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 ?

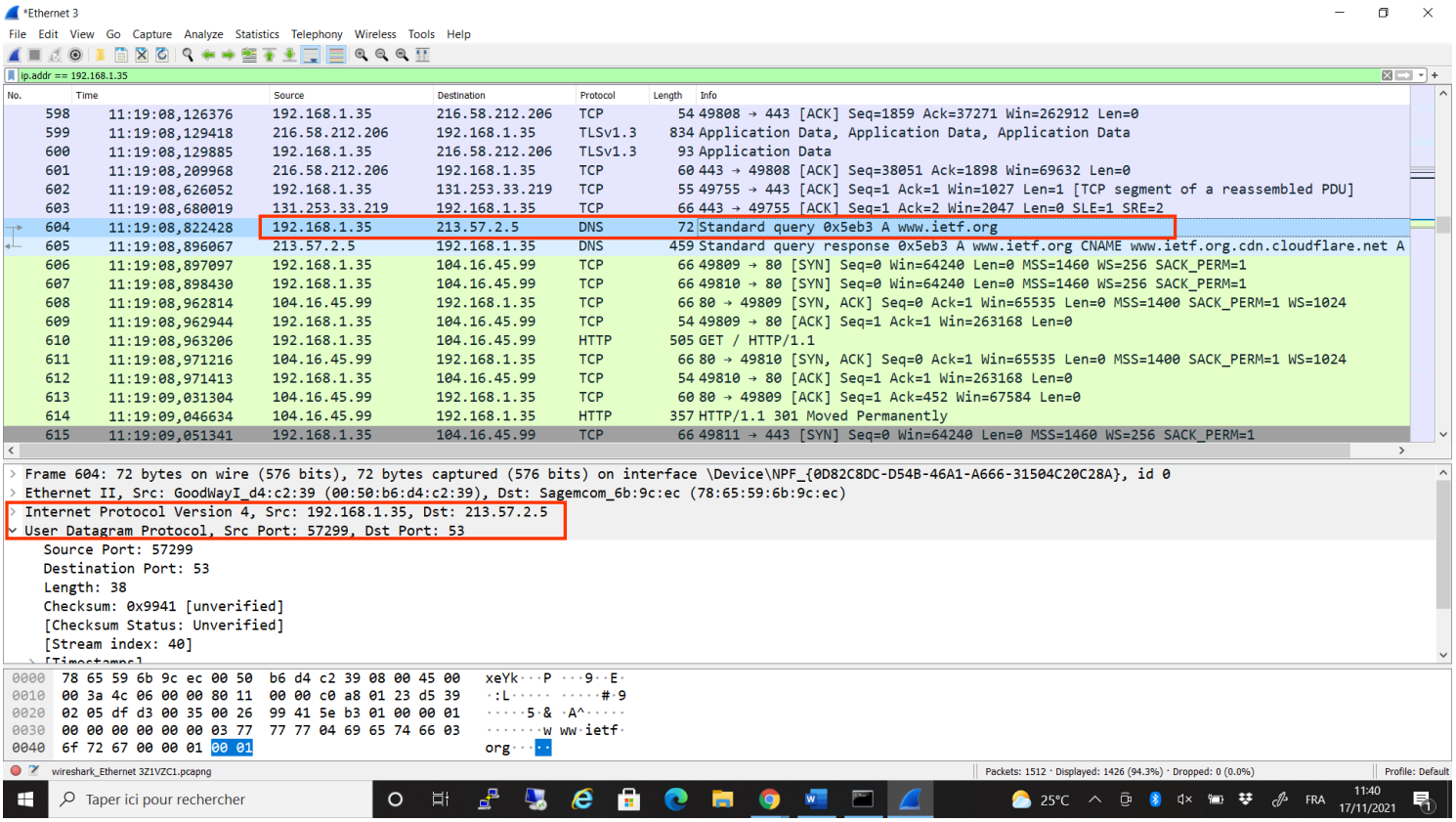
```
C:\Users\Thierry>nslookup www.sorbonne-universite.fr mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Serveur :   UnKnown
Address:  87.248.118.22

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 addreess for the DNS server obtained in Question 2 if queried for the Yahoo! mail server is :

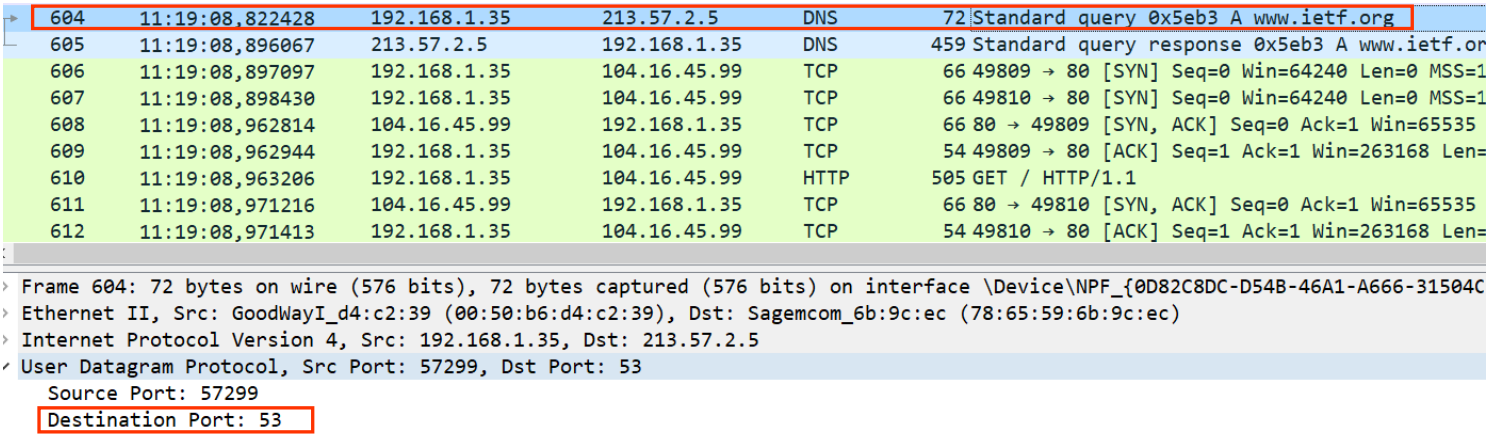
- **87.248.118.22**

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



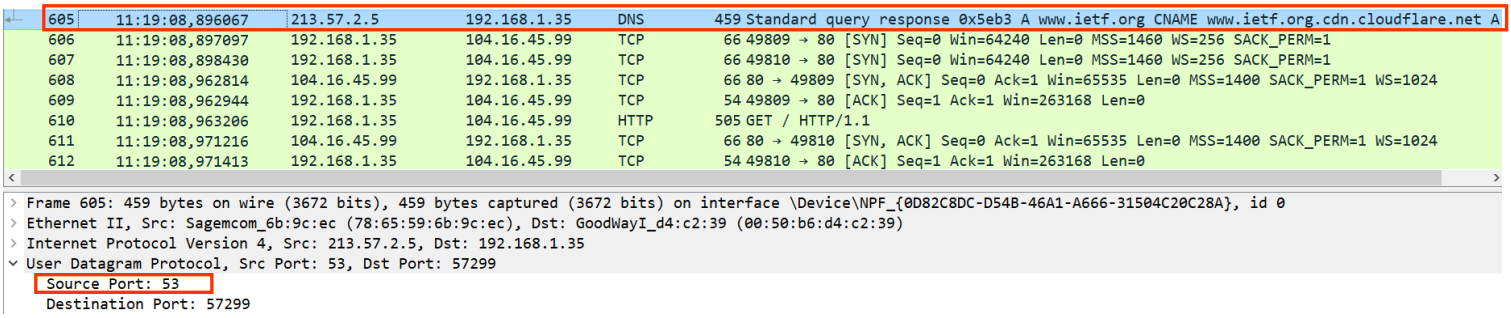
They are sent over **UDP.**

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.or
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=
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=

