Práctica 6:

Requisitos:

- Haber hecho la práctica 3.
- Durante todo el proceso de la práctica deberán hacerse capturas de imagen de cada uno de los pasos dados así como capturas y almacenaje de los paquetes de wireshark. Algunos de ellos serán solicitados por el profesor una vez concluida la práctica.
- Esta práctica ha de realizarse 2 veces. Una en clase y otra en casa, con configuraciones de reenvío diferente.

Antes de empezar:

- Recuerda que tienes a tu disposición la documentación de Zytrax donde puedes consultar sobre conceptos y sintaxis.
- Sustituye el valor 'XX' por tu número de puesto asignado que venimos utilizando
- Toma nota de todo lo que vayas haciendo, incluyendo errores y soluciones sobre los mismos, así como capturas
- Debes utilizar el cliente WindowsXX para hacer todas las consultas DNS de prueba.
- Recuerda que cada vez que actualices un fichero de zona tienes que incrementar el número de serie del SOA.
- Recuerda que dispones de 'rndc' para poder interactuar con los servidores DNS

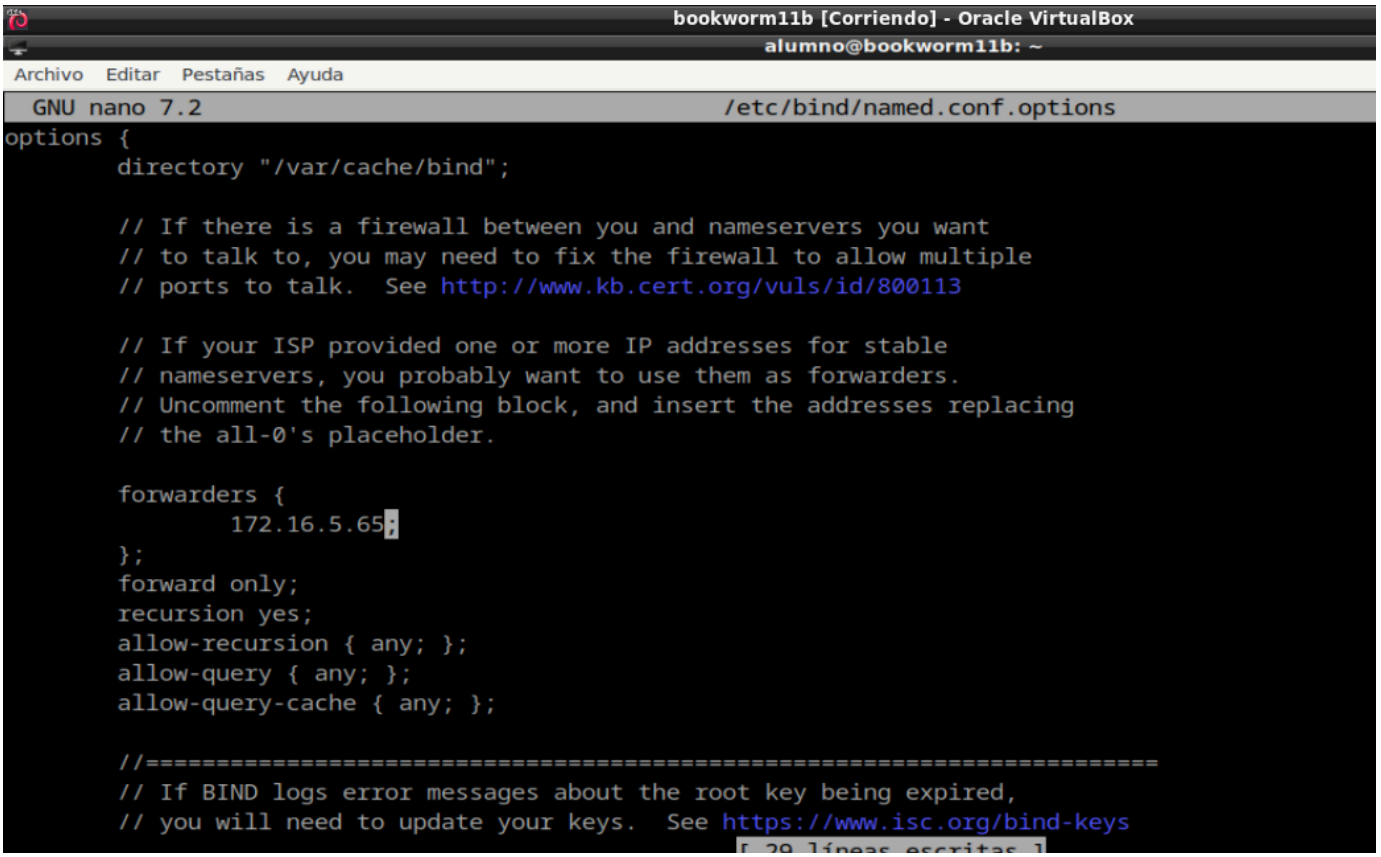
Prueba:

