

Assignment - 2

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

- **Ans: the IP address of the Web server is 210.152.243.234**

```
C:\Users\ZAsus>nslookup www.u-tokyo.ac.jp
Server:    UnKnown
Address:   172.20.10.1

Non-authoritative answer:
Name:      www.u-tokyo.ac.jp
Address:   210.152.243.234
```

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

- **Ans: you can see the cmd's output of the following command**

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

Non-authoritative answer:
ox.ac.uk   nameserver = dns1.ox.ac.uk
ox.ac.uk   nameserver = ns2.ja.net
ox.ac.uk   nameserver = auth4.dns.ox.ac.uk
ox.ac.uk   nameserver = dns0.ox.ac.uk
ox.ac.uk   nameserver = dns2.ox.ac.uk
ox.ac.uk   nameserver = auth5.dns.ox.ac.uk
ox.ac.uk   nameserver = auth6.dns.ox.ac.uk

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

ox.ac.uk
primary name server = raptor.dns.ox.ac.uk
responsible mail addr = hostmaster.ox.ac.uk
serial = 2021112276
refresh = 3600 (1 hour)
retry = 1800 (30 mins)
expire = 1209600 (14 days)
default TTL = 900 (15 mins)
```

Assignment - 2

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?

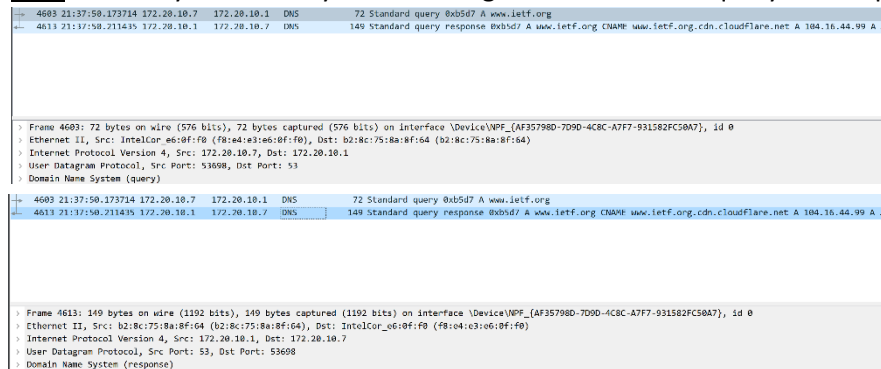
- **Ans:** The IP for the DNS server if queried for the Yahoo! mail server is 87.248.107.204

```
C:\Users\ZASus>nslookup -type=NS www.ox.ac.uk 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.
*** Request to UnKnown timed-out
```

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

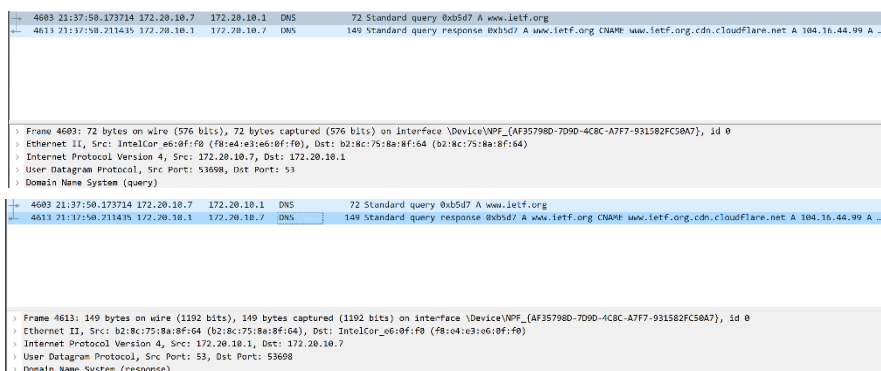
- **Ans:** Ans: as you can see by the following screen shot's the query and response messages



sent over UDP

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

- **Ans: the destination port is 53 and the source port of the DNS response is 53**



Assignment - 2

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?

- **Ans: the IP addresses the message is was sent is 172.20.10.1 and you can see by the picture that those ip's are the same , my local**

