HERRAMIENTAS DE CONSULTA A SERVIDORES DNS

Índice

1. INTRODUCCIÓN

Para probar el correcto funcionamiento de nuestro propio servidor DNS o realizar comprobaciones de seguridad en servidores externos, es muy útil conocer las utilidades que tenemos a nuestra disposición.
Un buen uso de estas herramientas, bien sean a traves de linea de comandos (CLI) o mediante alguna GUI más sofisticada nos va a permitir sin duda mejorar nuestras configuraciones y conocer mejor el funcionamiento de este servicio. Vamos a conocer las siguientes:

- ping
- nslookup
- dig
- host
- whois

El objetivo de esta documentación no es conocer todas las opciones de todos los comandos, sino conocerlos brevemente para ser capaces de, mediante consultas a las paginas de manual (MAN) obtener la información que queremos.

2. PING

Aunque, en un principio no es para lo que está pensado (recordemos que el protocolo ICMP en el que se basa se ideó para comprobar si un equipo está activo en la red), este comando nos va a permitir realizar traducciones DNS básicas, consultando únicamente a los servidores DNS que tengamos configurados por defecto en nuestra configuración de red.
Cuando se utiliza, es la traducción inicial que realiza lo que nos importa, no la respuesta afirmativa o negativa de los paquetes ICMP que se envían.

```
tomas@hpPavilion15ns:~$ ping aules.edu.gva.es
PING aules.edu.gva.es (193.145.206.157) 56(84) bytes of data.
```

Con la opción -a, y si está la zona inversa con su registro PTR correspondiente, nos traduciría una IP por un FQDN.

3. NSLOOKUP

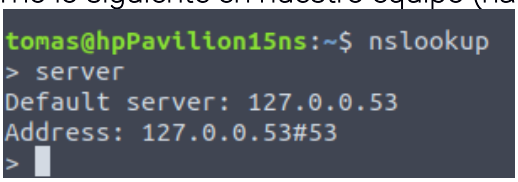
Esta sería la herramienta más conocida hasta ahora, sobretodo por que es la única de las que vamos a ver, que existe tanto en sistemas Windows como Linux. Tiene la particularidad que permite trabajar en modo interactivo, ya que si únicamente escribimos *nslookup*, entramos en la interfaz que interpreta los comandos y opciones específicas.

```
tomas@hpPavilion15ns:~$ nslookup
> server 192.168.1.1
Default server: 192.168.1.1
Address: 192.168.1.1#53
> cuacua.formacion.es
Server:         192.168.1.1
Address:  192.168.1.1#53
```

```
Non-authoritative answer:
cuacua.formacion.es        canonical name = parkingsrv0.dondominio.com.
Name:    parkingsrv0.dondominio.com
Address: 37.152.88.55
>
```

Teclear un nombre directamente en la interfaz de nslookup, supone su busqueda, devolviendo los datos del servidor que nos ha contestado y su respuesta.
>server x.x.x.x, indica que todas las consultas a partir de ese momento se realizarán a ese servidor.
>set type=TIPO, indica que estamos consultando los registros de recursos (RR) de un TIPO concreto.
Una de los elementos que destacan en lo que devuelve el comando es que indica claramente si la respuesta es de un servidor autorizado sobre ese dominio o no.

Si nos encontramos algo como lo siguiente en nuestro equipo (hablamos de equipos Linux):



¿Esto tiene sentido para tu configuración de red?¿Podrías encontrar en la web porqué se produce esto?

EJEMPLOS DE USO NSLOOKUP

Ejemplo 1) Buscar la dirección IP de *www.yahoo.com* .

Para ello ejecutar nslookup *www.yahoo.com* desde el intérprete de comandos. También es posible ejecutar nslookup sin parámetros para entras en el entorno de la aplicación y desde éste dar el nombre del equipo cuya dirección IP queremos conocer. Se veria como:

```
[tomas@portatiLG ~]$ nslookup www.yahoo.com
Server:        62.42.63.52
Address:       62.42.63.52#53

Non-authoritative answer:
www.yahoo.com   canonical name = fd-fp3.wg1.b.yahoo.com.
fd-fp3.wg1.b.yahoo.com  canonical name = ds-fp3.wg1.b.yahoo.com.
ds-fp3.wg1.b.yahoo.com  canonical name = ds-eu-fp3-lfb.wa1.b.yahoo.com.
ds-eu-fp3-lfb.wa1.b.yahoo.com   canonical name = ds-eu-fp3.wa1.b.yahoo.com.
Name:   ds-eu-fp3.wa1.b.yahoo.com
Address: 87.248.122.122
Name:   ds-eu-fp3.wa1.b.yahoo.com
Address: 87.248.112.181
```

