

Work by - Nattanat Lertariyamaythee

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server? ([www.anet.net.th](http://www.anet.net.th) → 203.148.250.185)

```
PS C:\Users\ASUS> nslookup www.anet.net.th
Server:      UnKnown
Address:     172.20.10.1

Non-authoritative answer:
Name:        anet.wewyn.com
Address:     203.148.250.185
Aliases:     www.anet.net.th
```

2. Run nslookup to determine the authoritative DNS servers for a university in Europe. (auth4.dns.ox.ac.uk)

```
PS C:\Users\ASUS> nslookup www.ox.ac.uk
Server:      UnKnown
Address:     172.20.10.1

Non-authoritative answer:
Name:        www.ox.ac.uk.cdn.cloudflare.net
Addresses:   172.66.169.161
              104.20.34.13
Aliases:     www.ox.ac.uk

PS C:\Users\ASUS> nslookup -type=NS ox.ac.uk
Server:      UnKnown
Address:     172.20.10.1

Non-authoritative answer:
ox.ac.uk      nameserver = auth4.dns.ox.ac.uk
ox.ac.uk      nameserver = dns1.ox.ac.uk
ox.ac.uk      nameserver = auth5.dns.ox.ac.uk
ox.ac.uk      nameserver = auth6.dns.ox.ac.uk
ox.ac.uk      nameserver = dns0.ox.ac.uk
ox.ac.uk      nameserver = dns2.ox.ac.uk
PS C:\Users\ASUS>
```

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? (Cannot find mail.yahoo.com)

```
PS C:\Users\ASUS> nslookup www.mail.yahoo.com auth4.dns.ox.ac.uk
Server: UnKnown
Address: 45.33.127.156

*** UnKnown can't find www.mail.yahoo.com: Query refused
```

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

The image shows a Wireshark packet capture of a DNS query and response. The packet list shows a DNS query (No. 160) and a DNS response (No. 161). The packet details for the DNS query (No. 160) show it is a Standard query for www.ietf.org. The packet details for the DNS response (No. 161) show it is a Standard query response for www.ietf.org. A red arrow points to the 'User Datagram Protocol' section of the packet details, indicating it is sent over UDP.

5. What is the destination port for the DNS query message? What is the source port of DNS response message? (src: 37257, dst.: 53)

The image shows a Wireshark packet capture of a DNS query and response. The packet list shows a DNS query (No. 160) and a DNS response (No. 161). The packet details for the DNS query (No. 160) show it is a Standard query for www.ietf.org. The packet details for the DNS response (No. 161) show it is a Standard query response for www.ietf.org. The packet details for the DNS query (No. 160) show the source port is 37257 and the destination port is 53. The packet details for the DNS response (No. 161) show the source port is 53 and the destination port is 37257.

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? (Yes, they are the same)

```

(kali㉿kali)-[~]
$ nslookup www.ietf.org
Server:      172.20.10.1
Address:     172.20.10.1#53

Non-authoritative answer:
Name:   www.ietf.org
Address: 104.16.44.99
Name:   www.ietf.org
Address: 104.16.45.99
Name:   www.ietf.org
Address: 2606:4700::6810:2d63
Name:   www.ietf.org
Address: 2606:4700::6810:2c63

