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**

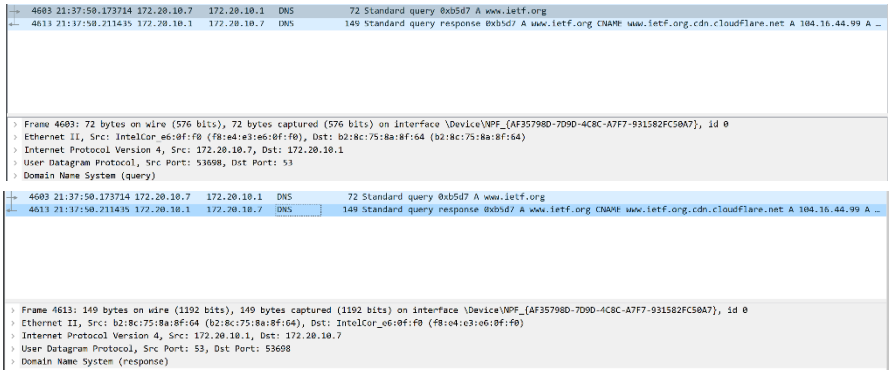
```
C:\Users\ZAsus>nslookup -type=NS ox.ac.uk
Server:  UnKnown
Address:  172.20.10.1

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: ass you can se by the fallowing screen shot's the query and response messaged



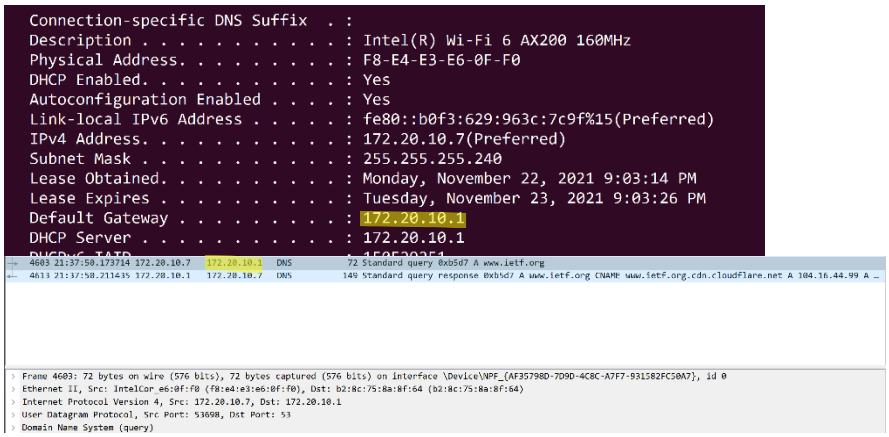
   sent over UDP

   -

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**

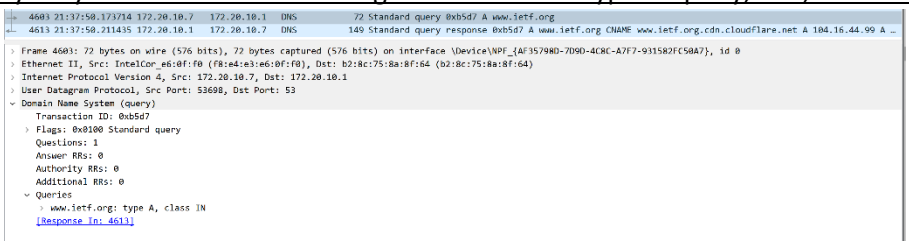
Assignment - 2

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**
   -

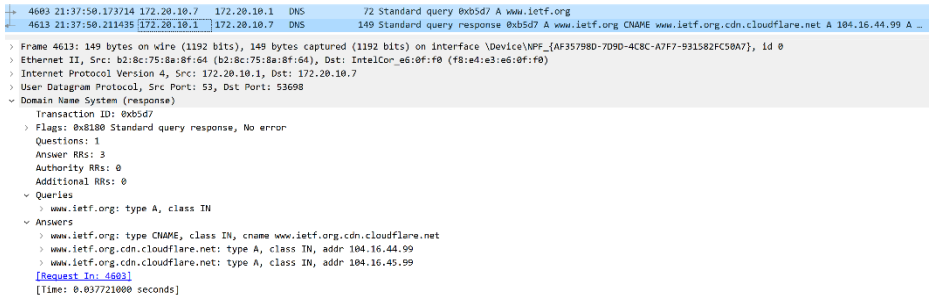


7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

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

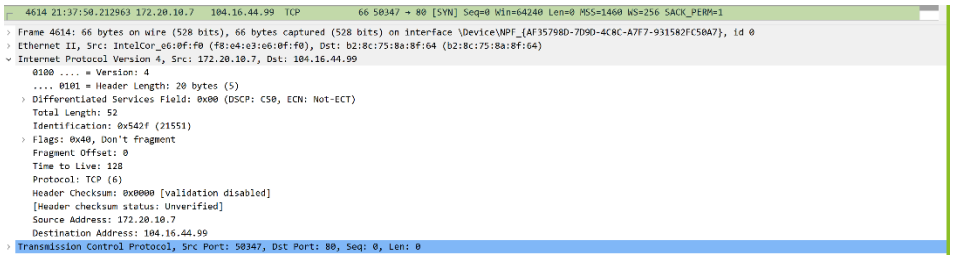


8. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
   - **Ans:** Ans: the first answer is the cname what is the actual name of the domain, while the other two answer's contains information about the at the web we queried like the IP and the address