```
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
```



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.or
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=
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=

```
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.

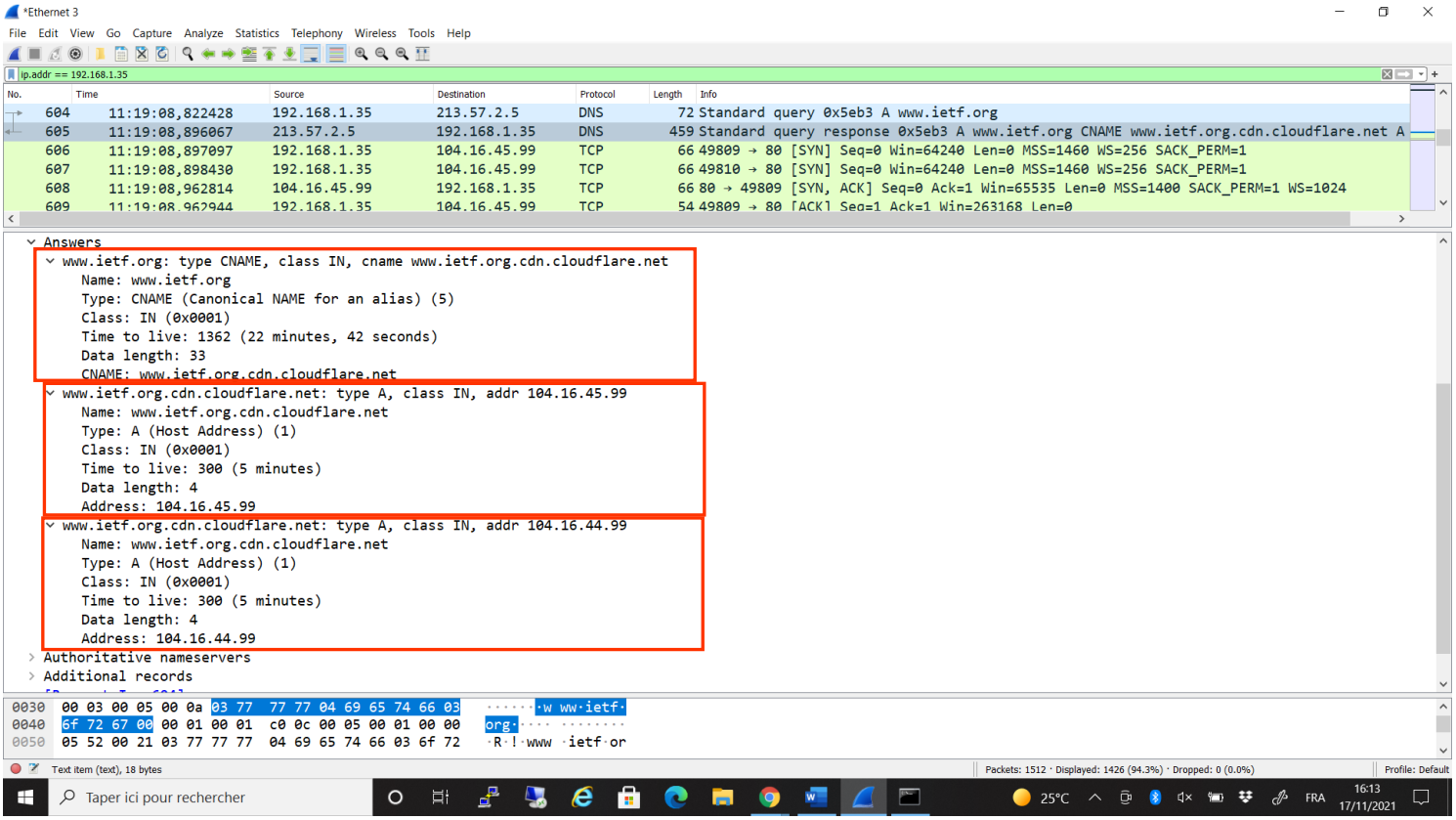
Question 7 : Examine the DNS query message. What “Type” of DNS query is it ? Does the query message contain any “answers” ?

