

Índice:

Ejercicio 1	2
a) Elaborar un informe sobre el protocolo Whois	2
b) Utilizar un cliente de comandos Whois o bien un cliente Web Whois	3

Ejercicio 1

a) Elaborar un informe sobre el protocolo Whois

Solución:

WHOIS es un protocolo TCP de solicitud y respuesta que permite identificar al propietario de un dominio o dirección IP en Internet. Acceder a esta base de datos a través de páginas web con WHOIS no solo revela la titularidad, sino también detalles adicionales como una miniatura de la página, tiempo online, servidores de alojamiento, entre otros.

Esta herramienta se usa como defensa contra piratas informáticos al proporcionar información crucial, como el nombre completo, dirección comercial y datos de contacto de los propietarios de dominios. Es esencial en la seguridad cibernética, utilizada para investigar ataques informáticos, rastrear direcciones de correo y descubrir la ubicación de posibles perpetradores de fraudes.

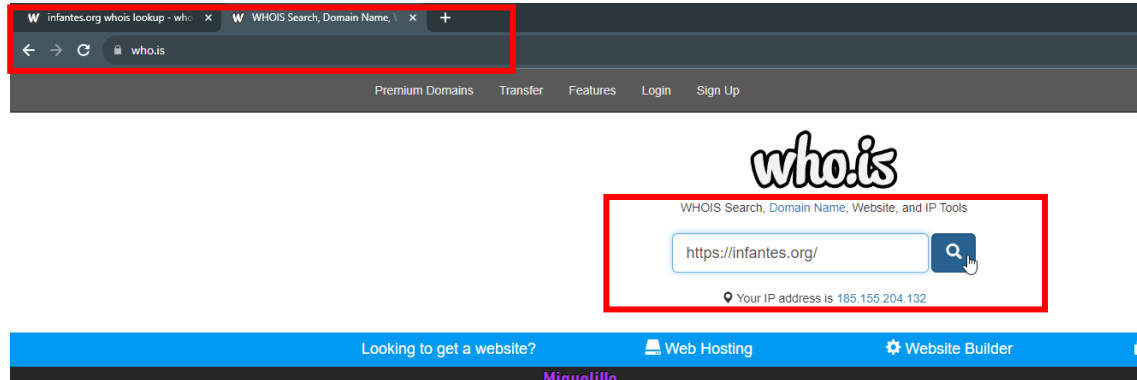
Además, WHOIS sirve para determinar la disponibilidad de un nombre de dominio, contactar a administradores de red, identificar problemas en registros, conocer operadores de servicios web, negociar transacciones comerciales secundarias y notificar obligaciones de mantenimiento de datos de registración. También ayuda a investigar correos no deseados (spam).

Aunque WHOIS ha sido criticado por posibles vulneraciones a la privacidad en Internet, ya que los datos podrían ser aprovechados por spammers, algunos registradores ofrecen registros de dominio privados para ocultar esta información, limitando la aplicabilidad de WHOIS en estos casos.

b) Utilizar un cliente de comandos Whois o bien un cliente Web Whois

Solución:

Vamos a la web de who.is



Nos dice si el sitio se encuentra activo o no, el nombre del dominio, la fecha en la que fue registrado, la fecha en la que expira, etc.

who.is Search for domains or IP addresses...

TLD	Price	Status
.com		Taken
.net		Taken
.org		Taken
.co	\$1667.50	Available
.io	\$34.99	Available
.app	\$8.49	Available
.live	\$3.99	Available

Purchase Selected Domains

infantes.org
whois information

Whois DNS Records Diagnostics

cache expires in 23 hours, 58 minutes and 10 seconds

Registrar Info

Field	Value
Name	Arsys Internet, S.L. dba NICLINE.COM
Whois Server	http://whois.nicline.com
Referral URL	http://nicline.com/whois/whois.htm
Status	ok https://icann.org/epp#ok

Important Dates

Field	Value
Expires On	2024-02-11
Registered On	2000-02-11
Updated On	2023-03-28

Name Servers

Server	IP
dns43.servidoresdns.net	217.76.128.179
dns44.servidoresdns.net	82.223.218.179

Similar Domains

Miguelillo

Use promo code WHOIS to save 15% on your first Name.com order.

Find the perfect domain at Name.com

Everything you need in one place.

SAVE 15% ON YOUR FIRST ORDER

USE PROMO CODE WHOIS

Podemos ver dominios similares al nombre del dominio

The screenshot shows the who.is website interface. The search bar contains 'infantes.org'. Below the search bar, there are three sections highlighted with red boxes:

- Name Servers:** A table with two rows.

Name Servers	IP Address
dns43.servidoresdns.net	217.76.128.179
dns44.servidoresdns.net	82.223.218.179
- Similar Domains:** A list of domains including infan-aerospace.com, infan-ls.ru, infan-tec.cl, infan-tec.com, infan.biz, infan.club, infan.cn, infan.co, infan.com, infan.com.br, infan.de, infan.fun, infan.in, infan.info, infan.io, infan.ir, infan.net, infan.nl, infan.org, and infan.org.ru.
- Registrar Data:** Shows 'Miquelillo' as the registrar.

Vemos información de contacto del dominio.