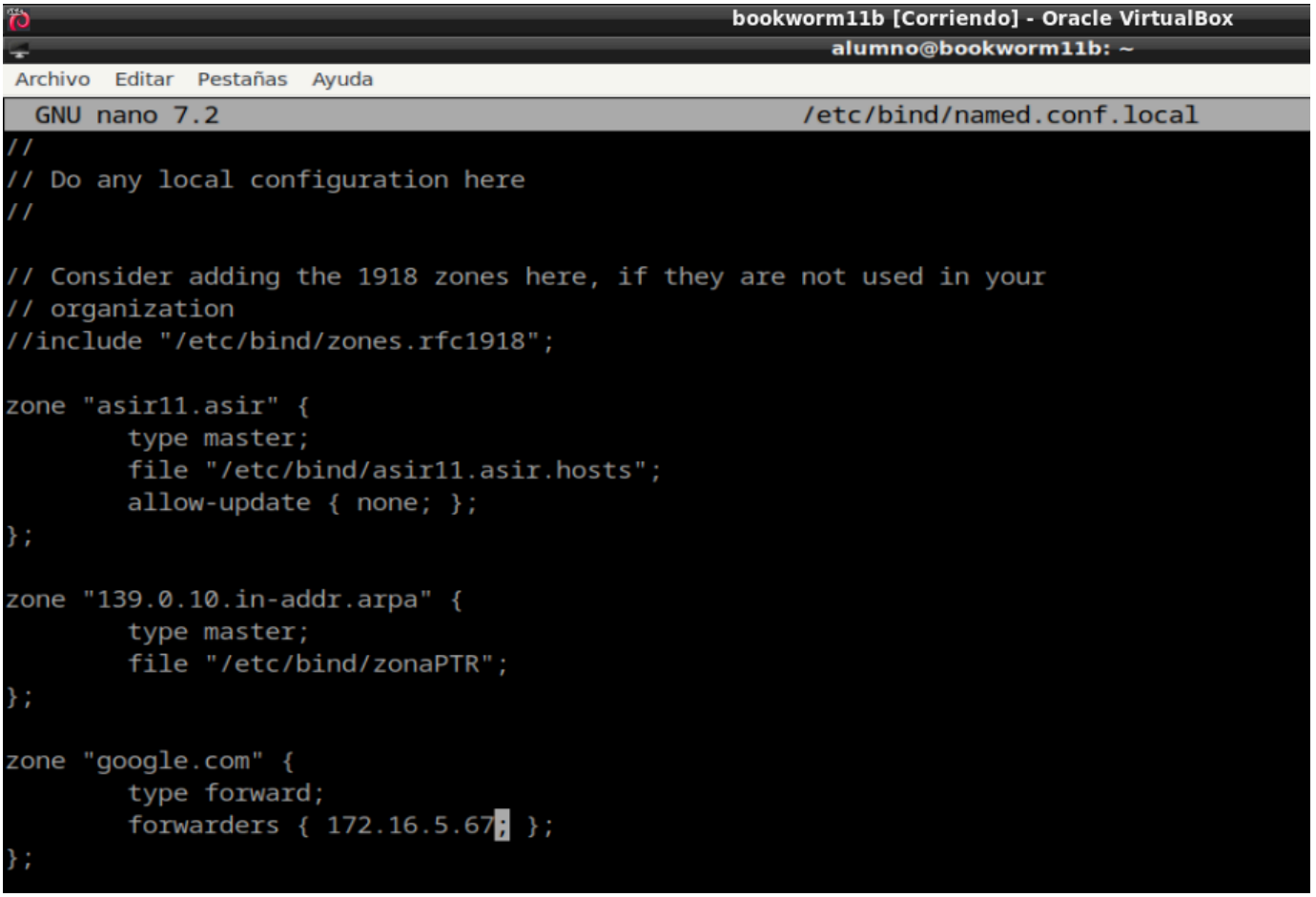
- Utiliza 'nslookup' para realizar las interrogaciones desde la máquina WINDOWSXX
- Dispones además de comandos de comprobación de sintaxis para el BIND9:
    - Podemos comprobar un archivo de configuración con, por ejemplo: named-checkconf /path/to/named.conf
    - Podemos comprobar una zona con, por ejemplo: named-checkzone example.net /etc/bind/example.net
    - Dispones de muchos otros comandos que te pueden resultar útiles en el apartado 15 del manual de BIND9, incluyendo la opción de interaccionar con los servidores DNS utilizando 'rndc'
    - En ocasiones puede ser bueno liberar la caché del servidor con el fin de que no use las resoluciones que se hayan producido momentos antes. Para ello podemos usar 'sudo rndc flush'

Pasos:

1. A partir de la configuración de la práctica 3, se pueden configurar reenviadores en el servidor B bien generales, bien para un dominio o dominios específicos.
2. La configuración para clase será: un reenviador general a la dirección 172.16.5.65 y un reenviador condicional para el dominio google.com al servidor 172.16.5.67. La configuración para casa será un reenviador general a la dirección 1.1.1.1 y un reenviador condicional para el dominio google.com al servidor 8.8.8.8.

