

# מטלה 2

סטודנט ראשון : אילן מאיר סופיר, ת"ז : 342615648

סטודנט שני : בן כהן, ת"ז : 207029786

**Question 1 :** Run nslookup to obtain the IP address of a Web server in Asia.  
What is the IP address of that server ?

```
C:\Users\Thierry>nslookup www.amazon.co.jp
Serveur : ns1-cache.hotnet.net.il
Address: 213.57.2.5

Réponse ne faisant pas autorité :
Nom : dtioykqj1u8de.cloudfront.net
Address: 65.9.108.170
Aliases: www.amazon.co.jp
         tp.4d5ad1d2b-frontier.amazon.co.jp
```

I wrote « nslookup www.amazon.co.jp » for the web server of amazon in Japan, Asia.

The IP address of that server is : **65.9.108.170**

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

```
C:\Users\Thierry>nslookup -type=NS sorbonne-universite.fr
Serveur : ns1-cache.hotnet.net.il
Address: 213.57.2.5

Réponse ne faisant pas autorité :
sorbonne-universite.fr nameserver = shiva.jussieu.fr
sorbonne-universite.fr nameserver = ganesh.upmc.fr
sorbonne-universite.fr nameserver = soleil.uvsq.fr

soleil.uvsq.fr internet address = 193.51.24.1
shiva.jussieu.fr internet address = 134.157.0.129
ganesh.upmc.fr internet address = 134.157.192.1
```

I wrote « nslookup -type=NS sorbonne-universite.fr » it's a university in Paris, France.

The servers are :

- shiva.jussieu.fr
- ganesh.upmc.fr
- soleil.uvsq.fr

**Question 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 ?

```
C:\Users\Thierry>nslookup www.sorbonne-universite.fr mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server :    UnKnown
Address:    87.248.118.22

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Le délai de la requête sur UnKnown est dépassé.
```

I wrote « nslookup www.sorbonne-universite.fr mail.yahoo.com fr ». The IP address for the DNS server obtained in Question 2 if queried for the Yahoo! mail server is :

- 87.248.118.22

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

The image shows a Wireshark network capture of traffic on interface \Device\NPF\_{0D82C8DC-D54B-46A1-A666-31504C20C28A}. The capture filter is 'ip.addr == 192.168.1.35'. The packet list shows several packets, with packet 604 highlighted in blue. The packet details pane for packet 604 shows a DNS Standard query (0x5eb3) from 192.168.1.35 to 213.57.2.5. The packet bytes pane shows the raw data of the DNS query.

No.	Time	Source	Destination	Protocol	Length	Info
598	11:19:08,126376	192.168.1.35	216.58.212.206	TCP	54	49808 → 443 [ACK] Seq=1859 Ack=37271 Win=262912 Len=0
599	11:19:08,129418	216.58.212.206	192.168.1.35	TLSv1.3	834	Application Data, Application Data, Application Data
600	11:19:08,129885	192.168.1.35	216.58.212.206	TLSv1.3	93	Application Data
601	11:19:08,209968	216.58.212.206	192.168.1.35	TCP	60	443 → 49808 [ACK] Seq=38051 Ack=1898 Win=69632 Len=0
602	11:19:08,626052	192.168.1.35	131.253.33.219	TCP	55	49755 → 443 [ACK] Seq=1 Ack=1 Win=1027 Len=1 [TCP segment of a reassembled PDU]
603	11:19:08,680019	131.253.33.219	192.168.1.35	TCP	66	443 → 49755 [ACK] Seq=1 Ack=2 Win=2047 Len=0 SLE=1 SRE=2
604	11:19:08,822428	192.168.1.35	213.57.2.5	DNS	72	Standard query 0x5eb3 A www.ietf.org
605	11:19:08,896067	213.57.2.5	192.168.1.35	DNS	459	Standard query response 0x5eb3 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A
606	11:19:08,897097	192.168.1.35	104.16.45.99	TCP	66	49809 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
607	11:19:08,898430	192.168.1.35	104.16.45.99	TCP	66	49810 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
608	11:19:08,962814	104.16.45.99	192.168.1.35	TCP	66	80 → 49809 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
609	11:19:08,962944	192.168.1.35	104.16.45.99	TCP	54	49809 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
610	11:19:08,963206	192.168.1.35	104.16.45.99	HTTP	505	GET / HTTP/1.1
611	11:19:08,971216	104.16.45.99	192.168.1.35	TCP	66	80 → 49810 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
612	11:19:08,971413	192.168.1.35	104.16.45.99	TCP	54	49810 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
613	11:19:09,031304	104.16.45.99	192.168.1.35	TCP	60	80 → 49809 [ACK] Seq=1 Ack=452 Win=67584 Len=0
614	11:19:09,046634	104.16.45.99	192.168.1.35	HTTP	357	HTTP/1.1 301 Moved Permanently
615	11:19:09,051341	192.168.1.35	104.16.45.99	TCP	66	49811 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