-

```
Connection-specific DNS Suffix  . : 
Description . . . . . : Intel(R) Wi-Fi 6 AX200 160MHz
Physical Address. . . . . : F8-E4-E3-E6-0F-F0
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b0f3:629:963c:7c9f%15(Preferred)
IPv4 Address. . . . . : 172.20.10.7(Preferred)
Subnet Mask . . . . . : 255.255.255.240
Lease Obtained. . . . . : Monday, November 22, 2021 9:03:14 PM
Lease Expires . . . . . : Tuesday, November 23, 2021 9:03:26 PM
Default Gateway . . . . . : 172.20.10.1
DHCP Server . . . . . : 172.20.10.1
DHCPv6 Server . . . . . : fe80::b0f3:629:963c:7c9f%15

4603 2137:50:173714 172.20.10.7 172.20.10.1 DNS 72 Standard query 0xb5d7 A www.ietf.org
4613 2137:50:211435 172.20.10.1 172.20.10.7 DNS 149 Standard query response 0xb5d7 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A ...

> Frame 4603: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{AF35798D-709D-4C8C-A7F7-931582FC50A7}, id 0
> Ethernet II, Src: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0), Dst: b2:8c:75:8a:8f:64 (b2:8c:75:8a:8f:64)
> Internet Protocol Version 4, Src: 172.20.10.7, Dst: 172.20.10.1
> User Datagram Protocol, Src Port: 53698, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0xb5d7
  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 4613]
```

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

Ans: ”? pretty easy to se that we are dealing a standard DNS type of query, and, we aint got answers

```
4603 2137:50:173714 172.20.10.7 172.20.10.1 DNS 72 Standard query 0xb5d7 A www.ietf.org
4613 2137:50:211435 172.20.10.1 172.20.10.7 DNS 149 Standard query response 0xb5d7 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A ...

> Frame 4603: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{AF35798D-709D-4C8C-A7F7-931582FC50A7}, id 0
> Ethernet II, Src: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0), Dst: b2:8c:75:8a:8f:64 (b2:8c:75:8a:8f:64)
> Internet Protocol Version 4, Src: 172.20.10.7, Dst: 172.20.10.1
> User Datagram Protocol, Src Port: 53698, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0xb5d7
  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 4613]
```

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

- **Ans:** Ans: the first answer is the cname what is the actual name of the domain, while the other two answer’s contains information about the at the web we queried like the IP and the address

-

```
4603 2137:50:173714 172.20.10.7 172.20.10.1 DNS 72 Standard query 0xb5d7 A www.ietf.org
4613 2137:50:211435 172.20.10.1 172.20.10.7 DNS 149 Standard query response 0xb5d7 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A ...

> Frame 4613: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{AF35798D-709D-4C8C-A7F7-931582FC50A7}, id 0
> Ethernet II, Src: b2:8c:75:8a:8f:64 (b2:8c:75:8a:8f:64), Dst: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0)
> Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.7
> User Datagram Protocol, Src Port: 53, Dst Port: 53698
> Domain Name System (response)
  Transaction ID: 0xb5d7
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
  Queries
    > www.ietf.org: type A, class IN
  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: 4603]
  [Time: 0.037721000 seconds]
```

Assignment - 2

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?
- **Ans: the first packet was sent to 104.16.44.99 and it co respond to the IP address in the DNS message**

```
4614 21:37:50.212563 172.20.10.7 104.16.44.99 TCP 66 50347 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
> Frame 4614: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{AF35798D-7D9D-4C8C-A7F7-931582FC50A7}, id 0
> Ethernet II, Src: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0), Dst: b2:8c:75:8a:8f:64 (b2:8c:75:8a:8f:64)
> Internet Protocol Version 4, Src: 172.20.10.7, Dst: 104.16.44.99
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 52
  Identification: 0x540f (21551)
> Flags: 0x40, Don't fragment
  Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x0000 [validation disabled]
  [header checksum status: Unverified]
  Source Address: 172.20.10.7
  Destination Address: 104.16.44.99
> Transmission Control Protocol, Src Port: 50347, Dst Port: 80, Seq: 0, Len: 0
```

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

- **Ans: no**

