Lab Report

CSE351, Computer Networks

Name: Malak Mohamed Helmy Elbakry ID: 20P2434

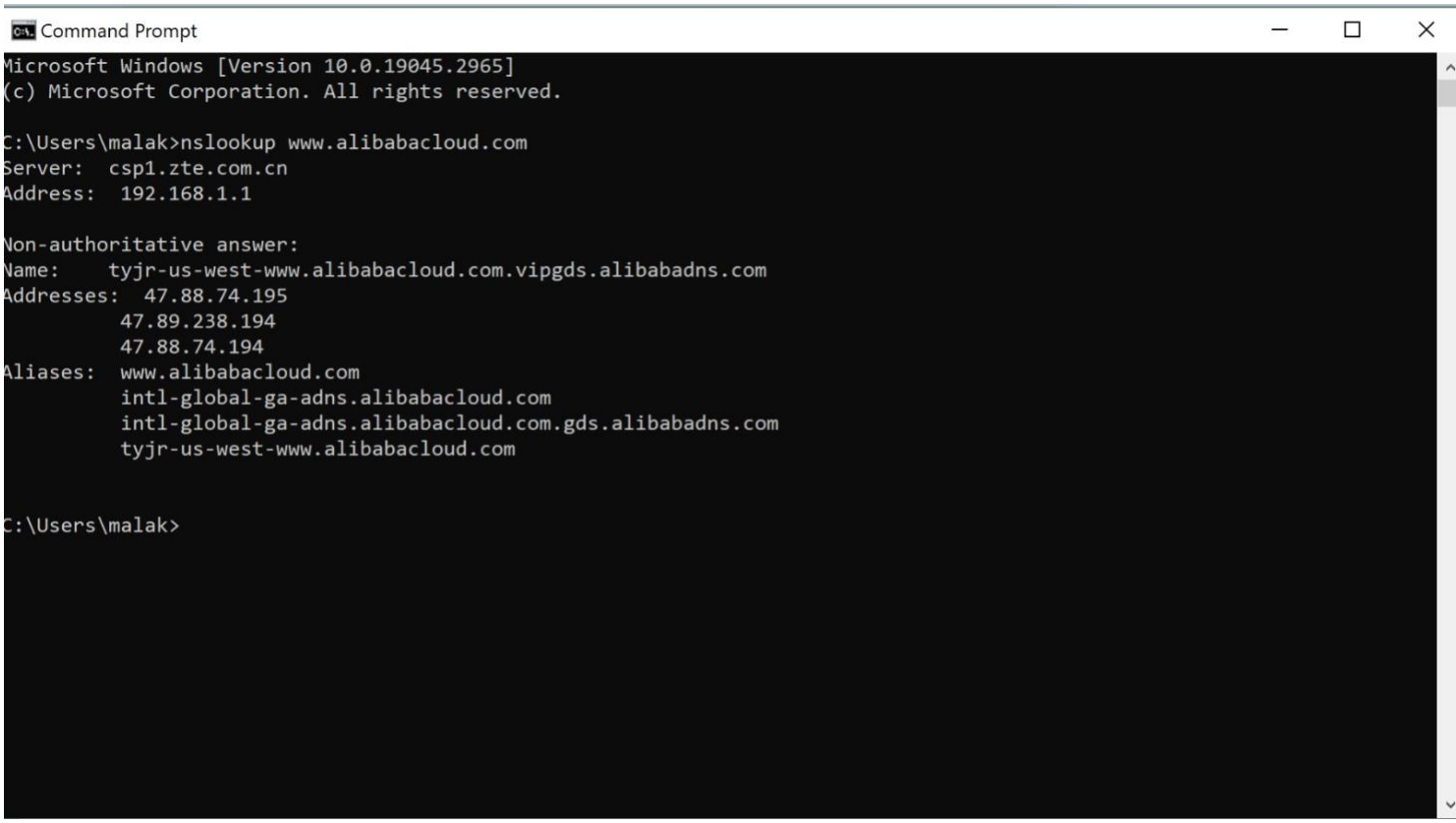
Lab No: (3) Experiment Title: Wireshark_DNS_v7.0

Date: 25 / 10 /2023

Note: I am a mac user so I had to run the commands on windows which is the cause of the different fonts and ip addresses.

nslookup

1. Question 1



The IP Address of middle-east.alibabacloud.com: 47.88.74.195

2. Question 2

```
C:\Users\malak>nslookup -type=NS cam.ac.uk
Server:  csp3.zte.com.cn
Address:  192.168.1.1

Non-authoritative answer:
cam.ac.uk       nameserver = ns2.ic.ac.uk
cam.ac.uk       nameserver = ns3.mythic-beasts.com
cam.ac.uk       nameserver = ns1.mythic-beasts.com
cam.ac.uk       nameserver = auth0.dns.cam.ac.uk
cam.ac.uk       nameserver = dns0.cl.cam.ac.uk
cam.ac.uk       nameserver = dns0.eng.cam.ac.uk
```

3. Question 3

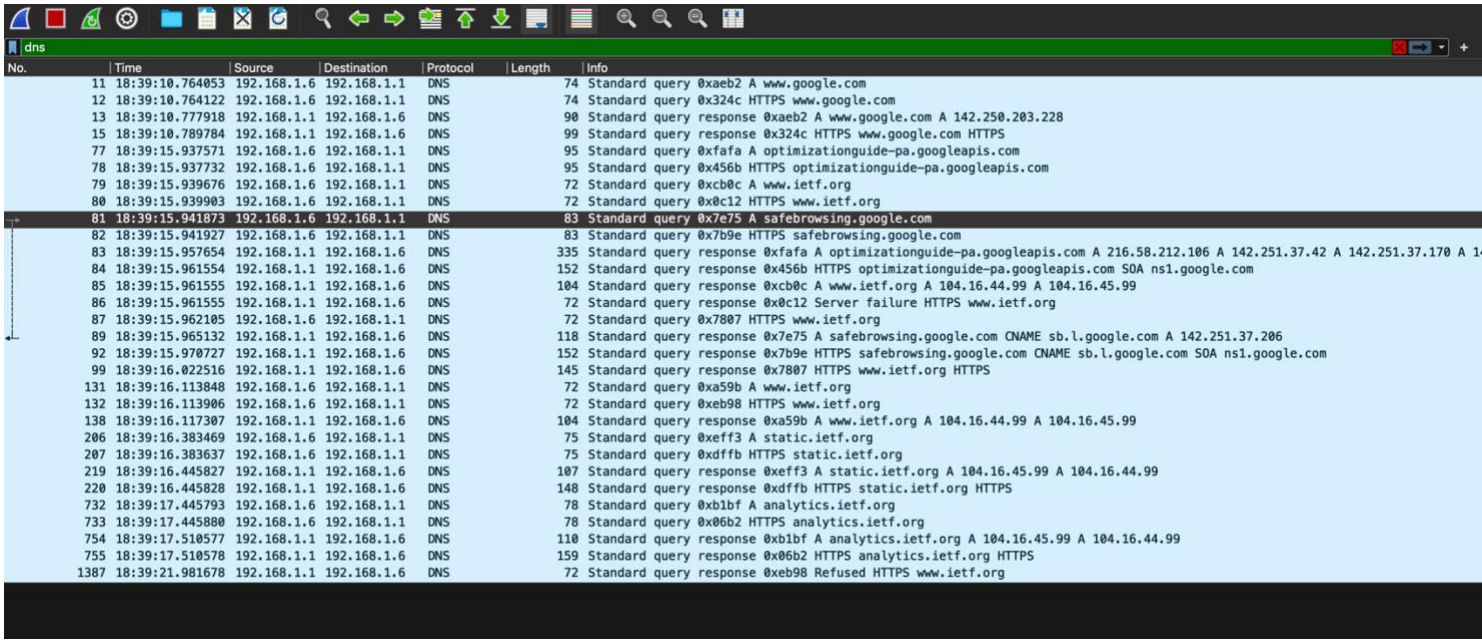
```
C:\Users\malak>nslookup ns3.mythic-beasts.com mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  87.248.119.251

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.
*** Request to UnKnown timed-out
```