```

No.	Time	Source	Destination	Protocol	Length	Info
150	6.496585245	10.0.2.15	192.124.249.13	TLSv1.3	78	Application Data
151	6.496678772	10.0.2.15	192.124.249.13	TCP	54	55546 → 443 [FIN, ACK] Seq=888 Ack=4233 Win=55535 Len=0
152	6.496918003	192.124.249.13	10.0.2.15	TCP	60	443 → 55548 [ACK] Seq=4233 Ack=880 Win=55535 Len=0
153	6.496918134	192.124.249.13	10.0.2.15	TCP	60	443 → 55548 [ACK] Seq=4233 Ack=881 Win=55535 Len=0
154	6.497981819	192.124.249.13	10.0.2.15	TLSv1.3	699	Application Data, Application Data, Application Data
155	6.498014778	10.0.2.15	192.124.249.13	TCP	54	55546 → 443 [ACK] Seq=839 Ack=4233 Win=55535 Len=0
156	6.498299019	10.0.2.15	192.124.249.13	TLSv1.3	85	Application Data
157	6.498564215	192.124.249.13	10.0.2.15	TCP	60	443 → 55546 [ACK] Seq=4233 Ack=870 Win=55535 Len=0
158	6.598413957	192.124.249.13	10.0.2.15	TCP	60	443 → 55548 [FIN, ACK] Seq=881 Ack=4234 Win=9344 Len=0
159	6.598442731	10.0.2.15	192.124.249.13	TCP	54	55548 → 443 [ACK] Seq=881 Ack=4234 Win=9344 Len=0
160	7.757280377	10.0.2.15	172.20.10.1	DNS	72	Standard query 0x7bfc A www.ietf.org
161	7.757425577	10.0.2.15	172.20.10.1	DNS	72	Standard query 0x51f2 AAAA www.ietf.org
162	7.823281522	10.0.2.15	172.20.10.1	DNS	75	Standard query 0x1857 A static.ietf.org
163	7.823389301	10.0.2.15	172.20.10.1	DNS	75	Standard query 0x9454 AAAA static.ietf.org
164	8.058636079	172.20.10.1	10.0.2.15	DNS	128	Standard query response 0x51f2 AAAA www.ietf.org AAAA 2606:4700::6810:2d63 AAAA 2606:4700::6810:2c63
165	8.058637108	172.20.10.1	10.0.2.15	DNS	107	Standard query response 0x1857 A static.ietf.org
166	11.582347045	172.20.10.1	10.0.2.15	DNS	104	Standard query response 0x7bfc A www.ietf.org A 104.16.45.99 A 104.16.44.99
167	11.582347419	172.20.10.1	10.0.2.15	DNS	131	Standard query response 0x9454 AAAA static.ietf.org AAAA 2606:4700::6810:2d63 AAAA 2606:4700::6810:2c63
168	11.583054888	10.0.2.15	104.16.45.99	TCP	74	35072 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3150339278 TSecr=0 WS=128
169	11.583420409	10.0.2.15	104.16.45.99	TCP	74	35072 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3150339278 TSecr=0 WS=128
170	11.586332384	10.0.2.15	104.16.45.99	QUIC	1399	Initial, DCID=44575bd4a186b0eb, SCID=590a30, PKN: 0, CRYPTO

```

Name: www.ietf.org
[Name Length: 12]
[Label Count: 3]
Type: A (1) (Host Address)
Class: IN (0x0001)

+ Answers
- www.ietf.org: type A, class IN, addr 104.16.45.99
  Name: www.ietf.org
  Type: A (1) (Host Address)
  Class: IN (0x0001)
  Time to live: 377 (6 minutes, 17 seconds)
  Data length: 4
  Address: 104.16.45.99
- www.ietf.org: type A, class IN, addr 104.16.44.99
  Name: www.ietf.org
  Type: A (1) (Host Address)
  Class: IN (0x0001)
  Time to live: 377 (6 minutes, 17 seconds)
  Data length: 4
  Address: 104.16.44.99
[Request In: 160]
[Time: 3.82566668 seconds]

```

7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? (Type A, no answers)

