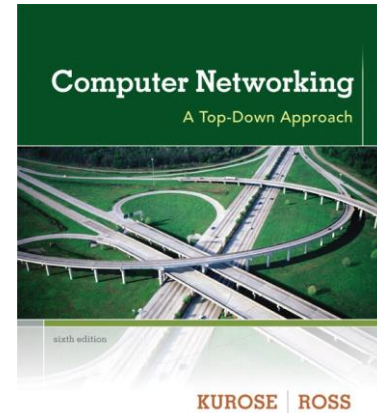


Wireshark Lab: DNS v6.01

Supplement to *Computer Networking: A Top-Down Approach*, 6th ed., J.F. Kurose and K.W. Ross

“Tell me and I forget. Show me and I remember. Involve me and I understand.” Chinese proverb

© 2005-21012, J.F Kurose and K.W. Ross, All Rights Reserved



As described in Section 2.5 of the text¹, the Domain Name System (DNS) translates hostnames to IP addresses, fulfilling a critical role in the Internet infrastructure. In this lab, we'll take a closer look at the client side of DNS. Recall that the client's role in the DNS is relatively simple – a client sends a *query* to its local DNS server, and receives a *response* back. As shown in Figures 2.21 and 2.22 in the textbook, much can go on “under the covers,” invisible to the DNS clients, as the hierarchical DNS servers communicate with each other to either recursively or iteratively resolve the client's DNS query. From the DNS client's standpoint, however, the protocol is quite simple – a query is formulated to the local DNS server and a response is received from that server.

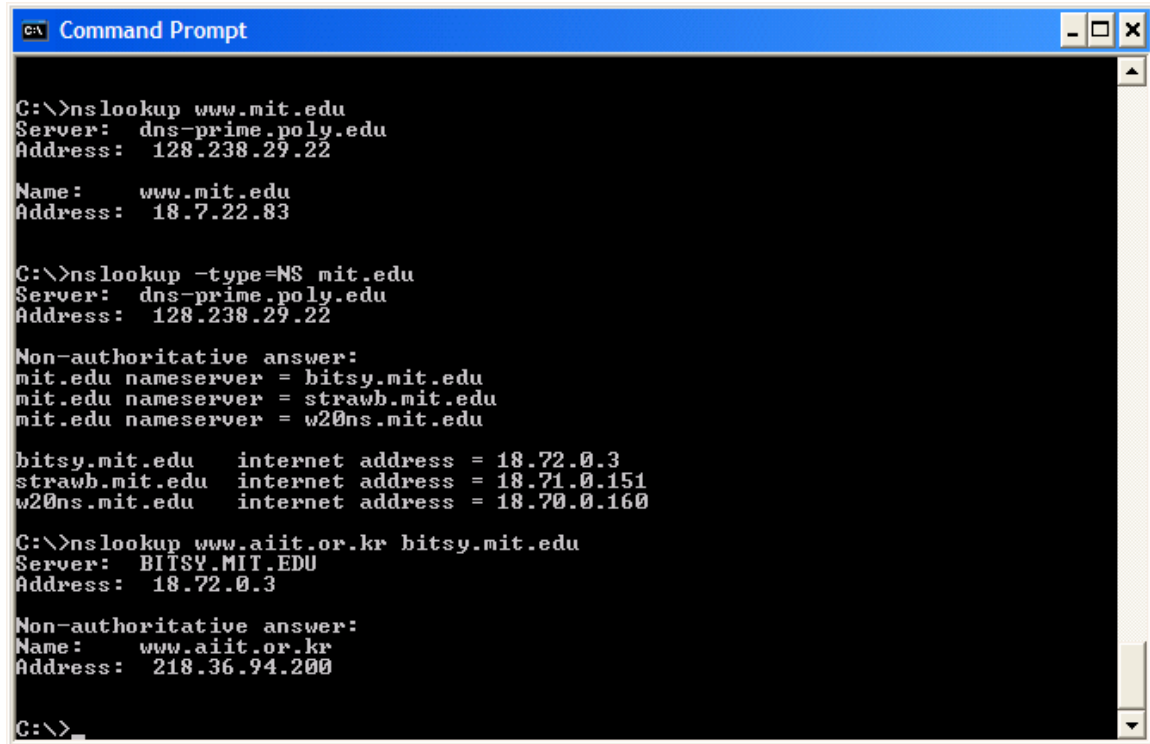
Before beginning this lab, you'll probably want to review DNS by reading Section 2.5 of the text. In particular, you may want to review the material on **local DNS servers**, **DNS caching**, **DNS records and messages**, and the **TYPE field** in the DNS record.

1. nslookup

In this lab, we'll make extensive use of the *nslookup* tool, which is available in most Linux/Unix and Microsoft platforms today. To run *nslookup* in Linux/Unix, you just type the *nslookup* command on the command line. To run it in Windows, open the Command Prompt and run *nslookup* on the command line.

In its most basic operation, *nslookup* tool allows the host running the tool to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level-domain DNS server, an authoritative DNS server, or an intermediate DNS server (see the textbook for definitions of these terms). To accomplish this task, *nslookup* sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.