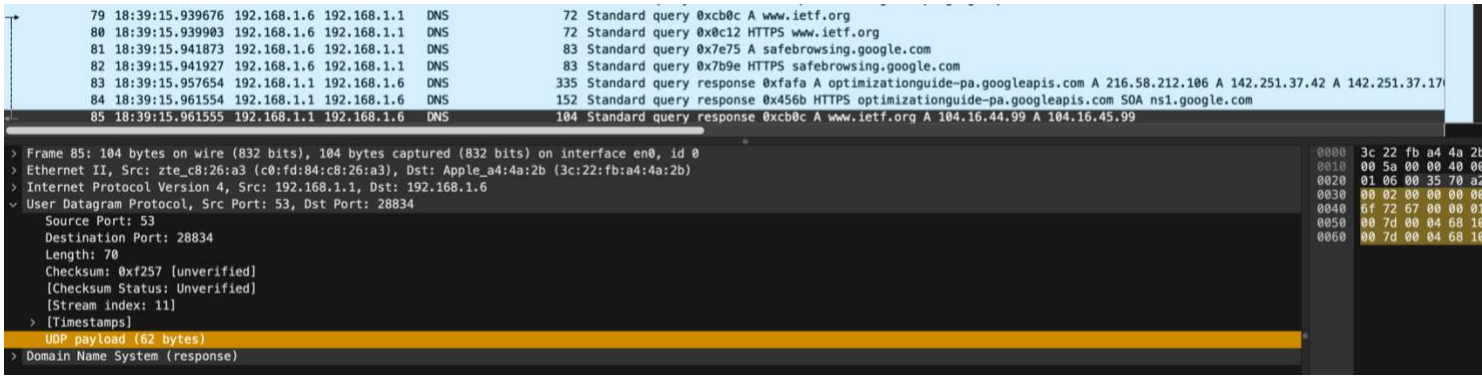
ipconfig

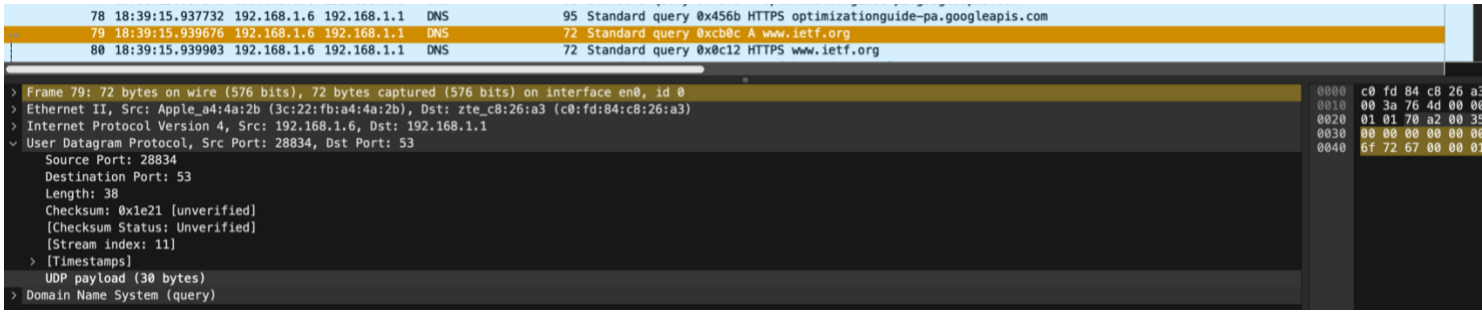
```
C:\Users\malak>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-6DGMV0G
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Broadcom 802.11ac Network Adapter
   Physical Address. . . . . . . . . : 3C-22-FB-A4-4A-2B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::1342:7169:6849:2702%9(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.6(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, October 26, 2023 6:14:16 PM
   Lease Expires . . . . . . . . . . : Friday, October 27, 2023 6:14:16 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 71049979
