, di posizione sovranista, registrando il dominio "italexit.it" che, interrogato tramite whois, presentava le seguenti caratteristiche:

1. Il dominio è registrato dalla società In Movimento S.r.l.s. il cui amministratore unico è Gianluca Luciano, titolare di New European Media Ltd, gestore di siti web tra cui Stranieri in Italia e Cara Italia di Stephen Ogongo
2. L'email è di myownmedia.co.uk, un network a favore di politiche di immigrazione permissive
3. Il telefono registrato era collegato a Stephen Ogongo di stranieriitalia.it

14 Possibili mitigazioni

Alcuni hosting providers e registrar offrono strumenti di protezione della privacy relativi al comando `whois`, che proteggono l'identità dell'intestatario del dominio. Ad esempio effettuando una whois lookup per il dominio `wikipedia.it` si può vedere come le informazioni riguardo i contatti di amministrazione e tecnici non siano disponibili.

15 Autore

Giuseppe Maurizio Facchi

16 Licenza

CC BY