```
4603 21:37:50.173714 172.20.10.7 172.20.10.1 DNS 72 Standard query 0xb5d7 A www.ietf.org
4613 21:37:50.211435 172.20.10.1 172.20.10.7 DNS 140 Standard query response 0xb5d7 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A ...
4624 21:37:50.239270 172.20.10.7 104.16.44.99 HTTP 484 GET / HTTP/1.1
4639 21:37:50.292045 104.16.44.99 172.20.10.7 HTTP 357 HTTP/1.1 301 Moved Permanently
1545 21:37:50.060100 172.20.10.7 172.20.10.15 NBNS 92 Name query NB LAPTOP-QRJUSEKRC1c>
1683 21:37:50.818505 172.20.10.7 172.20.10.15 NBNS 92 Name query NB LAPTOP-QRJUSEKRC1c>
1810 21:37:50.573011 172.20.10.7 172.20.10.15 NBNS 92 Name query NB LAPTOP-QRJUSEKRC1c>
2876 21:37:42.199295 172.20.10.7 216.58.211.2 QUIC 1292 Initial, DCID=b9a0a6a72fa725f0, PKN: 1, PADDING, CRYPTO, CRYPTO, PING, PADDING, CRYPTO, CRYPTO, CRYPTO...
2879 21:37:42.211246 172.20.10.7 216.58.211.2 QUIC 120 0-RTT, DCID=b9a0a6a72fa725f0
2880 21:37:42.211686 172.20.10.7 216.58.211.2 QUIC 472 0-RTT, DCID=b9a0a6a72fa725f0
> Frame 4639: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface \Device\NPF_{AF35798D-7D9D-4C8C-A7F7-931582FC50A7}, id 0
> Ethernet II, Src: b2:8c:75:8a:8f:64 (b2:8c:75:8a:8f:64), Dst: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0)
> Internet Protocol Version 4, Src: 104.16.44.99, Dst: 172.20.10.7
> Transmission Control Protocol, Src Port: 80, Dst Port: 50347, Seq: 1, Ack: 431, Len: 303
> Hypertext Transfer Protocol
```

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

- **Ans: the destination port for the DNS query is 53 and source is 53 as well**

```
593 22:09:05.468187 172.20.10.7 172.20.10.1 DNS 67 Standard query 0x0003 AAAA mit.edu
612 22:09:05.546855 172.20.10.1 172.20.10.7 DNS 123 Standard query response 0x0003 AAAA mit.edu AAAA 2a02:26f0:a1:6b1::255e AAAA 2a02:26f0:a1:696::255e

> Frame 593: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{AF35798D-7D9D-4C8C-A7F7-931582FC50A7}, id 0
> Ethernet II, Src: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0), Dst: b2:8c:75:8a:8f:64 (b2:8c:75:8a:8f:64)
> Internet Protocol Version 4, Src: 172.20.10.7, Dst: 172.20.10.1
> User Datagram Protocol, Src Port: 62890, Dst Port: 53
> Domain Name System (query)

593 22:09:05.468187 172.20.10.7 172.20.10.1 DNS 67 Standard query 0x0003 AAAA mit.edu
612 22:09:05.546855 172.20.10.1 172.20.10.7 DNS 123 Standard query response 0x0003 AAAA mit.edu AAAA 2a02:26f0:a1:6b1::255e AAAA 2a02:26f0:a1:696::255e

> Frame 612: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface \Device\NPF_{AF35798D-7D9D-4C8C-A7F7-931582FC50A7}, id 0
> Ethernet II, Src: b2:8c:75:8a:8f:64 (b2:8c:75:8a:8f:64), Dst: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0)
> Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.7
> User Datagram Protocol, Src Port: 53, Dst Port: 62890
> Domain Name System (response)
```

Assignment - 2

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

- **Ans: the DNS query message sent to 172.20.10.1 and you can see that my local address .**