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-B6-88-FB-3C-22-FB-A4-4A-2B
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 14-7D-DA-15-89-E1
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

Tracing DNS with Wireshark

4. Question 4







The Photos show that there are UDP and they are the query and its response

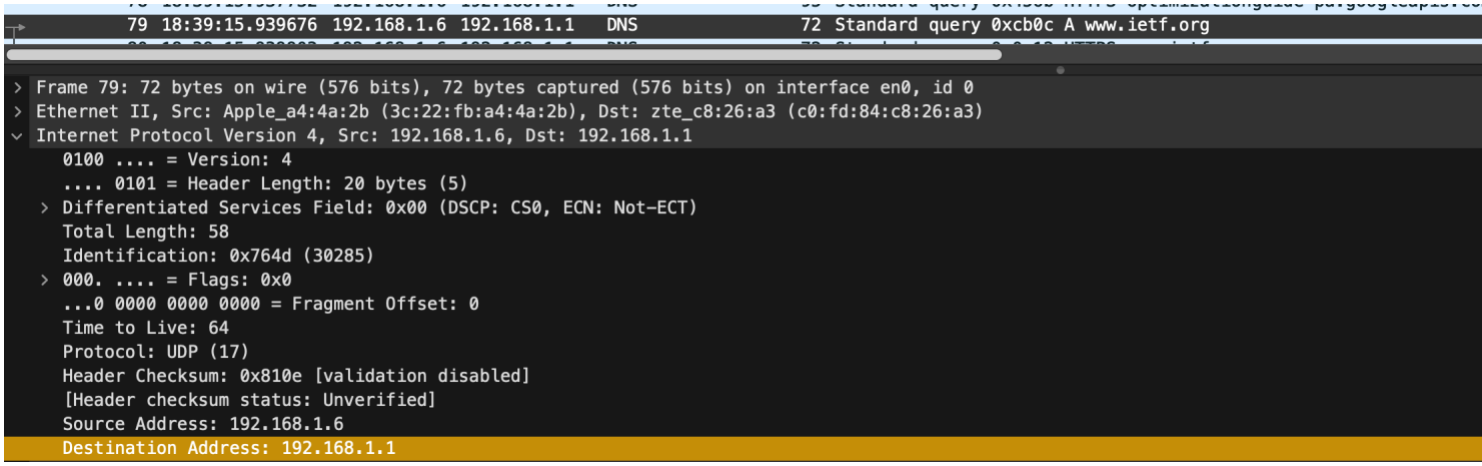
5. Question 5

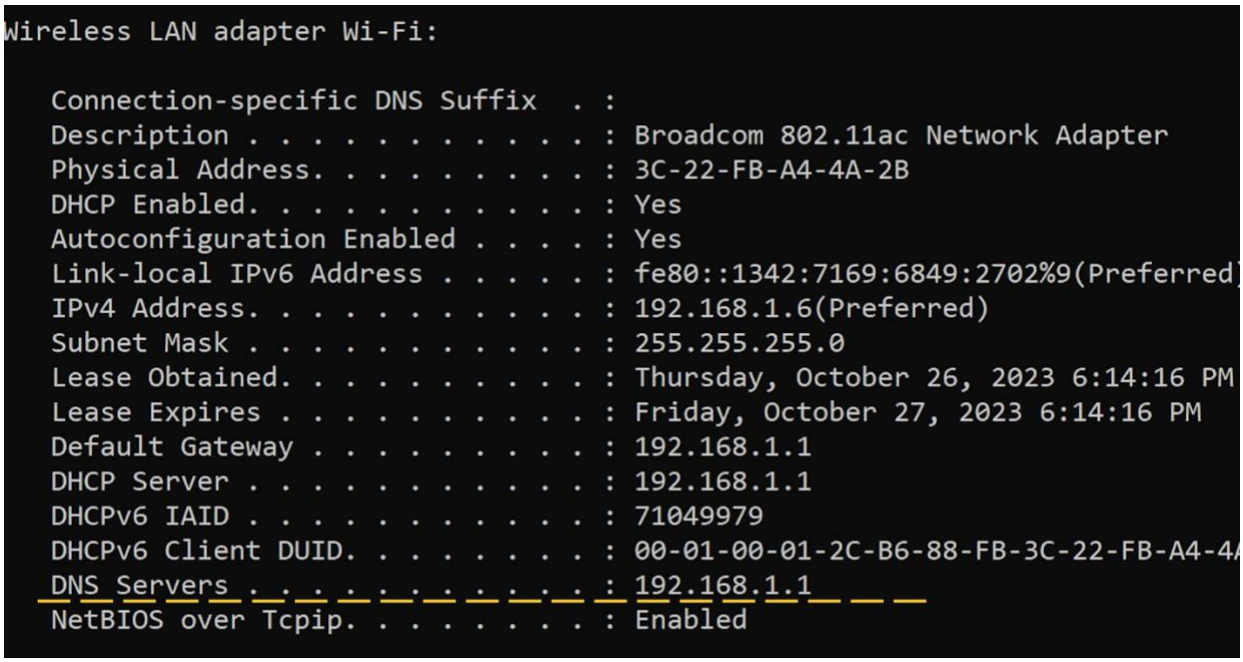
   (Using Question 4 Photo)

   The Destination port of query: 28843

   The Source Port of response: 28834

6. Question 6



