DNS – Comandos

1.1 En la máquina virtual Prueba a hacer: $ nslookup www.educa.madrid.org

```
root@sriserver:/home/alumno# nslookup www.educa.madrid.org
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.educa.madrid.org
Address: 193.146.123.100
```

1.2 Repite el comando sobre el dominio

```
root@sriserver:/home/alumno# nslookup educa.madrid.org
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   educa.madrid.org
Address: 193.146.123.93
```

1.3 Ahora consulta solo el o los registros de servidores de nombres

```
root@sriserver:~# nslookup -query=NS educa.madrid.org
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
educa.madrid.org        nameserver = sun.rediris.es.
educa.madrid.org        nameserver = chico.rediris.es.

Authoritative answers can be found from:
```

1.4 Observa que puedes consultar hasta el registro SOA

```
root@sriserver:~# nslookup -query=SOA educa.madrid.org
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
educa.madrid.org
        origin = sun.rediris.es
        mail addr = iris-nic.rediris.es
        serial = 2022121400
        refresh = 14400
        retry = 7200
        expire = 2419200
        minimum = 7200

Authoritative answers can be found from:
```

1.5 Repite la primera consulta, pero haciéndosela al servidor de nombres de EducaMadrid

```
root@sriserver:~# nslookup www.educa.madrid.org ns1.csi-mad.es.colt.net
Server:         ns1.csi-mad.es.colt.net
Address:        212.74.77.56#53

Non-authoritative answer:
Name:   www.educa.madrid.org
Address: 193.146.123.100
```

¿Qué diferencia ves con la consulta del paso 1.1? ¿Qué quiere decir?
La principal diferencia entre estos dos comandos es que el segundo especifica un servidor de nombres específico al que se debe solicitar la información de DNS, mientras que el primero utiliza el servidor de nombres predeterminado.

¿Qué piensas que es el servidor ns1.csi-mad.es.colt.net?

Se solicita información sobre el nombre de dominio "www.educa.madrid.org" al servidor de nombres especificado, que en este caso es "ns1.csi-mad.es.colt.net".

¿Quién es “colt”?
"colt.net" es un dominio de nivel superior que se utiliza por la empresa Colt para sus servicios de internet y redes. Por lo tanto, "ns1.csi-mad.es.colt.net" es un nombre de servidor de nombres que pertenece a Colt y se utiliza para resolver nombres de dominio.

1.6 También se puede hacer una consulta inversa poniendo la dirección IP a consultar en lugar del nombre. ¿qué resultado obtienes? ¿por qué? ¿cómo es posible?

```
root@sriserver:~# nslookup 193.146.123.100
** server can't find 100.123.146.193.in-addr.arpa: NXDOMAIN
```

Si el comando `nslookup` devuelve "NXDOMAIN", significa que el servidor de nombres no ha podido encontrar una entrada de dominio para el nombre de dominio que has solicitado.

Hay varias razones por las que el servidor de nombres podría devolver "NXDOMAIN". Algunas posibles causas incluyen:

1. El nombre de dominio que has solicitado no existe: Si has escrito el nombre de dominio incorrectamente o si el nombre de dominio simplemente no existe, el servidor de nombres no podrá encontrar una entrada para él y devolverá "NXDOMAIN".
2. El servidor de nombres no está configurado correctamente: Si el servidor de nombres está configurado de manera incorrecta o está inaccesible, es posible que no pueda proporcionar información de DNS para el nombre de dominio que has solicitado.
3. El servidor de nombres no tiene información de DNS para el nombre de dominio: Si el servidor de nombres no tiene información de DNS para el nombre de dominio que has solicitado, devolverá "NXDOMAIN". Esto podría deberse a que el nombre de dominio no está registrado o a que el servidor de nombres no ha sincronizado su información de DNS con otros servidores de nombre

2. Comando host

2.1 El comando host es una opción básica y que devuelve información concreta. Es una versión simplificada de nslookup que devuelve un solo valor de conversión nombre <-> IP

```
root@sriserver:~# host www.educa.madrid.org
www.educa.madrid.org has address 193.146.123.100
```

2.2 También podemos consultar a un servidor concreto

```
root@sriserver:~# host www.educa.madrid.org 1.1.1.1
Using domain server:
Name: 1.1.1.1
Address: 1.1.1.1#53
Aliases:

www.educa.madrid.org has address 193.146.123.100
```

2.3 Y realizar consultas inversas

```
root@sriserver:~# host 1.1.1.1
1.1.1.1.in-addr.arpa domain name pointer one.one.one.one.
```

3. Comando whois

3.1 Instalación de la utilidad

```
root@sriserver:~# apt-get install whois
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Se instalarán los siguientes paquetes NUEVOS:
  whois
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 52 no actualizados.
Se necesita descargar 53,4 kB de archivos.
Se utilizarán 279 kB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu jammy/main amd64 whois amd64 5.5.13 [53,4 kB
Descargados 53,4 kB en 0s (121 kB/s)
```