Frame 604: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF\_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id 0  
 Ethernet II, Src: GoodWayI\_d4:c2:39 (00:50:b6:d4:c2:39), Dst: Sagemcom\_6b:9c:ec (78:65:59:6b:9c:ec)  
 Internet Protocol Version 4, Src: 192.168.1.35, Dst: 213.57.2.5  
 User Datagram Protocol, Src Port: 57299, Dst Port: 53  
 Source Port: 57299  
 Destination Port: 53  
 Length: 38  
 Checksum: 0x9941 [unverified]  
 [Checksum Status: Unverified]  
 [Stream index: 40]

0000 78 65 59 6b 9c ec 00 50 b6 d4 c2 39 08 00 45 00 xeYk...P...9...E-  
 0010 00 3a 4c 06 00 00 80 11 00 00 c0 a8 01 23 d5 39 :L...#...9  
 0020 02 05 df d3 00 35 00 26 99 41 5e b3 01 00 00 01 .....5...A^.....  
 0030 00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03 .....w ww.ietf-  
 0040 6f 72 67 00 00 01 00 01 org...x

They are sent over UDP.

**Question 5 :** What is the destination port for the DNS query message ?  
What is the source port of DNS response message ?

604	11:19:08,822428	192.168.1.35	213.57.2.5	DNS	72 Standard query 0x5eb3 A www.ietf.org
605	11:19:08,896067	213.57.2.5	192.168.1.35	DNS	459 Standard query response 0x5eb3 A www.ietf.org
606	11:19:08,897097	192.168.1.35	104.16.45.99	TCP	66 49809 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1
607	11:19:08,898430	192.168.1.35	104.16.45.99	TCP	66 49810 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1
608	11:19:08,962814	104.16.45.99	192.168.1.35	TCP	66 80 → 49809 [SYN, ACK] Seq=0 Ack=1 Win=65535
609	11:19:08,962944	192.168.1.35	104.16.45.99	TCP	54 49809 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
610	11:19:08,963206	192.168.1.35	104.16.45.99	HTTP	505 GET / HTTP/1.1
611	11:19:08,971216	104.16.45.99	192.168.1.35	TCP	66 80 → 49810 [SYN, ACK] Seq=0 Ack=1 Win=65535
612	11:19:08,971413	192.168.1.35	104.16.45.99	TCP	54 49810 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0

> Frame 604: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF\_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id 0

> Ethernet II, Src: GoodWayI\_d4:c2:39 (00:50:b6:d4:c2:39), Dst: Sagemcom\_6b:9c:ec (78:65:59:6b:9c:ec)

> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 213.57.2.5

> User Datagram Protocol, Src Port: 57299, Dst Port: 53

Source Port: 57299

Destination Port: 53

605	11:19:08,896067	213.57.2.5	192.168.1.35	DNS	459 Standard query response 0x5eb3 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A
606	11:19:08,897097	192.168.1.35	104.16.45.99	TCP	66 49809 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
607	11:19:08,898430	192.168.1.35	104.16.45.99	TCP	66 49810 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
608	11:19:08,962814	104.16.45.99	192.168.1.35	TCP	66 80 → 49809 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
609	11:19:08,962944	192.168.1.35	104.16.45.99	TCP	54 49809 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
610	11:19:08,963206	192.168.1.35	104.16.45.99	HTTP	505 GET / HTTP/1.1
611	11:19:08,971216	104.16.45.99	192.168.1.35	TCP	66 80 → 49810 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
612	11:19:08,971413	192.168.1.35	104.16.45.99	TCP	54 49810 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0

> Frame 605: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits) on interface \Device\NPF\_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id 0

> Ethernet II, Src: Sagemcom\_6b:9c:ec (78:65:59:6b:9c:ec), Dst: GoodWayI\_d4:c2:39 (00:50:b6:d4:c2:39)

> Internet Protocol Version 4, Src: 213.57.2.5, Dst: 192.168.1.35

> User Datagram Protocol, Src Port: 53, Dst Port: 57299

Source Port: 53

Destination Port: 57299

The destination port for the DNS query is 53 and the source port of the DNS response is 53.

**Question 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 ?

604	11:19:08,822428	192.168.1.35	213.57.2.5	DNS	72	Standard query 0x5eb3 A www.ietf.org
605	11:19:08,896067	213.57.2.5	192.168.1.35	DNS	459	Standard query response 0x5eb3 A www.ietf.org
606	11:19:08,897097	192.168.1.35	104.16.45.99	TCP	66	49809 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1
607	11:19:08,898430	192.168.1.35	104.16.45.99	TCP	66	49810 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1
608	11:19:08,962814	104.16.45.99	192.168.1.35	TCP	66	80 → 49809 [SYN, ACK] Seq=0 Ack=1 Win=65535
609	11:19:08,962944	192.168.1.35	104.16.45.99	TCP	54	49809 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
610	11:19:08,963206	192.168.1.35	104.16.45.99	HTTP	505	GET / HTTP/1.1
611	11:19:08,971216	104.16.45.99	192.168.1.35	TCP	66	80 → 49810 [SYN, ACK] Seq=0 Ack=1 Win=65535
612	11:19:08,971413	192.168.1.35	104.16.45.99	TCP	54	49810 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0

> Frame 604: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF\_{0D82C8DC-D54B-46A1-A666-31504C}

> Ethernet II, Src: GoodWayI\_d4:c2:39 (00:50:b6:d4:c2:39), Dst: Sagemcom\_6b:9c:ec (78:65:59:6b:9c:ec)

> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 213.57.2.5

> User Datagram Protocol, Src Port: 57299, Dst Port: 53

Source Port: 57299

Destination Port: 53

```

Serveurs DNS. . . . . : 213.57.2.5
                     213.57.22.5

```

The DNS query message sent to **213.57.2.5** which is the IP address of one of my local DNS servers.