CLASE:




bookworm11b [Corriendo] - Oracle VirtualBox
alumno@bookworm11b: ~
Archivo Editar Pestañas Ayuda
GNU nano 7.2 /etc/bind/named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "asir11.asir" {
type master;
file "/etc/bind/asir11.asir.hosts";
allow-update { none; };
};
zone "139.0.10.in-addr.arpa" {
type master;
file "/etc/bind/zonaPTR";
};
zone "google.com" {
type forward;
forwarders { 172.16.5.67; };
};

CASA:

alumno@bookworm11b: ~

Archivo Editar Pestañas Ayuda

GNU nano 7.2 /etc/bind/named.conf.options

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        forwarders {
                1.1.1.1;
        };
        forward only;
        recursion yes;
        allow-recursion { any; };
        allow-query { any; };
        allow-query-cache { any; };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation no;
        listen-on { any; };
        listen-on-v6 { any; };
};
```

alumno@bookworm11b: ~

Archivo Editar Pestañas Ayuda

GNU nano 7.2 /etc/bind/named.conf.local

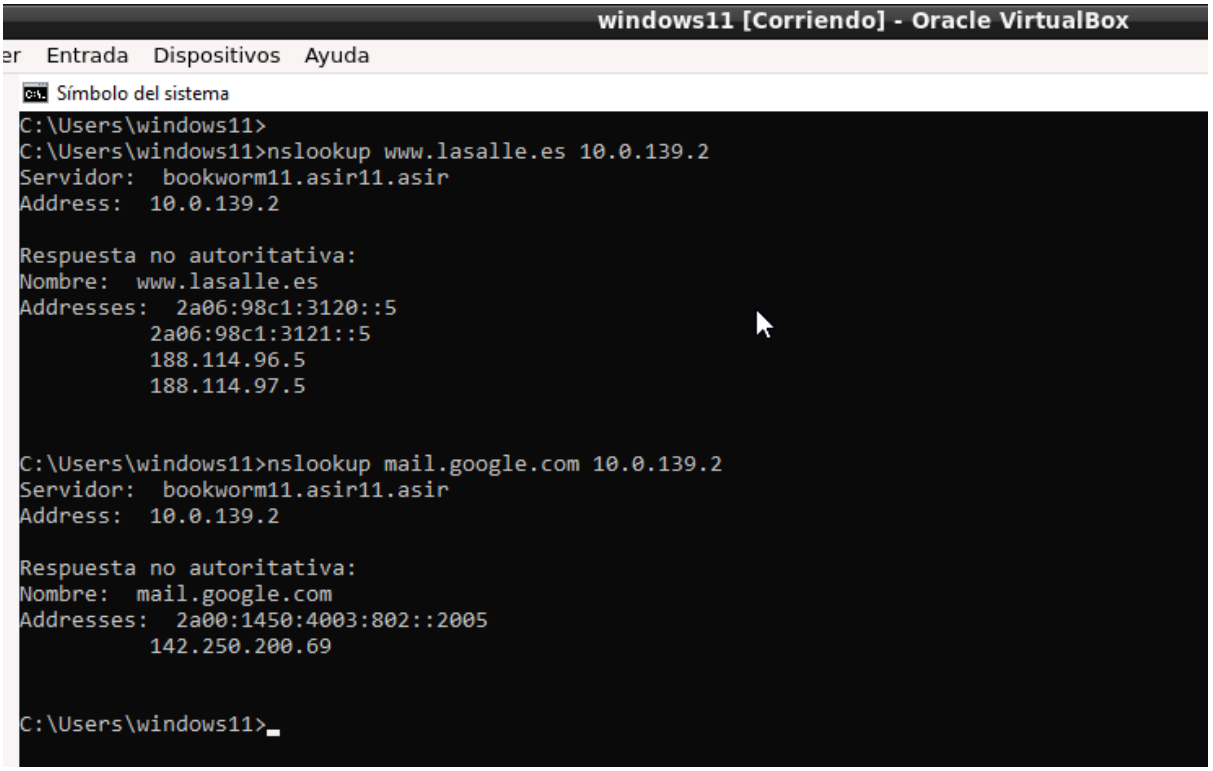
```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "asir11.asir" {
        type master;
        file "/etc/bind/asir11.asir.hosts";
        allow-update { none; };
};

zone "139.0.10.in-addr.arpa" {
        type master;
        file "/etc/bind/zonaPTR";
};