¹ References to figures and sections are for the 6th edition of our text, *Computer Networks, A Top-down Approach*, 6th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2012.



```
C:\>nslookup www.mit.edu
Server:  dns-prime.poly.edu
Address: 128.238.29.22

Name:    www.mit.edu
Address: 18.7.22.83

C:\>nslookup -type=NS mit.edu
Server:  dns-prime.poly.edu
Address: 128.238.29.22

Non-authoritative answer:
mit.edu nameserver = bitsy.mit.edu
mit.edu nameserver = strawb.mit.edu
mit.edu nameserver = w20ns.mit.edu

bitsy.mit.edu    internet address = 18.72.0.3
strawb.mit.edu  internet address = 18.71.0.151
w20ns.mit.edu   internet address = 18.70.0.160

C:\>nslookup www.aiit.or.kr bitsy.mit.edu
Server:  BITSY.MIT.EDU
Address: 18.72.0.3

Non-authoritative answer:
Name:    www.aiit.or.kr
Address: 218.36.94.200

C:\>
```

The above screenshot shows the results of three independent *nslookup* commands (displayed in the Windows Command Prompt). In this example, the client host is located on the campus of Polytechnic University in Brooklyn, where the default local DNS server is dns-prime.poly.edu. When running *nslookup*, if no DNS server is specified, then *nslookup* sends the query to the default DNS server, which in this case is dns-prime.poly.edu. Consider the first command:

```
nslookup www.mit.edu
```

In words, this command is saying “please send me the IP address for the host www.mit.edu”. As shown in the screenshot, the response from this command provides two pieces of information: (1) the name and IP address of the DNS server that provides the answer; and (2) the answer itself, which is the host name and IP address of www.mit.edu. Although the response came from the local DNS server at Polytechnic University, it is quite possible that this local DNS server iteratively contacted several other DNS servers to get the answer, as described in Section 2.5 of the textbook.

Now consider the second command:

```
nslookup -type=NS mit.edu
```

In this example, we have provided the option “-type=NS” and the domain “mit.edu”. This causes *nslookup* to send a query for a type-NS record to the default local DNS server. In

words, the query is saying, “please send me the host names of the authoritative DNS for mit.edu”. (When the `-type` option is not used, *nslookup* uses the default, which is to query for type A records.) The answer, displayed in the above screenshot, first indicates the DNS server that is providing the answer (which is the default local DNS server) along with three MIT nameservers. Each of these servers is indeed an authoritative DNS server for the hosts on the MIT campus. However, *nslookup* also indicates that the answer is “non-authoritative,” meaning that this answer came from the cache of some server rather than from an authoritative MIT DNS server. Finally, the answer also includes the IP addresses of the authoritative DNS servers at MIT. (Even though the type-NS query generated by *nslookup* did not explicitly ask for the IP addresses, the local DNS server returned these “for free” and *nslookup* displays the result.)

Now finally consider the third command:

```
nslookup www.aiit.or.kr bitsy.mit.edu
```

In this example, we indicate that we want the query sent to the DNS server bitsy.mit.edu rather than to the default DNS server (dns-prime.poly.edu). Thus, the query and reply transaction takes place directly between our querying host and bitsy.mit.edu. In this example, the DNS server bitsy.mit.edu provides the IP address of the host www.aiit.or.kr, which is a web server at the Advanced Institute of Information Technology (in Korea).

Now that we have gone through a few illustrative examples, you are perhaps wondering about the general syntax of *nslookup* commands. The syntax is:

```
nslookup -option1 -option2 host-to-find dns-server
```

In general, *nslookup* can be run with zero, one, two or more options. And as we have seen in the above examples, the dns-server is optional as well; if it is not supplied, the query is sent to the default local DNS server.

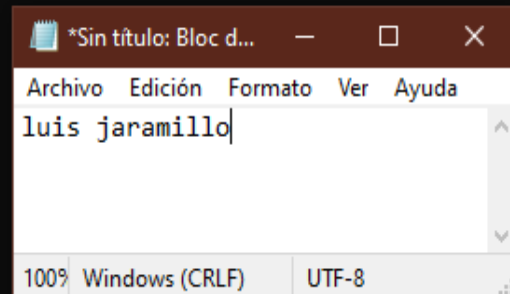
Now that we have provided an overview of *nslookup*, it is time for you to test drive it yourself. Do the following (and write down the results):

1. Run *nslookup* to obtain the IP address of a Web server in Asia. What is the IP address of that server?
se busca una pagina en asia
se pone nslookup spanish.china.org.cn

```
Microsoft Windows [Versión 10.0.19041.610]  
(c) 2020 Microsoft Corporation. Todos los derechos reservados.
```

```
C:\Users\Smart>nslookup spanish.china.org.cn  
Servidor: dns.google  
Address: 8.8.8.8
```

```
Respuesta no autoritativa:  
Nombre: uz95.v.bsghlb.cn  
Addresses: 38.122.90.197  
           38.122.90.195  
           38.122.90.198  
           38.122.90.196  
Aliases: spanish.china.org.cn  
          spanish.china.org.cn.bsghlb.cn
```



El servidor web en Asia en este caso contiene 3 direcciones ip que son:

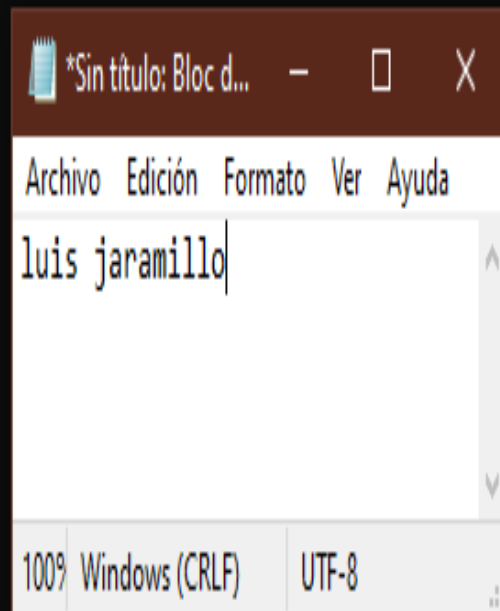
- 38.122.90.197
- 38.122.90.195
- 38.122.90.198
- 38.122.90.196

2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe.

