JAVAIRIA REHMAN

19P-0020

BS(CS) 19-5A

"COMPUTER NETWORKS "

WIRESHARK HOME WORK

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

```
C:\Users\Javairia>
C:\Users\Javairia>nslookup nu.edu.pk
Server:  UnKnown
Address:  fe80::1

Non-authoritative answer:
Name:    nu.edu.pk
Address:  203.124.43.201
```

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

```
C:\Users\Javairia>nslookup -type=NS www.tum.de
Server:  UnKnown
Address:  fe80::1

Non-authoritative answer:
www.tum.de      canonical name = wwwv11.tum.de

tum.de
        primary name server = dns1.lrz.de
        responsible mail addr = hostmaster.lrz.de
        serial  = 2021112572
        refresh = 21600 (6 hours)
        retry   = 1800 (30 mins)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 86400 (1 day)
```

3. **Run nslookup so that one of the DNS servers obtained in Question2 is queried forthe mail servers for Yahoo! mail. What is its IP address?**

```
C:\Users\Javairia>nslookup mail.yahoo.com dns1.lrz.de
Server:  dns1.lrz.de
Address:  2001:4ca0:0:100:0:53:1:1

*** dns1.lrz.de can't find mail.yahoo.com: Query refused
```

As query is refused.so ip address is 129.187.255.151

```
C:\Users\Javairia>nslookup www.tum.de dns1.lrz.de
Server:  dns1.lrz.de
Address:  2001:4ca0:0:100:0:53:1:1

Name:    wwwv11.tum.de
Addresses:  2001:4ca0:0:103::81bb:ff97
          129.187.255.151
Aliases:  www.tum.de
```

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

No.	Time	Source	Destination	Protocol	Length	Info
7	14.940183	fe80::11ba:c273:943…	fe80::1	DNS	99	Standard query 0xa9fb A fp-afd.azureedge.us
8	14.940354	fe80::11ba:c273:943…	fe80::1	DNS	99	Standard query 0x1294 AAAA fp-afd.azureedge.us
9	15.119680	fe80::1	fe80::11ba:c273:943…	DNS	295	Standard query response 0xa9fb A fp-afd.azureedge.us CNAME fp-afd.afd.azure
10	15.137574	192.168.18.21	192.168.18.1	DNS	79	Standard query 0x1294 AAAA fp-afd.azureedge.us
11	15.239023	fe80::1	fe80::11ba:c273:943…	DNS	368	Standard query response 0x1294 AAAA fp-afd.azureedge.us CNAME fp-afd.afd.az
12	15.324316	192.168.18.1	192.168.18.21	DNS	348	Standard query response 0x1294 AAAA fp-afd.azureedge.us CNAME fp-afd.afd.az
13	15.911474	fe80::11ba:c273:943…	fe80::1	DNS	95	Standard query 0x8b6e A mail.google.com
14	15.911707	fe80::11ba:c273:943…	fe80::1	DNS	95	Standard query 0x5331 AAAA mail.google.com
15	15.980874	fe80::1	fe80::11ba:c273:943…	DNS	150	Standard query response 0x5331 AAAA mail.google.com CNAME googlemail.l.goog
16	15.980874	fe80::1	fe80::11ba:c273:943…	DNS	138	Standard query response 0x8b6e A mail.google.com CNAME googlemail.l.google.

```
> Frame 1: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface \Device\NPF_{BD712CB6-602B-4A73-9C18-2E9F7C72BD99}, id 0
> Ethernet II, Src: AzureWav_61:d0:0d (80:91:33:61:d0:0d), Dst: HuaweiTe_9a:ae:b5 (44:a1:91:9a:ae:b5)
> Internet Protocol Version 6, Src: fe80::11ba:c273:943:34e4, Dst: fe80::1
v User Datagram Protocol, Src Port: 64979, Dst Port: 53
    Source Port: 64979
    Destination Port: 53
    Length: 55
    Checksum: 0xb6ce [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (47 bytes)
> Domain Name System (query)
```

```
0000  44 a1 91 9a ae b5 80 91  33 61 d0 0d 86 dd 60 08   D······ 3a····`·
0010  ed 57 00 37 11 40 fe 80  00 00 00 00 00 00 11 ba   ·W·7·@·· ********
0020  c2 73 09 43 34 e4 fe 80  00 00 00 00 00 00 00 00   ·s·C4··· ********
0030  00 00 00 00 00 01 fd d3  00 35 00 37 b6 ce 1a d2   ******** ·5·7····
0040  01 00 00 01 00 00 00 00  00 00 0e 64 32 37 78 78   ******** ···d27xx
0050  65 37 6a 75 68 31 75 73  36 0a 63 6c 6f 75 64 66   e7juh1us 6·cloudf
0060  72 6f 6e 74 03 6e 65 74  00 00 01 00 01            ront·net ·····
```

