

## **Práctica 5:**

### **Requisitos:**

- Haber hecho la práctica 4.
- 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 tanto el cliente LinuxXX como 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

### **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

### **Pasos:**

1. Preparación y acondicionamiento de la máquina BOOKWORMXXA como servidor DNS
  1. A partir de la máquina virtual clonada en origen crea una nueva máquina llamado BOOKWORMXXA, con características análogas a BOOKWORMXXB, pero con la dirección IP 10.0.128+XX.1/24 y el correspondiente cambio de nombre.

```
bookworm11a [Corriendo] - Oracle VirtualBox
alumno@bookworm11a: /etc/systemd/network

Archivo  Editar  Pestañas  Ayuda

alumno@bookworm11a:~$ cd /etc/systemd/network/
alumno@bookworm11a:/etc/systemd/network$ ls
20-wired.network  21-internal.network  loopback.network
alumno@bookworm11a:/etc/systemd/network$ sudo nano 20-wired.network
[sudo] contraseña para alumno:
Lo siento, pruebe otra vez.
[sudo] contraseña para alumno:
alumno@bookworm11a:/etc/systemd/network$ sudo nano 21-internal.network
alumno@bookworm11a:/etc/systemd/network$
```

```
bookworm11a [Corriendo] - Oracle VirtualBox
alumno@bookworm11a: /etc/systemd/network

Archivo  Editar  Pestañas  Ayuda

GNU nano 7.2 21-internal.network *

[Match]
Name= enp0s8

[Network]
Address= 10.0.139.1/24
```

2. Con respecto a la configuración de red, usa systemd-networkd para la configuración:
  - En el adaptador externo (enp0s3) desactiva el uso del DNS ofrecido por el servidor DHCP (UseDNS=false)

```
bookworm11a [Corriendo] - Oracle VirtualBox
alumno@bookworm11a: /etc/systemd/network

Archivo  Editar  Pestañas  Ayuda

GNU nano 7.2 20-wired.network

[Match]
Name=enp0s3

[Network]
DHCP=yes

[DHCPv4]
UseDNS=false

[DHCPv6]
UseDNS=false
```

- En el adaptador interno (enp0s8) especifica como DNS la propia máquina inicialmente (DNS=10.0.128+XX.1)

```

bookworm11a [Corriendo] - Oracle VirtualBox
alumno@bookworm11a: /etc/systemd/network

GNU nano 7.2 21-internal.network

[Match]
Name= enp0s8

[Network]
Address= 10.0.139.1/24
DNS=10.0.139.1

```

3. Con respecto a la configuración DNS hazla con systemd-resolved. En /etc/systemd/resolved.conf especifica:
  - Como servidor el 10.0128+XX.2
  - Deshabilita el DNSStubListener poniendo  
DNSStubListener=no

```

bookworm11a [Corriendo] - Oracle VirtualBox
alumno@bookworm11a: /etc/systemd/network

GNU nano 7.2 /etc/systemd/resolved.conf

#
# See resolved.conf(5) for details.

[Resolve]
# Some examples of DNS servers which may be used for DNS= and FallbackDNS=:
# Cloudflare: 1.1.1.1#cloudflare-dns.com 1.0.0.1#cloudflare-dns.com 2606:4700:4700::1111#
# Google:      8.8.8.8#dns.google 8.8.4.4#dns.google 2001:4860:4860::8888#dns.google 2001:
# Quad9:       9.9.9.9#dns.quad9.net 149.112.112.112#dns.quad9.net 2620:fe::fe#dns.quad9.n
#DNS=
#FallbackDNS=
#Domains=
#DNSSEC=no
#DNSOverTLS=no
#MulticastDNS=yes
#LLMNR=yes
#Cache=yes
#CacheFromLocalhost=no
#DNSStubListener=yes
#DNSStubListenerExtra=
#ReadEtcHosts=yes
#ResolveUnicastSingleLabel=no
DNS=10.0.139.2
DNSStubListener=no

```

[ 36 líneas escritas ]

^G Ayuda    ^O Guardar    ^W Buscar    ^K Cortar    ^T Ejecutar    ^C Ubicar  
 ^X Salir    ^R Leer fich.    ^\ Reemplazar    ^U Pegar    ^J Justificar    ^/ Ir a l