No.	Time	Source	Destination	Protocol	Length	Info
150	6.496585245	10.0.2.15	192.124.249.13	TLSv1.3	78	Application Data
151	6.496678772	10.0.2.15	192.124.249.13	TCP	54	55546 → 443 [FIN, ACK] Seq=888 Ack=4233 Win=55535 Len=0
152	6.496918003	192.124.249.13	10.0.2.15	TCP	60	443 → 55548 [ACK] Seq=4233 Ack=880 Win=55535 Len=0
153	6.496918134	192.124.249.13	10.0.2.15	TCP	60	443 → 55548 [ACK] Seq=4233 Ack=881 Win=55535 Len=0
154	6.497981819	192.124.249.13	10.0.2.15	TLSv1.3	699	Application Data, Application Data, Application Data
155	6.498014778	10.0.2.15	192.124.249.13	TCP	54	55546 → 443 [ACK] Seq=839 Ack=4233 Win=55535 Len=0
156	6.498299019	10.0.2.15	192.124.249.13	TLSv1.3	85	Application Data
157	6.498564215	192.124.249.13	10.0.2.15	TCP	60	443 → 55546 [ACK] Seq=4233 Ack=870 Win=55535 Len=0
158	6.598413957	192.124.249.13	10.0.2.15	TCP	60	443 → 55548 [FIN, ACK] Seq=881 Ack=4234 Win=9344 Len=0
159	6.598442731	10.0.2.15	192.124.249.13	TCP	54	55548 → 443 [ACK] Seq=881 Ack=4234 Win=9344 Len=0
160	7.757280377	10.0.2.15	172.20.10.1	DNS	72	Standard query 0x7bfc A www.ietf.org
161	7.757425577	10.0.2.15	172.20.10.1	DNS	72	Standard query 0x51f2 AAAA www.ietf.org
162	7.823281522	10.0.2.15	172.20.10.1	DNS	75	Standard query 0x1857 A static.ietf.org
163	7.823389301	10.0.2.15	172.20.10.1	DNS	75	Standard query 0x9454 AAAA static.ietf.org
164	8.058636079	172.20.10.1	10.0.2.15	DNS	128	Standard query response 0x51f2 AAAA www.ietf.org AAAA 2606:4700::6810:2d63 AAAA 2606:4700::6810:2c63
165	8.058637108	172.20.10.1	10.0.2.15	DNS	107	Standard query response 0x1857 A static.ietf.org
166	11.582347045	172.20.10.1	10.0.2.15	DNS	104	Standard query response 0x7bfc A www.ietf.org A 104.16.45.99 A 104.16.44.99
167	11.582347419	172.20.10.1	10.0.2.15	DNS	131	Standard query response 0x9454 AAAA static.ietf.org AAAA 2606:4700::6810:2d63 AAAA 2606:4700::6810:2c63
168	11.583054888	10.0.2.15	104.16.45.99	TCP	74	35072 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3150339278 TSecr=0 WS=128
169	11.583420409	10.0.2.15	104.16.45.99	TCP	74	35072 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3150339278 TSecr=0 WS=128
170	11.586332384	10.0.2.15	104.16.45.99	QUIC	1399	Initial, DCID=44575bd4a186b0eb, SCID=590a30, PKN: 0, CRYPTO

```

UDP payload (30 bytes)
- Domain Name System (query)
  Transaction ID: 0x7bfc
  - Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    ..00 0... .. = Opcode: Standard query (0)
    ....0... .. = Truncated: Message is not truncated
    ....1... .. = Recursion desired: Do query recursively
    ....0... .. = Z: reserved (0)
    ....0... .. = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  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 (1) (Host Address)
      Class: IN (0x0001)
      [Response In: 166]

```

8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? **(2 answers, they contain name, class, type, ttl, data, and address)**

159	6.598442/31	10.0.2.15	192.124.249.13	TCP	54	55948 → 443 [ACK] Seq=881 Ack=4234 Win=9344 Len=0
160	7.757280377	10.0.2.15	172.20.10.1	DNS	72	Standard query 0x7bfc A www.ietf.org
161	7.757425577	10.0.2.15	172.20.10.1	DNS	72	Standard query 0x51f2 AAAA www.ietf.org
162	7.823281522	10.0.2.15	172.20.10.1	DNS	75	Standard query 0x1857 A static.ietf.org
163	7.823389301	10.0.2.15	172.20.10.1	DNS	75	Standard query 0x9454 AAAA static.ietf.org
164	8.058636679	172.20.10.1	10.0.2.15	DNS	128	Standard query response 0x51f2 AAAA www.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63
165	8.058637188	172.20.10.1	10.0.2.15	DNS	167	Standard query response 0x1857 A static.ietf.org A 104.16.45.99 A 104.16.44.99
166	11.582347045	172.20.10.1	10.0.2.15	DNS	131	Standard query response 0x9454 AAAA static.ietf.org AAAA 2606:4700::6810:2d63 AAAA 2606:4700::6810:2c63
167	11.582347419	172.20.10.1	10.0.2.15	DNS	131	Standard query response 0x7bfc A www.ietf.org A 104.16.45.99 A 104.16.44.99
168	11.583054888	10.0.2.15	104.16.45.99	TCP	74	35062 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3150339270 TSecr=0 WS=128
169	11.583420409	10.0.2.15	104.16.45.99	TCP	74	35072 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3150339270 TSecr=0 WS=128
170	11.586332384	10.0.2.15	104.16.45.99	QUIC	1399	Initial, DCID=44575bd4a186b0eb, SCID=590a30, PKN: 0, CRYPTO