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.
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
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
608	11:19:08,962814	104.16.45.99	192.168.1.35	TCP	66	80 → 49809 [SYN, ACK] Seq=0 Ack=1 Win=6553
609	11:19:08,962944	192.168.1.35	104.16.45.99	TCP	54	49809 → 80 [ACK] Seq=1 Ack=1 Win=263168 Le
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=6553
612	11:19:08,971413	192.168.1.35	104.16.45.99	TCP	54	49810 → 80 [ACK] Seq=1 Ack=1 Win=263168 Le

```
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 ?

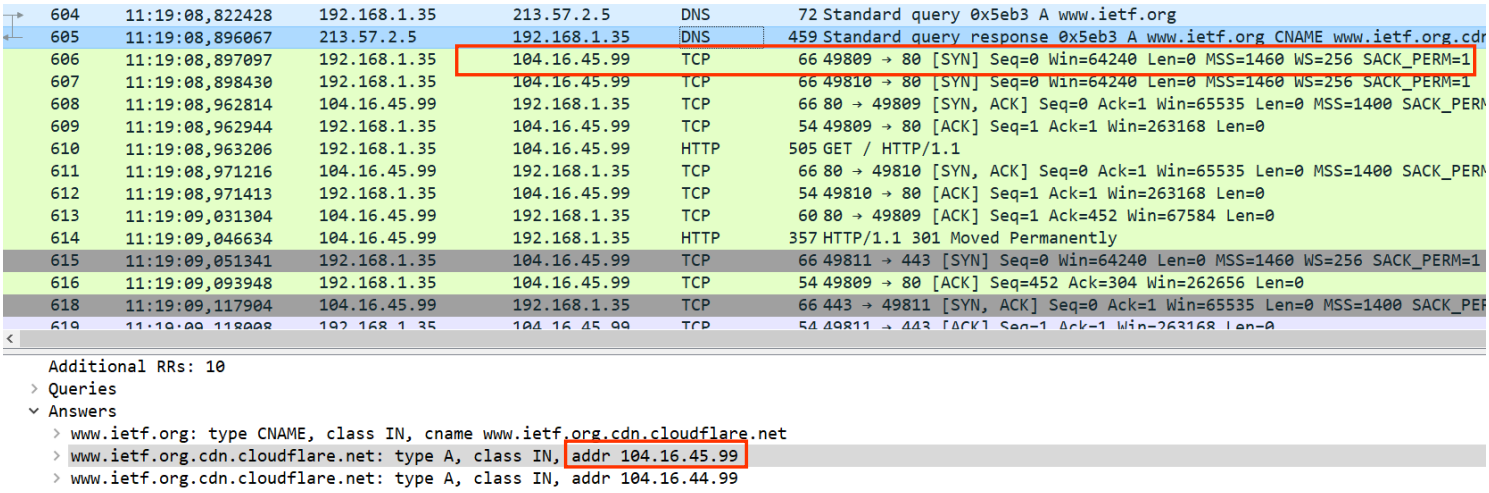


We can see that **3 answers** are provided, each one contain :

- **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.cdn
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
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
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_PER
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

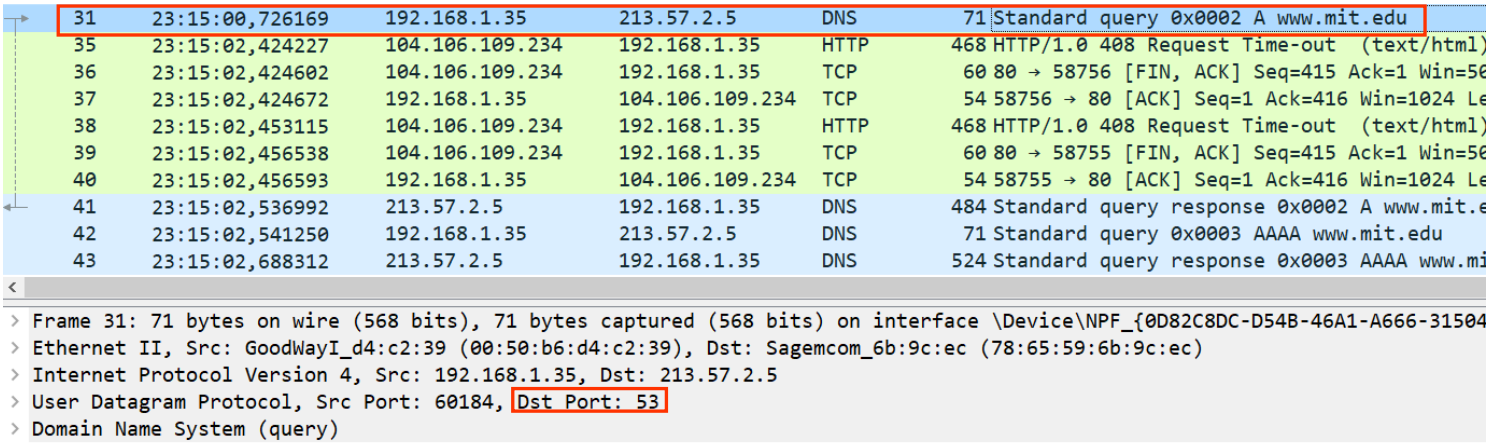
```
Additional RRs: 10
> Queries
v Answers
  > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
  > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
  > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
```

Yes we can see that the destination IP address of the SYN packet (**104.16.45.99**) correspond to the IP addresse 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 ?

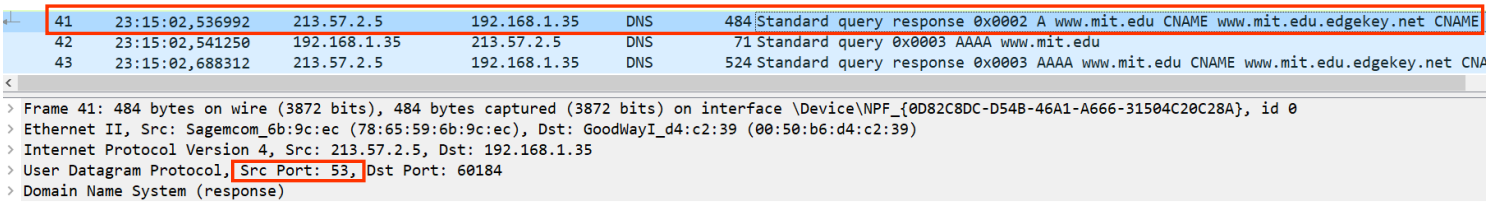
No because all the images coming from ietf.org so no need to use a new DNS queries.

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-A666-31504
> 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)
```



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=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-A666-31504
> 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” ?