zone "google.com" {
        type forward;
        forwarders { 8.8.8.8; };
};
```

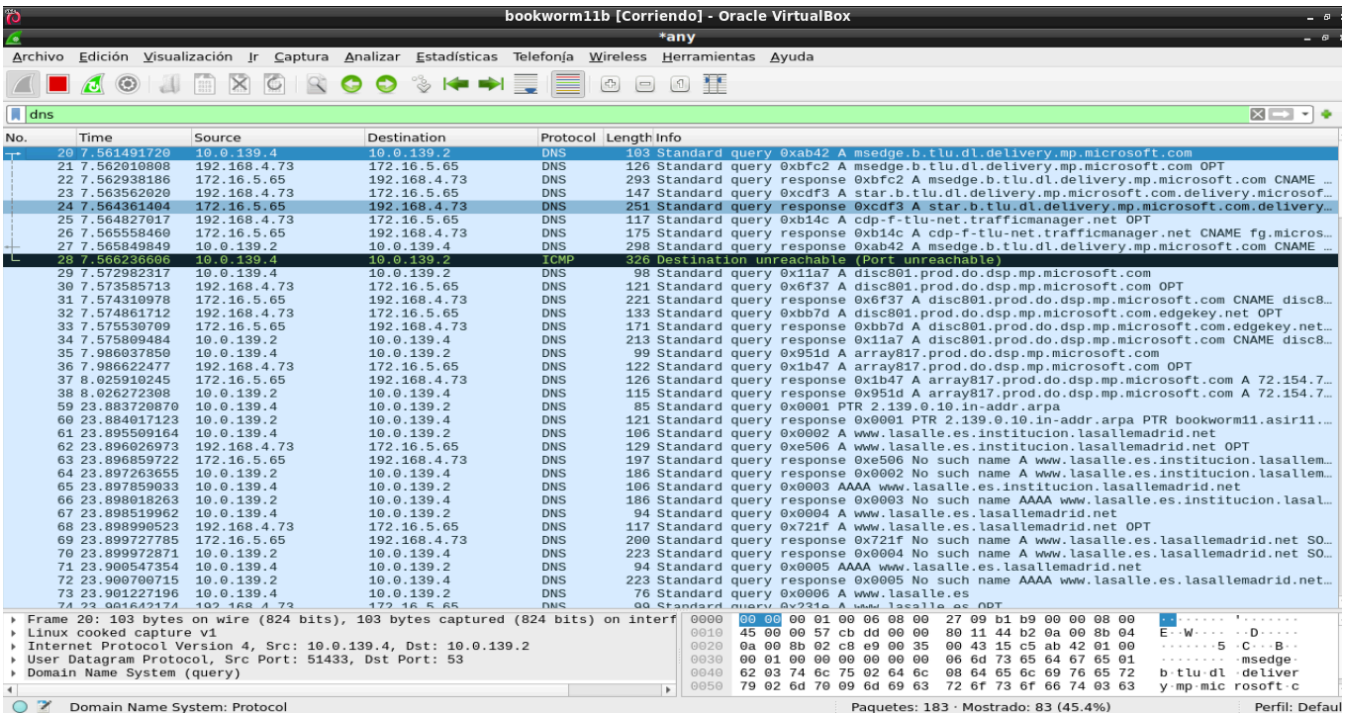
3. Si no tenemos ningún reenviador configurado el servidor DNS instalado en nuestro servidor B buscará hacer consultas recursivas para obtener respuestas, cachearlas y poder ofrecerlas al cliente WindowsXX. Si hacemos la configuración correspondiente que aparece en el punto 2 y optamos por la opción forward only nuestro servidor DNS dejará de usar la recursividad y reenviará las consultas a los servidores DNS configurados como reenviadores.

Pruebas

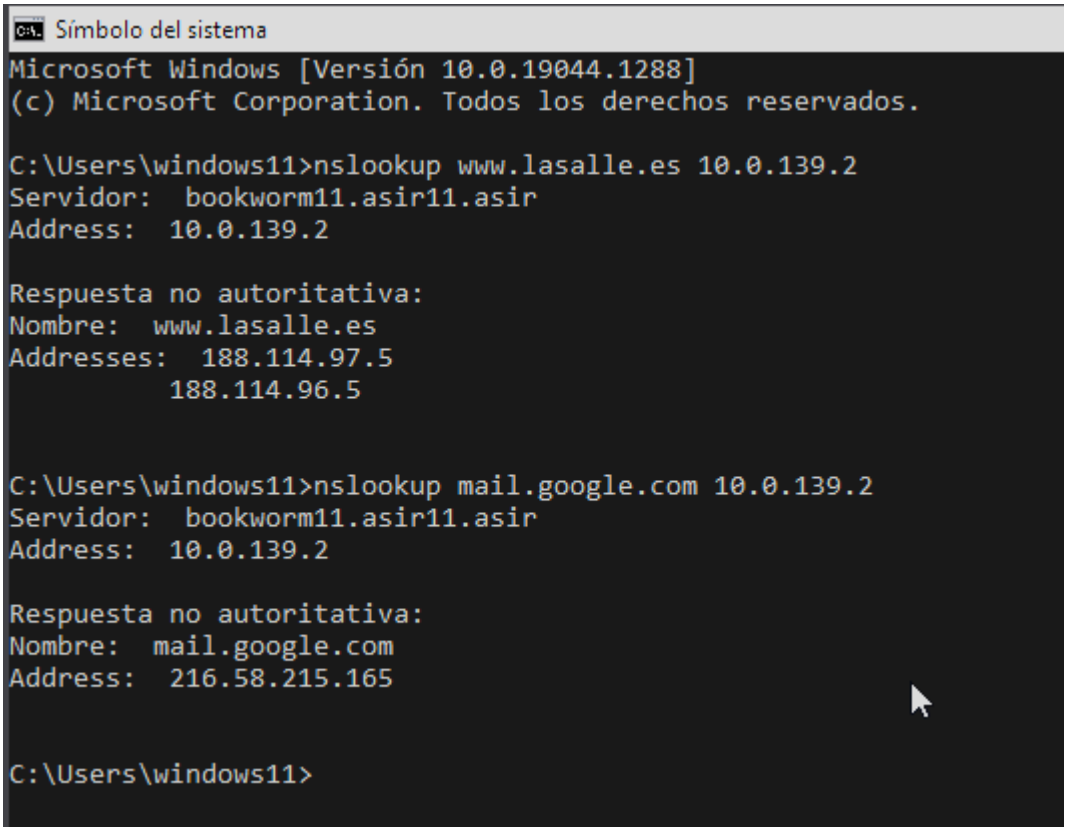
1. Consultas DNS a un registro www.lasalle.es y a un registro mail.google.com

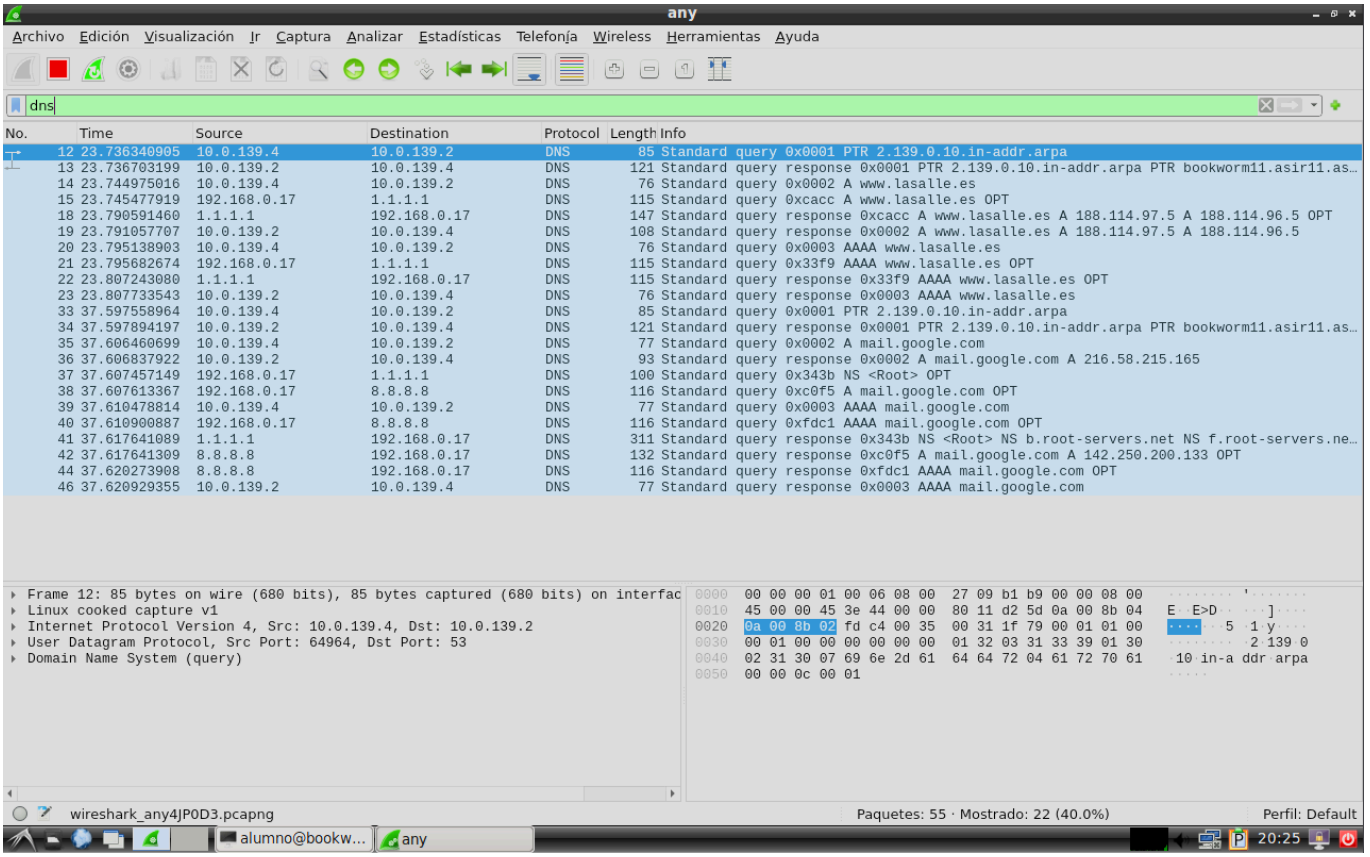
CLASE:




bookworm11b [Corriendo] - Oracle VirtualBox
*any
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
dns
No. Time Source Destination Protocol Length Info
20 7.561491720 10.0.139.4 10.0.139.2 DNS 103 Standard query 0xab42 A msedge.b.tlu.dl.delivery.mp.microsoft.com
21 7.562010808 192.168.4.73 172.16.5.65 DNS 126 Standard query 0xbfc2 A msedge.b.tlu.dl.delivery.mp.microsoft.com OPT
22 7.562938186 172.16.5.65 192.168.4.73 DNS 293 Standard query response 0xbfc2 A msedge.b.tlu.dl.delivery.mp.microsoft.com CNAME
23 7.563562020 192.168.4.73 172.16.5.65 DNS 147 Standard query 0xcdf3 A star.b.tlu.dl.delivery.mp.microsoft.com.delivery.microsof
24 7.564361404 172.16.5.65 192.168.4.73 DNS 251 Standard query response 0xcdf3 A star.b.tlu.dl.delivery.mp.microsoft.com.delivery
25 7.564827017 192.168.4.73 172.16.5.65 DNS 117 Standard query 0xb14c A cdp-f-tlu-net.trafficmanager.net OPT
