

# Práctica 3

## Capa de Aplicación - DNS

Grupo z

Integrantes: Herrera Francisco, Domé Luis y Gagliardi Pablo.

11. (Ejercicio de promoción)

NOTA: para quienes hagan la promoción, este será un ejercicio entregable. En la entrega deberán estar todas las preguntas respondidas y debidamente justificadas. En los puntos donde es necesario ejecutar comandos, los mismos deberán adjuntarse a la entrega así como las capturas. En el caso del código entregar solo los fuentes y un README/README.md que indique como se genera y como se utiliza.

**a. Indique un comando a ejecutar y respuesta (salida del comando) para consultar un ROOT-server por los servidores de nombre del dominio que Uds. elija, por ejemplo EDU.AR.**

Comando:

```
$ dig -t ns info.unlp.edu.ar.
```

Respuesta:

```
global options: +cmd
```

Got answer:

```
->HEADER<- opcode: QUERY, status: NOERROR, 1d: 7406
```

```
flags:qr rd ra ad; QUERY: 1, ANSWER: 6, AUTHORITYS 0, ADDITIONAL: 11
```

```
OPT PSEUDOSECTIONS:
```

```
EDNS version: 0, flags::; udp: 1232
```

```
COOKIE: 2424417338387650010000006267216fd5baf117ec855806 (good)
```

```
:: ANSWER SECTION:
```

```
info.unlp.edu.ar.      300    IN      NS      ns1.info.unlp.edu.ar.
```

```
info.unlp.edu.ar.      300    IN      NS      ns.linti.unlp.edu.ar.
```

```
info.unlp.edu.ar.      300    IN      NS      anubis.unlp.edu.ar.
```

:: ADDITIONAL SECTION:

anubis.unlp.edu.ar. 2423 IN A 163.10.0.65

anubis.unlp.edu.ar. 548 IN AAAA 2800:340:0:64::65

:: Query time: 12 msec

:: SERVER: 186.130.128.250#53(186.130.128.250) (UDP)

:: WHEN: Sat Apr 23 11:40:22 -03 2022

:: MSG SIZE rcvd: 151

**i. ¿La solicitud fue recursiva o iterativa? ¿Y la respuesta? ¿Cómo lo sabe?**

Esta información se obtiene con los flags, el flag “rd” (recursion desired) indica que la solicitud, en caso de poderse, se realiza de forma recursiva.

Por otra parte la respuesta también se indica con los flags, en este caso el flag “ra” (recursion available) el cual indica si la respuesta recursiva está habilitada en ese servidor.

Sin embargo ninguno es categórico, la información de si se dió de forma recursiva o no, por más que fuese deseado y estuviese disponible, podría pasar, por ejemplo, que la información solicitada estuviese almacenada en caché y la recursividad no fuera necesaria.

**¿Se puede cambiar algo en la consulta o la respuesta para que cambie este comportamiento? ¿Cómo lo haría?**

Si, en la consulta se puede utilizar la opción `norecurse`, la cual desactiva automáticamente la recursividad, la cual está configurada de forma predeterminada en el bit `rd` (recursividad deseada). La recursión se deshabilita automáticamente cuando las opciones de consulta `-nssearch` o `-trace` son usadas.

**ii. ¿Puede indicar si se trata de una respuesta autoritativa? ¿Qué significa que lo sea? Realizar la misma consulta a alguno de los servidores obtenidos como respuesta y analizar nuevamente. ¿A quién se debería consultar para que fuese autoritativa la respuesta?**

Las respuestas autoritativas se indican con el flag “aa” (Authoritative Answer), indica que la respuesta fue brindada por el servidor dns que tiene la información (registro) de la zona en cuestión. Es decir que el servidor al que le hicimos la consulta tiene autoridad sobre el dominio, entonces, puede responder la consulta con el resultado definitivo, sin tener que seguir iterando en otros servidores.

**b. ¿Cuáles son los servidores de correo del dominio seleccionado?. En el caso que el dominio seleccionado no los tenga buscar otro que sí. Indicar el significado de cada uno de los campos de los registros obtenidos.**

// comando dig, tipo de registro MX, al dominio seleccionado y preguntandole a la ip que me dió como respuesta la consulta anterior en la parte de

:: SERVER: 186.130.128.250

\$dig -t MX info.unlp.edu.ar @186.130.128.250

:: ANSWER SECTION:

info.unlp.edu.ar.	300	IN	MX	20	anubis.unlp.edu.ar.
info.unlp.edu.ar.	300	IN	MX	30	mail.linti.unlp.edu.ar.
info.unlp.edu.ar.	300	IN	MX	10	ada.info.unlp.edu.ar.

Los servidores de correo del dominio son mail.linti.unlp.edu.ar., anubis.unlp.edu.ar., ada.info.unlp.edu.ar., los cuales rotarán si se repite la consulta a fin de dividir la carga de trabajo y también por si alguno se cae, para tener un servidor funcionando.