```
Connection-specific DNS Suffix  : 
Description . . . . . : Intel(R) Wi-Fi 6 AX200 160MHz
Physical Address. . . . . : F8-E4-E3-E6-0F-F0
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::b0f3:629:963c:7c9f%15(Preferred)
IPv4 Address. . . . . : 172.20.10.7(Preferred)
Subnet Mask . . . . . : 255.255.255.240
Lease Obtained. . . . . : Monday, November 22, 2021 9:03:12 PM
Lease Expires . . . . . : Tuesday, November 23, 2021 9:03:25 PM
Default Gateway . . . . . : 172.20.10.1
DHCP Server . . . . . : 172.20.10.1
DHCPv6 IAID . . . . . : 150529251
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-C1-B2-D5-F8-E4-E3-E6-0F-F0
DNS Servers . . . . . : 172.20.10.1
NetBIOS over Tcpip. . . . . : Enabled
```

No.	Time	Source	Destination	Protocol	Length	Info
593	22:09:05.468187	172.20.10.7	172.20.10.1	DNS	67	Standard query 0x0003 AAAA mit.edu
612	22:09:05.546855	172.20.10.1	172.20.10.7	DNS	123	Standard query response 0x0003 AAAA mit.edu AAAA 2a02:26f0:a1:6b1::255e AAAA 2a02:26f0:a1:696::255e

> Frame 593: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{AF35798D-7D9D-4C8C-A7F7-931582FC50A7}, id 0
> Ethernet II, Src: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0), Dst: b2:8c:75:8a:8f:64 (b2:8c:75:8a:8f:64)
> Internet Protocol Version 4, Src: 172.20.10.7, Dst: 172.20.10.1
> User Datagram Protocol, Src Port: 62890, Dst Port: 53
> Domain Name System (query)

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

- **Ans: the DNS query message is an A type but we aint got any answers here**

No.	Time	Source	Destination	Protocol	Length	Info
593	22:09:05.468187	172.20.10.7	172.20.10.1	DNS	67	Standard query 0x0003 AAAA mit.edu
612	22:09:05.546855	172.20.10.1	172.20.10.7	DNS	123	Standard query response 0x0003 AAAA mit.edu AAAA 2a02:26f0:a1:6b1::255e AAAA 2a02:26f0:a1:696::255e

> Frame 593: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{AF35798D-7D9D-4C8C-A7F7-931582FC50A7}, id 0
> Ethernet II, Src: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0), Dst: b2:8c:75:8a:8f:64 (b2:8c:75:8a:8f:64)
> Internet Protocol Version 4, Src: 172.20.10.7, Dst: 172.20.10.1
> User Datagram Protocol, Src Port: 62890, Dst Port: 53
> Domain Name System (query)
Transaction ID: 0x0003
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
✓ Queries
mit.edu: type AAAA, class IN
[\[Response In: 612\]](#)

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

- **Ans: we got one answer who contains the host name, address type, class and the IP**

No.	Time	Source	Destination	Protocol	Length	Info
593	22:09:05.468187	172.20.10.7	172.20.10.1	DNS	67	Standard query 0x0003 AAAA mit.edu
612	22:09:05.546855	172.20.10.1	172.20.10.7	DNS	123	Standard query response 0x0003 AAAA mit.edu AAAA 2a02:26f0:a1:6b1::255e AAAA 2a02:26f0:a1:696::255e

> Frame 612: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface \Device\NPF_{AF35798D-7D9D-4C8C-A7F7-931582FC50A7}, id 0
> Ethernet II, Src: b2:8c:75:8a:8f:64 (b2:8c:75:8a:8f:64), Dst: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0)
> Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.7
> User Datagram Protocol, Src Port: 53, Dst Port: 62890
> Domain Name System (response)
Transaction ID: 0x0003
> Flags: 0x8100 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
✓ Queries
mit.edu: type AAAA, class IN
✓ Answers
mit.edu: type AAAA, class IN, addr: 2a02:26f0:a1:6b1::255e
mit.edu: type AAAA, class IN, addr: 2a02:26f0:a1:696::255e
[\[Request In: 593\]](#)
[Time: 0.07868000 seconds]

Assignment - 2

15. Provide a screenshot.

- **Ans:**