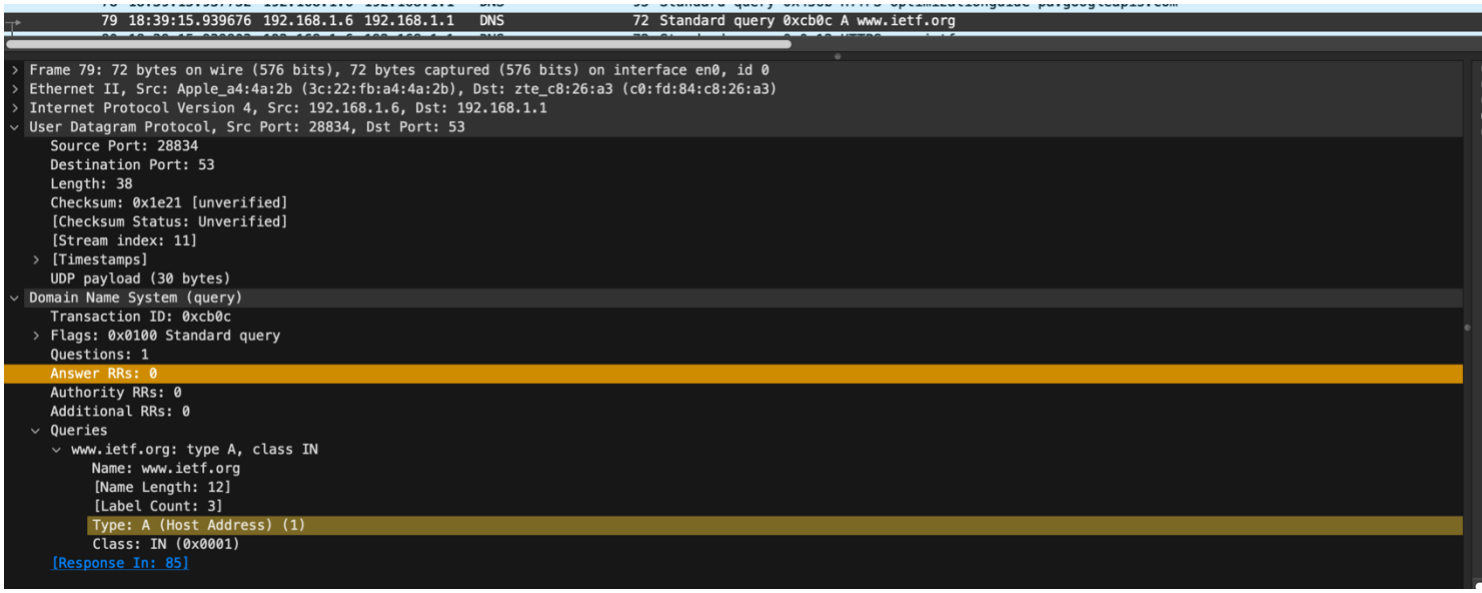


Both the destination IP address of the query and the DNS Server IP address are the same

7. Question 7

   Type: A

   Answer: 0

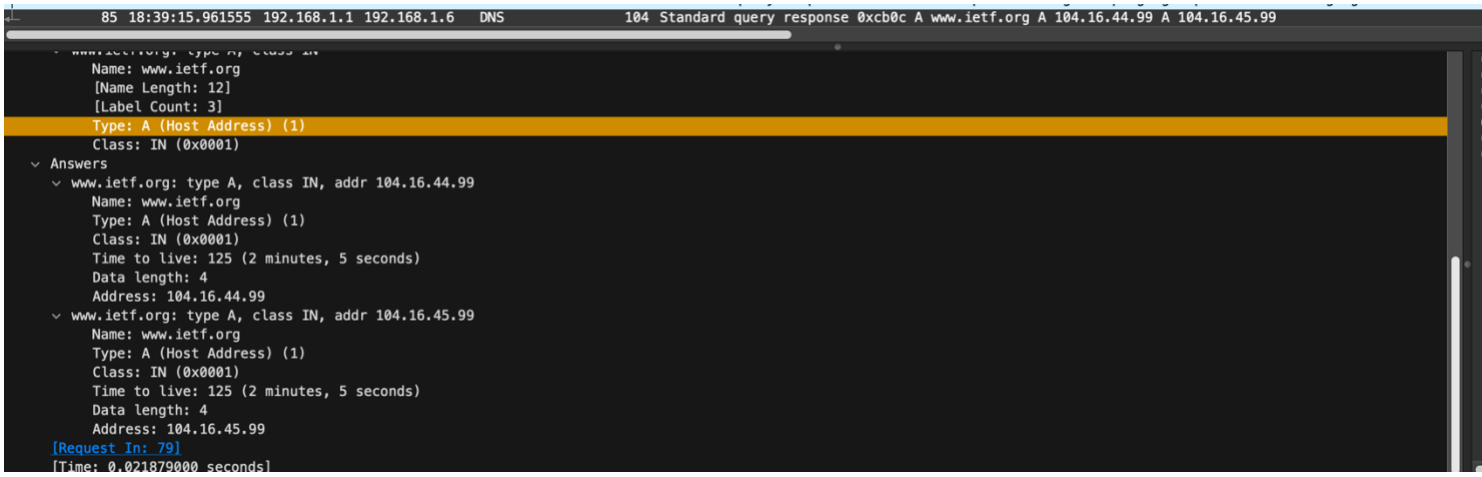


8. Question 8

   2 answers were sent

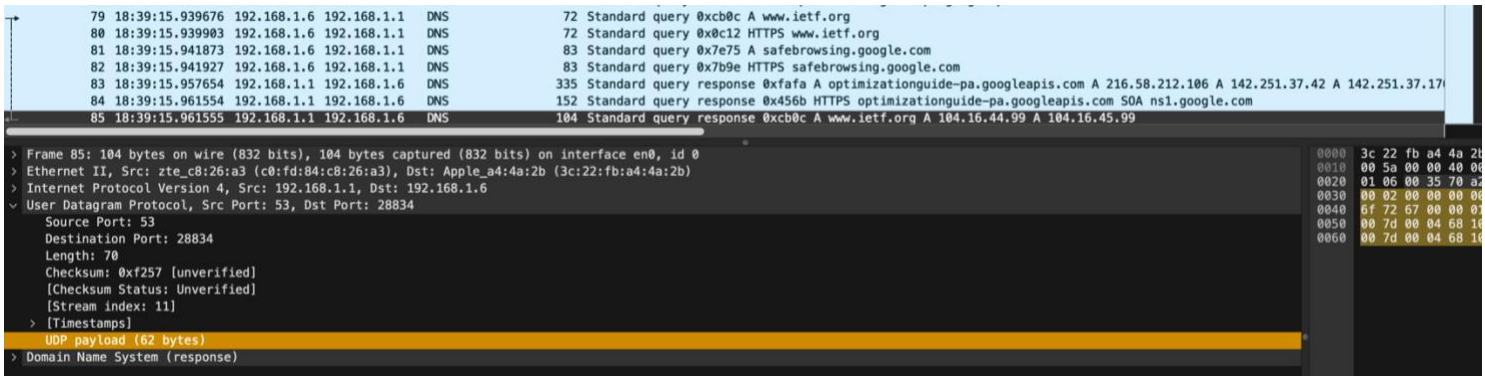
The Answers contains:

Name, type, class, time-to-leave, data-length, address

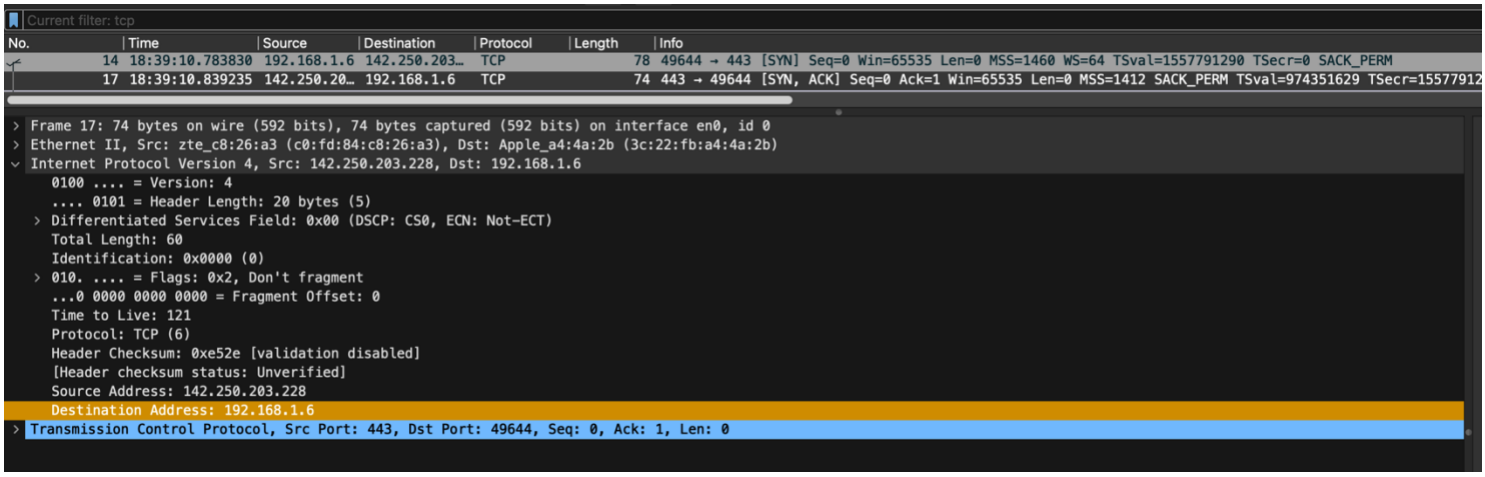


9. Question 9

DNS response:



TCP :

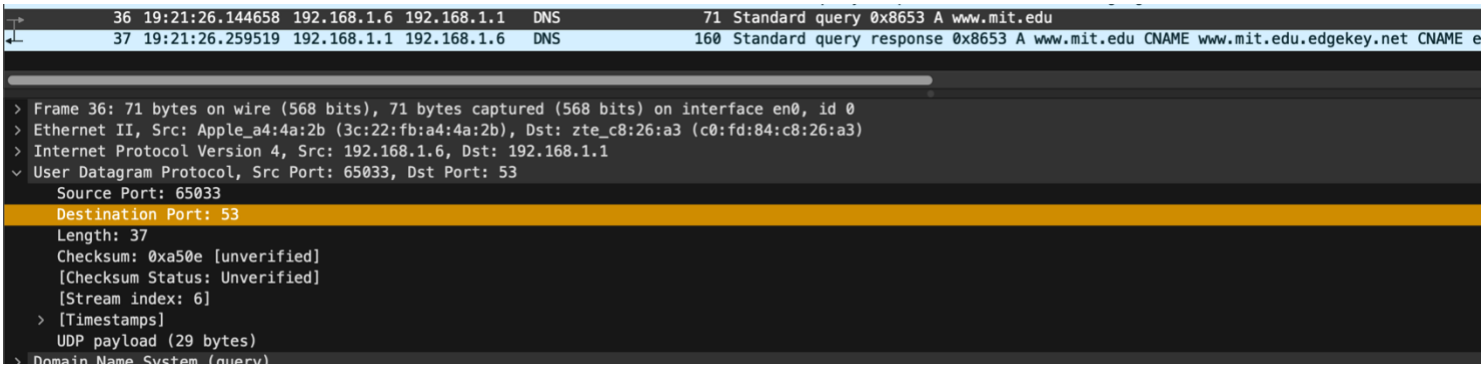


10. Question 10

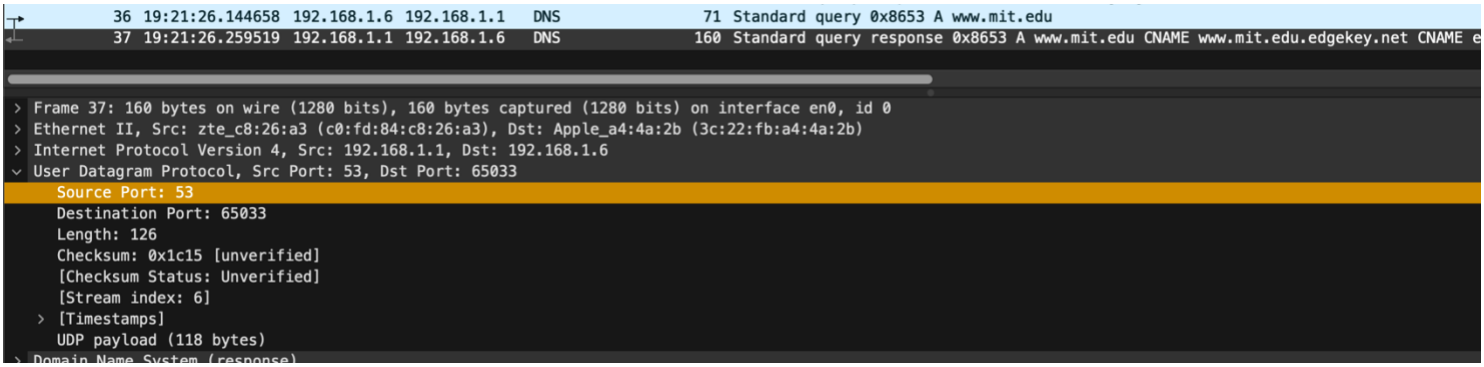
No there was not issued any images