La salida que se genera se compone en primer lugar del nombre simbólico junto con la dirección IP del servidor de nombres utilizado y en segundo lugar el nombre simbólico objeto de consulta y de su dirección IP correspondiente. Observar que una misma dirección IP puede tener asociada más de un nombre simbólico.
¿Que significa EXÁCTAMENTE LA SALIDA de este comando?. Sabrías explicar lo que devuelve esta respuesta de NSLOOKUP . ¿Cómo activarías/desactivarías la recursión en las consultas?

Ejemplo 2) Buscar los servidores de nombres para el dominio upv.es.

Para ello ejecutar nslookup para entrar en el entorno de esta aplicación (Ej.: $ nslookup). Una vez en el entorno de la aplicación nslookup ejecutar la sentencia set type=NS (con lo que se cambia el modo de consulta). En este momento ejecutar upv.es. Se veria como:

```
[tomas@portatiLG ~]$ nslookup
> set type=NS
> upv.es
Server:         62.42.63.52
Address:        62.42.63.52#53

Non-authoritative answer:
upv.es  nameserver = sun.rediris.es.
upv.es  nameserver = vega.cc.upv.es.
upv.es  nameserver = chico.rediris.es.
upv.es  nameserver = mirzam.ccc.upv.es.

Authoritative answers can be found from:
>
```

La información que obtenemos empieza como antes con el nombre y la dirección IP del servidor de nombres utilizado por defecto. Después una lista de los nombres de todos los servidores de nombres asociados al dominio dado. Por último las direcciones IP de todos estos servidores de nombres.

¿Que significan los términos *Authoritative/Non-authoritative answers* ? ¿Como podriamos obtener una respuesta autorizada?

Ejemplo 3) Obtener las características del NS del dominio terra.es.

Entrar en el entorno de la aplicación nslookup (Ej.: $ nslookup). Cambiar el modo de consulta a TODOS LOS REGISTROS (Ej.: > set type=ANY). Ejecutar terra.es.

```
tomas@portatiLG ~]$ nslookup
> set type=ANY
> terra.es
Server:                 127.0.0.53
Address:  127.0.0.53#53

Non-authoritative answer:
terra.es    text = "v=spf1 ip4:208.84.242.0/23 ip4:98.142.233.64/28 -all"
Name:     terra.es
Address: 2604:600:0:aaaa:208:84:244:10
terra.es    nameserver = b.dns.terra.com.br.
terra.es    nameserver = d.dns.terra.com.br.
terra.es    nameserver = a.dns.terra.com.
terra.es    nameserver = c.dns.terra.com.
terra.es
  origin = a.dns.terra.com
  mail addr = sysadm.terra.com.br
  serial = 2017041883
  refresh = 28800
  retry = 7200
  expire = 2592000
  minimum = 172800
Name:     terra.es
Address: 208.84.244.10
terra.es    rdata_99 = "v=spf1 ip4:208.84.242.0/23 ip4:98.142.233.64/28 -all"

Authoritative answers can be found from:
>
```

¿ Cuál es el servidor de nombres principal? ¿ Cuál es el tiempo de vida por defecto de los registros del dominio?. ¿Que deberias hacer para obtener una respuesta autorizada sobre este dominio terra.es?

Ejemplo 4) Obtener el inicio de autoridad.

