Ejercicios 4: Funcionamiento del servicio DNS

1. Windows

Inicia sesión en una máquina virtual con Windows (y acceso a internet)

Utiliza el comando nslookup para obtener las direcciones IP asociadas al nombre DNS www.madrid.org.

nslookup www.madrid.org

```
victor.garmur.1: ~ ❯ nslookup www.madrid.org
Servidor:  serviciosda.educa.jcyl.es
Address:  10.151.123.21

Respuesta no autoritativa:
Nombre:  d3omk6xn5p4d3d.cloudfront.net
Addresses:  2600:9000:237f:800:1a:83ee:1240:93a1
          2600:9000:237f:f800:1a:83ee:1240:93a1
          2600:9000:237f:a200:1a:83ee:1240:93a1
          2600:9000:237f:a400:1a:83ee:1240:93a1
          2600:9000:237f:8400:1a:83ee:1240:93a1
          2600:9000:237f:7400:1a:83ee:1240:93a1
          2600:9000:237f:d600:1a:83ee:1240:93a1
          2600:9000:237f:8c00:1a:83ee:1240:93a1
          108.157.109.87
          108.157.109.78
          108.157.109.10
          108.157.109.2
Aliases:  www.madrid.org
```

Observa que el servidor DNS que responde es el que está configurado en las propiedades TCP/IP del equipo.

En el aula esta la red de educa, por lo tanto, tenemos como DNS el configurador por ellos.

```
Servidor:  serviciosda.educa.jcyl.es
Address:  10.151.123.21
```

Desde mi casa, aparece como servidor desconocido.

```
Victor: ~ ❯ nslookup www.madrid.org
Servidor:  UnKnown
Address:  212.230.135.1
```

Observa que existen varias IPs asociadas al nombre de dominio.

```
Addresses:  2600:9000:237f:800:1a:83ee:1240:93a1
          2600:9000:237f:f800:1a:83ee:1240:93a1
          2600:9000:237f:a200:1a:83ee:1240:93a1
          2600:9000:237f:a400:1a:83ee:1240:93a1
          2600:9000:237f:8400:1a:83ee:1240:93a1
          2600:9000:237f:7400:1a:83ee:1240:93a1
          2600:9000:237f:d600:1a:83ee:1240:93a1
          2600:9000:237f:8c00:1a:83ee:1240:93a1
          108.157.109.87
          108.157.109.78
          108.157.109.10
          108.157.109.2
```

Observa los nombres de dominio que son equivalentes (alias)

```
Nombre:  d3omk6xn5p4d3d.cloudfront.net
```

```
Aliases:  www.madrid.org
```

Observa que la respuesta no es autorizada.

```
Respuesta no autoritativa:
```

Realiza la consulta inversa, usa el comando nslookup con el nombre que viene asociado en el resultado anterior ¿te sale que su alias es www.madrid.org? ¿Por qué?

```
victor.garmur.1: ~ ❯ nslookup d3omk6xn5p4d3d.cloudfront.net
Servidor:  serviciosda.educa.jcyl.es
Address:  10.151.123.21

Respuesta no autoritativa:
Nombre:  d3omk6xn5p4d3d.cloudfront.net
Addresses:  2600:9000:237f:7600:1a:83ee:1240:93a1
          2600:9000:237f:8000:1a:83ee:1240:93a1
          2600:9000:237f:3e00:1a:83ee:1240:93a1
          2600:9000:237f:9200:1a:83ee:1240:93a1
          2600:9000:237f:e000:1a:83ee:1240:93a1
          2600:9000:237f:a800:1a:83ee:1240:93a1
          2600:9000:237f:5800:1a:83ee:1240:93a1
          2600:9000:237f:6400:1a:83ee:1240:93a1
          108.157.109.10
          108.157.109.2
          108.157.109.87
          108.157.109.78
```

No sale el alias de www.madrid.org, porque el servidor ofrecerá servicios a muchos servidores y no tiene sentido que aparezca el nombre de uno de los dominios a los que ofrece servicios.

Utiliza el comando nslookup para obtener el/los nombres de dominio asociados a la dirección IP 130.206.13.20.

```
nslookup 130.206.13.20
```

El nombre de dominio es www.rediris.es.

```
victor.garmur.1: ~ ❯ nslookup 130.206.13.20
Servidor:  serviciosda.educa.jcyl.es
Address:  10.151.123.21

Nombre:  www.rediris.es
Address:  130.206.13.20
```

Utiliza el comando nslookup para obtener las direcciones IP asociadas al nombre DNS www.madrid.org preguntando al servidor DNS 8.8.4.4

```
nslookup www.madrid.org 8.8.4.4
```

En los ordenadores de clase da error porque está utilizando un servidor que no está en la red. Pero desde casa sí que puedo enviar la petición sin problema.

```
Victor: ~ ❯ nslookup www.madrid.org 8.8.4.4
Servidor:  dns.google
Address:  8.8.4.4
```

Utiliza el comando nslookup para obtener las direcciones IP asociadas al nombre DNS www.educa.jcyl.es.