Se pone nslookup -type=NS www.ucm.es

```
C:\Users\Smart>nslookup -type=NS www.ucm.es  
Servidor: dns.google  
Address: 8.8.8.8
```

```
Respuesta no autoritativa:  
www.ucm.es canonical name = ucm.es  
ucm.es nameserver = sun.rediris.es  
ucm.es nameserver = chico.rediris.es  
ucm.es nameserver = ucdns.sis.ucm.es  
ucm.es nameserver = crispin.sim.ucm.es
```



3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

Se pone nslookup mail.yahoo.com con una dns obtenida antes sun.rediris.es

```
C:\Users\Smart> nslookup mail.yahoo.com chico.rediris.es
Servidor: ns1.d-zone.ca
Address: 162.219.54.2

*** ns1.d-zone.ca no encuentra mail.yahoo.com: Query refused

C:\Users\Smart>
```

```
C:\Users\Smart> nslookup mail.yahoo.com 8.8.8.8
Servidor: dns.google
Address: 8.8.8.8

Respuesta no autoritativa:
Nombre: edge.gycpi.b.yahoodns.net
Addresses: 2804:1bc:f046:1fa::2000
           2804:1bc:f046:1fa::3000
           200.152.165.204
           200.152.165.205
Aliases: mail.yahoo.com
```

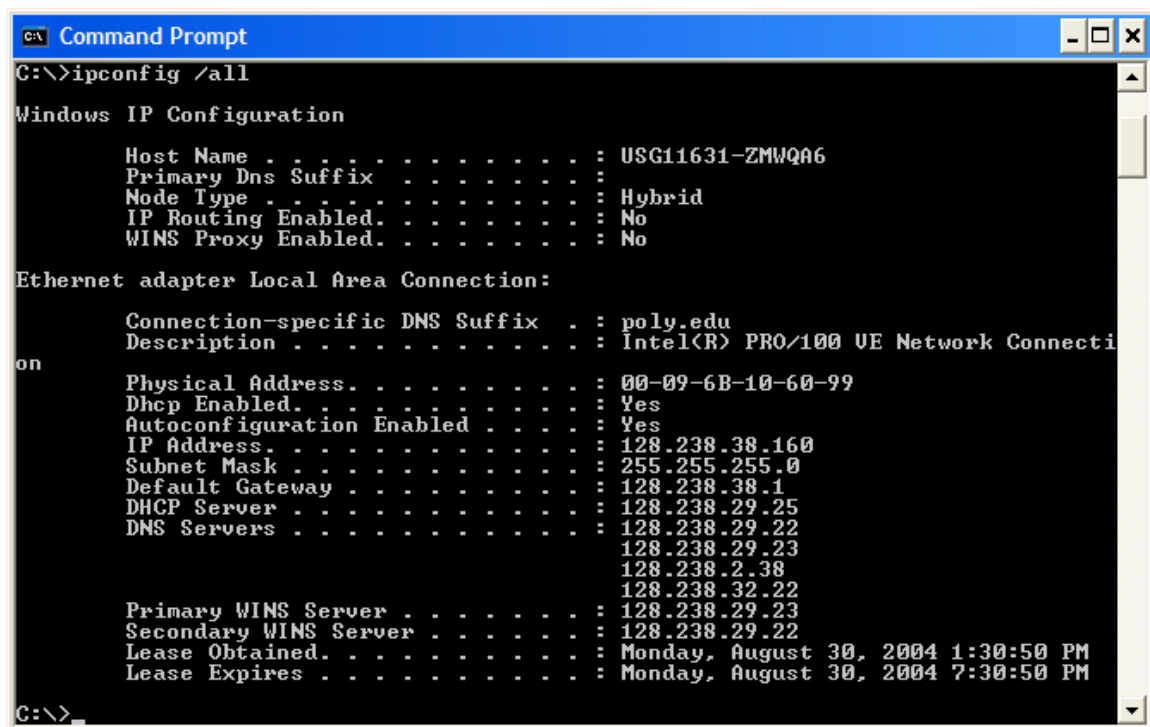
- Dado que algunos normas de seguridad no permiten acceder si no eres parte de la Universidad , se ha dedicado usar el servidor DNS de mi proveedor de internet

2. ipconfig

ipconfig (for Windows) and *ifconfig* (for Linux/Unix) are among the most useful little utilities in your host, especially for debugging network issues. Here we'll only describe *ipconfig*, although the Linux/Unix *ifconfig* is very similar. *ipconfig* can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on. For example, if you all this information about your host simply by entering

```
ipconfig \all
```

into the Command Prompt, as shown in the following screenshot.



```
C:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : USG11631-ZMWQA6
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : poly.edu
    Description . . . . . : Intel(R) PRO/100 VE Network Connecti
on
    Physical Address. . . . . : 00-09-6B-10-60-99
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 128.238.38.160
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 128.238.38.1
    DHCP Server . . . . . : 128.238.29.25
    DNS Servers . . . . . : 128.238.29.22
                           128.238.29.23
                           128.238.2.38
                           128.238.32.22
    Primary WINS Server . . . . . : 128.238.29.23
    Secondary WINS Server . . . . . : 128.238.29.22
    Lease Obtained. . . . . : Monday, August 30, 2004 1:30:50 PM
    Lease Expires . . . . . : Monday, August 30, 2004 7:30:50 PM

C:\>
```

ipconfig is also very useful for managing the DNS information stored in your host. In Section 2.5 we learned that a host can cache DNS records it recently obtained. To see these cached records, after the prompt `C:\>` provide the following command:

```
ipconfig /displaydns
```

Each entry shows the remaining Time to Live (TTL) in seconds. To clear the cache, enter

```
ipconfig /flushdns
```

Flushing the DNS cache clears all entries and reloads the entries from the hosts file.