   -

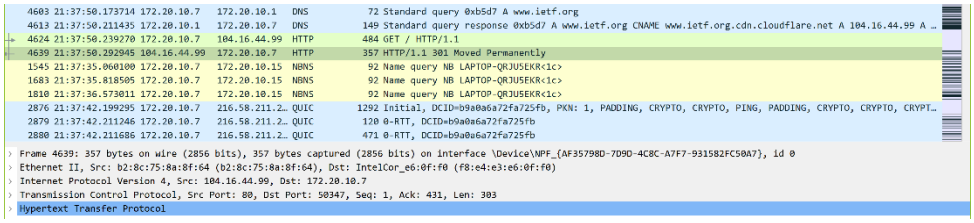


Assignment - 2

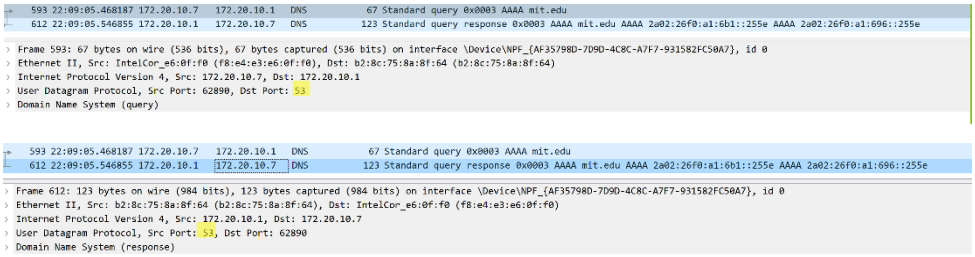
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
   - **Ans: the first packet was sent to 104.16.44.99 and it co respond to the IP address in the DNS message**



10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?
    - **Ans: no**



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**



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
```

```
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**

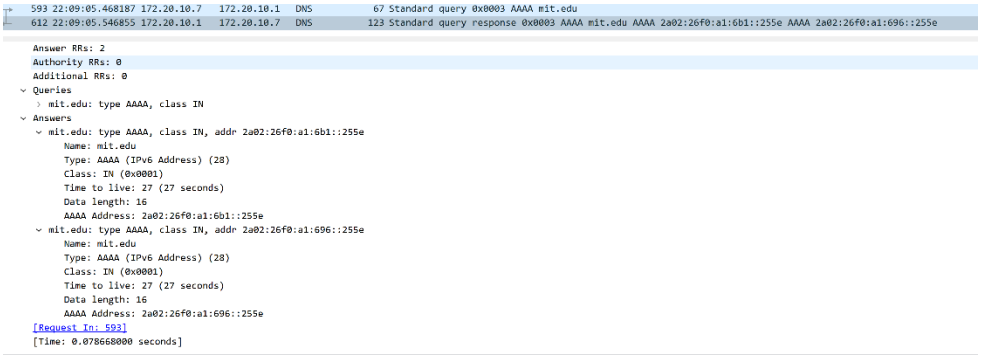
```
593 22:09:05.468187 172.20.10.7   172.20.10.1   DNS          67 Standard query 0x0003 AAAA mit.edu
612 22:09:05.546855 172.20.10.1   172.20.10.7   DNS         123 Standard query response 0x0003 AAAA mit.edu AAAA 2a02:26f0:a1:6b1::255e AAAA 2a02:26f0:a1:696::255e