La dirección IP asociada es 10.16.159.21.

```
victor.garmur.1: ~ ❯ nslookup www.educa.jcyl.es
Servidor:  serviciosda.educa.jcyl.es
Address:  10.151.123.21

Nombre:  www.educa.jcyl.es
Address:  10.16.159.21
```

Utiliza el comando siguiente para descubrir sus servidores autorizados:

nslookup -type=ns www.educa.jcyl.es

Los servidores autorizados es el propio www.educa.jcyl.es y edgc0exp01.educa.jcyl.es.

```
victor.garmur.1: ~ ❯ nslookup -type=ns www.educa.jcyl.es
Servidor:  serviciosda.educa.jcyl.es
Address:  10.151.123.21

educa.jcyl.es
        primary name server = edgc0exp01.educa.jcyl.es
        responsible mail addr = hostmaster.educa.jcyl.es
```

Puedes comprobar en la respuesta su servidor autorizado. Ejecuta el siguiente comando para que te dé respuesta el servidor autorizado:

nslookup www.educa.jcyl.es edgc0exp01.educa.jcyl.es

```
victor.garmur.1: ~ ❯ nslookup www.educa.jcyl.es edgc0exp01.educa.jcyl.es
Servidor:  edgc0exp01.educa.jcyl.es
Address:  10.151.126.21

Nombre:  www.educa.jcyl.es
Address:  10.16.159.21
```

Observa que la respuesta sí es autorizada.

La respuesta es autorizada ya que no pone lo contrario.

```
Nombre:  www.educa.jcyl.es
Address:  10.16.159.21
```

Intenta realizar una consulta autorizada al servidor de la web www.madrid.org ¿qué sucede?

Aparecen los servidores autorizados con los que puedes acceder al dominio.

```
Victor: ~ ❯ nslookup -type=ns www.madrid.org
Servidor:  UnKnown
Address:  212.230.135.1

Respuesta no autoritativa:
www.madrid.org  canonical name = d3omk6xn5p4d3d.cloudfront.net
d3omk6xn5p4d3d.cloudfront.net   nameserver = ns-529.awsdns-02.net
d3omk6xn5p4d3d.cloudfront.net   nameserver = ns-1394.awsdns-46.org
d3omk6xn5p4d3d.cloudfront.net   nameserver = ns-1573.awsdns-04.co.uk
d3omk6xn5p4d3d.cloudfront.net   nameserver = ns-205.awsdns-25.com

ns-1394.awsdns-46.org   internet address = 205.251.197.114
ns-1394.awsdns-46.org   AAAA IPv6 address = 2600:9000:5305:7200::1
ns-1573.awsdns-04.co.uk internet address = 205.251.198.37
ns-1573.awsdns-04.co.uk AAAA IPv6 address = 2600:9000:5306:2500::1
ns-205.awsdns-25.com    internet address = 205.251.192.205
ns-205.awsdns-25.com    AAAA IPv6 address = 2600:9000:5300:cd00::1
ns-529.awsdns-02.net    internet address = 205.251.194.17
ns-529.awsdns-02.net    AAAA IPv6 address = 2600:9000:5302:1100::1
```

2. Linux

Inicia sesión en una máquina virtual con Linux (y acceso a internet)

Utiliza el comando nslookup para obtener las direcciones IP asociadas al nombre DNS www.madrid.org.

nslookup www.madrid.org

Las direcciones IP asociadas se muestran debajo de la dirección www.madrid.org no autorizada.

```
usuario@usuario:~$ nslookup www.madrid.org
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.madrid.org  canonical name = d3omk6xn5p4d3d.cloudfront.net.
Name:   d3omk6xn5p4d3d.cloudfront.net
Address: 108.157.109.87
Name:   d3omk6xn5p4d3d.cloudfront.net
Address: 108.157.109.10
Name:   d3omk6xn5p4d3d.cloudfront.net
Address: 108.157.109.2
Name:   d3omk6xn5p4d3d.cloudfront.net
Address: 108.157.109.78
Name:   d3omk6xn5p4d3d.cloudfront.net
Address: 2600:9000:237f:4e00:1a:83ee:1240:93a1
Name:   d3omk6xn5p4d3d.cloudfront.net
Address: 2600:9000:237f:b000:1a:83ee:1240:93a1
Name:   d3omk6xn5p4d3d.cloudfront.net
Address: 2600:9000:237f:e400:1a:83ee:1240:93a1
Name:   d3omk6xn5p4d3d.cloudfront.net
Address: 2600:9000:237f:a00:1a:83ee:1240:93a1
Name:   d3omk6xn5p4d3d.cloudfront.net
Address: 2600:9000:237f:9a00:1a:83ee:1240:93a1
Name:   d3omk6xn5p4d3d.cloudfront.net
Address: 2600:9000:237f:1600:1a:83ee:1240:93a1
Name:   d3omk6xn5p4d3d.cloudfront.net
Address: 2600:9000:237f:ba00:1a:83ee:1240:93a1
Name:   d3omk6xn5p4d3d.cloudfront.net
Address: 2600:9000:237f:ee00:1a:83ee:1240:93a1
```