The screenshot shows the who.is website interface. The search bar contains 'infantes.org'. Below the search bar, there are two sections highlighted with red boxes:

- Similar Domains:** A list of domains including infan-aerospace.com, infan-ls.ru, infan-tec.cl, infan-tec.com, infan.biz, infan.club, infan.cn, infan.co, infan.com, infan.com.br, infan.de, infan.fun, infan.in, infan.info, infan.io, infan.ir, infan.net, infan.nl, infan.org, and infan.org.ru.
- Registrar Data:** A section titled 'Registrar Data' with a green button 'Make Private Now'. It contains three sub-sections: Registrant Contact Information, Administrative Contact Information, and Technical Contact Information. Each sub-section lists fields like Name, Organization, Address, City, State / Province, Postal Code, Country, Phone, Fax, and Email. The values for these fields are mostly 'REDACTED FOR PRIVACY' or 'AYUNTAMIENTO DE VILLANUEVA DE LOS INFANTES'. A note at the bottom of each sub-section says 'Please query the RDNS service of the Registrar of Record for identification information'. The information was updated on 2023-11-27 17:48:12.

En **DNS Records** podemos ver información del **DNS** de ese dominio

who.is Search for domains or IP addresses... Premium Domains Transfer Features Login Sign Up

Interested in domain names? [Click here](#) to stay up to date with domain name news and promotions at Name.com

infantes.org is already registered. Interested in buying it? [Make an Offer](#)

.com	.net	.org	.co \$1667.50	.io \$34.99	.app \$8.49
Taken	Taken	Taken	Available	Available	Available

[Purchase Selected Domains](#)

infantes.org
DNS information

Whois **DNS Records** Diagnostics

DNS Records for infantes.org cache e

Hostname	Type	TTL	Priority	Content
infantes.org	SOA	3600		dns43.servidoresdns.net hostmaster@servidoresdns.net 2021032340 21600 3600 2419200 60
infantes.org	NS	3600		dns43.servidoresdns.net
infantes.org	NS	3600		dns44.servidoresdns.net
infantes.org	A	3600		217.76.142.247
infantes.org	MX	3600	10	mx.serviciodecorreo.es
www.infantes.org	A	3600		217.76.142.247

Miguelillo

En **Diagnostics** podemos ver si tenemos conectividad con el dominio

who.is Search for domains or IP addresses... Premium Domains Transfer Features Login Sign Up

infantes.org
diagnostic tools

Whois **DNS Records** **Diagnostics**

Ping

```
PING infantes.org (217.76.142.247) 56(84) bytes of data:
64 bytes from llgm941.servidoresdns.net (217.76.142.247): icmp_seq=1 ttl=50 time=112 ms
64 bytes from llgm941.servidoresdns.net (217.76.142.247): icmp_seq=2 ttl=50 time=112 ms
64 bytes from llgm941.servidoresdns.net (217.76.142.247): icmp_seq=3 ttl=50 time=113 ms
64 bytes from llgm941.servidoresdns.net (217.76.142.247): icmp_seq=4 ttl=50 time=112 ms
64 bytes from llgm941.servidoresdns.net (217.76.142.247): icmp_seq=5 ttl=50 time=113 ms

--- infantes.org ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 112.898/112.989/113.100/0.432 ms
```

Traceroute

```
traceroute to infantes.org (217.76.142.247), 30 hops max, 60 byte packets
 1 ip-10-0-0-14.ec2.internal (10.0.0.14) 1.069 ms 1.081 ms 1.131 ms
 2 ec2-3-236-63-87.compute-1.amazonaws.com (3.236.63.87) 112.318 ms ec2-3-236-63-125.compute-1.amazonaws.com (3.236.63.125) 3.847 ms ec2-3-236-63-11.compute-1.amazonaws.com (3.236.63.11) 1.716 ms
 3 240.0.224.97 (240.0.224.97) 1.651 ms 1.648 ms 240.0.224.98 (240.0.224.98) 1.716 ms
 4 242.2.112.67 (242.2.112.67) 2.864 ms 242.2.113.67 (242.2.113.67) 2.869 ms 242.2.112.197 (242.2.112.197) 2.244 ms
 5 240.0.236.3 (240.0.236.3) 95.636 ms 95.688 ms 240.0.236.1 (240.0.236.1) 2.464 ms
 6 242.2.212.67 (242.2.212.67) 3.431 ms 242.2.212.195 (242.2.212.195) 2.348 ms 242.2.212.67 (242.2.212.67) 2.125 ms
 7 100.100.2.6 (100.100.2.6) 1.908 ms 100.100.2.2 (100.100.2.2) 1.742 ms 100.100.34.44 (100.100.34.44) 1.905 ms
 8 ash-b2-link.ip.twelve99.net (213.248.92.170) 2.235 ms 2.449 ms ash-b2-link.ip.twelve99.net (62.115.63.80) 16.157 ms
 9 ash-bb2-link.ip.twelve99.net (62.115.123.124) 3.246 ms rest-bb1-link.ip.twelve99.net (62.115.123.122) 3.377 ms ash-bb2-link.ip.twelve99.net (62.115.123.122) 3.377 ms
```

Miguelillo