#### 4. Instala el servidor BIND9 en la máquina

```
bookworm11a [Corriendo] - Oracle VirtualBox
alumno@bookworm11a: /etc/systemd/network

Archivo  Editar  Pestañas  Ayuda

alumno@bookworm11a:/etc/systemd/network$ sudo apt install bind9
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  bind9-utils
```

#### 5. Comprueba el estado del servicio utilizando los comandos que ya conoces

```
bookworm11a [Corriendo] - Oracle VirtualBox
alumno@bookworm11a: /etc/systemd/network

Archivo  Editar  Pestañas  Ayuda

alumno@bookworm11a:/etc/systemd/network$ systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Mon 2025-10-06 09:31:20 CEST; 1min 14s ago
     Docs: man:named(8)
  Main PID: 1998 (named)
    Status: "running"
     Tasks: 5 (limit: 4617)
    Memory: 13.1M
       CPU: 64ms
    CGroup: /system.slice/named.service
            └─1998 /usr/sbin/named -f -u bind
alumno@bookworm11a:/etc/systemd/network$
```

#### 2. Creación de la zona "delegadoasirXX.asirXX.asir."

1. Crea el archivo de zona en el directorio correspondiente y modifica el archivo de configuración correspondiente para añadir la zona.

```
bookworm11a [Corriendo] - Oracle VirtualBox
alumno@bookworm11a: /etc/bind

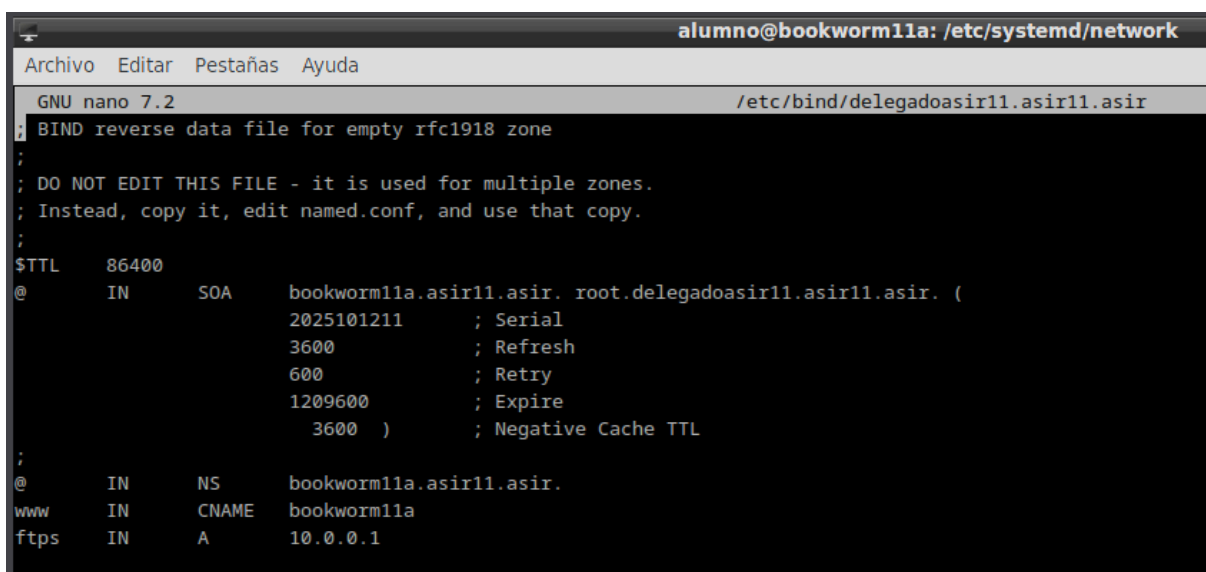
GNU nano 7.2                                named.conf.local *

//
// 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 "delegadoasir11.asir11.asir." {
    type master;
    file "/etc/bind/delegadoasir11.asir11.asir";
};
```