26 7.565558460 172.16.5.65 192.168.4.73 DNS 175 Standard query response 0xb14c A cdp-f-tlu-net.trafficmanager.net CNAME fg.micros
27 7.565849849 10.0.139.2 10.0.139.4 DNS 298 Standard query response 0xab42 A msedge.b.tlu.dl.delivery.mp.microsoft.com CNAME
28 7.566236606 10.0.139.4 10.0.139.2 ICMP 326 Destination unreachable (Port unreachable)
29 7.572982317 10.0.139.4 10.0.139.2 DNS 98 Standard query 0x11a7 A disc801.prod.do.dsp.mp.microsoft.com
30 7.573585713 192.168.4.73 172.16.5.65 DNS 121 Standard query 0x6f37 A disc801.prod.do.dsp.mp.microsoft.com OPT
31 7.574310978 172.16.5.65 192.168.4.73 DNS 221 Standard query response 0x6f37 A disc801.prod.do.dsp.mp.microsoft.com CNAME disc8
32 7.574861712 192.168.4.73 172.16.5.65 DNS 133 Standard query 0xbb7d A disc801.prod.do.dsp.mp.microsoft.com.edgekey.net OPT
33 7.575530709 172.16.5.65 192.168.4.73 DNS 171 Standard query response 0xbb7d A disc801.prod.do.dsp.mp.microsoft.com.edgekey.net
34 7.575809484 10.0.139.2 10.0.139.4 DNS 213 Standard query response 0x11a7 A disc801.prod.do.dsp.mp.microsoft.com CNAME disc8
35 7.986037850 10.0.139.4 10.0.139.2 DNS 99 Standard query 0x951d A array817.prod.do.dsp.mp.microsoft.com
36 7.986622477 192.168.4.73 172.16.5.65 DNS 122 Standard query 0x1b47 A array817.prod.do.dsp.mp.microsoft.com OPT
37 8.025910245 172.16.5.65 192.168.4.73 DNS 126 Standard query response 0x1b47 A array817.prod.do.dsp.mp.microsoft.com A 72.154.7
38 8.026272308 10.0.139.2 10.0.139.4 DNS 115 Standard query response 0x951d A array817.prod.do.dsp.mp.microsoft.com A 72.154.7