Name: www.ietf.org	0000	08 00 27 83 c9 25 52 55	0a 00 02 02 00 00 45 00	' %RU .....E
[Name Length: 12]	0010	00 5a 1b 84 00 00 40 11	9c eb ac 14 0a 01 0a 00	Z...@.....
[Label Count: 3]	0020	02 0f 00 35 91 89 00 46	df bc 7b fc 81 80 00 01	...5...F...{
Type: A (1) (Host Address)	0030	00 02 00 00 00 00 03 77	77 77 04 69 65 74 66 03	.....w ww.ietf
Class: IN (0x0001)	0040	0f 72 67 00 00 01 00 01	c0 0c 00 01 00 01 00 00	org.....
Answers	0050	01 79 00 04 08 10 2d 63	c0 0c 00 01 00 01 00 00	y...h...c
www.ietf.org: type A, class IN, addr 104.16.45.99	0060	01 79 00 04 08 10 2c 63		
Name: www.ietf.org				
Type: A (1) (Host Address)				
Class: IN (0x0001)				
Time to live: 377 (6 minutes, 17 seconds)				
Data length: 4				
Address: 104.16.45.99				
www.ietf.org: type A, class IN, addr 104.16.44.99				
Name: www.ietf.org				
Type: A (1) (Host Address)				
Class: IN (0x0001)				
Time to live: 377 (6 minutes, 17 seconds)				
Data length: 4				
Address: 104.16.44.99				
[Request In: 166]				
[Time: 3.825666668 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? **(Yes)**

160	7.757280377	10.0.2.15	172.20.10.1	DNS	72	Standard query 0x7bfc A www.ietf.org
161	7.757425577	10.0.2.15	172.20.10.1	DNS	72	Standard query 0x51f2 AAAA www.ietf.org
162	7.823281522	10.0.2.15	172.20.10.1	DNS	75	Standard query 0x1857 A static.ietf.org
163	7.823389301	10.0.2.15	172.20.10.1	DNS	75	Standard query 0x9454 AAAA static.ietf.org
164	8.058636679	172.20.10.1	10.0.2.15	DNS	128	Standard query response 0x51f2 AAAA www.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63
165	8.058637188	172.20.10.1	10.0.2.15	DNS	167	Standard query response 0x1857 A static.ietf.org A 104.16.45.99 A 104.16.44.99
166	11.582347045	172.20.10.1	10.0.2.15	DNS	131	Standard query response 0x9454 AAAA static.ietf.org AAAA 2606:4700::6810:2d63 AAAA 2606:4700::6810:2c63
167	11.582347419	172.20.10.1	10.0.2.15	DNS	131	Standard query response 0x7bfc A www.ietf.org A 104.16.45.99 A 104.16.44.99
168	11.583054888	10.0.2.15	104.16.45.99	TCP	74	35062 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3150339270 TSecr=0 WS=128
169	11.583420409	10.0.2.15	104.16.45.99	TCP	74	35072 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3150339270 TSecr=0 WS=128
170	11.586332384	10.0.2.15	104.16.45.99	QUIC	1399	Initial, DCID=44575bd4a186b0eb, SCID=590a30, PKN: 0, CRYPTO

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries? **(No)**

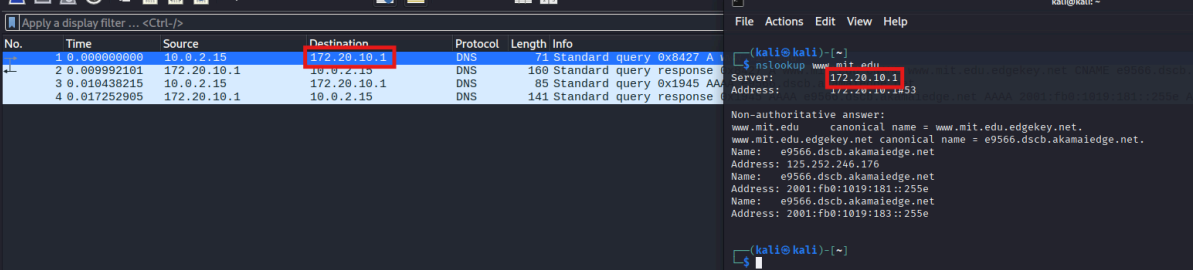
11. What is the destination port for the DNS query message? What is the source port of DNS response message? **(src: 44587, dst: 53)**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	172.20.10.1	DNS	71	Standard query 0x8427 A www.mit.edu
2	0.009992101	172.20.10.1	10.0.2.15	DNS	160	Standard query response 0x8427 A www.mit.edu
3	0.010438215	10.0.2.15	172.20.10.1	DNS	85	Standard query 0x1945 AAAA e9566.dscb.aka
4	0.017252905	172.20.10.1	10.0.2.15	DNS	141	Standard query response 0x1945 AAAA e9566.dscb.aka

