<u>Práctica 7</u>:

Requisitos:

- Haber hecho la práctica 5.
- 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.

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 LinuxXX 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

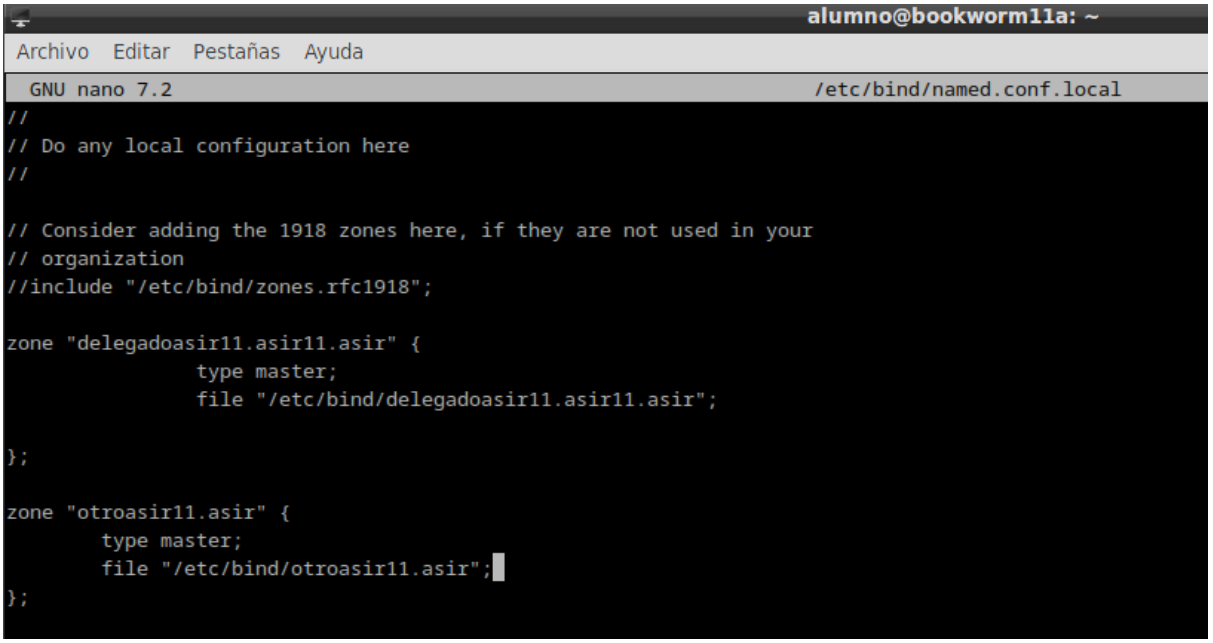
Prueba:

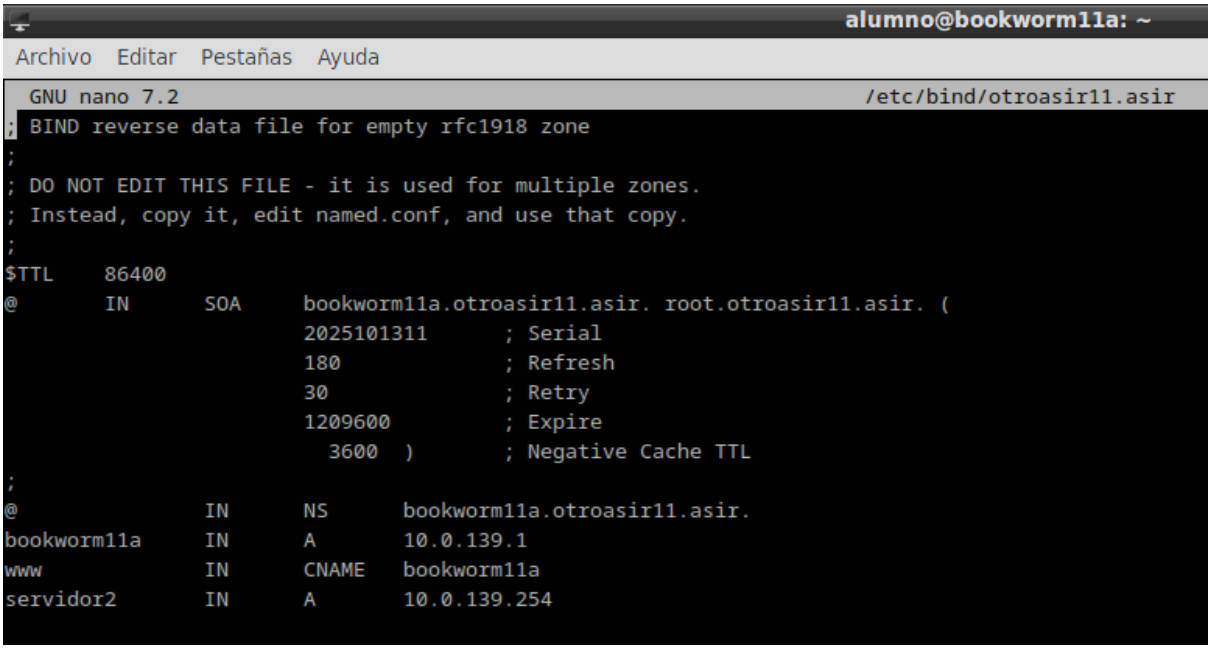
- Hay que utilizar el comando 'dig' para todas la pruebas
- Dispones además de comandos de comprobación de sintaxis para el BIND9:
    - Podemos comprobar un archivo de configuración con, por ejemplo: named-checkconf /path/to/named.conf
    - Podemos comprobar una zona con, por ejemplo: named-checkzone 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'

Pasos:

1. Crea una nueva zona maestra de resolución directa en 'BOOKWORMXXA' denominada "otroasirXX.asir" con las siguientes características y haz las correspondientes pruebas que verifiquen su correcto funcionamiento.
    1. SOA: bookwormXXa.otroasirXX.asir y parámetros de tiempo como en prácticas anteriores, salvo los indicados en las siguientes líneas
    2. NS: bookwormXXa.otroasirXX.asir.
    3. A: 10.0.128+XX.1 es la IP de bookwormXXa.otroasirXX.asir.
    4. CNAME: www es alias de bookwormXXa.otroasirXX.asir.
    5. Servidor2 tiene como IP 10.0.128+XX.254

6. El tiempo de refresco de la zona será de 180 segundos y el de reintento será de 30 segundos





2. Pon a capturar el tráfico en uno de los servidores
3. Crea una nueva zona "esclava" de resolución directa en BOOKWORMXXB denominada "otroasirXX.asir" (la zona del servidor maestro y del esclavo tienen que llamarse igual. El servidor maestro será 'bookwormXXa'. Se indicará con la correspondiente IP. Al recargar la configuración debería producirse una solicitud de SOA y la correspondiente transferencia de zona. Observa el tráfico que se produce y pregunta al servidor B por 'servidor2.otroasirXX.asir' para constatar que funciona.