UDP

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

Wireshark · Packet 33 · Wi-Fi (port 53)

```
> Frame 33: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface \Device\NPF_{BD712CB6-602B-4
> Ethernet II, Src: AzureWav_61:d0:0d (80:91:33:61:d0:0d), Dst: HuaweiTe_9a:ae:b5 (44:a1:91:9a:ae:b5)
> Internet Protocol Version 6, Src: fe80::11ba:c273:943:34e4, Dst: fe80::1
v User Datagram Protocol, Src Port: 64535, Dst Port: 53
    Source Port: 64535
    Destination Port: 53
    Length: 45
    Checksum: 0x0deb [unverified]
    [Checksum Status: Unverified]
    [Stream index: 16]
  > [Timestamps]
    UDP payload (37 bytes)
> Domain Name System (query)
```

```
0000  44 a1 91 9a ae b5 80 91  33 61 d0 0d 86 dd 60 0d   D······ 3a····`·
0010  4d 04 00 2d 11 40 fe 80  00 00 00 00 00 00 11 ba   M··-·@·· ********
0020  c2 73 09 43 34 e4 fe 80  00 00 00 00 00 00 00 00   ·s·C4··· ********
0030  00 00 00 00 00 01 fc 17  00 35 00 2d 0d eb ac 42   ******** ·5·-···B
0040  01 00 00 01 00 00 00 00  00 00 08 63 6c 69 65 6e   ******** ···clien
0050  74 73 32 06 67 6f 6f 67  6c 65 03 63 6f 6d 00 00   ts2·goog le·com··
0060  01 00 01                                           ···
```

Fig a

Wireshark · Packet 32 · Wi-Fi (port 53)

```
> Frame 32: 118 bytes on wire (944 bits), 118 bytes capture
> Ethernet II, Src: HuaweiTe_9a:ae:bc (44:a1:91:9a:ae:bc),
> Internet Protocol Version 6, Src: fe80::1, Dst: fe80::11b
v User Datagram Protocol, Src Port: 53, Dst Port: 58124
    Source Port: 53
    Destination Port: 58124
    Length: 64
    Checksum: 0x224c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 15]
  > [Timestamps]
    UDP payload (56 bytes)
> Domain Name System (response)
```

Fig b

Source of fig b and destination on fig a are same

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?

```
Connection-specific DNS Suffix  . : Home
Description . . . . . . . . . . . : Realtek RTL8188ETV Wireless LAN 802.11n USB 2.0 Network A
Physical Address. . . . . . . . . : 0C-9A-42-B5-BC-F9
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . . . . . . . : 192.168.1.5(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : Wednesday, December 1, 2021 6:59:15 PM
Lease Expires . . . . . . . . . . : Thursday, December 2, 2021 6:59:16 PM
Default Gateway . . . . . . . . . : 192.168.1.1
DHCP Server . . . . . . . . . . . : 192.168.1.1
DNS Servers . . . . . . . . . . . : 192.168.1.1
                                   192.168.1.1
NetBIOS over Tcpip. . . . . . . . : Enabled
```

yes

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

```
> [Timestamps]
  UDP payload (28 bytes)
Domain Name System (query)
  Transaction ID: 0xee96
> Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
v Queries
  > google.com: type AAAA, class IN
  [Response In: 32]
```

type AAAA with class IN

Wireshark · Packet 33 · Wi-Fi (port 53)

```
    UDP payload (37 bytes)
  Domain Name System (query)
    Transaction ID: 0xac42
    Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 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
```

```
0000  44 a1 91 9a ae b5 80 91  33 61 d0 0d 86 dd 60 0d   D······ 3a····`·
0010  4d 04 00 2d 11 40 fe 80  00 00 00 00 00 00 11 ba   M··-·@·· ·····
0020  c2 73 09 43 34 e4 fe 80  00 00 00 00 00 00 00 00   ·s·C4··· ·····
0030  00 00 00 00 00 01 fc 17  00 35 00 2d 0d eb ac 42   ····· ·5·-···B
0040  01 00 00 01 00 00 00 00  00 00 08 63 6c 69 65 6e   ····· ···clien
0050  74 73 32 06 67 6f 6f 67  6c 65 03 63 6f 6d 00 00   ts2·goog le·com··
0060  01 00 01                                           ···
```

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

Wireshark · Packet 32 · Wi-Fi (port 53)

```
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by th
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    > google.com: type AAAA, class IN, addr 2a00:1450:4019:800::200e
```

```
0000  80 91 33 61 d0 0d 44 a1  91 9a ae bc 86 dd 60 00   ··3a··D· ·····`··
0010  00 00 00 40 11 40 fe 80  00 00 00 00 00 00 00 00   ···@·@·· ·····
0020  00 00 00 00 00 01 fe 80  00 00 00 00 00 00 11 ba   ····· ·····
0030  c2 73 09 43 34 e4 00 35  e3 0c 00 40 22 4c ee 96   ·s·C4··5 ···@"L··
0040  81 80 00 01 00 01 00 00  00 00 06 67 6f 6f 67 6c   ····· ···googl
0050  65 03 63 6f 6d 00 00 1c  00 01 c0 0c 00 1c 00 01   e·com··· ·····
0060  00 00 00 eb 00 10 2a 00  14 50 40 19 08 00 00 00   ·····*· ·P@·····
0070  00 00 00 00 20 0e                                  ···· ··
```

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?