3. Tracing DNS with Wireshark

Now that we are familiar with *nslookup* and *ipconfig*, we're ready to get down to some serious business. Let's first capture the DNS packets that are generated by ordinary Web-surfing activity.

- Use *ipconfig* to empty the DNS cache in your host.
- Open your browser and empty your browser cache. (With Internet Explorer, go to Tools menu and select Internet Options; then in the General tab select Delete Files.)
- Open Wireshark and enter "ip.addr == your_IP_address" into the filter, where you obtain your_IP_address with ipconfig. This filter removes all packets that neither originate nor are destined to your host.
- Start packet capture in Wireshark.
- With your browser, visit the Web page: <http://www.ietf.org>
- Stop packet capture.

If you are unable to run Wireshark on a live network connection, you can download a packet trace file that was captured while following the steps above on one of the author's computers². Answer the following questions. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout³ to explain your answer. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line*, and select the minimum amount of packet detail that you need to answer the question.

4. Locate the DNS query and response messages. Are then sent over UDP or TCP?

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes Archivo, Edición, Visualización, Ir, Captura, Analizar, Estadísticas, Telefonía, Wireless, Herramientas, and Ayuda. The packet list pane shows a filter 'ip.addr == 192.168.50.101' and a list of captured packets. The selected packet is No. 327, a DNS query from 192.168.50.101 to 8.8.8.8. The packet details pane shows the User Datagram Protocol (UDP) section with Source Port 55691 and Destination Port 53. A small text editor window titled '*Sin título: Bloc d...' is open over the packet details, containing the text 'luis jaramillo'.

No.	Time	Source	Destination	Protocol	Length	Info
79	8.104316	8.8.8.8	192.168.50.101	DNS	204	Standard query response 0xad1a A api.bing.com CNAME api-bing-com.e-0001.e-msedge.net CNAME afd.e-0001.dc-ms...
80	8.106543	8.8.8.8	192.168.50.101	DNS	193	Standard query response 0x7097 A www.bing.com CNAME a-0001.a-afdentry.net.trafficmanager.net CNAME dual-a-0...
327	13.680363	192.168.50.101	8.8.8.8	DNS	72	Standard query 0xd9a6 A www.ietf.org
328	13.680369	192.168.50.101	8.8.8.8	DNS	72	Standard query 0xd9a6 A www.ietf.org
329	13.772302	8.8.8.8	192.168.50.101	DNS	149	Standard query response 0xd9a6 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16...
857	15.100132	192.168.50.101	8.8.8.8	DNS	78	Standard query 0x570d A analytics.ietf.org
858	15.100138	192.168.50.101	8.8.8.8	DNS	78	Standard query 0x570d A analytics.ietf.org
863	15.205706	8.8.8.8	192.168.50.101	DNS	108	Standard query response 0x570d A analytics.ietf.org CNAME ietf.org A 4.31.198.44
194	11.772128	192.168.50.101	190.98.153.26	HTTP	521	GET /img-resizer/tenant/amp/entityid/BB1aw9ae.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg HTTP/1.1
245	11.916965	190.98.153.26	192.168.50.101	HTTP	1037	HTTP/1.1 200 OK (JPEG JFIF image)

Frame 327: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{74B7E1A3-F256-4E13-944D-1978D99BF2D8}, id 0
> Ethernet II, Src: IntelCor_c0:17:4b (08:d4:0c:c0:17:4b), Dst: Qpcom_09:69:68 (88:a5:bd:09:69:68)
> Internet Protocol Version 4, Src: 192.168.50.101, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 55691, Dst Port: 53
Source Port: 55691
Destination Port: 53
Length: 38
Checksum: 0x26d8 [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
> [Timestamps]
UDP payload (30 bytes)
0000 88 a5 bd 09 69 68 08 04 0c c0 17 4b 08 00 45 00ih...K...E
0010 00 3a 9f d9 00 00 00 11 97 bc c0 a8 32 65 08 082e...
0020 08 08 d9 8b 00 35 00 26 26 d8 d9 a6 01 00 00 015&&.....
0030 00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03w ww.ietf
0040 6f 72 67 00 00 01 00 01org.....

- El protocolo que esta usando en esta ocasion es el UDP

5. What is the destination port for the DNS query message? What is the source port of DNS response message?

The image shows a Wireshark packet capture. The packet list on the left shows several DNS queries and responses, followed by an HTTP GET request. The packet details pane on the right shows the selected packet (No. 327) is a DNS Standard query. A context menu is open over the packet list, showing the text 'luis jaramillo'.