59 23.883720870 10.0.139.4 10.0.139.2 DNS 85 Standard query 0x0001 PTR 2.139.0.10.in-addr.arpa
60 23.884017123 10.0.139.2 10.0.139.4 DNS 121 Standard query response 0x0001 PTR 2.139.0.10.in-addr.arpa PTR bookworm11.asir11.
61 23.895509164 10.0.139.4 10.0.139.2 DNS 106 Standard query 0x0002 A www.lasalle.es.institucion.lasallemadrid.net
62 23.896026973 192.168.4.73 172.16.5.65 DNS 129 Standard query 0xe506 A www.lasalle.es.institucion.lasallemadrid.net OPT
63 23.896859722 172.16.5.65 192.168.4.73 DNS 197 Standard query response 0xe506 No such name A www.lasalle.es.institucion.lasallem
64 23.897263655 10.0.139.2 10.0.139.4 DNS 186 Standard query response 0x0002 No such name A www.lasalle.es.institucion.lasallem
65 23.897859033 10.0.139.4 10.0.139.2 DNS 106 Standard query 0x0003 AAAA www.lasalle.es.institucion.lasallemadrid.net
66 23.898018263 10.0.139.2 10.0.139.4 DNS 186 Standard query response 0x0003 No such name AAAA www.lasalle.es.institucion.lasal
67 23.898519962 10.0.139.4 10.0.139.2 DNS 94 Standard query 0x0004 A www.lasalle.es.lasallemadrid.net
68 23.898990523 192.168.4.73 172.16.5.65 DNS 117 Standard query 0x721f A www.lasalle.es.lasallemadrid.net OPT
69 23.899727785 172.16.5.65 192.168.4.73 DNS 200 Standard query response 0x721f No such name A www.lasalle.es.lasallemadrid.net SO
70 23.899972871 10.0.139.2 10.0.139.4 DNS 223 Standard query response 0x0004 No such name A www.lasalle.es.lasallemadrid.net SO
71 23.900547354 10.0.139.4 10.0.139.2 DNS 94 Standard query 0x0005 AAAA www.lasalle.es.lasallemadrid.net