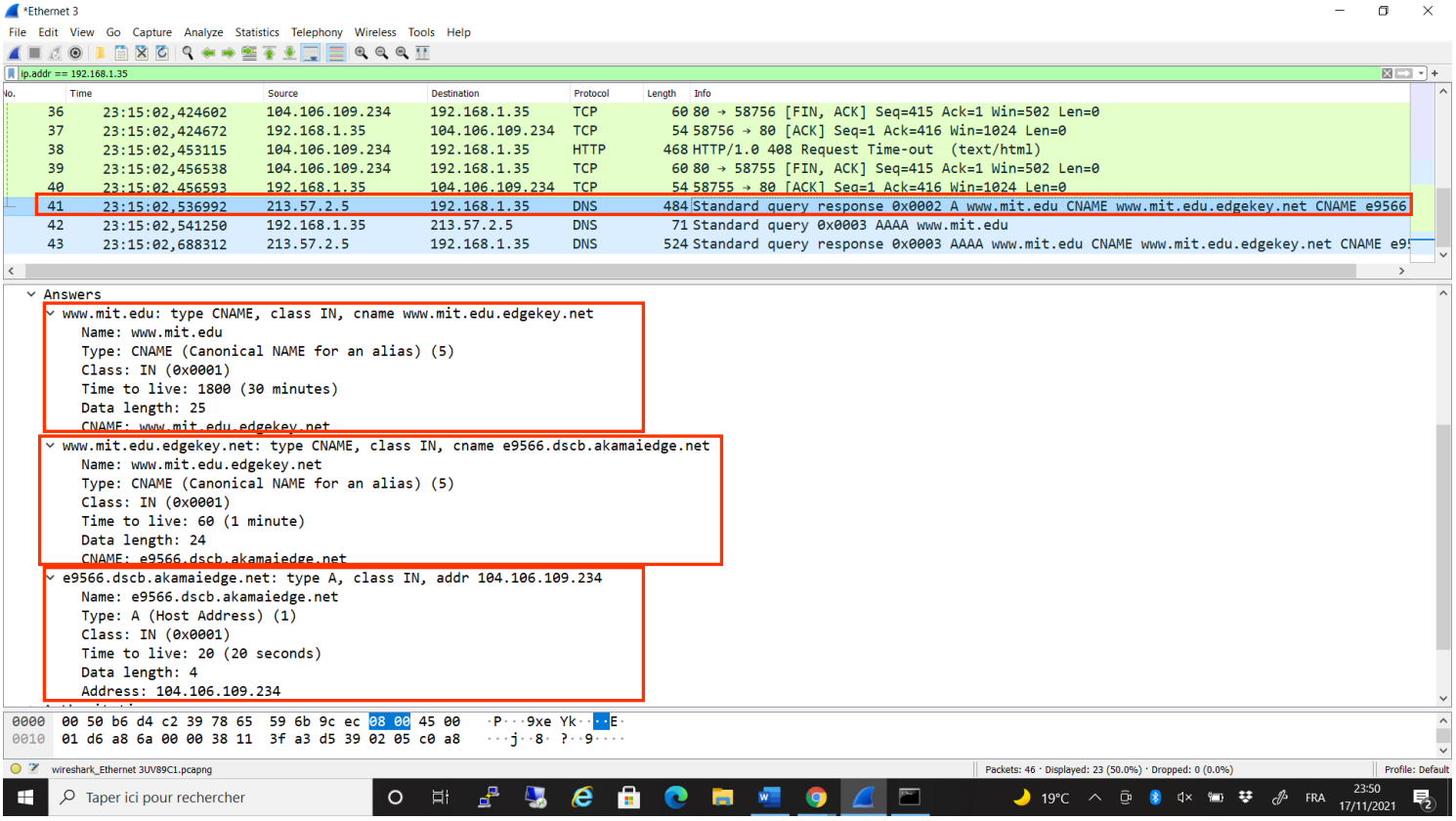
31	23:15:00,726169	192.168.1.35	213.57.2.5	DNS	71	Standard query 0x0002 A www.mit.edu
35	23:15:02,424227	104.106.109.234	192.168.1.35	HTTP	468	HTTP/1.0 408 Request Time-out (text/html)
36	23:15:02,424602	104.106.109.234	192.168.1.35	TCP	60	80 → 58756 [FIN, ACK] Seq=415 Ack=1 Win=502 Len=0
37	23:15:02,424672	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 e9

```
> 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
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.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.



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” ?

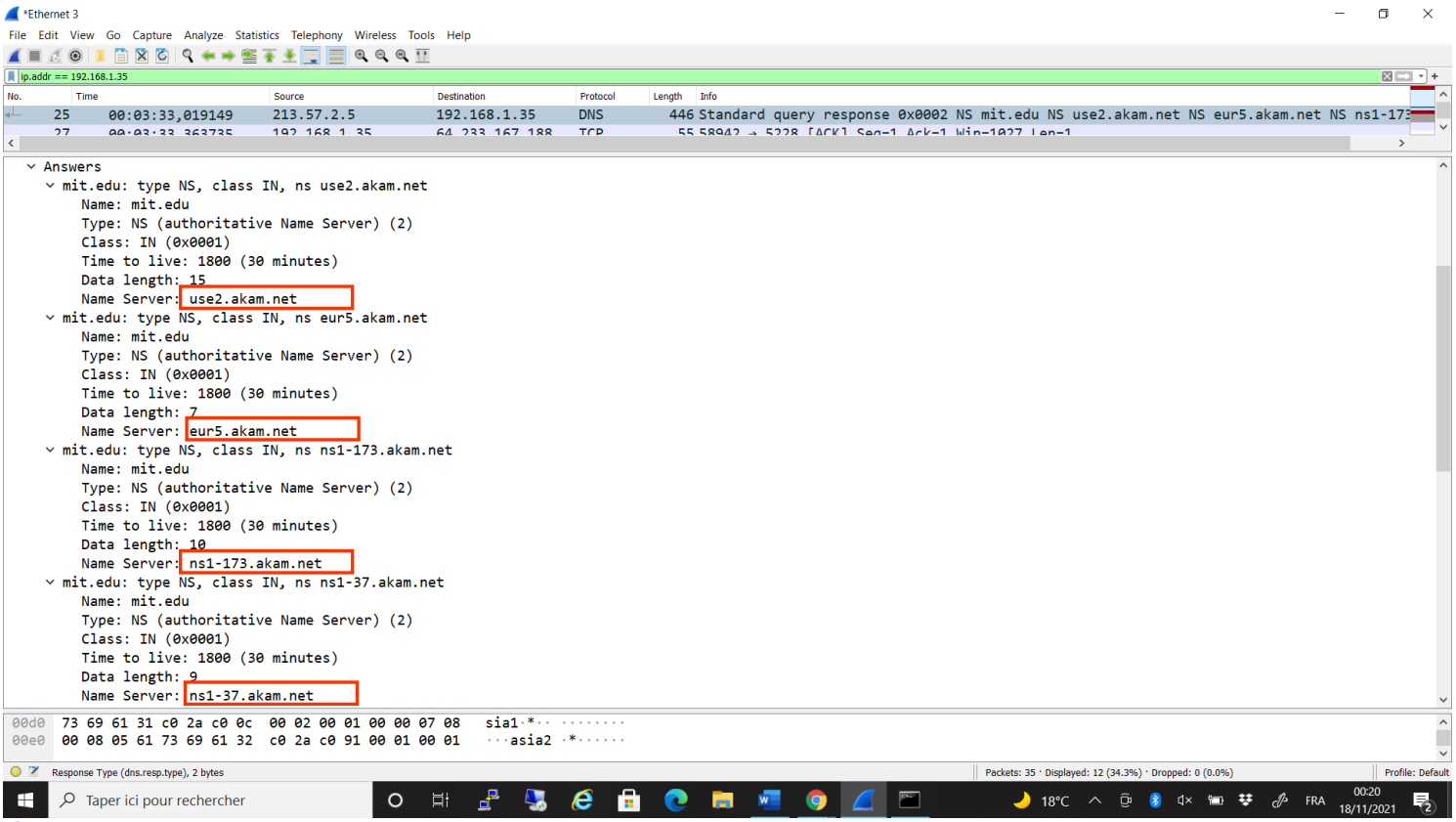
24	00:03:32,937251	192.168.1.35	213.57.2.5	DNS	67	Standard query 0x0002 NS mit.edu