11. Question 11

Destination of query:53

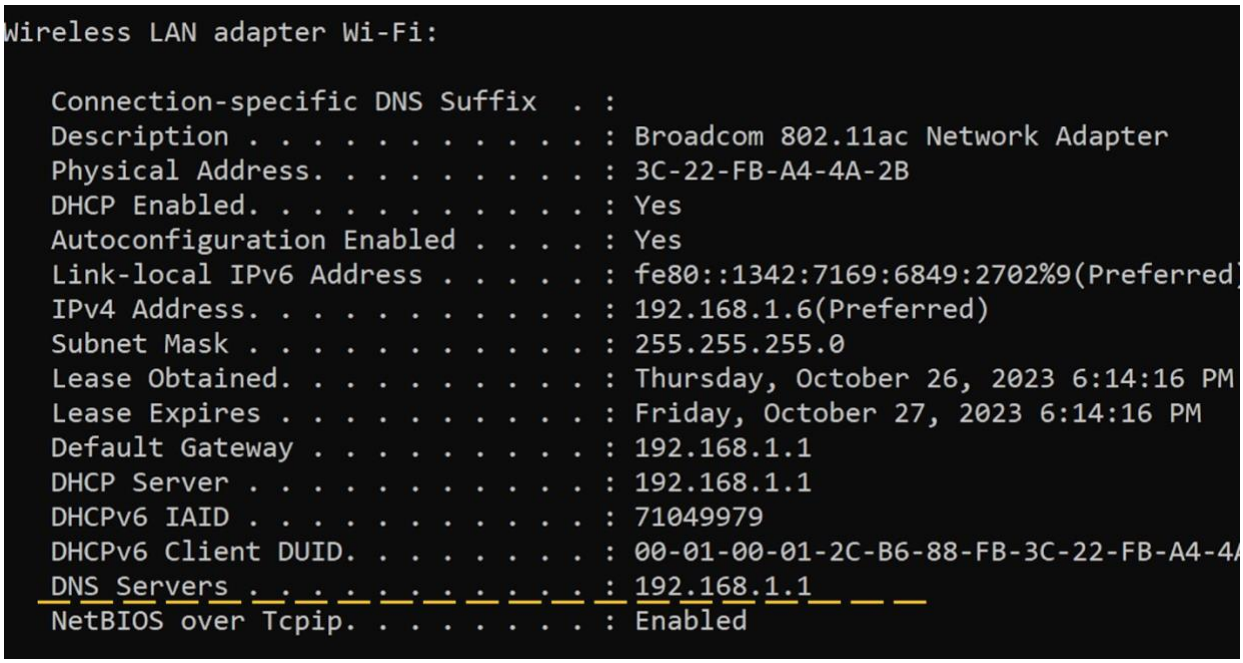


Source of response:53

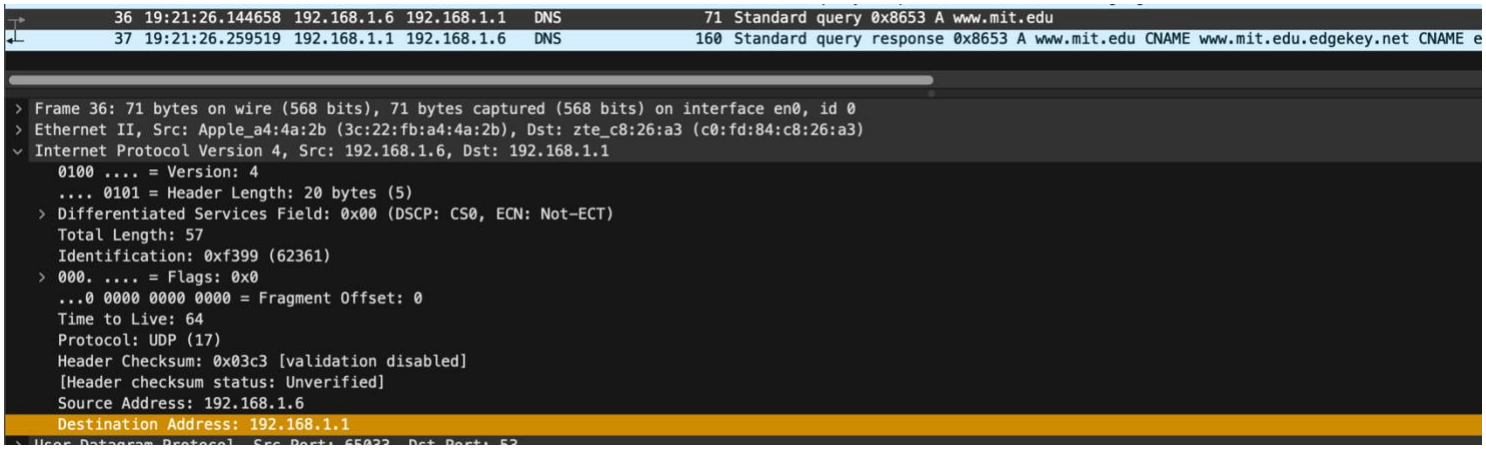


12. Question 12

local DNS server

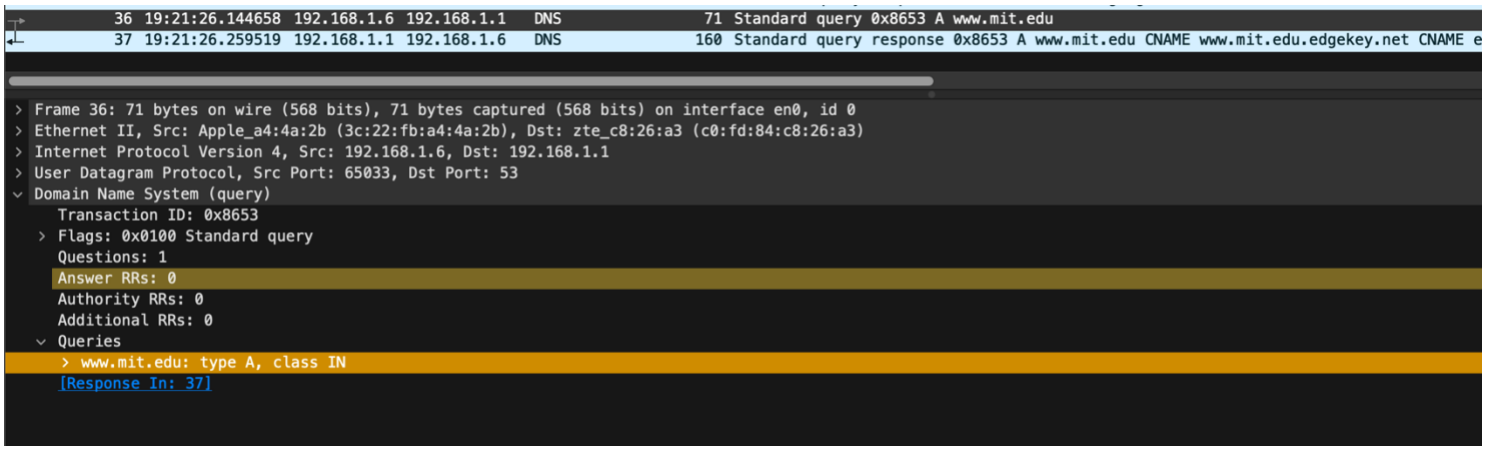

Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
Description . . . . . : Broadcom 802.11ac Network Adapter
Physical Address. . . . . : 3C-22-FB-A4-4A-2B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::1342:7169:6849:2702%9(Preferred)
IPv4 Address. . . . . : 192.168.1.6(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, October 26, 2023 6:14:16 PM