72 23.900700715 10.0.139.2 10.0.139.4 DNS 223 Standard query response 0x0005 No such name AAAA www.lasalle.es.lasallemadrid.net
73 23.901227196 10.0.139.4 10.0.139.2 DNS 76 Standard query 0x0006 A www.lasalle.es
Frame 20: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interf
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.0.139.4, Dst: 10.0.139.2
User Datagram Protocol, Src Port: 51433, Dst Port: 53
Domain Name System (query)
0000 00 00 00 01 00 06 08 00 27 09 b1 b9 00 00 08 00
0010 45 00 00 57 cb dd 00 00 80 11 44 b2 0a 00 8b 04
0020 0a 00 8b 02 c8 e9 00 35 00 43 15 c5 ab 42 01 00
0030 00 01 00 00 00 00 00 00 06 6d 73 65 64 67 65 01
0040 62 03 74 6c 75 02 64 6c 08 64 65 6c 69 76 65 72
0050 79 02 6d 70 09 6d 69 63 72 6f 73 6f 66 74 03 63
Domain Name System: Protocol
Paquetes: 183 · Mostrado: 83 (45.4%)
Perfil: Defaul

CASA:


Símbolo del sistema
Microsoft Windows [Versión 10.0.19044.1288]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Users\windows11>nslookup www.lasalle.es 10.0.139.2
Servidor: bookworm11.asir11.asir
Address: 10.0.139.2
Respuesta no autoritativa:
Nombre: www.lasalle.es
Addresses: 188.114.97.5
188.114.96.5
C:\Users\windows11>nslookup mail.google.com 10.0.139.2
Servidor: bookworm11.asir11.asir
Address: 10.0.139.2
Respuesta no autoritativa:
Nombre: mail.google.com
Address: 216.58.215.165
C:\Users\windows11>



2. Mismas consultas anteriores pero forzando la no recursividad con `set norecurse`

CLASE:

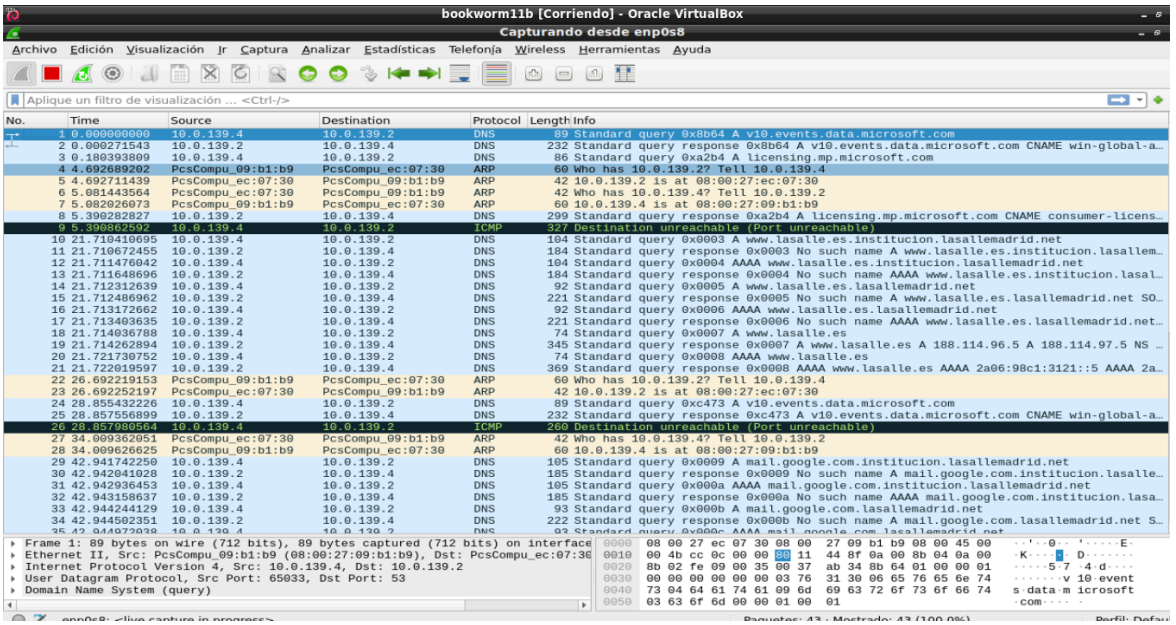
windows11 [Corriendo] - Oracle VirtualBox

Ver Entrada Dispositivos Ayuda

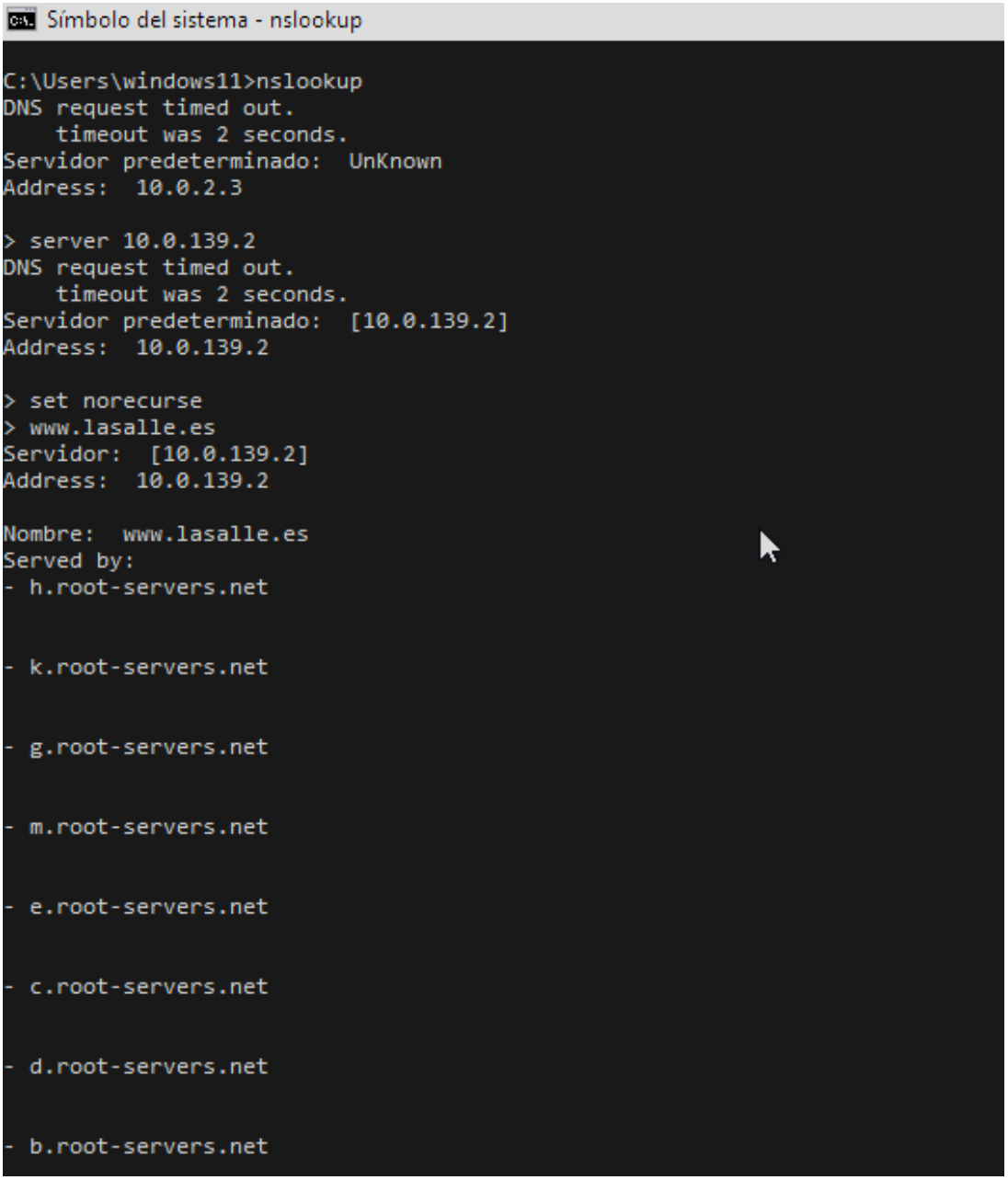
Símbolo del sistema - nslookup