Entrar en el entorno de la aplicación nslookup (Ej.: $ nslookup). Cambiar el modo de consulta a MX (Ej.: > set type=MX). Obtener los servidores de correo asociados al dominio upv.es.

```
[tomas@portatiLG ~]$ nslookup
> set type=SOA
> upv.es
Server:         62.42.63.52
Address:        62.42.63.52#53

Non-authoritative answer:
upv.es
        origin = mirzam.ccc.upv.es
        mail addr = hostmaster.upv.es
        serial = 2012112616
        refresh = 7200
        retry = 3600
        expire = 1296000
        minimum = 10800

Authoritative answers can be found from:
> server mirzam.ccc.upv.es
Default server: mirzam.ccc.upv.es
Address: 158.42.1.5#53
> set type=MX
> upv.es
Server:         mirzam.ccc.upv.es
Address:        158.42.1.5#53

upv.es  mail exchanger = 10 albali.cc.upv.es.
upv.es  mail exchanger = 20 mxv.cc.upv.es.
upv.es  mail exchanger = 30 mx2.cc.upv.es.
upv.es  mail exchanger = 50 vega.cc.upv.es.
upv.es  mail exchanger = 10 mx4.cc.upv.es.
```

¿ Cuáles son los servidores de correo para este dominio? ¿ Para el dominio uc3m.es cuál es el servidor de correo más prioritario?.

Ejemplo 5) Realizar una búsqueda inversa

Entrar en el entorno de la aplicación nslookup (Ej.: $ nslookup). Cambiar el modo de consulta a PTR (Ej.: > set type=PTR). Para que se cumpla lo marcado en negrita primero debes realizar una configuración.¿CUAL?

```
[tomas@portatiLG ~]$ nslookup
> server
Default server: 8.8.8.8
Address: 8.8.8.8#53
> set type=PTR
> set type=ptr
> 8.8.8.8.in-addr.arpa
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
8.8.8.8.in-addr.arpa    name = google-public-dns-a.google.com.
```

¿ Qué significa esta consulta y la respueta correspondiente?

En windows el comando puede devolver una salida un poco distinta. Por ejemplo prueba a poner la opción set debug y mira toda la información que devuelve.

4. DIG

Este comando, existente únicamente para Linux, es el que propone, por ejemplo el ISC(Internet System Consortium) para consultar a servidores DNS. En cualquier caso es una herramienta que, al igual que nslookup, nos va a permitir obtener información DNS. El comando DIG no trabaja en modo interactivo, es decir, funciona como un comando normal en el que tienes que pasar todas las opciones y parámetros en una sola llamada.

El formato de una llamada al comando DIG, sería:

$dig nombre

$dig @x.x.x.x nombre TIPO

nombre indica el nombre de dominio que queremos resolver.
@x.x.x.x le indica que queremos que esa búsqueda la resuelva un servidor en concreto.
TIPO filtra el tipo de RR que buscamos, por defecto DIG busca hosts(A)

DIG destaca, sobretodo, por la información tan extensa que nos devuelve en las consultas a los servidores DNS. Por ejemplo:

```
mtgimenez@lliurex:~$ dig www.lliurex.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.lliurex.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7632
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.lliurex.net.               IN      A

;; ANSWER SECTION:
www.lliurex.net.    14400   IN      CNAME lliurex.net.
lliurex.net.                14400   IN      A       192.168.80.31

;; AUTHORITY SECTION:
lliurex.net.                86400   IN      NS      dns2aulas.

;; Query time: 7 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Wed Oct 31 15:01:46 CET 2018
;; MSG SIZE  rcvd: 97
```

EJEMPLOS DE USO DIG

Ejemplo 1) Buscar por tipo de registro

Hasta ahora hemos visto que, por defecto, DIG devolverá el registro A, sin embargo, podemos especificar cualquier otro RR que deseamos consultar simplemente agregando el tipo de registro al final de la consulta. En este ejemplo, buscamos los registros MX asociados con google.com.

```
[root@centos7 ~]# dig @8.8.8.8 google.com MX

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.3 <<>> @8.8.8.8 google.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39927
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.                    IN      MX

;; ANSWER SECTION:
google.com.             599     IN      MX      30 alt2.aspmx.l.google.com.
google.com.             599     IN      MX      40 alt3.aspmx.l.google.com.
google.com.             599     IN      MX      10 aspmx.l.google.com.
google.com.             599     IN      MX      50 alt4.aspmx.l.google.com.
google.com.             599     IN      MX      20 alt1.aspmx.l.google.com.

;; Query time: 180 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Sep 06 09:17:54 AEST 2016
;; MSG SIZE  rcvd: 147
```