Frame 1: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface eth0, id 0	0000	52 55 00 00 00 00 00 00
Ethernet II, Src: PCSSystemtec_83:c9:25 (08:00:27:83:c9:25), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)	0010	00 39 00 00 00 00 00 00
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.20.10.1	0020	0a 01 00 00 00 00 00 00
User Datagram Protocol, Src Port: 44587, Dst Port: 53	0030	00 00 00 00 00 00 00 00
Source Port: 44587	0040	64 75 00 00 00 00 00 00
Destination Port: 53		
Length: 37		
Checksum: 0xc25a [unverified]		
[Checksum Status: Unverified]		
[Stream index: 0]		
[Stream Packet Number: 1]		
[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?(Yes, they are the same)



Wireshark packet capture showing a DNS query and response. The query is sent to 172.20.10.1. The response contains three answers: www.mit.edu (CNAME), www.mit.edu.edgekey.net (CNAME), and e9566.dscb.akamaiedge.net (A).

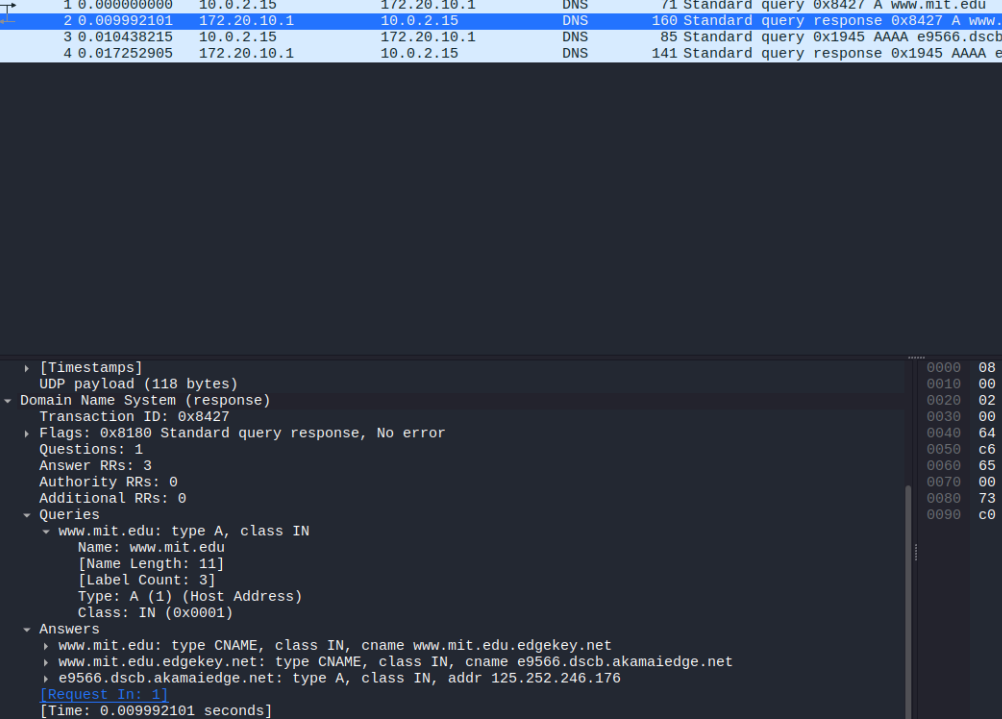
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	172.20.10.1	DNS	71	Standard query 0x8427 A www.mit.edu
2	0.009992101	172.20.10.1	10.0.2.15	DNS	160	Standard query response 0x8427 A www.mit.edu
3	0.010438215	10.0.2.15	172.20.10.1	DNS	85	Standard query 0x1945 AAAA e9566.dscb.akamaiedge.net
4	0.017252905	172.20.10.1	10.0.2.15	DNS	141	Standard query response 0x1945 AAAA e9566.dscb.akamaiedge.net

```
(kali@kali)~$ nslookup www.mit.edu
Server: 172.20.10.1
Address: 172.20.10.1#53

Non-authoritative answer:
www.mit.edu canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name: e9566.dscb.akamaiedge.net
Address: 125.252.246.176
Name: e9566.dscb.akamaiedge.net
Address: 2001:fb0:1019:181::255e
Name: e9566.dscb.akamaiedge.net
Address: 2001:fb0:1019:181::255e
```