No.	Time	Source	Destination	Protocol	Length	Info
327	13.680363	192.168.50.101	8.8.8.8	DNS	72	Standard query 0xd9a6 A www.ietf.org
328	13.680369	192.168.50.101	8.8.8.8	DNS	72	Standard query 0xd9a6 A www.ietf.org
329	13.772302	8.8.8.8	192.168.50.101	DNS	149	Standard query response 0xd9a6 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.44.100
857	15.100132	192.168.50.101	8.8.8.8	DNS	78	Standard query 0x570d A analytics.ietf.org
858	15.100138	192.168.50.101	8.8.8.8	DNS	78	Standard query 0x570d A analytics.ietf.org
863	15.205706	8.8.8.8	192.168.50.101	DNS	108	Standard query response 0x570d A analytics.ietf.org CNAME ietf.org A 4.31.198.44
194	11.772128	192.168.50.101	190.98.153.26	HTTP	521	GET /img-resizer/tenant/amp/entityid/BB1aw9ae.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg HTTP/1.1
245	11.916965	190.98.153.26	192.168.50.101	HTTP	1037	HTTP/1.1 200 OK (JPEG JFIF image)

Internet Protocol Version 4, Src: 192.168.50.101, Dst: 8.8.8.8

User Datagram Protocol, Src Port: 55691, Dst Port: 53

Source Port: 55691

Destination Port: 53

Length: 38

Checksum: 0x26d8 [unverified]

[Checksum Status: Unverified]

[Stream index: 2]

- El Puerto tanto de envi como de respuesta es el 53

6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

The image shows a Wireshark packet capture and a Windows command prompt. The packet list on the left shows several DNS queries and responses, followed by an HTTP GET request. The packet details pane on the right shows the selected packet (No. 327) is a DNS Standard query. A context menu is open over the packet list, showing the text 'luis jaramillo'.

No.	Time	Source	Destination	Protocol	Length	Info
79	8.104316	8.8.8.8	192.168.50.101	DNS	204	Standard query response 0xd9a6 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.44.100
80	8.106543	8.8.8.8	192.168.50.101	DNS	193	Standard query response 0xd9a6 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.44.100
327	13.680363	192.168.50.101	8.8.8.8	DNS	72	Standard query 0xd9a6 A www.ietf.org
328	13.680369	192.168.50.101	8.8.8.8	DNS	72	Standard query 0xd9a6 A www.ietf.org
329	13.772302	8.8.8.8	192.168.50.101	DNS	149	Standard query response 0xd9a6 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.44.100
857	15.100132	192.168.50.101	8.8.8.8	DNS	78	Standard query 0x570d A analytics.ietf.org
858	15.100138	192.168.50.101	8.8.8.8	DNS	78	Standard query 0x570d A analytics.ietf.org
863	15.205706	8.8.8.8	192.168.50.101	DNS	108	Standard query response 0x570d A analytics.ietf.org CNAME ietf.org A 4.31.198.44
194	11.772128	192.168.50.101	190.98.153.26	HTTP	521	GET /img-resizer/tenant/amp/entityid/BB1aw9ae.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg HTTP/1.1

Dirección física. : 08-D4-0C-C0-17-4B

DHCP habilitado : sí

Configuración automática habilitada : sí

Vínculo: dirección IPv6 local. : fe80::ecef:1dc5:a1e0:d683%6(Preferido)

Dirección IPv4. : 192.168.50.101(Preferido)

Máscara de subred : 255.255.255.0

Concesión obtenida. : sábado, 7 de noviembre de 2020 12:03:16:AM

La concesión expira : viernes, 13 de noviembre de 2020 07:47:23:AM

Puerta de enlace predeterminada : 192.168.50.254

Servidor DHCP : 192.168.50.254

IAID DHCPv6 : 67687436

DUID de cliente DHCPv6. : 00-01-00-01-26-57-1F-D5-50-7B-9D-B5-C7-83

Servidores DNS. : 8.8.8.8

NetBIOS sobre TCP/IP. : habilitado

Adaptador de Ethernet Conexión de red Bluetooth:

Estado de los medios. : medios desconectados

Sufijo DNS específico para la conexión. :

Descripción : Bluetooth Device (Personal Area Network)

Dirección física. : 08-D4-0C-C0-17-4F

DHCP habilitado : sí

Configuración automática habilitada : sí

- Como Podemos observar si es la misma

7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Internet Protocol Version 4, Src: 192.168.50.101, Dst: 8.8.8.8

User Datagram Protocol, Src Port: 55691, Dst Port: 53

Domain Name System (query)

Transaction ID: 0xd9a6

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

www.ietf.org: type A, class IN

Name: www.ietf.org

[Name Length: 12]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

- El mensaje de consulta es de *type A*, pero el mensaje de consulta no contiene ninguna respuesta

8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

ip.addr == 192.168.50.101

No.	Time	Source	Destination	Protocol	Length	Info
79	8.104316	8.8.8.8	192.168.50.101	DNS	204	Standard query response 0xad1a A api.bing.com CNAME api-bing-com.e-0001.e-msedge.net CNAME afd.e-0001.dc-ms...
80	8.106543	8.8.8.8	192.168.50.101	DNS	193	Standard query response 0x7097 A www.bing.com CNAME a-0001.a-afdentry.net.trafficmanager.net CNAME dual-a-0...
327	13.680363	192.168.50.101	8.8.8.8	DNS	72	Standard query 0xd9a6 A www.ietf.org
328	13.680369	192.168.50.101	8.8.8.8	DNS	72	Standard query 0xd9a6 A www.ietf.org
329	13.772302	8.8.8.8	192.168.50.101	DNS	149	Standard query response 0xd9a6 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16...

... .. 0. = Answer authenticated: Answer/authority portion was not authenticated

... .. 0. = Non-authenticated data: Unacceptable

... .. 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 3

Authority RRs: 0

Additional RRs: 0

Queries

www.ietf.org: type A, class IN

Name: www.ietf.org

[Name Length: 12]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

Answers

www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net

www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99

www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99

[Request In: 327]

[Time: 0.091939000 seconds]

9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Wireshark packet capture showing DNS and HTTP traffic. The filter is `ip.addr == 192.168.50.101`.