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

604	11:19:08,822428	192.168.1.35	213.57.2.5	DNS	72	Standard query 0x5eb3 A www.ietf.org
605	11:19:08,896067	213.57.2.5	192.168.1.35	DNS	459	Standard query response 0x5eb3 A www.ietf.org
606	11:19:08,897097	192.168.1.35	104.16.45.99	TCP	66	49809 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1
607	11:19:08,898430	192.168.1.35	104.16.45.99	TCP	66	49810 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1
608	11:19:08,962814	104.16.45.99	192.168.1.35	TCP	66	80 → 49809 [SYN, ACK] Seq=0 Ack=1 Win=65535
609	11:19:08,962944	192.168.1.35	104.16.45.99	TCP	54	49809 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
610	11:19:08,963206	192.168.1.35	104.16.45.99	HTTP	505	GET / HTTP/1.1
611	11:19:08,971216	104.16.45.99	192.168.1.35	TCP	66	80 → 49810 [SYN, ACK] Seq=0 Ack=1 Win=65535
612	11:19:08,971413	192.168.1.35	104.16.45.99	TCP	54	49810 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0

<

▼ Domain Name System (query)

Transaction ID: 0x5eb3

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

> www.ietf.org: type A, class IN

[Response In: 605]

The type of DNS query is **type A**. The query message **doesn't contain** any answers.

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

The image shows a Wireshark packet capture of a DNS response. The packet list at the top shows a DNS response (packet 605) from 213.57.2.5 to 192.168.1.35. The packet details pane shows the DNS response structure, with three answers highlighted in red boxes:

- Answer 1:** www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net. Name: www.ietf.org. Type: CNAME (Canonical NAME for an alias) (5). Class: IN (0x0001). Time to live: 1362 (22 minutes, 42 seconds). Data length: 33. CNAME: www.ietf.org.cdn.cloudflare.net.
- Answer 2:** www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99. Name: www.ietf.org.cdn.cloudflare.net. Type: A (Host Address) (1). Class: IN (0x0001). Time to live: 300 (5 minutes). Data length: 4. Address: 104.16.45.99.
- Answer 3:** www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99. Name: www.ietf.org.cdn.cloudflare.net. Type: A (Host Address) (1). Class: IN (0x0001). Time to live: 300 (5 minutes). Data length: 4. Address: 104.16.44.99.

The packet bytes pane at the bottom shows the raw data of the DNS response, with the three answers highlighted in blue boxes.

We can see that **3 answers** are provided, each one contain :

- **Name**
- **Type**
- **Class**
- **Time to live**
- **Data length**

And then the first answer contain a **CNAME** and the two others an **adress**.

**Question 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 ?

604	11:19:08,822428	192.168.1.35	213.57.2.5	DNS	72 Standard query 0x5eb3 A www.ietf.org
605	11:19:08,896067	213.57.2.5	192.168.1.35	DNS	459 Standard query response 0x5eb3 A www.ietf.org CNAME www.ietf.org.cdr
606	11:19:08,897097	192.168.1.35	104.16.45.99	TCP	66 49809 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
607	11:19:08,898430	192.168.1.35	104.16.45.99	TCP	66 49810 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
608	11:19:08,962814	104.16.45.99	192.168.1.35	TCP	66 80 → 49809 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1
609	11:19:08,962944	192.168.1.35	104.16.45.99	TCP	54 49809 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
610	11:19:08,963206	192.168.1.35	104.16.45.99	HTTP	505 GET / HTTP/1.1
611	11:19:08,971216	104.16.45.99	192.168.1.35	TCP	66 80 → 49810 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1
612	11:19:08,971413	192.168.1.35	104.16.45.99	TCP	54 49810 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
613	11:19:09,031304	104.16.45.99	192.168.1.35	TCP	60 80 → 49809 [ACK] Seq=1 Ack=452 Win=67584 Len=0
614	11:19:09,046634	104.16.45.99	192.168.1.35	HTTP	357 HTTP/1.1 301 Moved Permanently
615	11:19:09,051341	192.168.1.35	104.16.45.99	TCP	66 49811 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
616	11:19:09,093948	192.168.1.35	104.16.45.99	TCP	54 49809 → 80 [ACK] Seq=452 Ack=304 Win=262656 Len=0
618	11:19:09,117904	104.16.45.99	192.168.1.35	TCP	66 443 → 49811 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1
619	11:19:09,118008	192.168.1.35	104.16.45.99	TCP	54 49811 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0

Additional RRs: 10

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

**Yes** we can see that the destination IP address of the SYN packet (**104.16.45.99**) correspond to the IP address provided number 2 in the DNS response message.