13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? (Type A, and no answers)

14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? (3 answers, each contain name, class, type, ttl, data, and address)

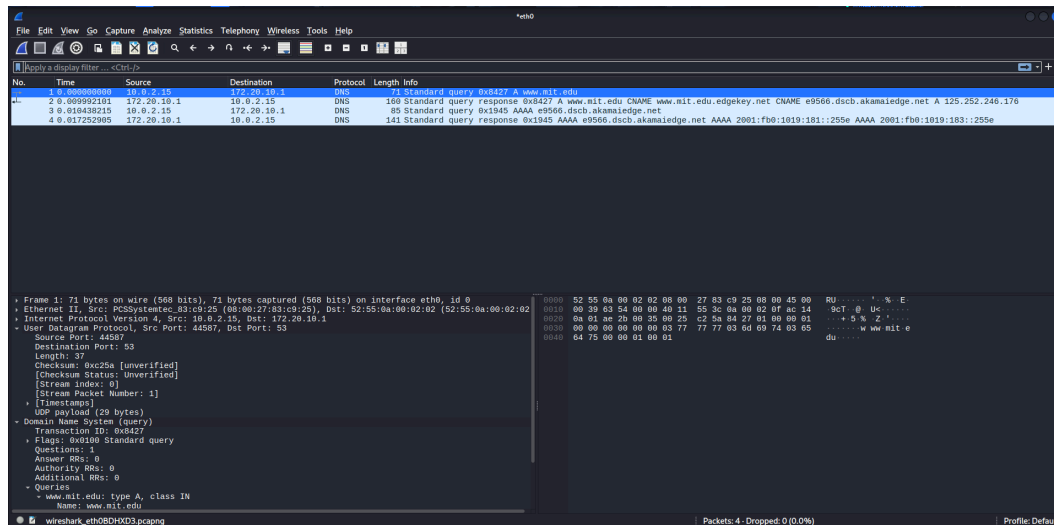


Wireshark packet capture showing a DNS query and response. The query is sent to 172.20.10.1. The response contains three answers: www.mit.edu (CNAME), www.mit.edu.edgekey.net (CNAME), and e9566.dscb.akamaiedge.net (A).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	172.20.10.1	DNS	71	Standard query 0x8427 A www.mit.edu
2	0.009992101	172.20.10.1	10.0.2.15	DNS	160	Standard query response 0x8427 A www.mit.edu
3	0.010438215	10.0.2.15	172.20.10.1	DNS	85	Standard query 0x1945 AAAA e9566.dscb.akamaiedge.net
4	0.017252905	172.20.10.1	10.0.2.15	DNS	141	Standard query response 0x1945 AAAA e9566.dscb.akamaiedge.net

```
[Timestamps]
  UDP payload (118 bytes)
  Domain Name System (response)
    Transaction ID: 0x8427
    Flags: 0x8100 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  Queries
    www.mit.edu: type A, class IN
      Name: www.mit.edu
      [Name Length: 11]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
  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 A, class IN, addr 125.252.246.176
  [Request In: 1]
  [Time: 0.009992101 seconds]
```

15. Provide a screenshot.



16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? **(Yes, they are the same)**