Lease Expires . . . . . : Friday, October 27, 2023 6:14:16 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 71049979
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-B6-88-FB-3C-22-FB-A4-4A
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled

IP address is the DNS query message sent



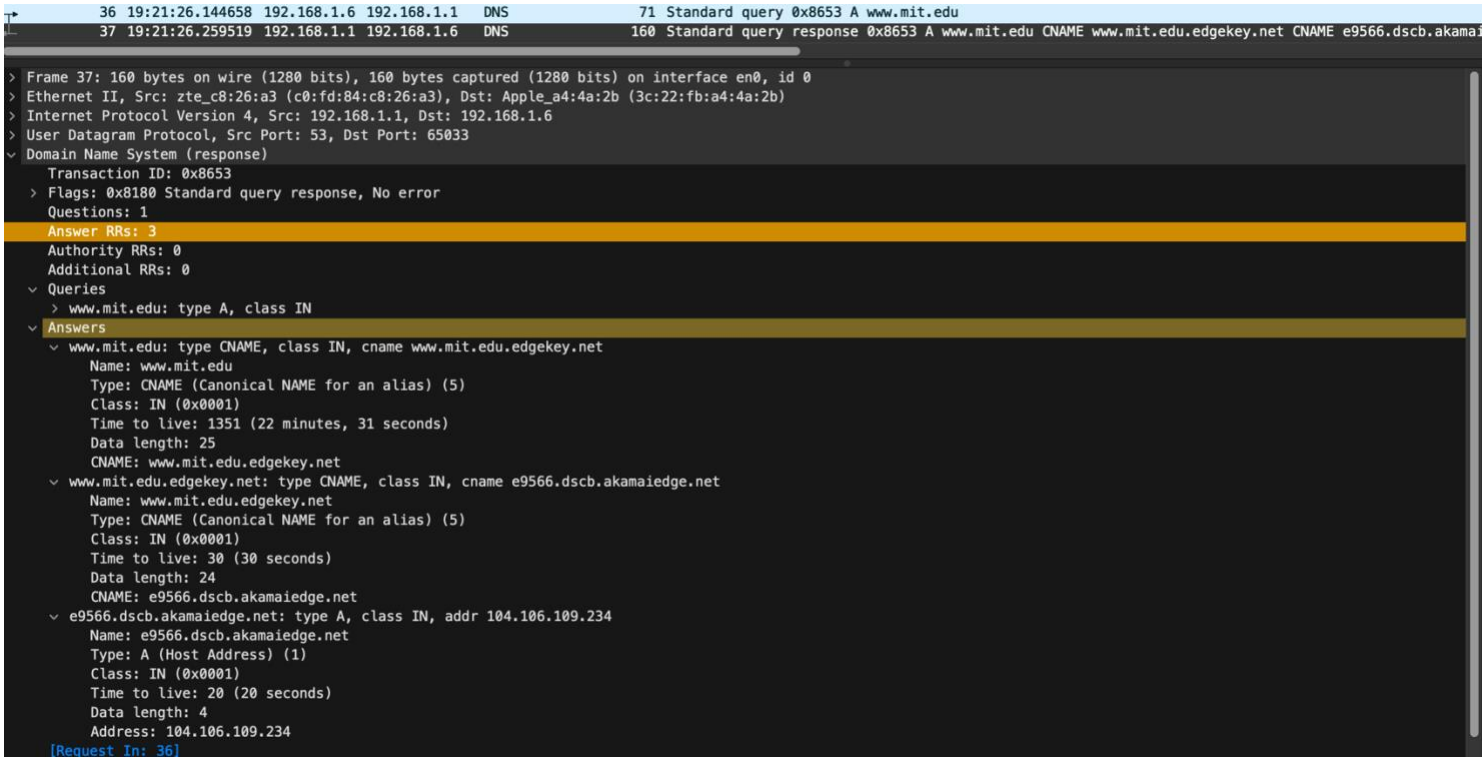
13. Question 13

“Type” of DNS query :A



Answers: 0

14. Question 14



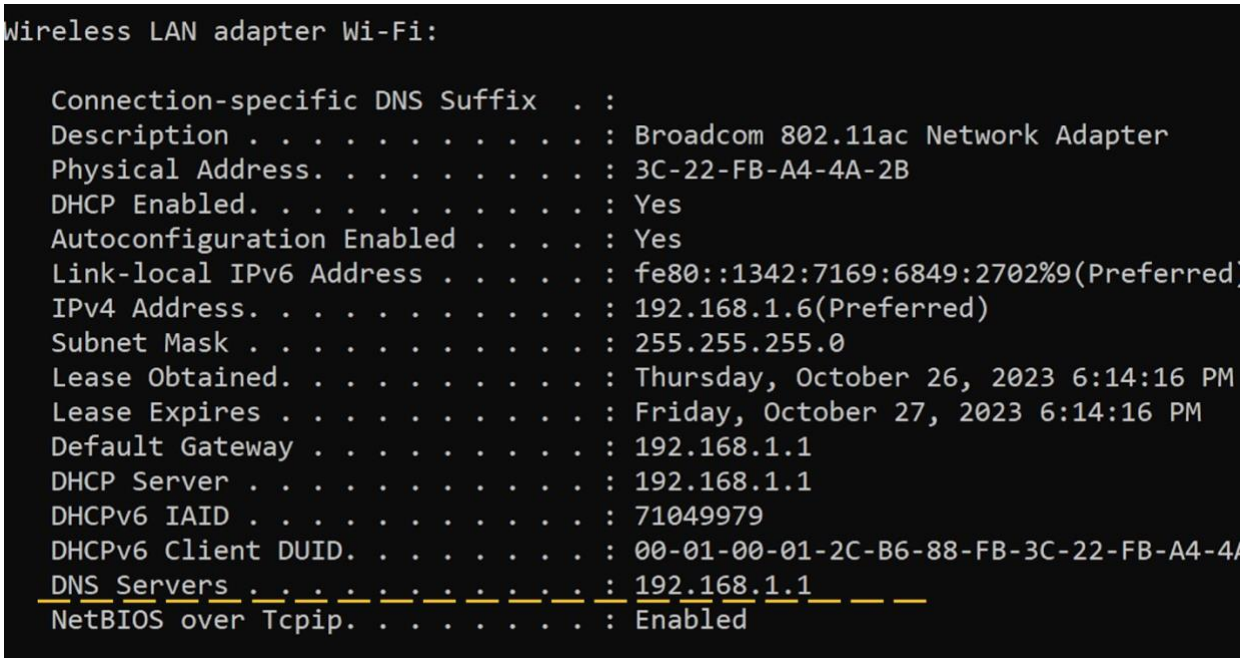
Answers: 3
Provide: Name, class, type, time to live, data length, CNAME

15. Question 15

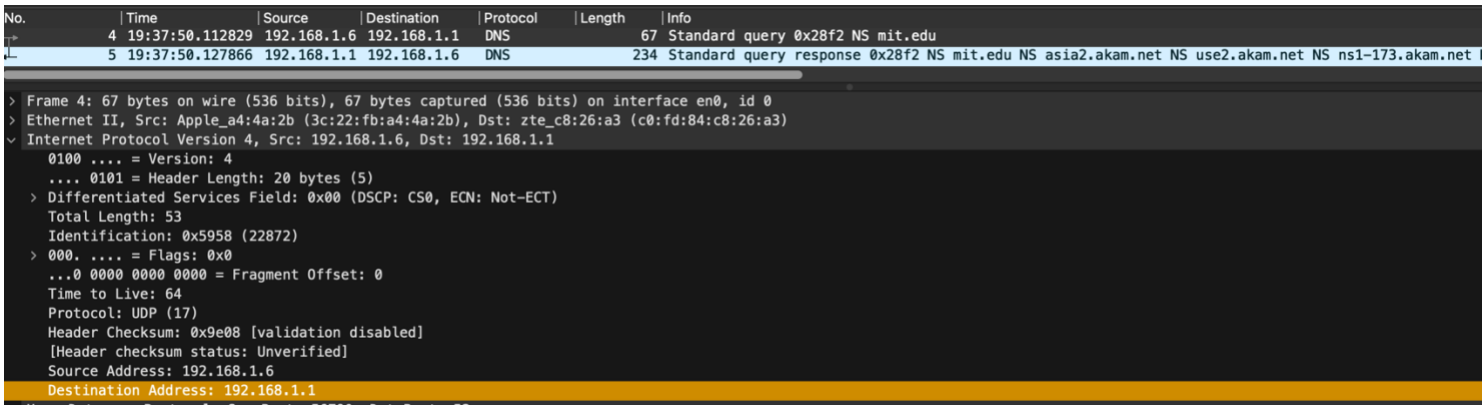
Done under every question its screenshot.