```
593 22:09:05.468187 172.20.10.7 172.20.10.1 DNS 67 Standard query 0x0003 AAAA mit.edu
612 22:09:05.546855 172.20.10.1 172.20.10.7 DNS 123 Standard query response 0x0003 AAAA mit.edu AAAA 2a02:26f0:a1:6b1::255e AAAA 2a02:26f0:a1:696::255e

Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
  > mit.edu: type AAAA, class IN
Answers
  > mit.edu: type AAAA, class IN, addr 2a02:26f0:a1:6b1::255e
    Name: mit.edu
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 27 (27 seconds)
    Data length: 16
    AAAA Address: 2a02:26f0:a1:6b1::255e
  > mit.edu: type AAAA, class IN, addr 2a02:26f0:a1:696::255e
    Name: mit.edu
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 27 (27 seconds)
    Data length: 16
    AAAA Address: 2a02:26f0:a1:696::255e
[Request In: 593]
[Time: 0.078668000 seconds]
```

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

- **Ans: just ad before we infer that the DNS query was sent to 172.20.10.1 which again is my**

```
C:\Users\ZAsus>nslookup -type=NS mit.edu
Server: UnKnown
Address: 172.20.10.1

Non-authoritative answer:
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net
```

```
Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Wi-Fi 6 AX200 160MHz
Physical Address. . . . . : F8-E4-E3-E6-0F-F0
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . : Yes
Link-local IPv6 Address . . . . : fe80::b0f3:629:963c:7c9f%15(Preferred)
IPv4 Address. . . . . : 172.20.10.7(Preferred)
Subnet Mask . . . . . : 255.255.255.240
Lease Obtained. . . . . : Monday, November 22, 2021 9:03:12 PM
Lease Expires . . . . . : Tuesday, November 23, 2021 9:03:25 PM
Default Gateway . . . . . : 172.20.10.1
DHCP Server . . . . . : 172.20.10.1
DHCPv6 IAID . . . . . : 150529251
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-C1-B2-D5-F8-E4-E3-E6-0F-F0
DNS Servers . . . . . : 172.20.10.1
NetBIOS over Tcpip. . . . . : Enabled
```

local DNS address

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

- **Ans: the type is NS DNS who doesn't contains any answers**

```
925 22:12:10.668137 172.20.10.7 172.20.10.1 DNS 67 Standard query 0x0002 NS mit.edu
926 22:12:10.673578 172.20.10.1 172.20.10.7 DNS 234 Standard query response 0x0002 NS mit.edu NS asia1.akam.net NS use2.akam.net NS usw2.akam.net NS use5.akam.net

Frame 925: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{AF35798D-709D-4C8C-A7F7-933582FC0A77}, Id 0
Ethernet II, Src: IntelCor_e8:0f:f0 (f8:e4:e3:e6:0f:f0), Dst: b2:8c:75:8a:0f:64 (02:8c:75:8a:0f:64)
Internet Protocol Version 4, Src: 172.20.10.7, Dst: 172.20.10.1
User Datagram Protocol, Src Port: 64575, 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
    > mit.edu: type NS, class IN
[Response In: 926]
```

Assignment - 2

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?

- **Ans: the response message of the name servers are visible at the next to screen shot but we cannot see any IP addresses**

```
925 22:21:00.668137 172.20.10.7 172.20.10.1 DNS 67 Standard query 0x0002 NS mit.edu
926 22:21:00.671570 172.20.10.1 172.20.10.7 DNS 234 Standard query response 0x0002 NS mit.edu NS asia1.akan.net NS usa2.akan.net NS usa2.akan.net NS usa5.akan.net

Questions: 1
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 (authoritative Name Server) (2)
    Class: IN (0x0001)
Answers
  mit.edu: type NS, class IN, ns asia1.akan.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 2149 (35 minutes, 49 seconds)
    Data length: 16
    Name server: asia1.akan.net
  mit.edu: type NS, class IN, ns usa2.akan.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 2149 (35 minutes, 49 seconds)
```

19. Provide a screenshot