**Question 10 :** This web page contains images. Before retrieving each image, does your host issue new DNS queries ?

No because all the images coming from ietf.org so no need to use a new DNS queries.



**Question 11 :** What is the destination port for the DNS query message ?  
What is the source port of DNS response message ?

31	23:15:00,726169	192.168.1.35	213.57.2.5	DNS	71 Standard query 0x0002 A www.mit.edu
35	23:15:02,424227	104.106.109.234	192.168.1.35	HTTP	468 HTTP/1.0 408 Request Time-out (text/html)
36	23:15:02,424602	104.106.109.234	192.168.1.35	TCP	60 80 → 58756 [FIN, ACK] Seq=415 Ack=1 Win=50
37	23:15:02,424672	192.168.1.35	104.106.109.234	TCP	54 58756 → 80 [ACK] Seq=1 Ack=416 Win=1024 Le
38	23:15:02,453115	104.106.109.234	192.168.1.35	HTTP	468 HTTP/1.0 408 Request Time-out (text/html)
39	23:15:02,456538	104.106.109.234	192.168.1.35	TCP	60 80 → 58755 [FIN, ACK] Seq=415 Ack=1 Win=50
40	23:15:02,456593	192.168.1.35	104.106.109.234	TCP	54 58755 → 80 [ACK] Seq=1 Ack=416 Win=1024 Le
41	23:15:02,536992	213.57.2.5	192.168.1.35	DNS	484 Standard query response 0x0002 A www.mit.e
42	23:15:02,541250	192.168.1.35	213.57.2.5	DNS	71 Standard query 0x0003 AAAA www.mit.edu
43	23:15:02,688312	213.57.2.5	192.168.1.35	DNS	524 Standard query response 0x0003 AAAA www.mi

<

- > Frame 31: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF\_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id 0
- > Ethernet II, Src: GoodWayI\_d4:c2:39 (00:50:b6:d4:c2:39), Dst: Sagemcom\_6b:9c:ec (78:65:59:6b:9c:ec)
- > Internet Protocol Version 4, Src: 192.168.1.35, Dst: 213.57.2.5
- > User Datagram Protocol, Src Port: 60184, Dst Port: 53
- > Domain Name System (query)

41	23:15:02,536992	213.57.2.5	192.168.1.35	DNS	484 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME
42	23:15:02,541250	192.168.1.35	213.57.2.5	DNS	71 Standard query 0x0003 AAAA www.mit.edu
43	23:15:02,688312	213.57.2.5	192.168.1.35	DNS	524 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNA

<

- > Frame 41: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits) on interface \Device\NPF\_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id 0
- > Ethernet II, Src: Sagemcom\_6b:9c:ec (78:65:59:6b:9c:ec), Dst: GoodWayI\_d4:c2:39 (00:50:b6:d4:c2:39)
- > Internet Protocol Version 4, Src: 213.57.2.5, Dst: 192.168.1.35
- > User Datagram Protocol, Src Port: 53, Dst Port: 60184
- > Domain Name System (response)

The destination port for the DNS query is **53** and the source port of the DNS response is **53**.

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

31	23:15:00,726169	192.168.1.35	213.57.2.5	DNS	71 Standard query 0x0002 A www.mit.edu
35	23:15:02,424227	104.106.109.234	192.168.1.35	HTTP	468 HTTP/1.0 408 Request Time-out (text/html)
36	23:15:02,424602	104.106.109.234	192.168.1.35	TCP	60 80 → 58756 [FIN, ACK] Seq=415 Ack=1 Win=502 Len=0
37	23:15:02,424672	192.168.1.35	104.106.109.234	TCP	54 58756 → 80 [ACK] Seq=1 Ack=416 Win=1024 Len=0
38	23:15:02,453115	104.106.109.234	192.168.1.35	HTTP	468 HTTP/1.0 408 Request Time-out (text/html)
39	23:15:02,456538	104.106.109.234	192.168.1.35	TCP	60 80 → 58755 [FIN, ACK] Seq=415 Ack=1 Win=502 Len=0
40	23:15:02,456593	192.168.1.35	104.106.109.234	TCP	54 58755 → 80 [ACK] Seq=1 Ack=416 Win=1024 Len=0
41	23:15:02,536992	213.57.2.5	192.168.1.35	DNS	484 Standard query response 0x0002 A www.mit.edu
42	23:15:02,541250	192.168.1.35	213.57.2.5	DNS	71 Standard query 0x0003 AAAA www.mit.edu
43	23:15:02,688312	213.57.2.5	192.168.1.35	DNS	524 Standard query response 0x0003 AAAA www.mit.edu

> Frame 31: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF\_{0D82C8DC-D54B-46A1-A666-31504}

> Ethernet II, Src: GoodWayI\_d4:c2:39 (00:50:b6:d4:c2:39), Dst: Sagemcom\_6b:9c:ec (78:65:59:6b:9c:ec)

> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 213.57.2.5

> User Datagram Protocol, Src Port: 60184, Dst Port: 53

> Domain Name System (query)

```
Serveurs DNS. . . . . : 213.57.2.5
                        213.57.22.5
```

The DNS query message sent to the IP address : **213.57.2.5** which is my DNS default IP address as seen in the ipconfig picture.