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; };
};

zone "otroasir11.asir" {
        type slave;
        file "otroasir11.asir";
        masters { 10.0.139.1; };
};
```

alumno@bookworm11a: /etc/systemd/network

Archivo Editar Pestañas Ayuda

```
alumno@bookworm11a:/etc/systemd/network$ sudo wiresahrk
[sudo] contraseña para alumno:
sudo: a password is required
alumno@bookworm11a:/etc/systemd/network$ sudo wireshark
```

enp0s8

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

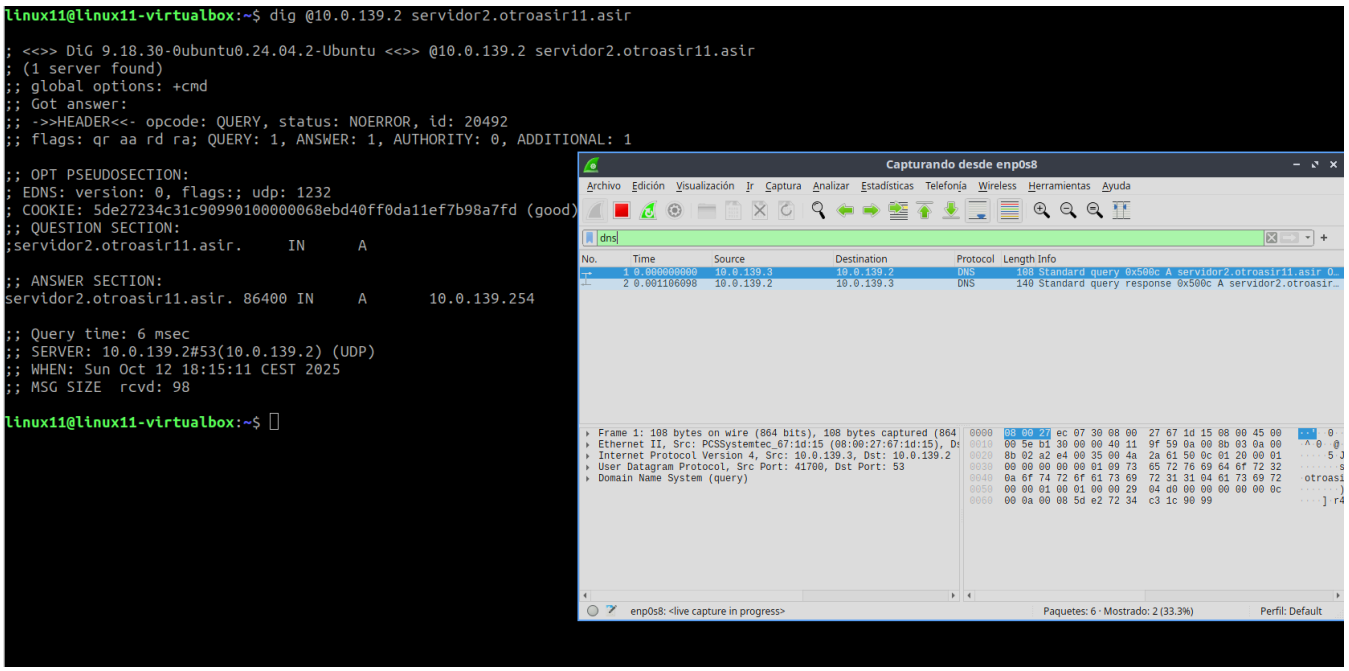