```
(base) malakelbakry@malaks-mbp ~ % nslookup -type=NS mit.edu

Server:         192.168.1.1
Address:        192.168.1.1#53

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

16. Question 16
local DNS server



IP address is the DNS query message sent

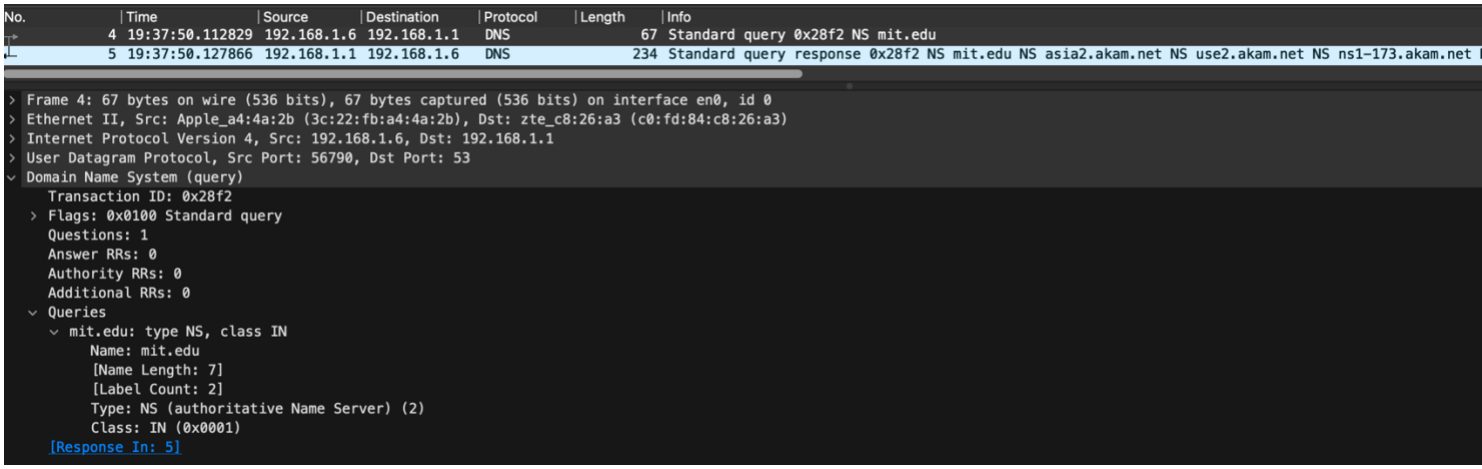


They are the same.

17. Question 17

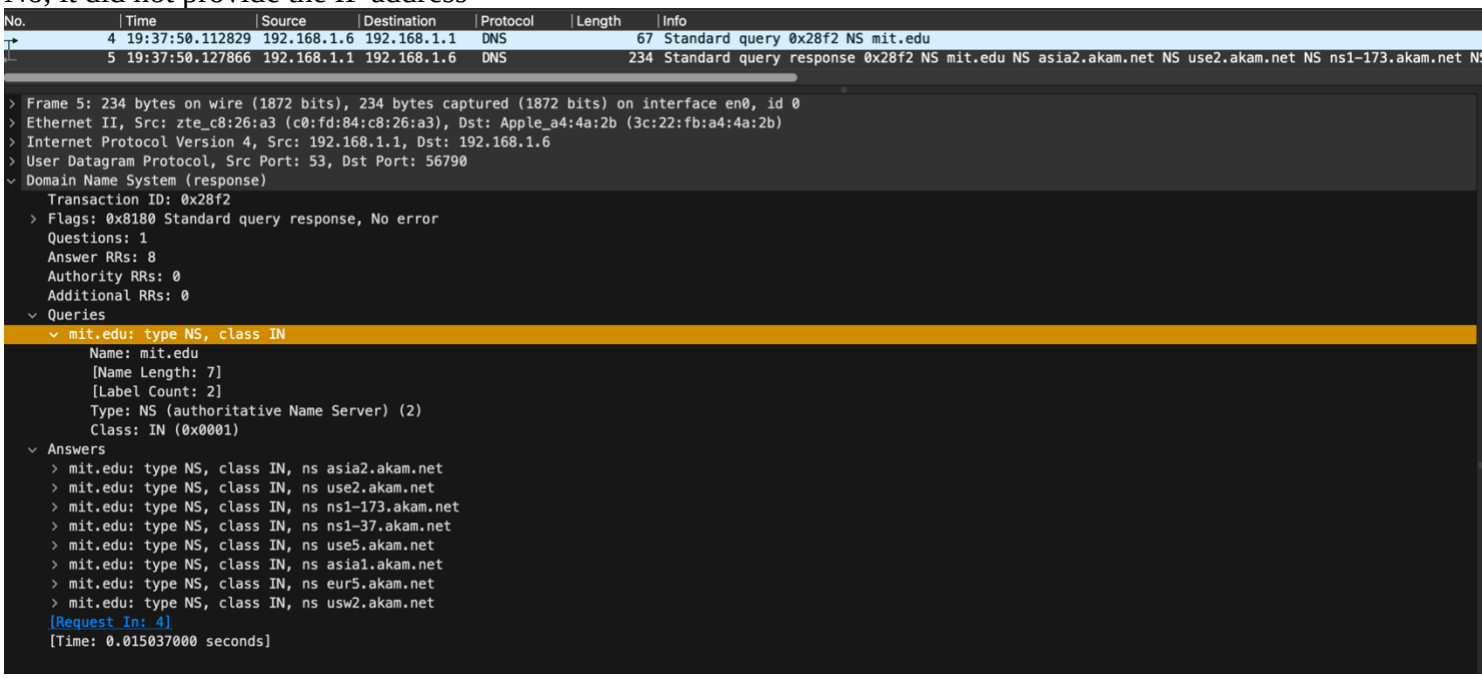
“Type” of DNS query : NS

Answers: 0



18. Question 18

Answers:8
Provided 8 nameservers for MIT
No, it did not provide the IP address



19. Question 19

Done under every question its screenshot.