Los números entre MX y el nombre indican la prioridad del servidor, a menor valor mayor prioridad.

En caso de querer enviar un correo destinado a redes.unlp.edu.ar, se le entregará al servidor de mayor prioridad ( mail.linti.unlp.edu.ar. en este caso). En caso de que falle mail.linti.unlp.edu.ar., se entregará al otro servidor.

**c. Intente determinar si existe un servidor primario para el dominio.**

podemos determinarlo mediante el comando:

\$ dig info.unlp.edu.ar SOA

:: ANSWER SECTION:

info.unlp.edu.ar.	300	IN	SOA	ns1.info.unlp.edu.ar.	root.info.unlp.edu.ar.
2022041901 28800 14400 3600000 300					

El servidor DNS primario es el correspondiente al primer nombre que figura en el archivo SOA.(ns1.info.unlp.edu.ar. )

**d. Capturar los mensajes de la primer consulta con la herramienta wireshark y responder:**

**i. Los mensajes son ASCII como HTTP1.1?**

No, los mensajes son en binario representado hexadecimal.

0000	00 f4 8d ef 64 ed a4 97 33 99 42 a0 08 00 45 00	...d... 3·B...E·
0010	00 b3 65 ee 40 00 fc 11 1b 02 ba 82 80 fa c0 a8	...e·@... .....
0020	01 24 00 35 8a a2 00 9f 86 e6 6c 57 81 80 00 01	·\$·5... ..lW...
0030	00 03 00 00 00 03 04 69 6e 66 6f 04 75 6e 6c 70	.....i nfo·unlp
0040	03 65 64 75 02 61 72 00 00 02 00 01 c0 0c 00 02	·edu·ar· .....
0050	00 01 00 00 01 2c 00 0b 02 6e 73 05 6c 69 6e 74	.....,· ..ns·lint
0060	69 c0 11 c0 0c 00 02 00 01 00 00 01 2c 00 09 06	i· .....
0070	61 6e 75 62 69 73 c0 11 c0 0c 00 02 00 01 00 00	anubis· .....
0080	01 2c 00 06 03 6e 73 31 c0 0c c0 45 00 01 00 01	·,· ..ns1 ...E...
0090	00 00 18 56 00 04 a3 0a 00 41 c0 45 00 1c 00 01	·V· ..V· ..A·E...
00a0	00 00 06 fb 00 10 28 00 03 40 00 00 00 64 00 00	.....(· ..@· ..d·
00b0	00 00 00 00 00 65 00 00 29 10 00 00 00 00 00 00	.....e· )· .....
00c0	00	.

ii. Indicar el significado y el valor de 4 flags.

- AA: Respuesta autoritativa. 0
- TC: Mensaje truncado. 0
- RD: Consulta recursiva. 1
- RA: Indica si el servidor soporta consultas recursivas. 1

Wireshark · Packet 31 · [no capture file]	
main Name System (response)	
Transaction ID: 0x6c57	
Flags: 0x8180 Standard query response, No error	
1...	Response: Message is a response
.000 0...	Opcode: Standard query (0)
.... .0.	Authoritative: Server is not an authority for domain
.... .0.	Truncated: Message is not truncated
.... .1	Recursion desired: Do query recursively
.... .1..	Recursion available: Server can do recursive queries
.... .0..	Z: reserved (0)
.... .0.	Answer authenticated: Answer/authority portion was not authenticated
.... .0	Non-authenticated data: Unacceptable
.... .0000	Reply code: No error (0)

iii. Indicar el significado y el valor del campo Transaction ID.

Este campo identifica la consulta del cliente, que debe coincidir con la respuesta del servidor.