dns

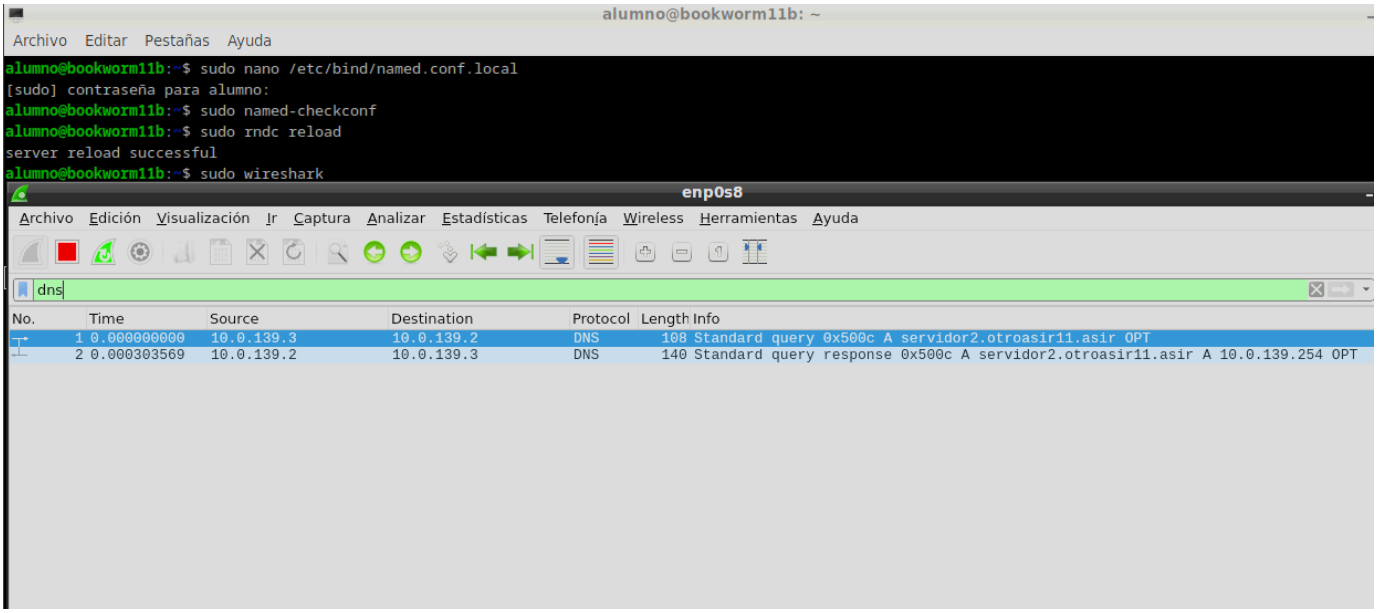
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.139.2	10.0.139.1	DNS	90	Standard query 0xc77b SOA otroasir11.asir OPT
2	0.000373804	10.0.139.1	10.0.139.2	DNS	177	Standard query response 0xc77b SOA otroasir11.asir SOA bookworm11a.otroasir11.…
6	0.002459561	10.0.139.2	10.0.139.1	DNS	101	Standard query 0xac1e AXFR otroasir11.asir
8	0.004188892	10.0.139.1	10.0.139.2	DNS	264	Standard query response 0xac1e AXFR otroasir11.asir SOA bookworm11a.otroasir11…