2. La zona creada será maestra y de resolución directa.
3. El SOA es el servidor bookwormXXa.asirXX.asir.
4. Debe tener un registro NS que apunte al servidor bookwormXXa.asirXX.asir., pero no necesita un registro A que resuelva dicho nombre por la IP del servidor (10.0.128+XX.1). Este registro A deberá estar en la zona "asirXX.asir".
5. Debe tener un registro CNAME que permita resolver el nombre www.delegadoasirXX.asirXX.asir. por el nombre del servidor 'bookwormXXa'
6. Debe tener un registro A que permita resolver ftps.delegadoasirXX.asirXX.asir. por la IP 10.0.0.1



The screenshot shows a terminal window with the title 'alumno@bookworm11a: /etc/systemd/network'. The terminal is running the GNU nano 7.2 editor, editing the file '/etc/bind/delegadoasir11.asir11.asir'. The content of the file is as follows:

```

; 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.asir11.asir. root.delegadoasir11.asir11.asir. (
                                2025101211      ; Serial
                                3600              ; Refresh
                                600               ; Retry
                                1209600          ; Expire
                                3600 )           ; Negative Cache TTL
;
@          IN      NS       bookworm11a.asir11.asir.
www        IN      CNAME    bookworm11a
ftps       IN      A        10.0.0.1

```

3. En el servidor 'bookwormXXb' debes modificar la zona "asirXX.asir" para que el subdominio "delegadoasirXX" se delegue en el servidor 'bookwormXXa'. Para ello crea un registro NS que apunte a dicho servidor, según hemos visto en clase (bookwormXXa.asirXX.asir.). Además tendrás que crear un registro A para el servidor en la zona del fichero adecuada para que bookwormXXa.asirXX.asir se resuelva por su dirección IP (10.0.128+XX.1). Prueba que:

```
alumno@bookworm11b: ~  
Archivo Editar Pestañas Ayuda  
GNU nano 7.2 /etc/bind/asir11.asir.hosts  
;  
; BIND data file for dns server  
;  
$TTL      3600  
@          IN      SOA      bookworm11b.asir11.asir. admin.asir11.asir. (  
                                2025101311      ; Serial  
                                3600              ; Refresh  
                                600               ; Retry  
                                1209600           ; Expire  
                                3600 )            ; Negative Cache TTL  
;  
          IN      NS       bookworm11b.asir11.asir.  
bookworm11b.asir11.asir.      IN      A       10.0.139.2  
bookworm11      IN      A       10.0.139.2  
servidor        IN      A       10.0.139.200  
servidor        IN      AAAA     fe80::11:11::211  
www             IN      CNAME    bookworm11b  
correo          IN      MX       10 bookworm11b.asir11.asir.  
bookworm11a     IN      A       10.0.139.1  
delegadoasir11  IN      NS       bookworm11a.asir11.asir.  
$origin subasir11.asir11.asir.  
servidor1       IN      CNAME    servidor.asir11.asir.  
ftp             IN      A       10.0.139.2  
;$origin delegadoasir11.asir11.asir.  
;$origin @      IN      NS       servidor.asir11.asir.
```

1. Existe conectividad entre las máquinas (2 servidores y 1 cliente)

```
linux11@linux11-virtualbox: /  
Archivo Acciones Editar Vista Ayuda  
linux11@linux11-virtualbox: /  
linux11@linux11-virtualbox:/$ ping 10.0.139.2  
PING 10.0.139.2 (10.0.139.2) 56(84) bytes of data.  
64 bytes from 10.0.139.2: icmp_seq=1 ttl=64 time=0.419 ms  
64 bytes from 10.0.139.2: icmp_seq=2 ttl=64 time=0.993 ms  
64 bytes from 10.0.139.2: icmp_seq=3 ttl=64 time=0.470 ms  
^C  
--- 10.0.139.2 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2002ms  
rtt min/avg/max/mdev = 0.419/0.627/0.993/0.259 ms  
linux11@linux11-virtualbox:/$ ping -c 3 10.0.139.1  
PING 10.0.139.1 (10.0.139.1) 56(84) bytes of data.  
64 bytes from 10.0.139.1: icmp_seq=1 ttl=64 time=1.31 ms  
64 bytes from 10.0.139.1: icmp_seq=2 ttl=64 time=0.862 ms  
64 bytes from 10.0.139.1: icmp_seq=3 ttl=64 time=0.972 ms  
--- 10.0.139.1 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2002ms  
rtt min/avg/max/mdev = 0.862/1.048/1.311/0.191 ms  
linux11@linux11-virtualbox:/$
```