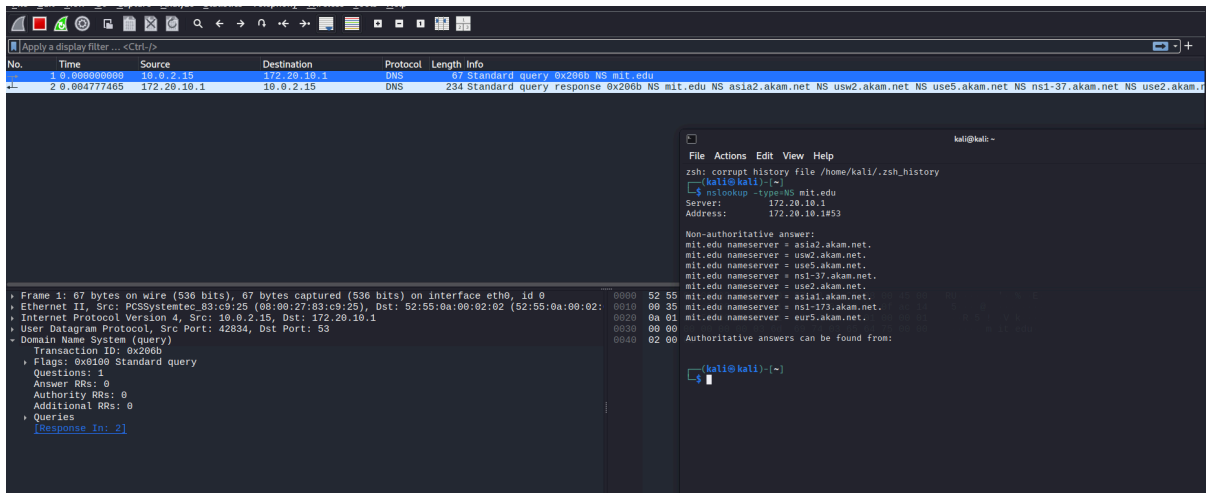
17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? **(Type NS, no answers.)**

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? **(No IP address provided.)**



```
Answer RRs: 8
Authority RRs: 0
Additional RRs: 0
▼ Queries
  ▼ mit.edu: type NS, class IN
    Name: mit.edu
    [Name Length: 7]
    [Label Count: 2]
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
  ▼ Answers
    ▼ mit.edu: type NS, class IN, ns asia2.akam.net
      Name: mit.edu
      Type: NS (2) (authoritative Name Server)
      Class: IN (0x0001)
      Time to live: 2252 (37 minutes, 32 seconds)
      Data length: 16
      Name Server: asia2.akam.net
    ▼ mit.edu: type NS, class IN, ns usw2.akam.net
      Name: mit.edu
      Type: NS (2) (authoritative Name Server)
      Class: IN (0x0001)
      Time to live: 2252 (37 minutes, 32 seconds)
      Data length: 7
      Name Server: usw2.akam.net
    ▼ mit.edu: type NS, class IN, ns use5.akam.net
      Name: mit.edu
      Type: NS (2) (authoritative Name Server)
      Class: IN (0x0001)
      Time to live: 2252 (37 minutes, 32 seconds)
      Data length: 7
      Name Server: use5.akam.net
    ▼ mit.edu: type NS, class IN, ns ns1-37.akam.net
      Name: mit.edu
      Type: NS (2) (authoritative Name Server)
      Class: IN (0x0001)
      Time to live: 2252 (37 minutes, 32 seconds)
      Data length: 9
      Name Server: ns1-37.akam.net
    - mit.edu: type NS, class IN, ns use2.akam.net
```

## 19. Provide a screenshot



Note: I change [bitsy.mit.edu](https://bitsy.mit.edu) to [cesar.ns.cloudflare.com](https://cesar.ns.cloudflare.com)

```
(kali@kali)-[~]
$ nslookup -type=NS aiiit.or.kr
Server:          172.20.10.1
Address:         172.20.10.1#53

Non-authoritative answer:
aiiit.or.kr      nameserver = cesar.ns.cloudflare.com.
aiiit.or.kr      nameserver = sydney.ns.cloudflare.com.

Authoritative answers can be found from:

(kali@kali)-[~]
$ nslookup www.aiiit.or.kr cesar.ns.cloudflare.com
Server:          cesar.ns.cloudflare.com
Address:         172.64.35.119#53

Name:   www.aiiit.or.kr
Address: 104.21.74.8
Name:   www.aiiit.or.kr
Address: 172.67.152.120
Name:   www.aiiit.or.kr
Address: 2606:4700:3031::ac43:9878
Name:   www.aiiit.or.kr
Address: 2606:4700:3036::6815:4a08
```

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?