```
▸ Frame 6: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on inte
▸ Ethernet II, Src: PcsCompu_ec:07:30 (08:00:27:ec:07:30), Dst: PcsCompu_ce:c2
▸ Internet Protocol Version 4, Src: 10.0.139.2, Dst: 10.0.139.1
▸ Transmission Control Protocol, Src Port: 42721, Dst Port: 53, Seq: 1, Ack: 1,
▸ Domain Name System (query)
```

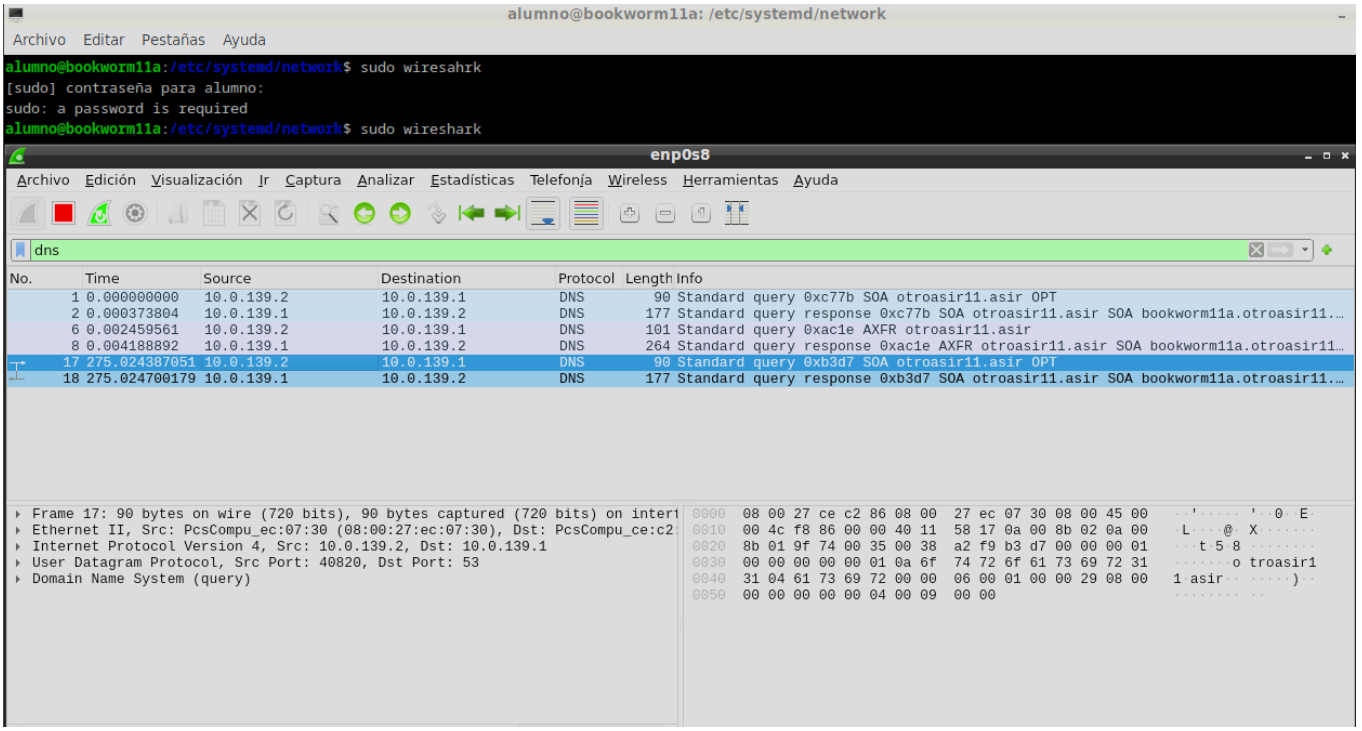
```
0000  08 00 27 ce c2 86 08 00  27 ec 07 30 08 00 45 00   ··'·····  '··0··E·
0010  00 57 47 43 40 00 40 06  c9 5a 0a 00 8b 02 0a 00   ·WGC@·@·  ·Z······