2. Que desde el cliente se resuelven consultas que se hacen sobre registros de la zona "asirXX.asir" sobre el DNS de 'bookwormXXb'

```
linux11@linux11-virtualbox: /
Archivo Acciones Editar Vista Ayuda
linux11@linux11-virtualbox: / x
linux11@linux11-virtualbox:/$ dig @10.0.139.2 www.asir11.asir

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> @10.0.139.2 www.asir11.asir
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25307
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a22b36f1dec05d4c0100000068e3e54fc847bd7885011c93 (good)
;; QUESTION SECTION:
;www.asir11.asir.                IN      A

;; ANSWER SECTION:
www.asir11.asir.                3600    IN      CNAME   bookworm11b.asir11.asir.
bookworm11b.asir11.asir. 3600    IN      A       10.0.139.2

;; Query time: 0 msec
;; SERVER: 10.0.139.2#53(10.0.139.2) (UDP)
;; WHEN: Mon Oct 06 17:50:39 CEST 2025
;; MSG SIZE rcvd: 114

linux11@linux11-virtualbox:/$
```

3. Que desde el cliente se resuelven consultas que se hacen sobre registros de la zona delegada "delegadoasirXX.asirXX.asir" sobre el DNS de 'bookwormXXa'. Explicita en este caso en la consulta que el servidor consultado es el A.

```
linux11@linux11-virtualbox: /
Archivo Acciones Editar Vista Ayuda
linux11@linux11-virtualbox: / x
linux11@linux11-virtualbox:/$ dig @10.0.139.1 ftps.delegadoasir11.asir11.asir.

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> @10.0.139.1 ftps.delegadoasir11.asir11.asir.
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16801
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d5b24e3d273d02810100000068e3e59ce7b02317c7ea0058 (good)
;; QUESTION SECTION:
; ftps.delegadoasir11.asir11.asir. IN A

;; ANSWER SECTION:
ftps.delegadoasir11.asir11.asir. 86400 IN A 10.0.0.1

;; Query time: 2 msec
;; SERVER: 10.0.139.1#53(10.0.139.1) (UDP)
;; WHEN: Mon Oct 06 17:51:56 CEST 2025
;; MSG SIZE rcvd: 104

linux11@linux11-virtualbox:/$
```

4. Realiza las siguientes consultas poniendo previamente a capturar el tráfico en los interfaces correspondientes:
  1. Haz una consulta RECURSIVA al servidor b (10.0.128+XX.2) preguntando por "ftps.delegadoasirXX.asirXX.asir" y extrae conclusiones. Observa la captura de wireshark para ello.

```
linux11@linux11-virtualbox: ~
Archivo Máquina Ver Entrada Dispositivos Ayuda
linux11@linux11-virtualbox: ~ x
linux11@linux11-virtualbox:~$ dig @10.0.139.2 ftps.delegadoasir11.asir11.asir +rec

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @10.0.139.2 ftps.delegadoasir11.asir11.asir +rec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27166
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c45da470b26fb17c0100000068ebcd916e2f80851b432512 (good)
;; QUESTION SECTION:
; ftps.delegadoasir11.asir11.asir. IN A

;; ANSWER SECTION:
ftps.delegadoasir11.asir11.asir. 86400 IN A 10.0.0.1

;; Query time: 7 msec
;; SERVER: 10.0.139.2#53(10.0.139.2) (UDP)
;; WHEN: Sun Oct 12 17:47:29 CEST 2025
;; MSG SIZE rcvd: 104

linux11@linux11-virtualbox:~$
```

enp0s8

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.139.3	10.0.139.2	DNS	114	Standard query 0x6a1e A ftps.delegadoasir11.asir11.asir OPT
2	0.004547969	10.0.139.2	10.0.139.3	DNS	146	Standard query response 0x6a1e A ftps.delegadoasir11.asir11.asir A 10.0.0.1 OPT

Frame 1: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface enp0s8  
Ethernet II, Src: PCSSystemtec\_67:1d:15 (08:00:27:67:1d:15), Dst: PCSSystemtec\_10:00:00:00:00:00  
Internet Protocol Version 4, Src: 10.0.139.3, Dst: 10.0.139.2  
User Datagram Protocol, Src Port: 38882, Dst Port: 53  
Domain Name System (query)