No.	Time	Source	Destination	Protocol	Length	Info
80	8.106543	8.8.8.8	192.168.50.101	DNS	193	Standard query response 0x7097 A www.bing.com CNAME a-0001.a-afdentry.net.trafficmanager.net CNAME dual-a-0...
327	13.680363	192.168.50.101	8.8.8.8	DNS	72	Standard query 0xd9a6 A www.ietf.org
328	13.680369	192.168.50.101	8.8.8.8	DNS	72	Standard query 0xd9a6 A www.ietf.org
329	13.772302	8.8.8.8	192.168.50.101	DNS	149	Standard query response 0xd9a6 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16...
857	15.100132	192.168.50.101	8.8.8.8	DNS	78	Standard query 0x570d A analytics.ietf.org
858	15.100138	192.168.50.101	8.8.8.8	DNS	78	Standard query 0x...
863	15.205706	8.8.8.8	192.168.50.101	DNS	108	Standard query re...
194	11.772128	192.168.50.101	190.98.153.26	HTTP	521	GET /img-resizer/...
245	11.916965	190.98.153.26	192.168.50.101	HTTP	1037	HTTP/1.1 200 OK
340	13.876683	192.168.50.101	104.16.44.99	HTTP	354	GET / HTTP/1.1

User Datagram Protocol, Src Port: 53, Dst Port: 55691

Domain Name System (response)

- Transaction ID: 0xd9a6
- Flags: 0x8180 Standard query response, No error
- Questions: 1
- Answer RRs: 3
- Authority RRs: 0
- Additional RRs: 0

Queries

Answers

- `www.ietf.org`: type CNAME, class IN, cname `www.ietf.org.cdn.cloudflare.net`
- `www.ietf.org.cdn.cloudflare.net`: type A, class IN, addr `104.16.44.99`
- `www.ietf.org.cdn.cloudflare.net`: type A, class IN, addr `104.16.45.99`

[Request In: 327]

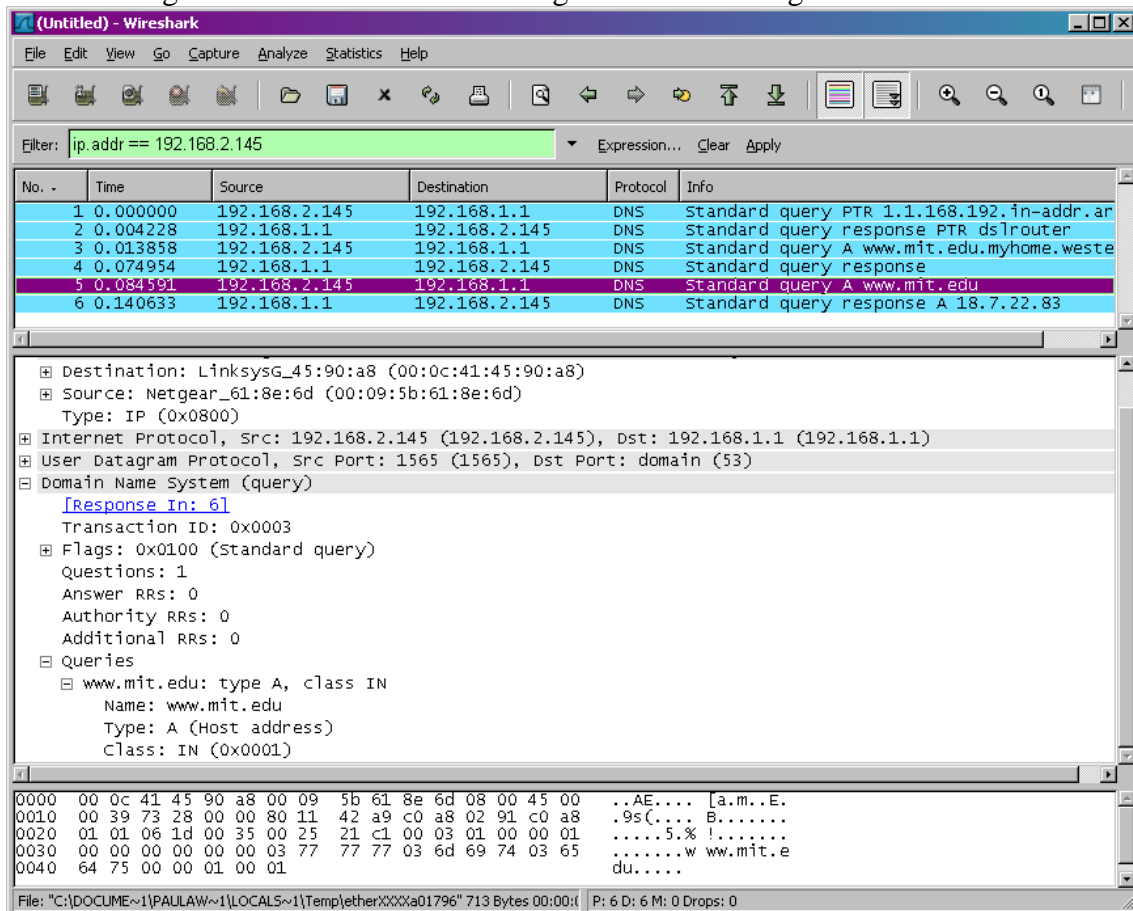
[Time: 0.091939000 seconds]

- El destino del paquete SYN subsiguiente es 104.16.44.99, la misma que se encuentra en el mensaje de respuesta DNS que es de *type A*.
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?
- En este caso no se emitió nuevas consultas para obtener las imágenes

Now let's play with *nslookup*⁴.