> 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
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v 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**

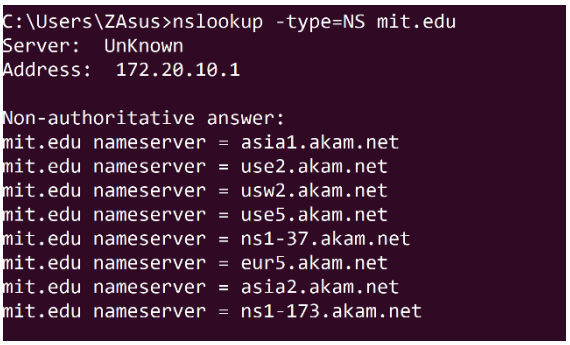
```
593 22:09:05.468187 172.20.10.7   172.20.10.1   DNS          67 Standard query 0x0003 AAAA mit.edu
612 22:09:05.546855 172.20.10.1   172.20.10.7   DNS         123 Standard query response 0x0003 AAAA mit.edu AAAA 2a02:26f0:a1:6b1::255e AAAA 2a02:26f0:a1:696::255e

> 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
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > mit.edu: type AAAA, class IN
  v 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: 0.078668000 seconds]
```

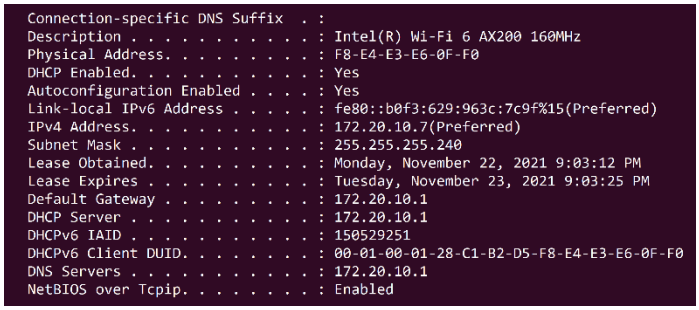
Assignment - 2

15. Provide a screenshot.
    - **Ans:**



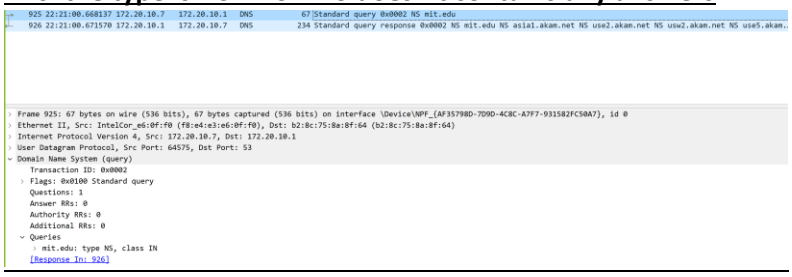
16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    - **Ans: just ad before we infer that the DNS query was sent to 172.20.10.1 which again is my**