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

31	23:15:00,726169	192.168.1.35	213.57.2.5	DNS	71 Standard query 0x0002 A www.mit.edu
35	23:15:02,424227	104.106.109.234	192.168.1.35	HTTP	468 HTTP/1.0 408 Request Time-out (text/html)
36	23:15:02,424602	104.106.109.234	192.168.1.35	TCP	60 80 → 58756 [FIN, ACK] Seq=415 Ack=1 Win=502 Len=0
37	23:15:02,424672	192.168.1.35	104.106.109.234	TCP	54 58756 → 80 [ACK] Seq=1 Ack=416 Win=1024 Len=0
38	23:15:02,453115	104.106.109.234	192.168.1.35	HTTP	468 HTTP/1.0 408 Request Time-out (text/html)
39	23:15:02,456538	104.106.109.234	192.168.1.35	TCP	60 80 → 58755 [FIN, ACK] Seq=415 Ack=1 Win=502 Len=0
40	23:15:02,456593	192.168.1.35	104.106.109.234	TCP	54 58755 → 80 [ACK] Seq=1 Ack=416 Win=1024 Len=0
41	23:15:02,536992	213.57.2.5	192.168.1.35	DNS	484 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566
42	23:15:02,541250	192.168.1.35	213.57.2.5	DNS	71 Standard query 0x0003 AAAA www.mit.edu
43	23:15:02,688312	213.57.2.5	192.168.1.35	DNS	524 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566

> Ethernet II, Src: GoodWayI\_d4:c2:39 (00:50:b6:d4:c2:39), Dst: Sagemcom\_6b:9c:ec (78:65:59:6b:9c:ec)

> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 213.57.2.5

> User Datagram Protocol, Src Port: 60184, Dst Port: 53

> Domain Name System (query)

Transaction ID: 0x0002

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

> www.mit.edu: type A, class IN

The DNS query is of **type A** and it **doesn't** contain any answers.



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

**Question 15 :** Provide a screenshot.

The screenshot shows a Wireshark capture of a network packet. The packet list at the top shows packet 41 as a DNS Standard query response from 213.57.2.5 to 192.168.1.35. The packet details pane shows the DNS structure, and the packet bytes pane shows the raw data. The 'Answers' section in the packet details pane is expanded, showing three entries:

- www.mit.edu:** type CNAME, class IN, cname www.mit.edu.edgekey.net  
Name: www.mit.edu  
Type: CNAME (Canonical NAME for an alias) (5)  
Class: IN (0x0001)  
Time to live: 1800 (30 minutes)  
Data length: 25  
CNAME: www.mit.edu.edgekey.net
- www.mit.edu.edgekey.net:** type CNAME, class IN, cname e9566.dscb.akamaiedge.net  
Name: www.mit.edu.edgekey.net  
Type: CNAME (Canonical NAME for an alias) (5)  
Class: IN (0x0001)  
Time to live: 60 (1 minute)  
Data length: 24  
CNAME: e9566.dscb.akamaiedge.net
- e9566.dscb.akamaiedge.net:** type A, class IN, addr 104.106.109.234  
Name: e9566.dscb.akamaiedge.net  
Type: A (Host Address) (1)  
Class: IN (0x0001)  
Time to live: 20 (20 seconds)  
Data length: 4  
Address: 104.106.109.234

We can see that **3 answers** are provided, each one contain :

- **Name**
- **Type**
- **Class**
- **Time to live**
- **Data length**

And then the first answer contain a **CNAME** : www.mit.edu.edgekey.net

the second answer contain a **CNAME** : e9566.dscb.akamaiedge.net

the third answer contain an **address** : 104.106.109.234

**Question 16 :** To what IP address is the DNS query message sent ? Is this the IP address of your default local DNS server ?

24	00:03:32,937251	192.168.1.35	213.57.2.5	DNS	67 Standard query 0x0002 NS mit.edu
25	00:03:33,019149	213.57.2.5	192.168.1.35	DNS	446 Standard query response 0x0002 NS mit.edu NS use2.akam.net NS eur5.akam.
27	00:03:33,363735	192.168.1.35	64.233.167.188	TCP	55 58942 → 5228 [ACK] Seq=1 Ack=1 Win=1027 Len=1
28	00:03:33,440962	64.233.167.188	192.168.1.35	TCP	60 5228 → 58942 [RST] Seq=1 Win=0 Len=0
30	00:03:36,168221	192.168.1.35	20.54.24.148	TCP	54 58950 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1026 Len=0
31	00:03:36,250807	20.54.24.148	192.168.1.35	TCP	60 443 → 58950 [FIN, ACK] Seq=1 Ack=2 Win=2048 Len=0

> Frame 24: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF\_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id 0  
> Ethernet II, Src: GoodWayI\_d4:c2:39 (00:50:b6:d4:c2:39), Dst: Sagemcom\_6b:9c:ec (78:65:59:6b:9c:ec)  
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 213.57.2.5  
> User Datagram Protocol, Src Port: 49401, Dst Port: 53  
v Domain Name System (query)  
Transaction ID: 0x0002  
> Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
> Queries

```
Serveurs DNS. . . . . : 213.57.2.5  
                       213.57.22.5
```

The DNS query message sent to the IP address : **213.57.2.5** which is my DNS default IP address as seen in the ipconfig picture.