For Question 20, 21,22,23: I used my mobile data and I could not execute and capture at the same time as the mac os and windows are not parallel to each other, so I used the trace files provided by Wireshark .

20. Question 20

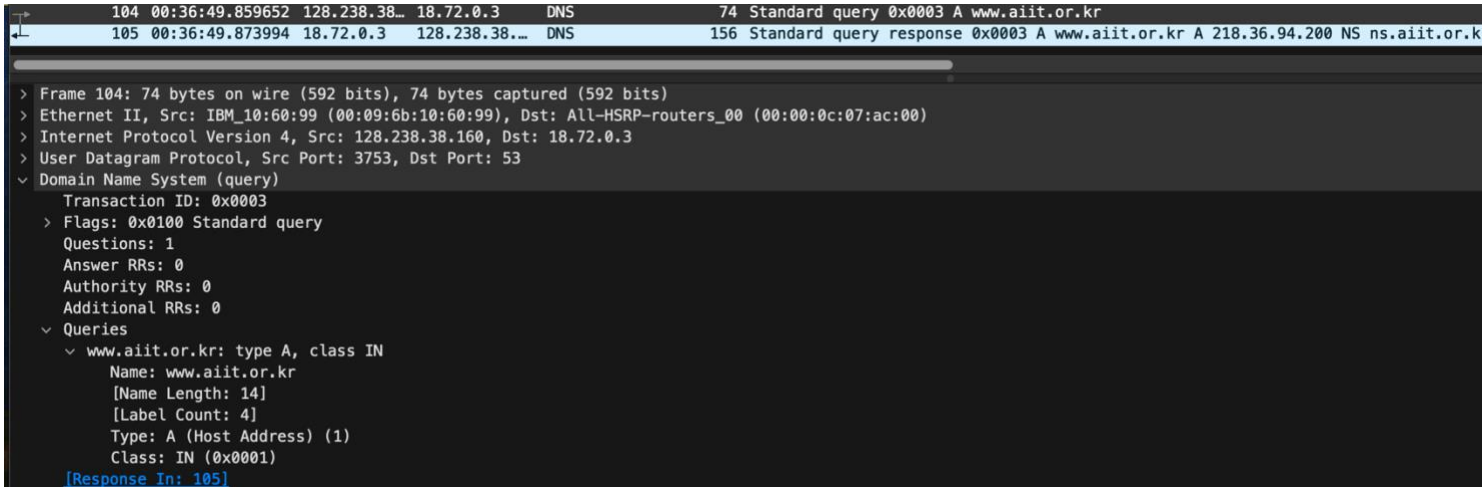
local DNS server

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Broadcom 802.11ac Network Adapter
   Physical Address. . . . . . . . . : 3C-22-FB-A4-4A-2B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::1342:7169:6849:2702%9(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.6(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, October 26, 2023 6:14:16 PM
   Lease Expires . . . . . . . . . . : Friday, October 27, 2023 6:14:16 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 71049979
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-B6-88-FB-3C-22-FB-A4-4A
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

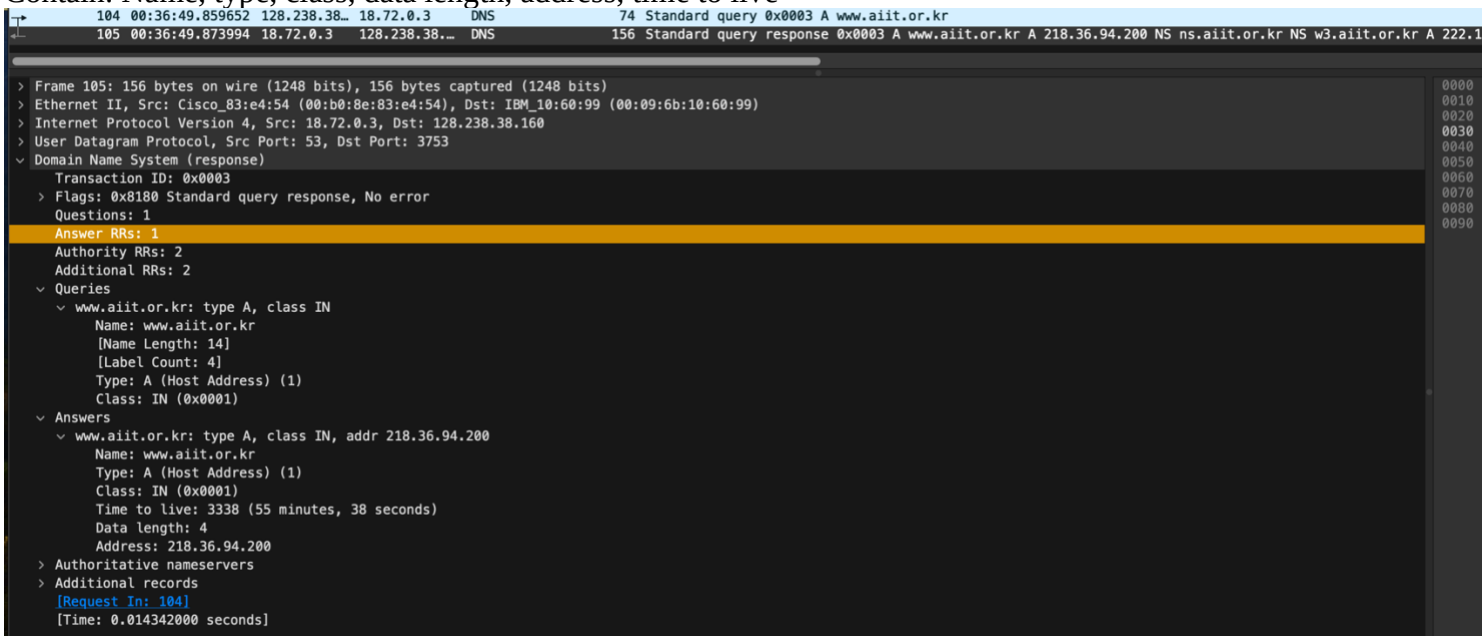
```
104 00:36:49.859652 128.238.38… 18.72.0.3     DNS   74 Standard query 0x0003 A www.aiit.or.kr
105 00:36:49.873994 18.72.0.3   128.238.38.…  DNS   156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.k

> Frame 104: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
v Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x2805 (10245)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x58d3 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.238.38.160
    Destination Address: 18.72.0.3
> User Datagram Protocol, Src Port: 3753, Dst Port: 53
> Domain Name System (query)
```

21. Question 21

Type: A
Answers:0



22. Question 22
Answers: 1
Contain: Name, type, class, data length, address, time to live



23. Question 23
Done under every question its screenshot.