- Start packet capture.
- Do an *nslookup* on *www.mit.edu*
- Stop packet capture.

You should get a trace that looks something like the following:



We see from the above screenshot that *nslookup* actually sent three DNS queries and received three DNS responses. For the purpose of this assignment, in answering the following questions, ignore the first two sets of queries/responses, as they are specific to *nslookup* and are not normally generated by standard Internet applications. You should instead focus on the last query and response messages.

⁴ If you are unable to run Wireshark and capture a trace file, use the trace file *dns-ethereal-trace-2* in the zip file <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>

11. What is the destination port for the DNS query message? What is the source port of DNS response message?

Wireshark packet capture showing a DNS query and response. The query (frame 6199) is sent to 8.8.8.8 on port 53. The response (frame 6217) is received on port 52675. A packet details pane for the query shows the destination port as 53.

No.	Time	Source	Destination	Protocol	Length	Info
6198	37.428282	192.168.50.101	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
6199	37.428288	192.168.50.101	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
6217	37.532242	8.8.8.8	192.168.50.101	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net

Packet details for frame 6199:

- Ethernet II, Src: IntelCor_c0:17:4b (08:d4:0c:c0:17:4b), Dst: Qpcom_09:00:00:00:00:00
- Internet Protocol Version 4, Src: 192.168.50.101, Dst: 8.8.8.8
- User Datagram Protocol, Src Port: 52675, Dst Port: 53
 - Source Port: 52675
 - Destination Port: 53
 - Length: 37
 - Checksum: 0xc0df [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 10]
 - [Timestamps]
 - UDP payload (29 bytes)
- Domain Name System (query)

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Wireshark packet capture showing a DNS query and response. The query (frame 6199) is sent to 8.8.8.8 on port 53. The response (frame 6217) is received on port 52675. A packet details pane for the query shows the destination port as 53.

No.	Time	Source	Destination	Protocol	Length	Info
6198	37.428282	192.168.50.101	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
6199	37.428288	192.168.50.101	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
6217	37.532242	8.8.8.8	192.168.50.101	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net

Packet details for frame 6199:

- Ethernet II, Src: IntelCor_c0:17:4b (08:d4:0c:c0:17:4b), Dst: Qpcom_09:00:00:00:00:00
- Internet Protocol Version 4, Src: 192.168.50.101, Dst: 8.8.8.8
- User Datagram Protocol, Src Port: 52675, Dst Port: 53
 - Source Port: 52675
 - Destination Port: 53
 - Length: 37
 - Checksum: 0xc0df [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 10]
 - [Timestamps]
 - UDP payload (29 bytes)
- Domain Name System (query)

Windows command prompt output:

```

C:\Users\Smart>ipconfig /all

Puerta de enlace predeterminada . . . . . : 192.168.50.254
Servidor DHCP . . . . . : 192.168.50.254
IAID DHCPv6 . . . . . : 67687436
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-57-1F-D5-50-7B-9D-B5-C7-83
Servidores DNS. . . . . : 8.8.8.8
                          190.96.96.6
NetBIOS sobre TCP/IP. . . . . : habilitado
Adaptador de Ethernet Conexión de red Blueto...
Estado de los medios. . . . .
Sufijo DNS específico para la conexión. .
Descripción . . . . .
Dirección física. . . . .
DHCP habilitado . . . . .
Configuración automática habilitada . .

```

- Se envía a la dirección 8.8.8.8, y si es la misma dirección IP del servidor DNS local predeterminado

13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

6198	37.428282	192.168.50.101	8.8.8.8	DNS	71 Standard query 0x0003 AAAA www.mit.edu
6199	37.428288	192.168.50.101	8.8.8.8	DNS	71 Standard query 0x0003 AAAA www.mit.edu
6217	37.532242	8.8.8.8	192.168.50.101	DNS	200 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb
58	0.404887	192.168.50.101	157.240.14.15	TCP	86 [TCP Retransmission] 49624 → 443 [PSH, ACK] Seq=1 Ack=1 Win=512 Len=32
76	0.530791	157.240.14.15	192.168.50.101	TCP	60 443 → 49624 [ACK] Seq=1 Ack=33 Win=498 Len=0
86	0.580599	192.168.50.101	157.240.14.15	TCP	54 49624 → 443 [ACK] Seq=33 Ack=29 Win=512 Len=0
87	0.580606	192.168.50.101	157.240.14.15	TCP	54 [TCP Dup ACK 86#1] 49624 → 443 [ACK] Seq=33 Ack=29 Win=512 Len=0

Domain Name System (query)
 Transaction ID: 0x0003
 > Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 > www.mit.edu: type AAAA, class IN
 Name: www.mit.edu
 [Name Length: 11]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Response In: 6217]

*Sin título: Bloc d...
 Archivo Edición Formato Ver Ayuda
 luis jaramillo
 100% Windows (CRLF) UTF-8

- El mensaje de consulta es de *type AAAA*, y no contiene respuestas solo es un mensaje de consulta

14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

6217	37.532242	8.8.8.8	192.168.50.101	DNS	200 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb
58	0.404887	192.168.50.101	157.240.14.15	TCP	86 [TCP Retransmission] 49624 → 443 [PSH, ACK] Seq=1 Ack=1 Win=512 Len=32
76	0.530791	157.240.14.15	192.168.50.101	TCP	60 443 → 49624 [ACK] Seq=1 Ack=33 Win=498 Len=0
86	0.580599	192.168.50.101	157.240.14.15	TCP	54 49624 → 443 [ACK] Seq=33 Ack=29 Win=512 Len=0
87	0.580606	192.168.50.101	157.240.14.15	TCP	54 [TCP Dup ACK 86#1] 49624 → 443 [ACK] Seq=33 Ack=29 Win=512 Len=0