**Question 17 :** Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers” ?

24	00:03:32,937251	192.168.1.35	213.57.2.5	DNS	67 Standard query 0x0002 NS mit.edu
25	00:03:33,019149	213.57.2.5	192.168.1.35	DNS	446 Standard query response 0x0002 NS mit.edu
27	00:03:33,363735	192.168.1.35	64.233.167.188	TCP	55 58942 → 5228 [ACK] Seq=1 Ack=1 Win=1027 Len=1
28	00:03:33,440962	64.233.167.188	192.168.1.35	TCP	60 5228 → 58942 [RST] Seq=1 Win=0 Len=0
30	00:03:36,168221	192.168.1.35	20.54.24.148	TCP	54 58950 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1026 Len=0
31	00:03:36,250807	20.54.24.148	192.168.1.35	TCP	60 443 → 58950 [FIN, ACK] Seq=1 Ack=2 Win=2048 Len=0

Frame 24: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF\_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id 0  
Ethernet II, Src: GoodWayI\_d4:c2:39 (00:50:b6:d4:c2:39), Dst: Sagemcom\_6b:9c:ec (78:65:59:6b:9c:ec)  
Internet Protocol Version 4, Src: 192.168.1.35, Dst: 213.57.2.5  
User Datagram Protocol, Src Port: 49401, Dst Port: 53  
Domain Name System (query)  
Transaction ID: 0x0002  
> Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
v Queries  
> mit.edu: type NS, class IN

The DNS query is of **type NS** and it **doesn't contain** any answers.

**Question 18** : 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 nameservers ?

**Question 19** : Provide a screenshot.

The first screenshot shows a DNS response message for mit.edu. The 'Answers' section lists four entries:

- mit.edu: type NS, class IN, ns use2.akam.net  
Name: mit.edu  
Type: NS (authoritative Name Server) (2)  
Class: IN (0x0001)  
Time to live: 1800 (30 minutes)  
Data length: 15  
Name Server: use2.akam.net
- mit.edu: type NS, class IN, ns eur5.akam.net  
Name: mit.edu  
Type: NS (authoritative Name Server) (2)  
Class: IN (0x0001)  
Time to live: 1800 (30 minutes)  
Data length: 7  
Name Server: eur5.akam.net
- mit.edu: type NS, class IN, ns ns1-173.akam.net  
Name: mit.edu  
Type: NS (authoritative Name Server) (2)  
Class: IN (0x0001)  
Time to live: 1800 (30 minutes)  
Data length: 10  
Name Server: ns1-173.akam.net
- mit.edu: type NS, class IN, ns ns1-37.akam.net  
Name: mit.edu  
Type: NS (authoritative Name Server) (2)  
Class: IN (0x0001)  
Time to live: 1800 (30 minutes)  
Data length: 9  
Name Server: ns1-37.akam.net

The second screenshot shows a DNS response message for mit.edu. The 'Answers' section lists four entries:

- mit.edu: type NS, class IN, ns use5.akam.net  
Name: mit.edu  
Type: NS (authoritative Name Server) (2)  
Class: IN (0x0001)  
Time to live: 1800 (30 minutes)  
Data length: 7  
Name Server: use5.akam.net
- mit.edu: type NS, class IN, ns usw2.akam.net  
Name: mit.edu  
Type: NS (authoritative Name Server) (2)  
Class: IN (0x0001)  
Time to live: 1800 (30 minutes)  
Data length: 7  
Name Server: usw2.akam.net
- mit.edu: type NS, class IN, ns asia1.akam.net  
Name: mit.edu  
Type: NS (authoritative Name Server) (2)  
Class: IN (0x0001)  
Time to live: 1800 (30 minutes)  
Data length: 8  
Name Server: asia1.akam.net
- mit.edu: type NS, class IN, ns asia2.akam.net  
Name: mit.edu  
Type: NS (authoritative Name Server) (2)  
Class: IN (0x0001)  
Time to live: 1800 (30 minutes)  
Data length: 8  
Name Server: asia2.akam.net

Additional records:

- Additional records

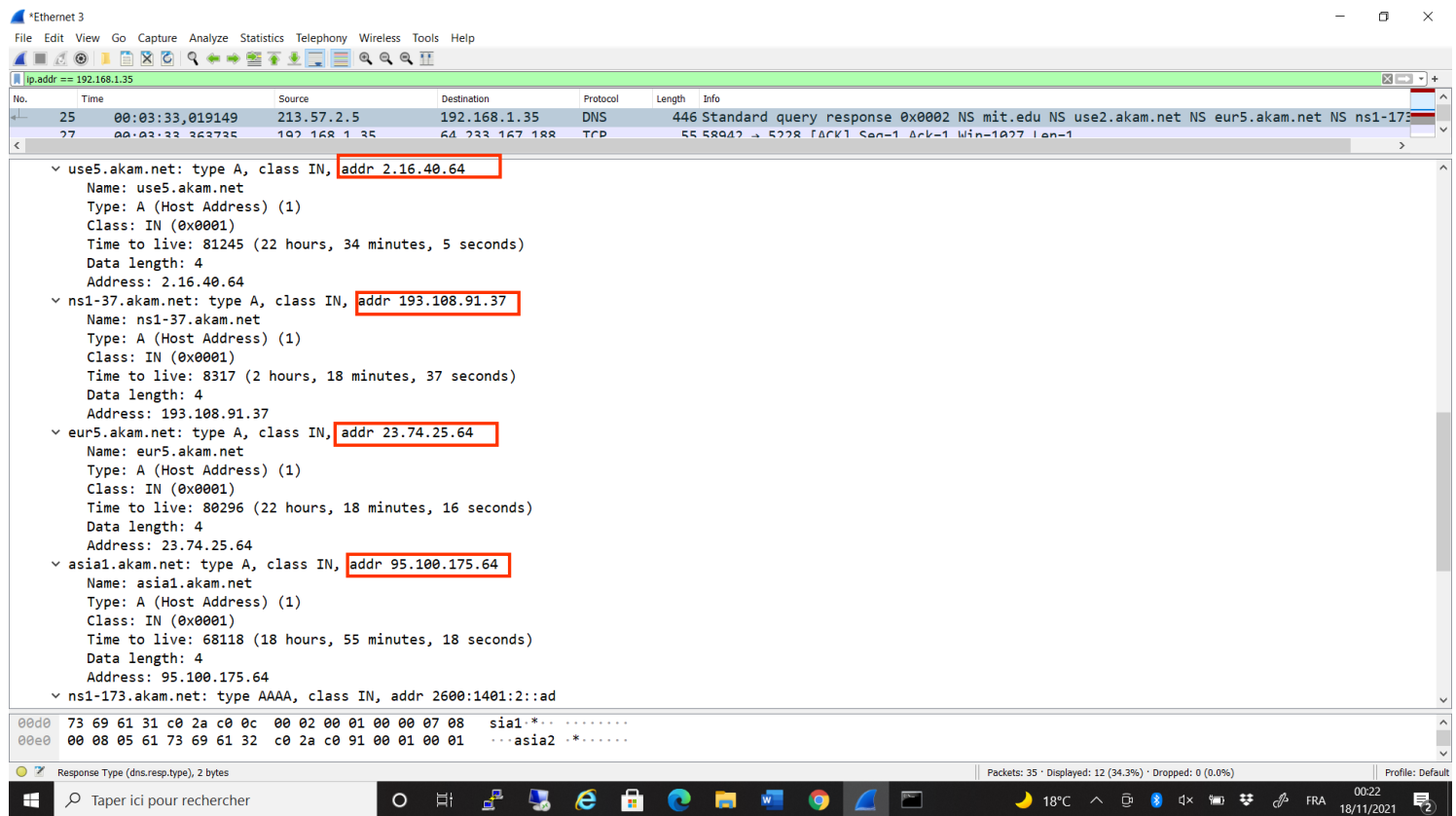
In the DNS response message, the response message provide 8 MIT nameservers :

- use2.akam.net
- eur5.akam.net
- ns1-173.akam.net
- ns1-37.akam.net
- use5.akam.net
- usw2.akam.net
- asia1.akam.net
- asia2.akam.net

The screenshot shows the Wireshark interface with a packet capture of a DNS response. The packet list at the top shows a DNS packet (No. 25) from 213.57.2.5 to 192.168.1.35. The packet details pane shows the 'Additional records' section, which lists four nameservers with their IP addresses highlighted in red boxes:

- usw2.akam.net: type A, class IN, addr 184.26.161.64
- ns1-173.akam.net: type A, class IN, addr 193.108.91.173
- asia2.akam.net: type A, class IN, addr 95.101.36.64
- use2.akam.net: type A, class IN, addr 96.7.49.64

The packet bytes pane at the bottom shows the raw data of the DNS response, including the question and answer sections.