0020  8b 01 a6 e1 00 35 a1 aa  43 8b a0 45 a9 5a 80 18   ·····5··  C··E·Z··
0030  01 fa f9 97 00 00 01 01  08 0a 01 f6 4a ed db e4   ········  ····J···
0040  d9 3e 00 21 ac 1e 00 00  00 01 00 00 00 00 00 00   ·>·!····  ········
0050  0a 6f 74 72 6f 61 73 69  72 31 31 04 61 73 69 72   ·otroasi r11·asir
0060  00 00 fc 00 01                                    ·····
```

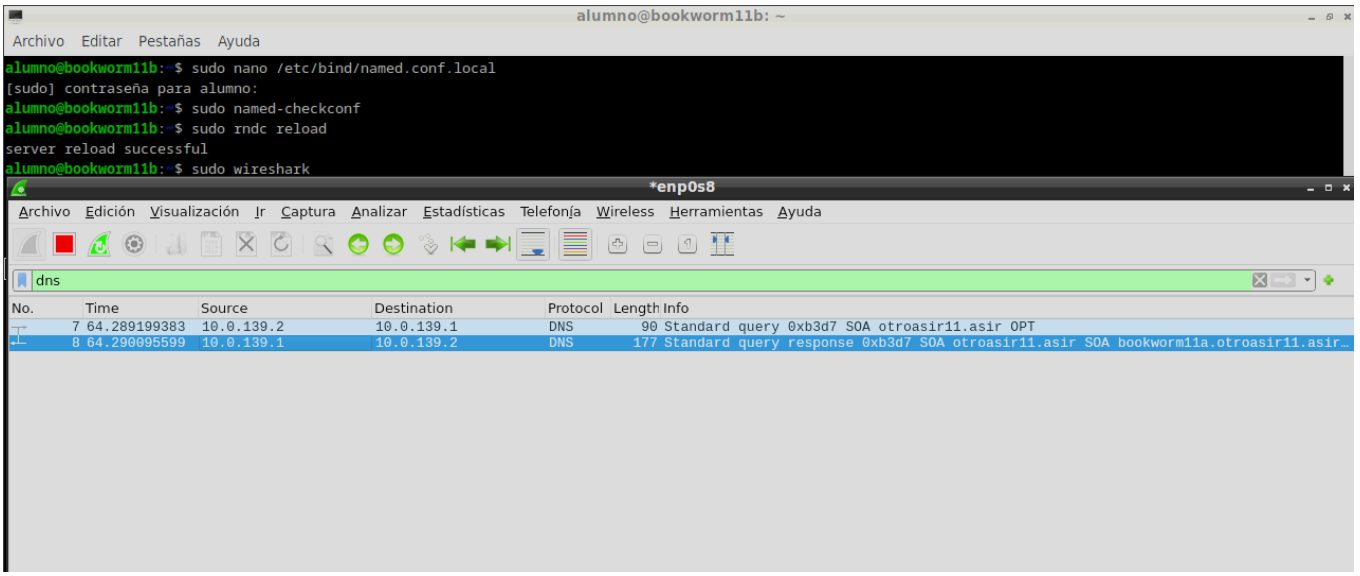
Domain Name System: Protocol — Paquetes: 16 · Mostrado: 4 (25.0%) — Perfil: Default