Ejemplo 2) Búsqueda DNS inversa

Podemos usar el comando para realizar una búsqueda DNS inversa, es decir, podemos consultar una dirección IP y encontrar el nombre de dominio al que apunta al consultar el registro PTR. Esto se hace mediante el uso de la opción -x.

```
[root@centos7 ~]# dig -x 216.58.220.110

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.3 <<>> -x 216.58.220.110
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19387
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0005 , udp: 4000
;; QUESTION SECTION:
;110.220.58.216.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
110.220.58.216.in-addr.arpa. 5  IN      PTR     syd10s01-in-f14.1e100.net.
110.220.58.216.in-addr.arpa. 5  IN      PTR     syd10s01-in-f110.1e100.net.

;; Query time: 2 msec
;; SERVER: 192.168.220.2#53(192.168.220.2)
;; WHEN: Tue Sep 06 09:20:38 AEST 2016
;; MSG SIZE  rcvd: 126
```

¿Que significa que hayan dos registros PTR?

Ejemplo 3) Consultar todos los tipos de registro DNS

Podemos usar la opción 'ANY' para consultar todos los tipos de registros de DNS, de esta manera podemos ver rápidamente todos los registros de DNS disponibles para un dominio.

En el siguiente ejemplo, podemos ver los resultados de todos los tipos de registros diferentes, incluidos A, AAAA, TXT, MX y NS.

```
mtgimenez@lliurex:~$ dig cloudflare.com ANY

; <<>> DiG 9.10.3-P4-Ubuntu <<>> cloudflare.com ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42785
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 13, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cloudflare.com.                IN      ANY

;; ANSWER SECTION:
cloudflare.com.         62      IN      RRSIG   A 13 2 600 20181101150849
20181030130849                  35273                   cloudflare.com.
BXoYDI5lFhOloqPGxxPQ2l2e9soQP2YMifOlnWGjtGdAHR53zGn2nEnC
WSg57lSznRSvWr6Fbjn5k5BTXz4uHw==
cloudflare.com.         62      IN      A       198.41.214.162
cloudflare.com.         62      IN      A       198.41.215.162
cloudflare.com.         51024   IN      RRSIG   DS 8 2 86400 20181107052404
20181031031404                  37490                   com.
SQsebvshO57NbIU+OsARz9T2gdwDEYbZYq1yjLwC7sQpCcIRgPpj4OWw
lArR8PO/niU/TKkTXb7t9Nk4sLyO01M29030JZxXPFWTLVafUfrp7la3
7M0PW5VfO0J4xW1Fmi0pvqkdFXBqzKpCXq1z72Y9cmfdPUlewm5KgGy2 ZjQ=
cloudflare.com.         51024   IN      DS      2371 13 2
32996839A6D808AFE3EB4A795A0E6A7A39A76FC52FF228B22B76F6D6 3826F2B9

;; AUTHORITY SECTION:
com.                    59197   IN      NS      a.gtld-servers.net.
com.                    59197   IN      NS      k.gtld-servers.net.
com.                    59197   IN      NS      e.gtld-servers.net.
com.                    59197   IN      NS      d.gtld-servers.net.
com.                    59197   IN      NS      m.gtld-servers.net.
com.                    59197   IN      NS      l.gtld-servers.net.
com.                    59197   IN      NS      g.gtld-servers.net.
com.                    59197   IN      NS      h.gtld-servers.net.
com.                    59197   IN      NS      i.gtld-servers.net.
com.                    59197   IN      NS      c.gtld-servers.net.
com.                    59197   IN      NS      b.gtld-servers.net.
com.                    59197   IN      NS      j.gtld-servers.net.
com.                    59197   IN      NS      f.gtld-servers.net.

;; ADDITIONAL SECTION:
a.gtld-servers.net. 11422   IN      A       192.5.6.30
a.gtld-servers.net. 9809    IN      AAAA    2001:503:a83e::2:30
b.gtld-servers.net. 78300   IN      A       192.33.14.30
b.gtld-servers.net. 78557   IN      AAAA    2001:503:231d::2:30
c.gtld-servers.net. 2700    IN      A       192.26.92.30
c.gtld-servers.net. 2338    IN      AAAA    2001:503:83eb::30
d.gtld-servers.net. 20069   IN      A       192.31.80.30
d.gtld-servers.net. 74569   IN      AAAA    2001:500:856e::30
e.gtld-servers.net. 11366   IN      A       192.12.94.30
e.gtld-servers.net. 18236   IN      AAAA    2001:502:1ca1::30
f.gtld-servers.net. 58210   IN      A       192.35.51.30
f.gtld-servers.net. 59687   IN      AAAA    2001:503:d414::30
g.gtld-servers.net. 66074   IN      A       192.42.93.30
g.gtld-servers.net. 9809    IN      AAAA    2001:503:eea3::30
```

```
h.gtld-servers.net.28139  IN      A       192.54.112.30
h.gtld-servers.net.74632  IN      AAAA    2001:502:8cc::30
i.gtld-servers.net. 35411  IN      A       192.43.172.30
i.gtld-servers.net. 78503  IN      AAAA    2001:503:39c1::30
j.gtld-servers.net. 57521  IN      A       192.48.79.30
j.gtld-servers.net. 63027  IN      AAAA    2001:502:7094::30
k.gtld-servers.net.57150  IN      A       192.52.178.30
k.gtld-servers.net.39179  IN      AAAA    2001:503:d2d::30
l.gtld-servers.net. 43731  IN      A       192.41.162.30
l.gtld-servers.net. 68164  IN      AAAA    2001:500:d937::30
m.gtld-servers.net.       15244   IN      A       192.55.83.30
m.gtld-servers.net.       447     IN      AAAA    2001:501:b1f9::30

;; Query time: 8 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Wed Oct 31 15:17:47 CET 2018
;; MSG SIZE  rcvd: 1192
```