```
925 22:21:00.668137 172.20.10.7 172.20.10.1 DNS 67 Standard query 0x0002 NS mit.edu
926 22:21:00.671570 172.20.10.1 172.20.10.7 DNS 234 Standard query response 0x0002 NS mit.edu NS asia1.akan.net NS usa2.akan.net NS usa2.akan.net NS usa5.akan.net

Frame 926: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on Interface \Device\NPF_{AF357980-7090-4C8C-A777-9315821C5BA7}, Id 0
Ethernet II, Src: b2:8c:75:8a:8f:64 (b2:8c:75:8a:8f:64), Dst: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0)
Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.7
User Datagram Protocol, Src Port: 53, Dst Port: 64575
Domain Name System (response)
  Transaction ID: 0x0002
  Flags: 0x0180 Standard query response, No error
  Questions: 1
  Answer RRs: 8
  Authority RRs: 0
  Additional RRs: 0
Queries
  mit.edu: type NS, class IN
Answers
  mit.edu: type NS, class IN, ns asia1.akan.net
  mit.edu: type NS, class IN, ns usa2.akan.net
  mit.edu: type NS, class IN, ns usa2.akan.net
  mit.edu: type NS, class IN, ns usa5.akan.net
  mit.edu: type NS, class IN, ns nsl-37.akan.net
  mit.edu: type NS, class IN, ns usa2.akan.net
  mit.edu: type NS, class IN, ns asia2.akan.net
  mit.edu: type NS, class IN, ns nsl-173.akan.net
[Request ID: 925]
[Time: 0.003433000 seconds]
```

- **Ans:**

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?

- **Ans: the DNS query message sent to 8.8.8.8 of google and it's pretty obvious that it isn't our address**

```
C:\Users\ZAsus>nslookup aiit.or.kr 8.8.8.8
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: aiit.or.kr
Address: 58.229.6.225
```

Assignment - 2

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

- **Ans: the type of the DNS is a A type but again we don't get any answers**

953 22:27:16.211560 172.20.10.7 8.8.8.8 DNS	78 Standard query 0x0002 A ailit.or.kr
1138 22:27:16.726095 8.8.8.8 172.20.10.7 DNS	86 Standard query response 0x0002 A ailit.or.kr A 58.229.6.225
1133 22:27:16.737795 172.20.10.7 8.8.8.8 DNS	78 Standard query 0x0003 AAAA ailit.or.kr
1548 22:27:17.722475 8.8.8.8 172.20.10.7 DNS	124 Standard query response 0x0003 AAAA ailit.or.kr SOA ns9.dnszi.com

> Frame 953: 78 bytes on wire (560 bits), 78 bytes captured (560 bits) on interface \Device\NPF_{AF35798D-7D90-4C8C-A7F7-931582FC58A7}, id 0
> Ethernet II, Src: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0), Dst: b2:8c:75:8a:8f:e4 (b2:8c:75:8a:8f:e4)
> Internet Protocol Version 4, Src: 172.20.10.7, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 52070, 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
> ailit.or.kr: type A, class IN
[Request In: 1138]

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

- **Ans: this time we have one answers who contains the address, the host name, the class And the IP**

1138 22:27:16.736694 8.8.8.8 172.20.10.7 DNS	86 Standard query response 0x0002 A ailit.or.kr A 58.229.6.225
1133 22:27:16.737795 172.20.10.7 8.8.8.8 DNS	78 Standard query 0x0003 AAAA ailit.or.kr
1548 22:27:17.722475 8.8.8.8 172.20.10.7 DNS	124 Standard query response 0x0003 AAAA ailit.or.kr SOA ns9.dnszi.com

> Flags: 0x0100 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
> ailit.or.kr: type A, class IN
Answers
> ailit.or.kr: type A, class IN, addr 58.229.6.225
Name: ailit.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: 953]
[Time: 0.519134000 seconds]

23. Provide a screenshot.

- **Ans:**