```
C:\Users\windows11>nslookup
Servidor predeterminado:  UnKnown
Address:  10.0.2.3

> server 10.0.139.2
Servidor predeterminado:  [10.0.139.2]
Address:  10.0.139.2

> set norecurse
> www.lasalle.es
Servidor:  [10.0.139.2]
Address:  10.0.139.2

Respuesta no autoritativa:
Nombre:  www.lasalle.es
Addresses:  2a06:98c1:3121::5
          2a06:98c1:3120::5
          188.114.96.5
          188.114.97.5

> mail.google.com
Servidor:  [10.0.139.2]
Address:  10.0.139.2

Respuesta no autoritativa:
Nombre:  mail.google.com
Address:  142.250.200.69

>
```

En este caso como el servidor tiene en cache la información de la consulta anterior me da la misma respuesta pero si no la tiene me daría referencias a los servidores encargados de ese dominio



CASA:


Símbolo del sistema - nslookup
C:\Users\windows11>nslookup
DNS request timed out.
timeout was 2 seconds.
Servidor predeterminado: UnKnown
Address: 10.0.2.3
> server 10.0.139.2
DNS request timed out.
timeout was 2 seconds.
Servidor predeterminado: [10.0.139.2]
Address: 10.0.139.2
> set norecurse
> www.lasalle.es
Servidor: [10.0.139.2]
Address: 10.0.139.2
Nombre: www.lasalle.es
Served by:
- h.root-servers.net
- k.root-servers.net
- g.root-servers.net
- m.root-servers.net
- e.root-servers.net
- c.root-servers.net
- d.root-servers.net
- b.root-servers.net

Símbolo del sistema - nslookup

```
>
> mail.google.com
Servidor:  [10.0.139.2]
Address:  10.0.139.2

Nombre:  mail.google.com
Served by:
- j.root-servers.net


- a.root-servers.net


- m.root-servers.net


- l.root-servers.net


- c.root-servers.net


- f.root-servers.net


- g.root-servers.net


- b.root-servers.net


- d.root-servers.net


- h.root-servers.net
```