Transaction ID: 0x0003
 > Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 4
 Authority RRs: 0
 Additional RRs: 0
 Queries
 > www.mit.edu: type AAAA, class IN
 Answers
 > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
 > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
 > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2001:1498:1:2088::255e
 > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2001:1498:1:2085::255e

*Sin título: Bloc d...
 Archivo Edición Formato Ver Ayuda
 luis jaramillo
 100% Windows (CRLF) UTF-8

Now repeat the previous experiment, but instead issue the command:

```
nslookup -type=NS mit.edu
```

15. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The image shows a Wireshark packet capture of a DNS query. The packet list shows a standard query for NS records of mit.edu sent to 8.8.8.8. The packet details pane shows the query structure. Overlaid on the Wireshark window is a 'Símbolo del sistema' (System Symbol) window displaying network configuration for 'Adaptador de Ethernet Conexión de red'. The configuration shows the default gateway as 192.168.50.254, which is the IP address of the local DNS server. A text editor window is also visible in the background with the text 'luis jaramillo'.

No.	Time	Source	Destination	Protocol	Length	Info
476	25.716029	8.8.8.8	192.168.50.101	DNS	104	Standard query response 0x0001 PTR 8.8.8.in-addr.arpa PTR dns.google
477	25.719912	192.168.50.101	8.8.8.8	DNS	67	Standard query 0x0002 NS mit.edu
478	25.719922	192.168.50.101	8.8.8.8	DNS	67	Standard query 0x0002 NS mit.edu
480	25.814534	8.8.8.8	192.168.50.101	DNS		
869	29.861862	192.168.50.101	8.8.8.8	DNS		
870	29.861868	192.168.50.101	8.8.8.8	DNS		
871	29.952524	8.8.8.8	192.168.50.101	DNS		
15	1.684239	192.168.50.101	192.168.50.254	HTTP		

Domain Name System (query)
Transaction ID: 0x0002
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
mit.edu: type NS, class IN
[Response In: 480]

Símbolo del sistema
Puerta de enlace predeterminada : 192.168.50.254
Servidor DHCP : 192.168.50.254
IAID DHCPv6 : 67687436
DUID de cliente DHCPv6 : 00-01-00-01-26-57-1F-D5-50-7B-9D-B5-C7-83
Servidores DNS : 8.8.8.8
NetBIOS sobre TCP/IP : habilitado

•Se envía a la dirección 8.8.8.8, y si es la misma dirección IP del servidor DNS local predeterminado

16. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The image shows a Wireshark packet capture of a DNS query. The packet list shows a standard query for NS records of mit.edu sent to 8.8.8.8. The packet details pane shows the query structure. Overlaid on the Wireshark window is a 'Símbolo del sistema' (System Symbol) window displaying network configuration for 'Adaptador de Ethernet Conexión de red'. The configuration shows the default gateway as 192.168.50.254, which is the IP address of the local DNS server. A text editor window is also visible in the background with the text 'luis jaramillo'.

No.	Time	Source	Destination	Protocol	Length	Info
477	25.719912	192.168.50.101	8.8.8.8	DNS	67	Standard query 0x0002 NS mit.edu
478	25.719922	192.168.50.101	8.8.8.8	DNS	67	Standard query 0x0002 NS mit.edu
480	25.814534	8.8.8.8	192.168.50.101	DNS	234	Standard query response 0x0002 NS mit.edu
869	29.861862	192.168.50.101	8.8.8.8	DNS	76	Standard query 0x10f6 A web.whatsapp.com
870	29.861868	192.168.50.101	8.8.8.8	DNS	76	Standard query 0x10f6 A web.whatsapp.com
871	29.952524	8.8.8.8	192.168.50.101	DNS	129	Standard query response 0x10f6 A web.whatsapp.com
15	1.684239	192.168.50.101	192.168.50.254	HTTP	266	GET /InternetGatewayDevice.xml HTTP/1.1

Domain Name System (query)
Transaction ID: 0x0002
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
mit.edu: type NS, class IN
Name: mit.edu
[Name Length: 7]
[Label Count: 2]
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)

17. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

```
nslookup www.aiit.or.kr bitsy.mit.edu
```

18. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

⁵ If you are unable to run Wireshark and capture a trace file, use the trace file dns-ethereal-trace-4 in the zip file <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>

The image shows a Wireshark packet capture of a DNS query. The packet list shows a query from 192.168.50.101 to 18.0.72.3. The packet details pane shows the query structure, including the transaction ID, flags, and the query type (Standard query). The packet bytes pane shows the raw data of the query. A system configuration window is also visible, showing network settings for IPv6 and DHCP.

- Se envía a la dirección IP 18.0.72.3, esto se debe a que se esta enviando la petición a otro servidor, la dirección pertenece al bitsy.mit.edu, y no se realiza al dns de mi servidor

19. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The image shows a Wireshark packet capture of a DNS query. The packet list shows a query from 192.168.50.101 to 18.0.72.3. The packet details pane shows the query structure, including the transaction ID, flags, and the query type (Standard query). The packet bytes pane shows the raw data of the query. A system configuration window is also visible, showing network settings for IPv6 and DHCP.

- El tipo de consulta es type AAAA, y no contiene respuestas

20. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

- No se encontró un mensaje de respuesta debido a que el servidor no esta activo.