25	00:03:33,019149	213.57.2.5	192.168.1.35	DNS	446	Standard query response 0x0002 NS mit.edu
27	00:03:33,363735	192.168.1.35	64.233.167.188	TCP	55	58942 → 5228 [ACK] Seq=1 Ack=1 Win=1027 Le
28	00:03:33,440962	64.233.167.188	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=10
31	00:03:36,250807	20.54.24.148	192.168.1.35	TCP	60	443 → 58950 [FIN, ACK] Seq=1 Ack=2 Win=20

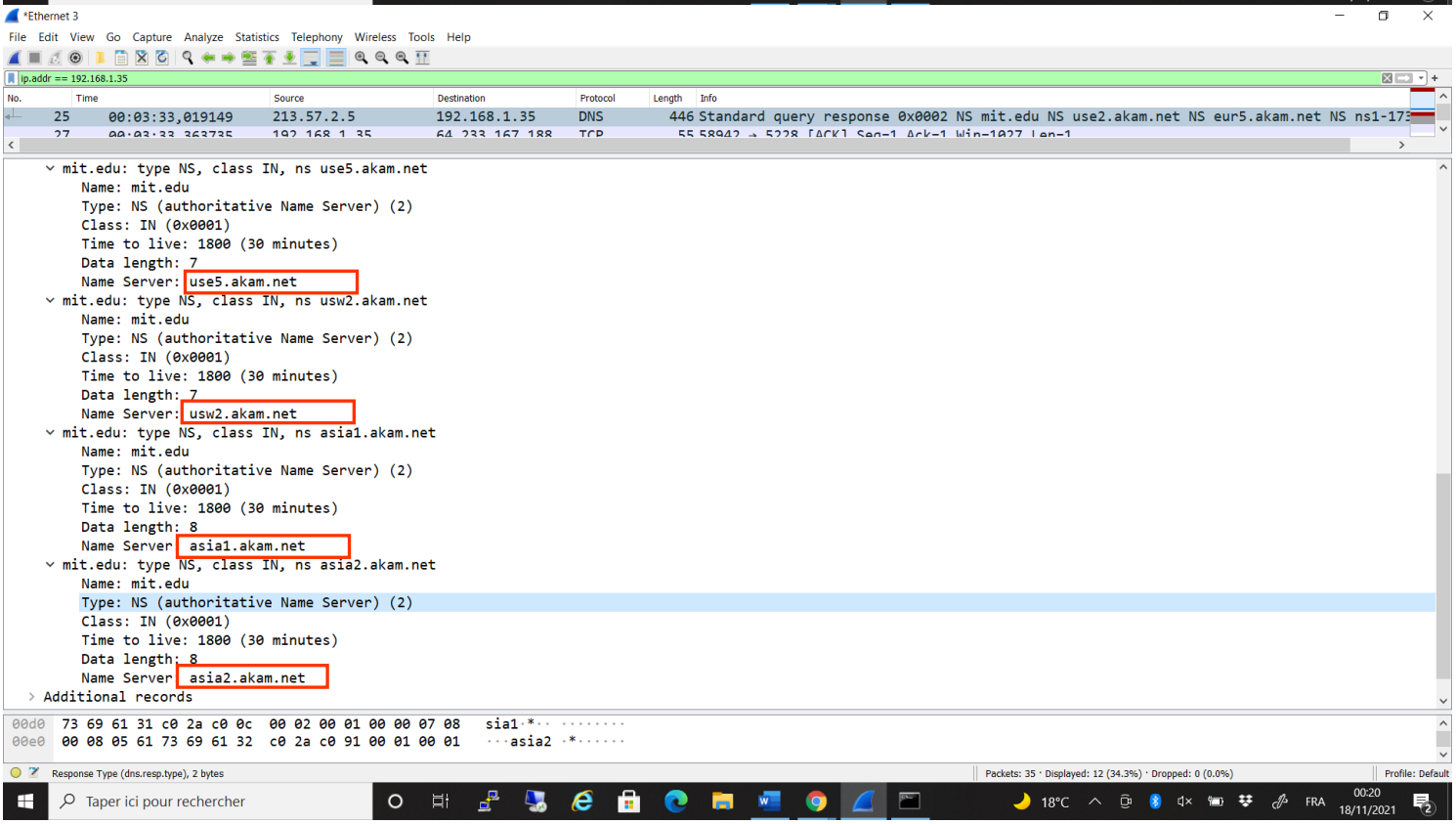
```
Frame 24: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{0D82C8DC-D54B-46A1-A666-31504
Ethernet II, Src: GoodWayI_d4:c2:39 (00:50:b6:d4:c2:39), Dst: Sagemcom_6b:9c:ec (78:65:59:6b:9c:ec)
Internet Protocol Version 4, Src: 192.168.1.35, Dst: 213.57.2.5
User Datagram Protocol, Src Port: 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.