- At first, it sent the query to default DNS(172.20.10.1) to find "[cesar.ns.cloudflare.com](https://cesar.ns.cloudflare.com)".
- We get that [cesar.ns.cloudflare.com](https://cesar.ns.cloudflare.com) IP is 172.64.35.119
- Then I sent query to [cesar.ns.cloudflare.com](https://cesar.ns.cloudflare.com) (172.64.35.119) to find "[www.aiiit.or.kr](https://www.aiiit.or.kr)"
- We get that [www.aiiit.or.kr](https://www.aiiit.or.kr) IP is 104.21.74.8



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

- **One with type A and one with type AAAA**
- **Both have no answers.**

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

- **For cloudflare, both type A and type AAA response have 3 answers, each composes of name, class, type, ttl, data, and address**

```
▶ Internet Protocol Version 4, Src: 172.20.10.1, Dst: 10.0.2.15
▶ User Datagram Protocol, Src Port: 53, Dst Port: 33687
▼ Domain Name System (response)
  Transaction ID: 0x1e27
  ▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ cesar.ns.cloudflare.com: type A, class IN
      Name: cesar.ns.cloudflare.com
      [Name Length: 23]
      [Label Count: 4]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
  ▼ Answers
    ▶ cesar.ns.cloudflare.com: type A, class IN, addr 172.64.35.119
    ▶ cesar.ns.cloudflare.com: type A, class IN, addr 162.159.44.119
    ▶ cesar.ns.cloudflare.com: type A, class IN, addr 108.162.195.119
    [Request In: 1]
    [Time: 0.006158660 seconds]
```

```
▶ Internet Protocol Version 4, Src: 172.20.10.1, Dst: 10.0.2.15
▶ User Datagram Protocol, Src Port: 53, Dst Port: 33687
▼ Domain Name System (response)
  Transaction ID: 0xb225
  ▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ cesar.ns.cloudflare.com: type AAAA, class IN
      Name: cesar.ns.cloudflare.com
      [Name Length: 23]
      [Label Count: 4]
      Type: AAAA (28) (IP6 Address)
      Class: IN (0x0001)
  ▼ Answers
    ▶ cesar.ns.cloudflare.com: type AAAA, class IN, addr 2a06:98c1:50::ac40:2377
    ▶ cesar.ns.cloudflare.com: type AAAA, class IN, addr 2803:f800:50::6ca2:c377
    ▶ cesar.ns.cloudflare.com: type AAAA, class IN, addr 2606:4700:58::a29f:2c77
    [Request In: 2]
    [Time: 0.005871993 seconds]
```

- for [www.aiit.or.kr](http://www.aiit.or.kr) both type A and type AAA response have 2 answers, each composes of name, class, type, ttl, data, and address

```

> Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_83:c9:25 (08:00:27:83:c9:25)
> Internet Protocol Version 4, Src: 172.64.35.119, Dst: 10.0.2.15
> User Datagram Protocol, Src Port: 53, Dst Port: 57683
> Domain Name System (response)
  Transaction ID: 0x4297
  Flags: 0x8500 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
  Queries
    > www.aiit.or.kr: type A, class IN
      Name: www.aiit.or.kr
      [Name Length: 14]
      [Label Count: 4]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
  Answers
    > www.aiit.or.kr: type A, class IN, addr 104.21.74.8
    > www.aiit.or.kr: type A, class IN, addr 172.67.152.120
    [Request In: 5]
    [Time: 0.061595654 seconds]

```

```

> Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_83:c9:25 (08:00:27:83:c9:25)
> Internet Protocol Version 4, Src: 172.64.35.119, Dst: 10.0.2.15
> User Datagram Protocol, Src Port: 53, Dst Port: 50764
> Domain Name System (response)
  Transaction ID: 0xda0a
  Flags: 0x8500 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
  Queries
    > www.aiit.or.kr: type AAAA, class IN
      Name: www.aiit.or.kr
      [Name Length: 14]
      [Label Count: 4]
      Type: AAAA (28) (IP6 Address)
      Class: IN (0x0001)
  Answers
    > www.aiit.or.kr: type AAAA, class IN, addr 2606:4700:3036::6815:4a08
    > www.aiit.or.kr: type AAAA, class IN, addr 2606:4700:3031::ac43:9878
    [Request In: 7]
    [Time: 0.019575259 seconds]

```

23. Provide a screenshot.