Utiliza el comando dig para obtener las direcciones IP asociadas al nombre DNS www.google.es

```
dig www.google.es
```

En el apartado ANSWER SECTION, la segunda línea muestra la dirección IP asociada.

```
usuario@usuario:~$ dig www.google.es

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> www.google.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43128
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.es.                 IN      A

;; ANSWER SECTION:
www.google.es.          4       IN      CNAME   forcesafesearch.google.com.
forcesafesearch.google.com. 75934 IN    A       216.239.38.120

;; Query time: 9 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Oct 25 06:58:36 UTC 2024
;; MSG SIZE  rcvd: 98
```

Utiliza el comando dig para obtener el/los nombres de dominio asociados a la dirección IP 130.206.13.20.

```
dig –x 130.206.13.20
```

Desde la respuesta “ANSWER SECTION”, se puede ver el nombre de dominio asociado, que es www.redis.es.

```
usuario@usuario:~$ dig -x 130.206.13.20

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> -x 130.206.13.20
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46660
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;20.13.206.130.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
20.13.206.130.in-addr.arpa. 7200 IN     PTR     www.rediris.es.

;; Query time: 137 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Oct 25 07:48:47 UTC 2024
;; MSG SIZE  rcvd: 83
```

Utiliza el comando dig para obtener las direcciones IP asociadas al nombre DNS www.madrid.org preguntando al servidor DNS 8.8.4.4

dig @8.8.4.4 www.madrid.org

Este comando en el aula no muestra ninguna información relevante, ya que no puede acceder al servidor DNS 8.8.4.4.

```
usuario@usuario:~$ dig @8.8.4.4 www.madrid.org
;; communications error to 8.8.4.4#53: timed out
;; communications error to 8.8.4.4#53: timed out
;; communications error to 8.8.4.4#53: timed out

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> @8.8.4.4 www.madrid.org
; (1 server found)
;; global options: +cmd
;; no servers could be reached
```

Ejecutando el comando desde una maquina virtual en mi casa, se pueden ver las diferentes direcciones IP asociadas desde la sección de respuesta.

```
usuario@usuario:~$ dig @8.8.4.4 www.madrid.org

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> @8.8.4.4 www.madrid.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55294
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.madrid.org.                        IN      A

;; ANSWER SECTION:
www.madrid.org.         304     IN      CNAME   d3omk6xn5p4d3d.cloudfront.net.
d3omk6xn5p4d3d.cloudfront.net. 60 IN    A       108.157.109.87
d3omk6xn5p4d3d.cloudfront.net. 60 IN    A       108.157.109.2
d3omk6xn5p4d3d.cloudfront.net. 60 IN    A       108.157.109.10
d3omk6xn5p4d3d.cloudfront.net. 60 IN    A       108.157.109.78

;; Query time: 22 msec
;; SERVER: 8.8.4.4#53(8.8.4.4) (UDP)
;; WHEN: Fri Oct 25 20:32:40 UTC 2024
;; MSG SIZE  rcvd: 150
```

Utiliza el comando dig para obtener las direcciones IP asociadas al nombre DNS www.google.es preguntando al servidor DNS ns1.google.com

dig @ns1.google.com www.google.es

Investiga la información en la salida del comando ¿Cómo sabemos que esta respuesta proviene de un servidor autorizado?

La primera línea muestra la versión del comando dig.

La sección HEADER detalla la consulta y respuesta del servidor DNS.

Sección OPT:

1. EDNS: Extensión DNS (si se usa)
2. flags: Objetivo (si se especifica)
3. udp: Tamaño del paquete

Sección QUESTION:

1. Nombre del dominio (www.google.es)
2. Tipo de consulta (IN = Internet)
3. Tipo de registro (A = Dirección)

Sección ANSWER:

1. Nombre del servidor consultado (www.google.es)
2. Tiempo de vida (TTL)
3. Tipo de consulta (IN = Internet)
4. Tipo de registro (A = Dirección)
5. dirección IP asociada al nombre de dominio (142.250.185.3)

Fin del comando

1. Query time: Tiempo que tardó en responder
2. SERVER: Dirección IP y puerto del servidor DNS que responde
3. WHEN: Fecha y hora de ejecución del comando
4. MSG SIZE: Tamaño de la respuesta del servidor

```
usuario@usuario:~$ dig @ns1.google.com www.google.es

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> @ns1.google.com www.google.es
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29713
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.google.es.                 IN      A

;; ANSWER SECTION:
www.google.es.          300     IN      A       142.250.185.3

;; Query time: 31 msec
;; SERVER: 216.239.32.10#53(ns1.google.com) (UDP)
;; WHEN: Fri Oct 25 20:37:23 UTC 2024
;; MSG SIZE  rcvd: 58
```