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

- use2.akam.net

- eur5.akam.net

- ns1-173.akam.net

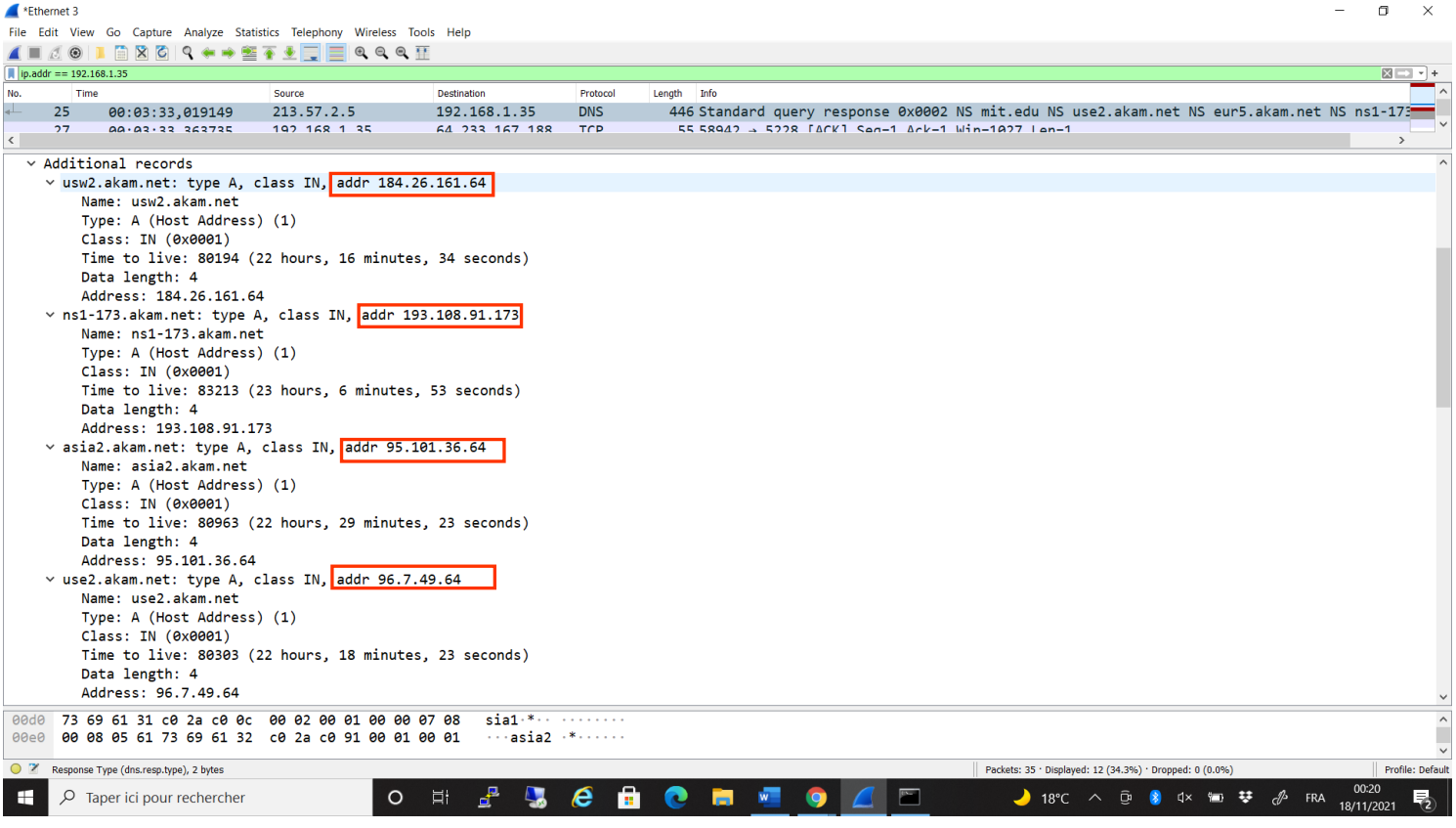
- ns1-37.akam.net

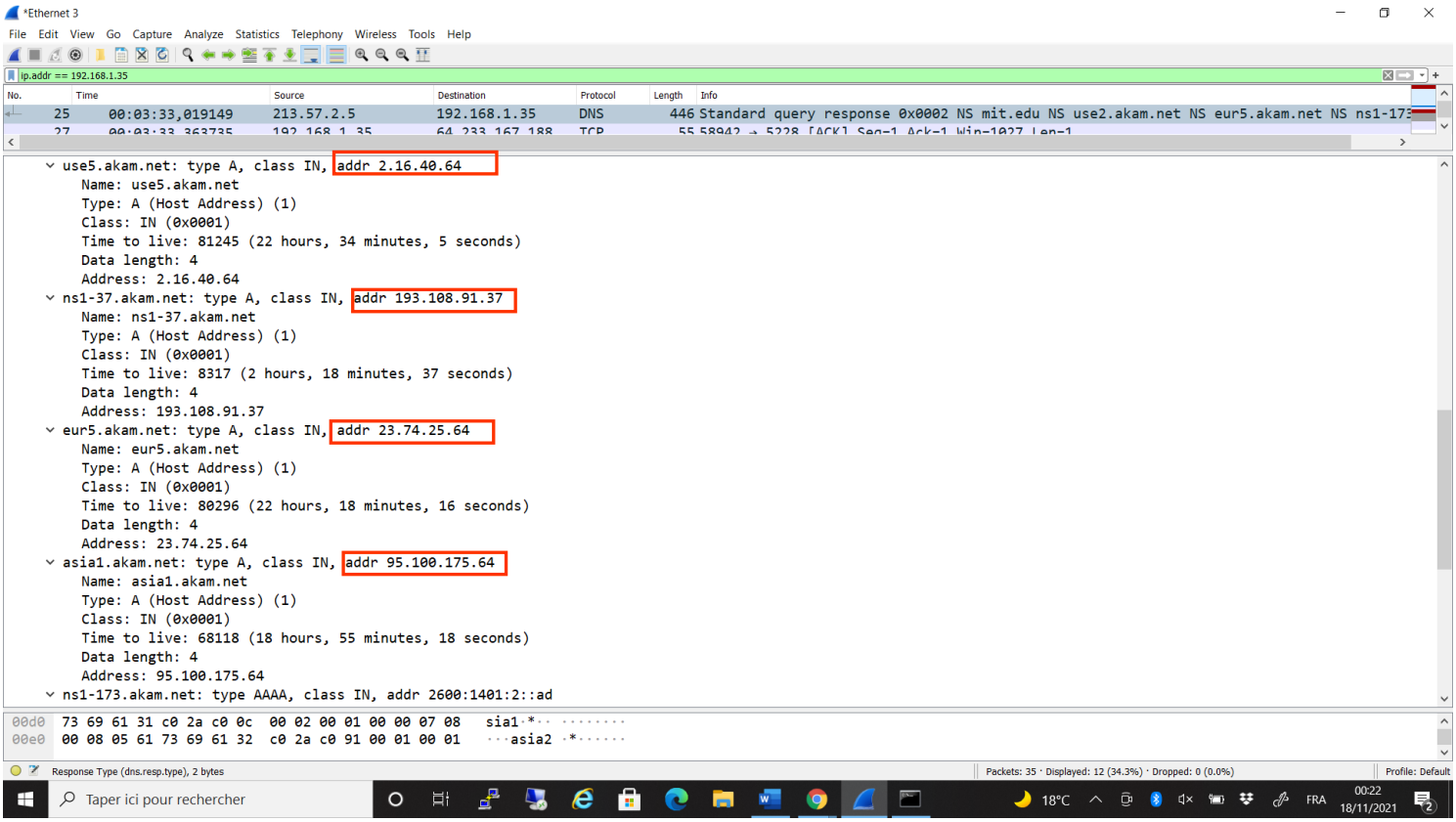
- use5.akam.net

- usw2.akam.net

- asia1.akam.net

- asia2.akam.net





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