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	114	Standard query 0x6a1e A ftps.delegadoasir11.asir11.asir OPT
2	0.001012336	10.0.139.2	10.0.139.1	DNS	114	Standard query 0x5eff A ftps.delegadoasir11.asir11.asir OPT
3	0.002471269	10.0.139.1	10.0.139.2	DNS	183	Standard query response 0x5eff A ftps.delegadoasir11.asir11.asir A 10.0.0.1 NS book...
4	0.002888355	10.0.139.2	10.0.139.3	DNS	146	Standard query response 0x6a1e A ftps.delegadoasir11.asir11.asir A 10.0.0.1 OPT

- Haz una consulta NO RECURSIVA al servidor 2 (10.0.128+XX.2) preguntando por "ftps.delegadoasirXX.asirXX.asir" y extrae conclusiones. Observa la captura de wireshark para ello.

```

linux11@linux11-virtualbox: /
Archivo Acciones Editar Vista Ayuda
linux11@linux11-virtualbox: / x linux11@linux11-virtualbox: / x
linux11@linux11-virtualbox:/$ dig @10.0.139.2 ftps.delegadoasir11.asir11.asir +norec
; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> @10.0.139.2 ftps.delegadoasir11.asir11.asir +norec
; (1 server found)
; global options: +cmd
; Got answer:
; ->HEADER<- opcode: QUERY, status: NOERROR, id:
; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 2
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 155f3bd80cfc03750100000068e3e93c81017ea9
; QUESTION SECTION:
; ftps.delegadoasir11.asir11.asir. IN A
; AUTHORITY SECTION:
delegadoasir11.asir11.asir. 3600 IN NS bo
delegadoasir11.asir11.asir. 3600 IN NS se
; Query time: 3 msec
; SERVER: 10.0.139.2#53(10.0.139.2) (UDP)
; WHEN: Mon Oct 06 18:07:24 CEST 2025
; MSG SIZE rcvd: 148
linux11@linux11-virtualbox:/$

```

Capturando desde enp0s8						
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda						
Aplique un filtro de visualización ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.139.3	10.0.139.2	DNS	114	Standard query 0xe6d7 A ftps.de...
2	0.001237911	10.0.139.2	10.0.139.3	DNS	198	Standard query response 0xe6d7 A...
3	5.313543182	PCSSystemtec_c6:d2::...	PCSSystemtec_ec:07::...	ARP	42	Who has 10.0.139.2? Tell 10.0.13...
4	5.314253875	PCSSystemtec_ec:07::...	PCSSystemtec_c6:d2::...	ARP	60	10.0.139.2 is at 08:00:27:ec:07:...
5	5.386545882	PCSSystemtec_ec:07::...	PCSSystemtec_c6:d2::...	ARP	60	Who has 10.0.139.3? Tell 10.0.13...
6	5.386566216	PCSSystemtec_c6:d2::...	PCSSystemtec_ec:07::...	ARP	42	10.0.139.3 is at 08:00:27:c6:d2:...
7	10.840466454	fe80::a00:27ff:fece...	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipp...
8	10.840467914	10.0.139.1	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _ipp...

```

Frame 1: 114 bytes on wire (912 bits), 114 bytes captured on interface enp0s8, 114 bytes from 10.0.139.3
Ethernet II, Src: PCSSystemtec_c6:d2:c7 (08:00:27:c6:d2:c7), Dst: 10.0.139.2 (08:00:27:c6:d2:c7)
Internet Protocol Version 4, Src: 10.0.139.3, Dst: 10.0.139.2
User Datagram Protocol, Src Port: 35047, Dst Port: 53
Domain Name System (query)

```

- Si la consulta 1 ha funcionado vuelve a realizarla y observa qué cambios ha habido en la misma. Observa la captura de wireshark para ello.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.139.3	10.0.139.2	DNS	114	Standard query 0x9122 A ftps.delegadoasir11.asir11.asir OPT
2	0.000342678	10.0.139.2	10.0.139.3	DNS	146	Standard query response 0x9122 A ftps.delegadoasir11.asir11.asir A 10.0.0.1 OPT

El servidor A no le pregunta A el servidor a pues ya guardó la información en caché