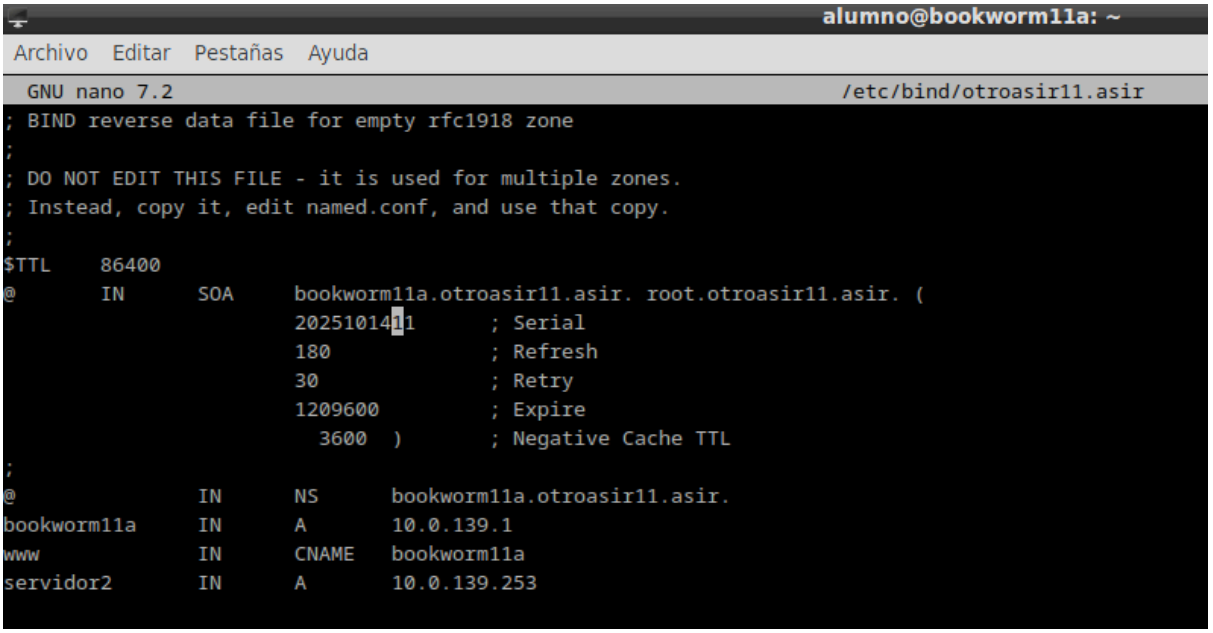


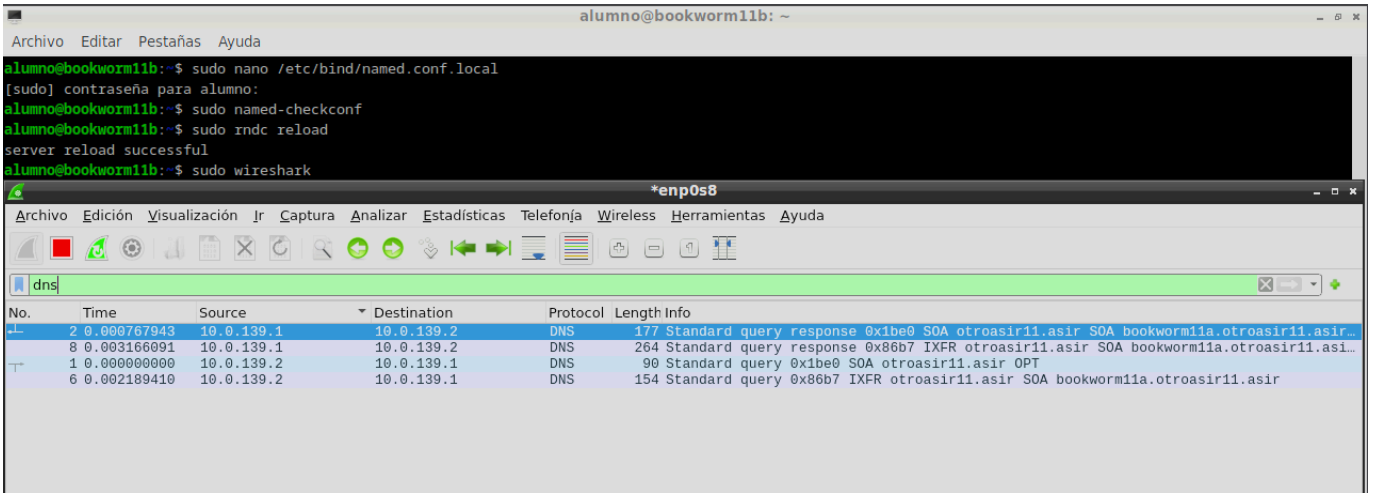
4. Observa como cada cierto tiempo se produce la consulta del SOA por parte del esclavo pero no hay transferencia de zona

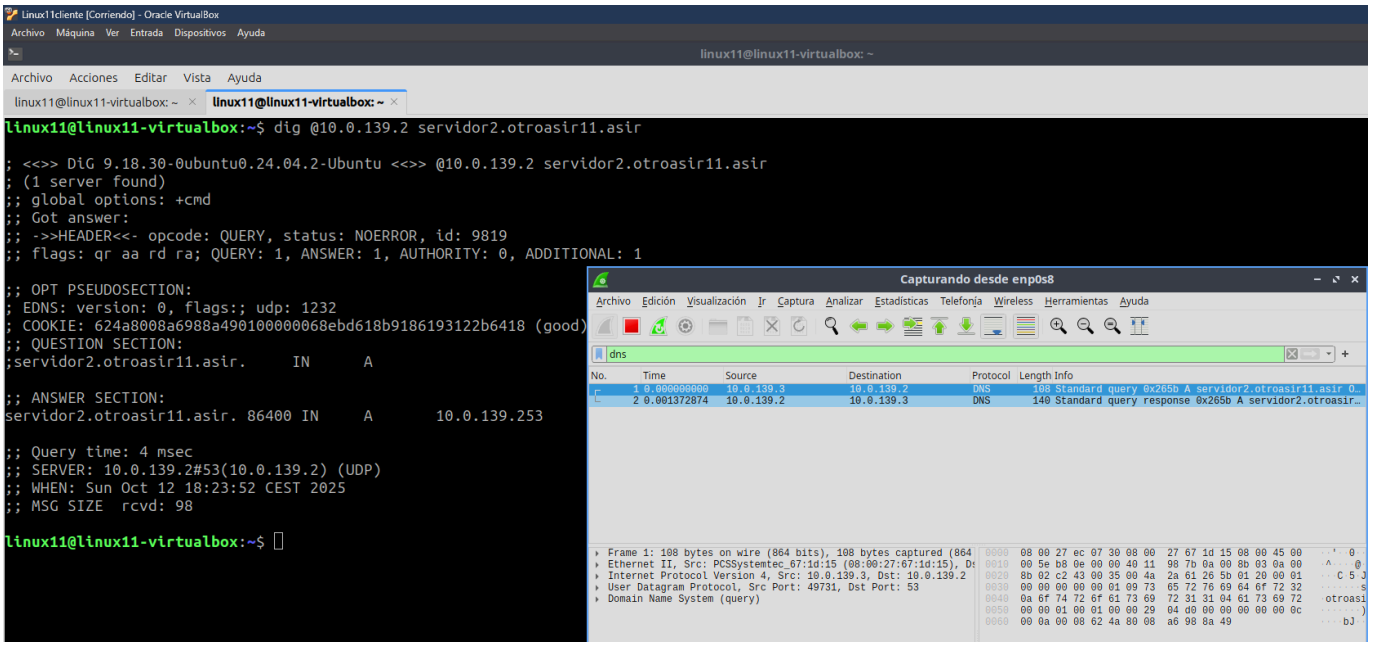




5. Modifica la zona maestra cambiando la IP 10.0.128+XX.254 por la 253, cambia el número de serie y recarga la zona. Observa si al recargar la zona se produce una notificación inmediata, una solicitud de SOA y la transferencia IXFR que permita actualizar la IP que ha cambiado.