3.2 Consulta sobre un dominio

```
root@sriserver:~# whois google.com
Web-based WHOIS:
  https://domains.markmonitor.com/whois

If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.

The data in MarkMonitor's WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name's registration record. While MarkMonitor believes the data to be accurate,
the data is provided "as is" with no guarantee or warranties regarding its
accuracy.

By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
  (1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
  (2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain name contacts (or
its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.

Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220
--
```

4. Comando dig

4.1 Ejecuta la siguiente consulta y documenta el resultado.

```
root@sriserver:~# whois google.com
Display all 166 possibilities? (y or n)
root@sriserver:~# dig educa.madrid.org

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> educa.madrid.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53054
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;educa.madrid.org.              IN      A

;; ANSWER SECTION:
educa.madrid.org.       601     IN      A       193.146.123.93

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Dec 20 18:00:48 UTC 2022
;; MSG SIZE  rcvd: 61
```

4.2 Ejecuta una consulta recursiva e interpreta el resultado con alguna búsqueda en Internet

```
root@sriserver:~# dig elmundo.es +trace @1.1.1.1

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> elmundo.es +trace @1.1.1.1
;; global options: +cmd
.                       4071    IN      NS      f.root-servers.net.
.                       4071    IN      NS      g.root-servers.net.
.                       4071    IN      NS      h.root-servers.net.
.                       4071    IN      NS      i.root-servers.net.
.                       4071    IN      NS      m.root-servers.net.
.                       4071    IN      NS      b.root-servers.net.
.                       4071    IN      NS      e.root-servers.net.
.                       4071    IN      NS      c.root-servers.net.
.                       4071    IN      NS      k.root-servers.net.
.                       4071    IN      NS      a.root-servers.net.
.                       4071    IN      NS      j.root-servers.net.
.                       4071    IN      NS      l.root-servers.net.
.                       4071    IN      NS      d.root-servers.net.
;; Received 267 bytes from 1.1.1.1#53(1.1.1.1) in 4 ms
```

¿Qué significa @1.1.1.1 en la consulta anterior?
El parámetro "@1.1.1.1" indica la dirección IP del servidor DNS que se utilizará para realizar la consulta.

En este caso, el comando "dig elmundo.es +trace @1.1.1.1" se utiliza para realizar una consulta de DNS para el dominio "elmundo.es" utilizando el servidor DNS en la dirección IP "1.1.1.1". La opción "trace" indica que se debe realizar un seguimiento completo de la consulta de DNS, mostrando todos los servidores DNS que se utilizan en el proceso de resolución del nombre de dominio.

4.3 Repite el paso 4.2. Verás que el resultado es diferente. ¿por qué?

```
root@sriserver:~# dig elmundo.es +trace @1.1.1.1

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> elmundo.es +trace @1.1.1.1
;; global options: +cmd
.                       3835    IN      NS      c.root-servers.net.
.                       3835    IN      NS      l.root-servers.net.
.                       3835    IN      NS      g.root-servers.net.
.                       3835    IN      NS      b.root-servers.net.
.                       3835    IN      NS      m.root-servers.net.
.                       3835    IN      NS      a.root-servers.net.
.                       3835    IN      NS      k.root-servers.net.
.                       3835    IN      NS      j.root-servers.net.
.                       3835    IN      NS      f.root-servers.net.
.                       3835    IN      NS      d.root-servers.net.
.                       3835    IN      NS      h.root-servers.net.
.                       3835    IN      NS      e.root-servers.net.
.                       3835    IN      NS      i.root-servers.net.
;; Received 267 bytes from 1.1.1.1#53(1.1.1.1) in 4 ms
```

Existen varias razones por las que el resultado de una consulta de DNS puede variar cada vez que se ejecuta el comando "dig". Algunas posibles explicaciones son:

1. La respuesta a una consulta de DNS puede variar dependiendo de la ubicación geográfica desde la que se realiza la consulta. Los servidores DNS pueden utilizar técnicas de balanceo de carga y georredirección para redirigir a los usuarios a servidores cercanos o más rápidos en función de su ubicación.
2. Los registros de DNS pueden cambiar con el tiempo. Por ejemplo, si el propietario del dominio "elmundo.es" modifica la configuración de DNS de su sitio web, esto podría afectar la respuesta a las consultas de DNS.
3. Los servidores DNS pueden utilizar técnicas de caché para almacenar temporalmente las respuestas a las consultas de DNS y proporcionarlas más rápidamente en el futuro. Si un servidor DNS utiliza caché, la respuesta a una consulta de DNS puede variar dependiendo de cuándo se realizó la última vez que se consultó ese registro.
4. Algunos servidores DNS pueden utilizar técnicas de "randomización" para distribuir la carga entre diferentes servidores de forma aleatoria. Esto puede hacer que las respuestas a las consultas de DNS varíen de una vez a otra.