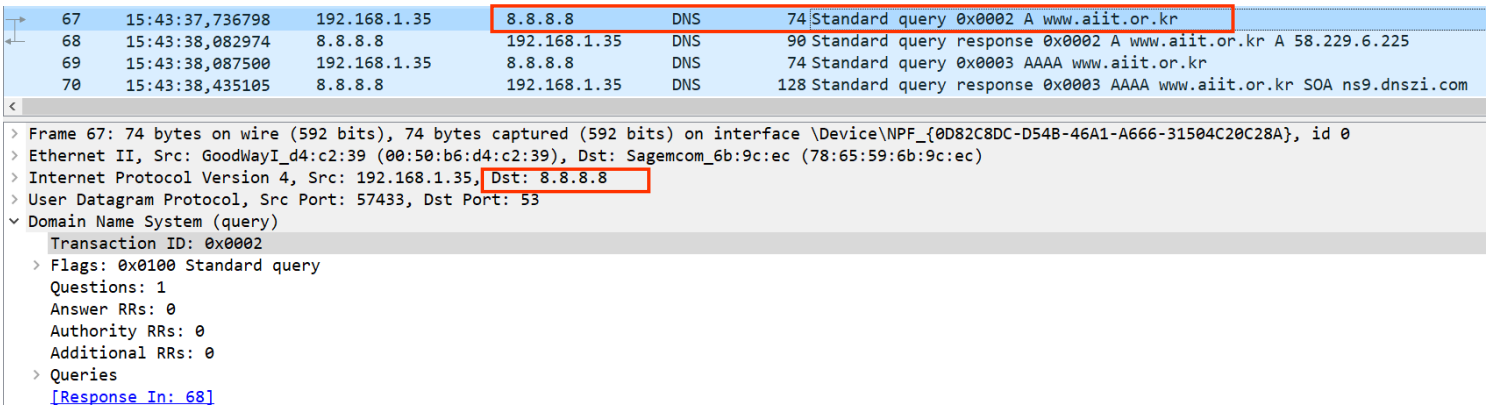
- for use5.akam.net : 2.16.40.64

- for usw2.akam.net : 184.26.161.64

- for asia1.akam.net : 95.100.175.64

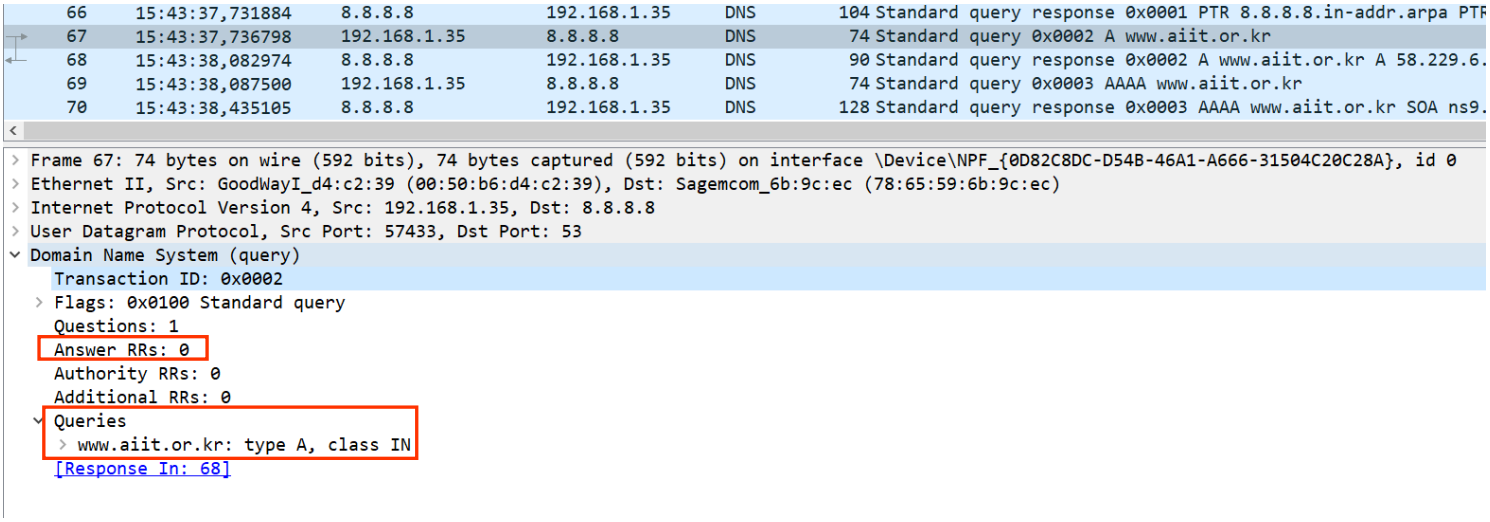
- for asia2.akam.net : 95.101.36.64

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 ?



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