alumno@bookworm11a: ~
Archivo Editar Pestañas Ayuda
GNU nano 7.2 /etc/bind/otroasir11.asir
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL 86400
@ IN SOA bookworm11a.otroasir11.asir. root.otroasir11.asir. (
2025101411 ; Serial
180 ; Refresh
30 ; Retry
1209600 ; Expire
3600) ; Negative Cache TTL
;
@ IN NS bookworm11a.otroasir11.asir.
bookworm11a IN A 10.0.139.1
www IN CNAME bookworm11a
servidor2 IN A 10.0.139.253


alumno@bookworm11b: ~
Archivo Editar Pestañas Ayuda
alumno@bookworm11b:~$ sudo nano /etc/bind/named.conf.local
[sudo] contraseña para alumno:
alumno@bookworm11b:~$ sudo named-checkconf
alumno@bookworm11b:~$ sudo rndc reload
server reload successful
alumno@bookworm11b:~$ sudo wireshark
*enp0s8
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
dns
No. Time Source Destination Protocol Length Info
2 0.000767943 10.0.139.1 10.0.139.2 DNS 177 Standard query response 0x1be0 SOA otroasir11.asir SOA bookworm11a.otroasir11.asir
8 0.003166091 10.0.139.1 10.0.139.2 DNS 264 Standard query response 0x86b7 IXFR otroasir11.asir SOA bookworm11a.otroasir11.asi
1 0.000000000 10.0.139.2 10.0.139.1 DNS 90 Standard query 0x1be0 SOA otroasir11.asir OPT
6 0.002189410 10.0.139.2 10.0.139.1 DNS 154 Standard query 0x86b7 IXFR otroasir11.asir SOA bookworm11a.otroasir11.asir


Linux11cliente [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
linux11@linux11-virtualbox: ~
Archivo Acciones Editar Vista Ayuda
linux11@linux11-virtualbox: ~
linux11@linux11-virtualbox: ~
linux11@linux11-virtualbox:~$ dig @10.0.139.2 servidor2.otroasir11.asir
; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @10.0.139.2 servidor2.otroasir11.asir
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9819
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 624a8008a6988a490100000068ebd618b9186193122b6418 (good)
;; QUESTION SECTION:
;servidor2.otroasir11.asir. IN A
;; ANSWER SECTION:
servidor2.otroasir11.asir. 86400 IN A 10.0.139.253
;; Query time: 4 msec
;; SERVER: 10.0.139.2#53(10.0.139.2) (UDP)
;; WHEN: Sun Oct 12 18:23:52 CEST 2025
;; MSG SIZE rcvd: 98
linux11@linux11-virtualbox:~$
Capturando desde enp0s8
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
dns
No. Time Source Destination Protocol Length Info
1 0.000000000 10.0.139.3 10.0.139.2 DNS 108 Standard query 0x265b A servidor2.otroasir11.asir O
2 0.001372874 10.0.139.2 10.0.139.3 DNS 140 Standard query response 0x265b A servidor2.otroasir
Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864
Ethernet II, Src: PCSSystemtec_67:1d:15 (08:00:27:67:1d:15), Ds
Internet Protocol Version 4, Src: 10.0.139.3, Dst: 10.0.139.2
User Datagram Protocol, Src Port: 49731, Dst Port: 53
Domain Name System (query)