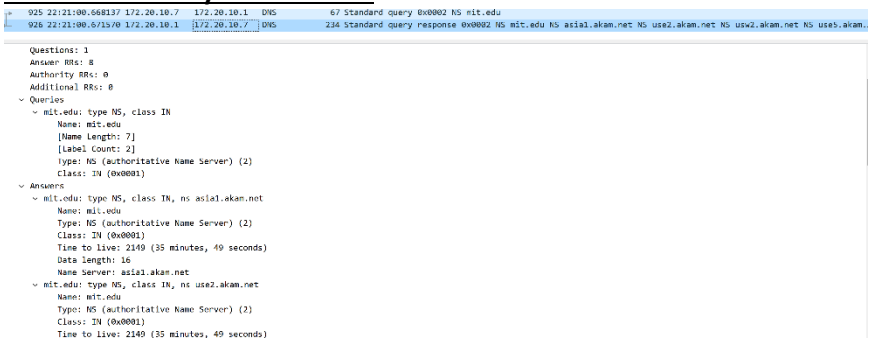
    local DNS address

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**

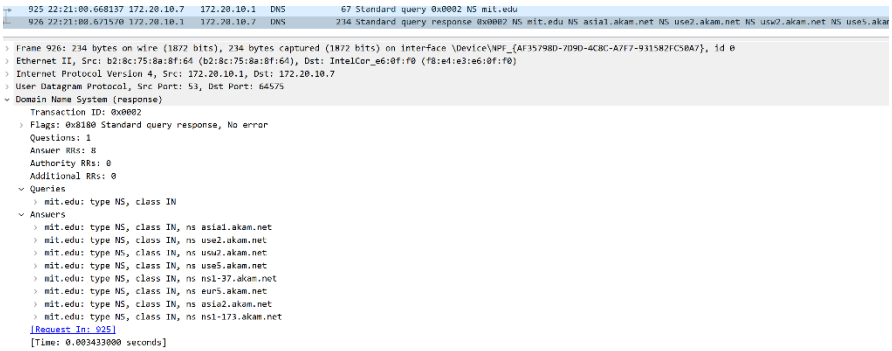


Assignment - 2

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 ate the next to screen shot but we cannot se any IP addresses**



19. Provide a screenshot



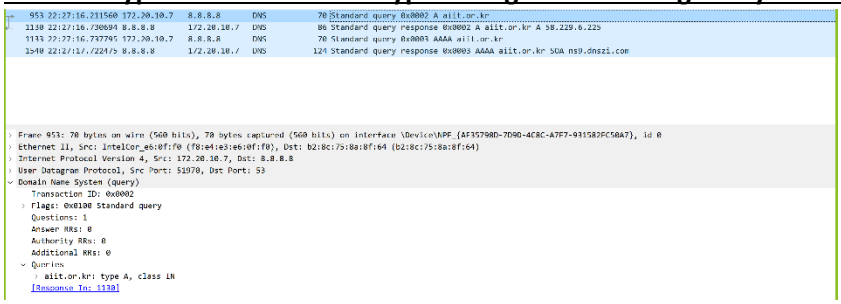
    - **Ans:**

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**

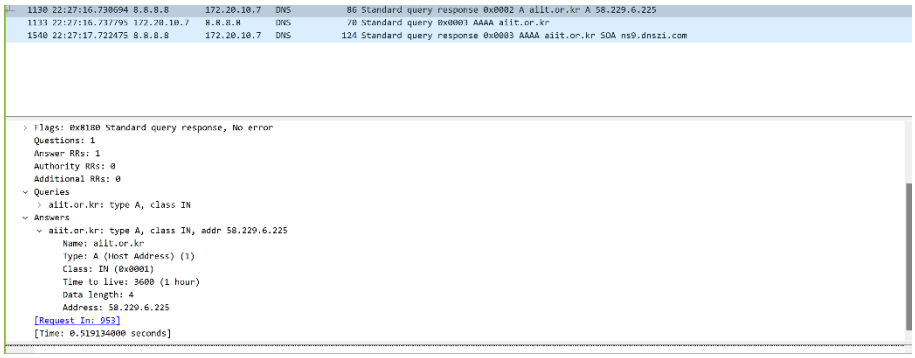
```
C:\Users\ZAsus>nslookup aiit.or.kr 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

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**



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**



23. Provide a screenshot.
    - **Ans:**