Ejemplo 4) Rastrear la ruta del DNS

Podemos realizar un seguimiento en la ruta de búsqueda de DNS con la opción +trace, como se muestra a continuación, al consultar google.com, podemos ver qué sucede realmente. Primero los servidores de nombres raíz para '.' se buscan, seguidos de los servidores de nombres para el dominio .com y, finalmente, se devuelven los servidores de nombres para google.com, seguidos de los registros de DNS correspondientes.

```
mtgimenez@lliurex:~$ dig +trace yahoo.es

; <<>> DiG 9.10.3-P4-Ubuntu <<>> +trace yahoo.es
;; global options: +cmd
.                       3600000 IN      NS      C.ROOT-SERVERS.NET.
.                       3600000 IN      NS      F.ROOT-SERVERS.NET.
.                       3600000 IN      NS      B.ROOT-SERVERS.NET.
.                       3600000 IN      NS      D.ROOT-SERVERS.NET.
.                       3600000 IN      NS      K.ROOT-SERVERS.NET.
.                       3600000 IN      NS      H.ROOT-SERVERS.NET.
.                       3600000 IN      NS      L.ROOT-SERVERS.NET.
.                       3600000 IN      NS      E.ROOT-SERVERS.NET.
.                       3600000 IN      NS      M.ROOT-SERVERS.NET.
.                       3600000 IN      NS      I.ROOT-SERVERS.NET.
.                       3600000 IN      NS      J.ROOT-SERVERS.NET.
.                       3600000 IN      NS      G.ROOT-SERVERS.NET.
.                       3600000 IN      NS      A.ROOT-SERVERS.NET.
;; Received 853 bytes from 127.0.1.1#53(127.0.1.1) in 8 ms

yahoo.es.               147     IN      A       212.82.100.151
yahoo.es.               147     IN      A       74.6.136.151
yahoo.es.               147     IN      A       98.136.103.24
yahoo.es.               147     IN      A       106.10.248.151
yahoo.es.               147     IN      A       124.108.115.101
;; Received 106 bytes from 192.36.148.17#53(I.ROOT-SERVERS.NET) in 14 ms
```

Fíjate en la primera columna, primero muestra . y luego yahoo.es. ¿Por que crees que pasa esto?