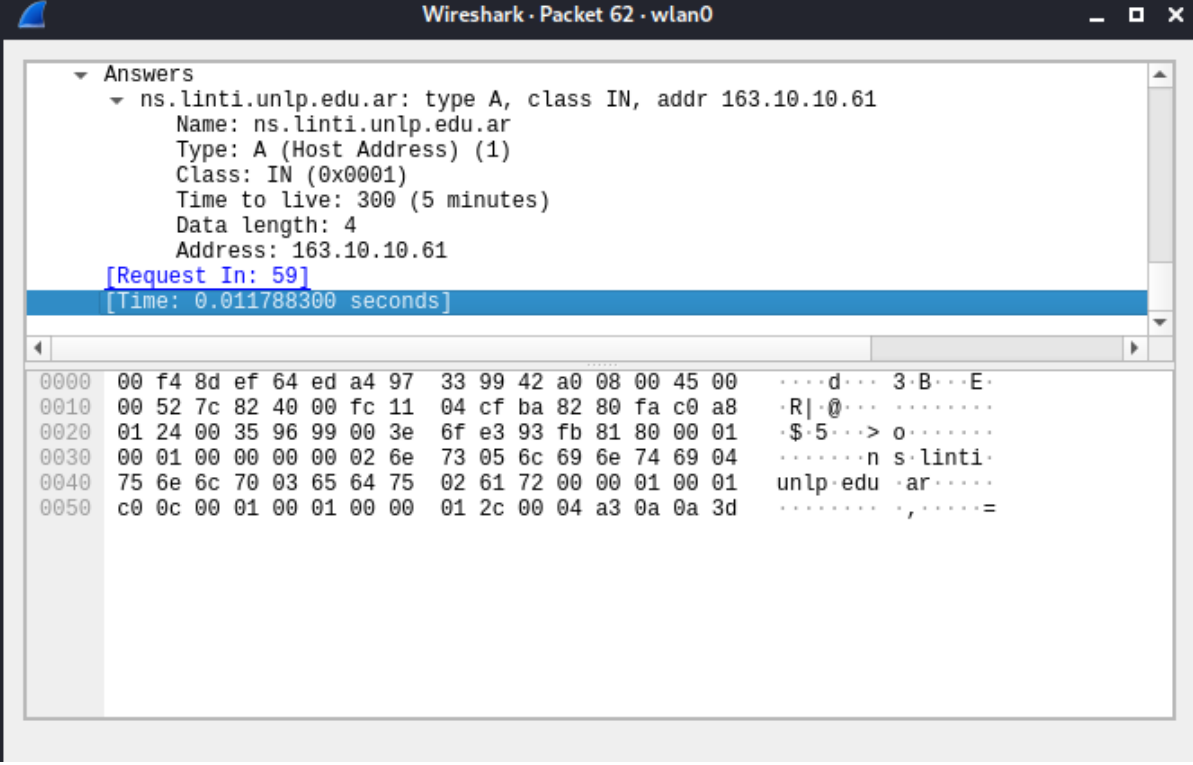
```

▶ Internet Protocol Version 4, Src: 192.168.1.36, Dst: 186.130.128.250
▶ User Datagram Protocol, Src Port: 38553, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x93fb
    ▼ Flags: 0x0100 Standard query
      0... .. = Response: Message is a query
      .000 0... .. = Opcode: Standard query (0)
      .... .0. .... = Truncated: Message is not truncated
      .... .1 .... = Recursion desired: Do query recursively
      .... .0.. .... = Z: reserved (0)
      .... .0 .... = Non-authenticated data: Unacceptable

      Questions: 1
      Answer RRs: 0

```

iv. ¿Cuál fue el RTT para la consulta dada? ¿Cómo se determina?



Wireshark · Packet 62 · wlan0

Answers

- ns.linti.unlp.edu.ar: type A, class IN, addr 163.10.10.61
  - Name: ns.linti.unlp.edu.ar
  - Type: A (Host Address) (1)
  - Class: IN (0x0001)
  - Time to live: 300 (5 minutes)
  - Data length: 4
  - Address: 163.10.10.61

[Request In: 59]

[Time: 0.011788300 seconds]

0000	00 f4 8d ef 64 ed a4 97 33 99 42 a0 08 00 45 00	...d... 3.B...E.
0010	00 52 7c 82 40 00 fc 11 04 cf ba 82 80 fa c0 a8	·R ·@... ..
0020	01 24 00 35 96 99 00 3e 6f e3 93 fb 81 80 00 01	·\$.5...> o.....
0030	00 01 00 00 00 00 02 6e 73 05 6c 69 6e 74 69 04	.....n s·linti·
0040	75 6e 6c 70 03 65 64 75 02 61 72 00 00 01 00 01	unlp·edu ·ar.....
0050	c0 0c 00 01 00 01 00 00 01 2c 00 04 a3 0a 0a 3d	..... ,.....=

```
;; Query time: 12 msec      Type: A (Host Address) (1)
;; SERVER: 163.10.10.61#53(ns.linti.unlp.edu.ar.) (UDP)
;; WHEN: Mon Apr 25 18:00:14 -03 2022
;; MSG SIZE rcvd: 155      Address: 163.10.10.61
```

e. Programar en el lenguaje de su elección un simple programa que reciba de línea de comando una lista de nombres de dominio e intente resolver a su correspondiente registro "A". Cámbielo para que resuelva a registros "AAAA".

```
#!/bin/bash
```

```
echo "Ingrese nombres de dominio, separados por espacio"
```

```
read list
```

```
clear
```

```
echo -e "RESULTADOS.\n"
```

```
for i in $list; do
```

```
    echo "- domain name:"
```

```
    echo " * $i"
```

```
    echo "- ipv4:"
```

```
    echo "$ (dig +short -t a $i | sed 's/^/ * /')"
```

```
    echo "- ipv6:"
```

```
    echo "$ (dig +short -t aaaa $i | sed 's/^/ * /')"
```

```
    echo "-----"
```

```
done
```