**Yes** this response message also provide the IP addresses of the MIT nameservers in the Additional records :

- for use2.akam.net : 96.7.49.64
- for eur5.akam.net : 23.74.25.64
- for ns1-173.akam.net : 193.108.91.173
- for ns1-37.akam.net : 193.108.91.37
- for use5.akam.net : 2.16.40.64
- for usw2.akam.net : 184.26.161.64
- for asia1.akam.net : 95.100.175.64
- for asia2.akam.net : 95.101.36.64

**Question 20 :** 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 ?

67	15:43:37,736798	192.168.1.35	8.8.8.8	DNS	74 Standard query 0x0002 A www.aiit.or.kr
68	15:43:38,082974	8.8.8.8	192.168.1.35	DNS	90 Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
69	15:43:38,087500	192.168.1.35	8.8.8.8	DNS	74 Standard query 0x0003 AAAA www.aiit.or.kr
70	15:43:38,435105	8.8.8.8	192.168.1.35	DNS	128 Standard query response 0x0003 AAAA www.aiit.or.kr SOA ns9.dnszi.com

> Frame 67: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id 0  
> Ethernet II, Src: GoodWayI\_d4:c2:39 (00:50:b6:d4:c2:39), Dst: Sagemcom\_6b:9c:ec (78:65:59:6b:9c:ec)  
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 8.8.8.8  
> User Datagram Protocol, Src Port: 57433, Dst Port: 53  
v Domain Name System (query)  
Transaction ID: 0x0002  
> Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
> Queries  
[Response In: 68]

The DNS query message sent to the IP address : **8.8.8.8** which is the **IP address of DNS.google**.

**Question 21 :** Examine the DNS query message. What “Type” of DNS query is it ? Does the query message contain any “answers” ?

66	15:43:37,731884	8.8.8.8	192.168.1.35	DNS	104 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR
67	15:43:37,736798	192.168.1.35	8.8.8.8	DNS	74 Standard query 0x0002 A www.aiit.or.kr
68	15:43:38,082974	8.8.8.8	192.168.1.35	DNS	90 Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.
69	15:43:38,087500	192.168.1.35	8.8.8.8	DNS	74 Standard query 0x0003 AAAA www.aiit.or.kr
70	15:43:38,435105	8.8.8.8	192.168.1.35	DNS	128 Standard query response 0x0003 AAAA www.aiit.or.kr SOA ns9.

> Frame 67: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id 0  
> Ethernet II, Src: GoodWayI\_d4:c2:39 (00:50:b6:d4:c2:39), Dst: Sagemcom\_6b:9c:ec (78:65:59:6b:9c:ec)  
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 8.8.8.8  
> User Datagram Protocol, Src Port: 57433, Dst Port: 53  
v Domain Name System (query)  
Transaction ID: 0x0002  
> Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
v Queries  
> www.aiit.or.kr: type A, class IN  
[Response In: 68]

It's a **type A** of DNS query and it **doesn't** contain any answers.



**Question 22 :** Examine the DNS response message. How many “answers” are provided ? What does each of these answers contain ?

**Question 23 :** Provide a screenshot.

The screenshot displays the Wireshark network protocol analyzer interface. The top pane shows a list of captured packets, with packet 68 selected. The middle pane shows the details of packet 68, which is a DNS response. The 'Domain Name System (response)' section is expanded, showing the 'Answers' section. A single answer is listed: 'www.aiit.or.kr: type A, class IN, addr 58.229.6.225'. The bottom pane shows the raw packet bytes in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
65	15:43:37.663848	192.168.1.35	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
66	15:43:37.731884	8.8.8.8	192.168.1.35	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
67	15:43:37.736798	192.168.1.35	8.8.8.8	DNS	74	Standard query 0x0002 A www.aiit.or.kr
68	15:43:38.082974	8.8.8.8	192.168.1.35	DNS	90	Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
69	15:43:38.087500	192.168.1.35	8.8.8.8	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
70	15:43:38.435105	8.8.8.8	192.168.1.35	DNS	128	Standard query response 0x0003 AAAA www.aiit.or.kr SOA ns9.dnszi.com

Frame 68: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF\_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id 0  
> Ethernet II, Src: Sagemcom\_6b:9c:ec (78:65:59:6b:9c:ec), Dst: GoodWayI\_d4:c2:39 (00:50:b6:d4:c2:39)  
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.35  
> User Datagram Protocol, Src Port: 53, Dst Port: 57433  
> Domain Name System (response)  
Transaction ID: 0x0002  
> Flags: 0x8180 Standard query response, No error  
Questions: 1  
Answer RRs: 1  
Authority RRs: 0  
Additional RRs: 0  
Queries  
> www.aiit.or.kr: type A, class IN  
Answers  
> www.aiit.or.kr: type A, class IN, addr 58.229.6.225  
Name: www.aiit.or.kr  
Type: A (Host Address) (1)  
Class: IN (0x0001)  
Time to live: 3600 (1 hour)  
Data length: 4  
Address: 58.229.6.225  
[Request In: 67]  
[Time: 0.346176000 seconds]

0020 01 23 00 35 e0 59 00 38 7b 0b 00 02 81 80 00 01 .# 5.Y.8 { .....  
0030 00 01 00 00 00 00 03 77 77 77 04 61 69 69 74 02 .....ww aiit.

We can see that **one** answer is provided and contain :

- **Name** : www.aiit.or.kr
- **Type** : A (Host Address) (1)
- **Class** : IN (0x0001)
- **Time to live** : 3600 (1 hour)
- **Data length** : 4
- **Address** : 58.229.6.225