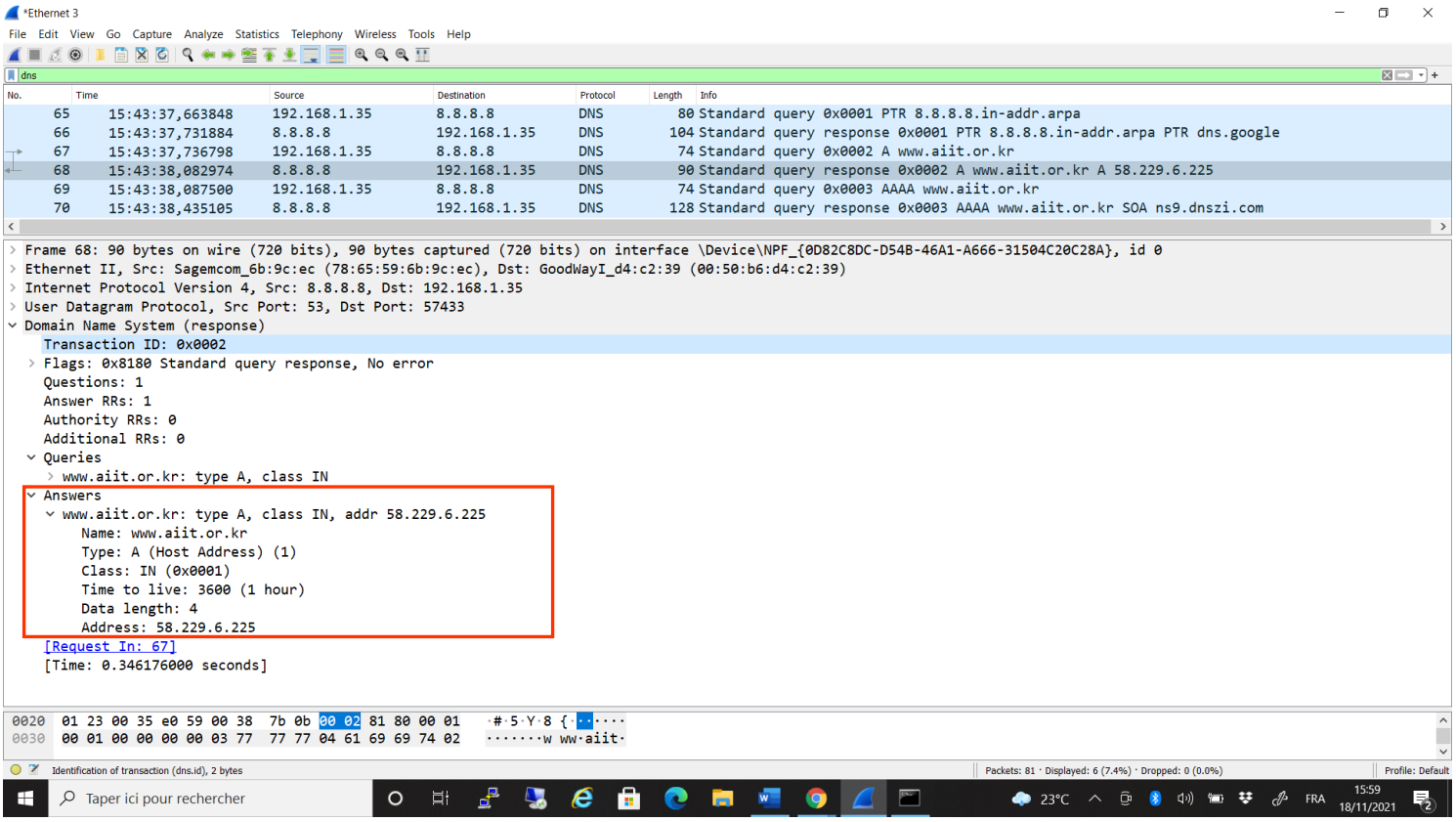
Question 21 : Examine the DNS query message. What “Type” of DNS query is it ? Does the query message contain any “answers” ?



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.



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

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