5. HOST

Host es un sencillo comando que, unicamente en sistemas Linux, tambien nos permite realizar sencillas consultas a servidores DNS. Puedes encontrar algunos ejemplos en el siguiente enlace.
Algunos ejemplos de uso pueden ser:

Ejemplo 1) Mostrar los registros SOA para el nombre de la zona

Con la opción -C se muestran los registros SOA para el nombre de la zona de **todos** los servidores de nombres autorizados de esa zona. Esto es útil para comparar los servidores de nombres autorizados:

```
tomas@hpPavilion15ns:~$ host -C cyberciti.biz
Nameserver 173.245.59.88:
  cyberciti.biz has SOA record clay.ns.cloudflare.com. dns.cloudflare.com. 2029200605 10000 2400 604800 3600
Nameserver 173.245.58.115:
  cyberciti.biz has SOA record clay.ns.cloudflare.com. dns.cloudflare.com. 2029200605 10000 2400 604800 3600
tomas@hpPavilion15ns:~$
```

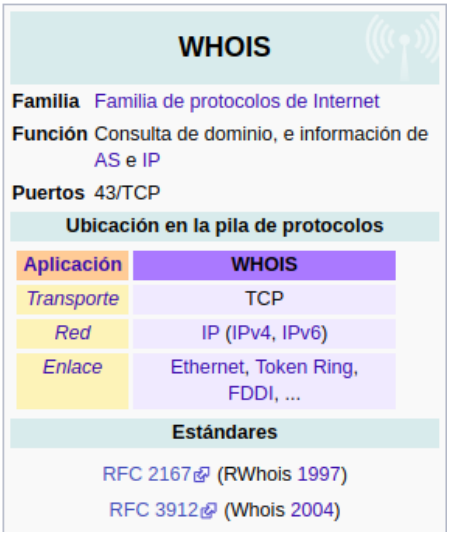
Ejemplo 2) Obtener todos los registros de una zona

Podemos usar tanto la opción **-a,** como la opción **-v,** obteniendo un resultado similar

```
tomas@hpPavilion15ns:~$ host -a cyberciti.biz
Trying "cyberciti.biz"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42762
;; flags: qr rd ra; QUERY: 1, ANSWER: 11, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;cyberciti.biz.                 IN      ANY

;; ANSWER SECTION:
cyberciti.biz.          266     IN      AAAA    2606:4700:10::6814:bb05
cyberciti.biz.          266     IN      AAAA    2606:4700:10::6814:ba05
cyberciti.biz.          86293   IN      NS      clay.ns.cloudflare.com.
cyberciti.biz.          86293   IN      NS      fay.ns.cloudflare.com.
cyberciti.biz.          266     IN      A       104.20.187.5
cyberciti.biz.          266     IN      A       104.20.186.5
cyberciti.biz.          266     IN      MX      5 alt2.aspmx.l.google.com.
cyberciti.biz.          266     IN      MX      1 aspmx.l.google.com.
cyberciti.biz.          266     IN      MX      10 aspmx2.googlemail.com.
cyberciti.biz.          266     IN      MX      10 aspmx3.googlemail.com.
cyberciti.biz.          266     IN      MX      5 alt1.aspmx.l.google.com.

Received 303 bytes from 127.0.0.53#53 in 75 ms
```

6. WHOIS

Tal y como describe Wikipedia, WHOIS es un protocolo TCP basado en petición/respuesta que se utiliza para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio o una dirección IP en Internet. Existen multitud de páginas web que permiten realizar estas consultas.



WHOIS

Familia Familia de protocolos de Internet

Función Consulta de dominio, e información de AS e IP

Puertos 43/TCP

Ubicación en la pila de protocolos

Aplicación	WHOIS
Transporte	TCP
Red	IP (IPv4, IPv6)
Enlace	Ethernet, Token Ring, FDDI, ...

Estándares

RFC 2167 (RWhois 1997)

RFC 3912 (Whois 2004)

Ejemplo 1) Mostrar los datos de propiedad de un dominio DNS

Un ejemplo de uso de este protocolo, mediante la web https://www.dondominio.com/whois/, sería:

Dominio: terra.es
Estado: ok
Fecha de creación: 17/01/2001
Fecha de expiración: 17/01/2019
Agente registrador: ACENS TECHNOLOGIES S.L.

Titular

ID: TS1667-ESNIC-F4
Nombre: TELEFONICA S.A.

Contacto administrativo

ID: 1EB79E-ESNIC-F5
Nombre: Manuel Crespo de la Mata

Contacto técnico

ID: TNES3-ESNIC-F4
Nombre: TERRA NETWORKS ESPAÑA, S.A.U.

Servidores DNS

c.dns.terra.com
b.dns.terra.com.br
a.dns.terra.com
d.dns.terra.com.br