Wireshark · Packet 5 · Wi-Fi

```
> Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{DCD995F2-E53D-49F3-A9BF-DE3
> Ethernet II, Src: Fn-LinkT_b5:bc:f9 (0c:9a:42:b5:bc:f9), Dst: Fiberhom_43:64:9e (34:bf:90:43:64:9e)
v Internet Protocol Version 4, Src: 192.168.1.5, Dst: 104.16.45.99
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0xa2af (41647)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x00f4 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.5
    Destination Address: 104.16.45.99
> Transmission Control Protocol, Src Port: 50538, Dst Port: 80, Seq: 0, Len: 0
```

```
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xb729 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.1
    Destination Address: 192.168.1.5
> User Datagram Protocol, Src Port: 53, Dst Port: 60132
v Domain Name System (response)
    Transaction ID: 0x748f
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org.cdn.cloudflare.net: type A, class IN
  v Answers
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
    v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
        Name: www.ietf.org.cdn.cloudflare.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 4
        Address: 104.16.45.99
```

yes

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

ip.addr == 192.168.1.5

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.5	172.217.19.174	TCP	55	50535 → 443 [A
2	0.167541	172.217.19.174	192.168.1.5	TCP	66	443 → 50535 [A
3	0.374970	192.168.1.5	192.168.1.1	DNS	72	Standard query
4	0.425031	192.168.1.1	192.168.1.5	DNS	149	Standard query
5	0.426132	192.168.1.5	104.16.45.99	TCP	66	50538 → 80 [SY
6	0.426138	192.168.1.5	192.168.1.1	DNS	91	Standard query
7	0.426256	192.168.1.5	104.16.45.99	TCP	66	50539 → 80 [SY
8	0.478574	192.168.1.1	192.168.1.5	DNS	123	Standard query
9	0.479144	192.168.1.5	192.168.1.1	DNS	91	Standard query
10	0.527935	192.168.1.1	192.168.1.5	DNS	147	Standard query
11	0.594108	104.16.45.99	192.168.1.5	TCP	66	80 → 50539 [SY
12	0.594203	192.168.1.5	104.16.45.99	TCP	54	50539 → 80 [AC
13	0.594445	192.168.1.5	104.16.45.99	HTTP	398	GET / HTTP/1.1
14	0.600835	104.16.45.99	192.168.1.5	TCP	66	80 → 50538 [SY
15	0.600878	192.168.1.5	104.16.45.99	TCP	54	50538 → 80 [AC
17	0.763938	104.16.45.99	192.168.1.5	TCP	54	80 → 50539 [AC
18	0.843422	104.16.45.99	192.168.1.5	HTTP	357	HTTP/1.1 301 M
19	0.847150	192.168.1.5	104.16.45.99	TCP	66	50540 → 443 [S
20	0.893739	192.168.1.5	104.16.45.99	TCP	54	50539 → 80 [AC
21	1.016338	104.16.45.99	192.168.1.5	TCP	66	443 → 50540 [S
22	1.016425	192.168.1.5	104.16.45.99	TCP	54	50540 → 443 [A
23	1.018695	192.168.1.5	104.16.45.99	TLSv1.3	571	Client Hello
24	1.193689	104.16.45.99	192.168.1.5	TCP	54	443 → 50540 [A

no

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

Wireshark · Packet 3 · Wi-Fi (port 53)

```
> Frame 3: 235 bytes on wire (1880 bits), 235 bytes captured (1880 bits) on inte
> Ethernet II, Src: HuaweiTe_9a:ae:b5 (44:a1:91:9a:ae:b5), Dst: AzureWav_61:d0:0
> Internet Protocol Version 4, Src: 192.168.18.1, Dst: 192.168.18.21
v User Datagram Protocol, Src Port: 53, Dst Port: 49883
    Source Port: 53
    Destination Port: 49883
    Length: 201
    Checksum: 0xf537 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (193 bytes)
v Domain Name System (response)
```

```
0000  80 91 33 61 d0 0d 44 a1  91 9a ae b5 08 00 45 00   ··3a··D· ····· ·E·
0010  00 dd d7 d5 40 00 40 11  bc d3 c0 a8 12 01 c0 a8   ····@·@· ····· ····
0020  12 15 00 35 c2 db 00 c9  f5 37 02 48 81 80 00 01   ···5···· ·7·H····
0030  00 06 00 00 00 00 20 62  36 65 36 32 39 38 61 64   ····· b 6e6298ad
0040  34 37 36 64 32 30 34 39  32 63 61 32 35 64 66 39   476d2049 2ca25df9
0050  33 32 65 62 65 64 32 03  6e 72 62 0c 66 6f 6f 74   32ebed2· nrb·foot
0060  70 72 69 6e 74 64 6e 73  03 63 6f 6d 00 00 01 00   printdns ·com····
0070  01 c0 0c 00 05 00 01 00  00 00 1e 00 17 0d 61 74   ····· ·····at
0080  6d 2d 66 70 2d 64 69 72  65 63 74 06 6f 66 66 69   m-fp-dir ect·offi
0090  63 65 c0 3e c0 53 00 05  00 01 00 00 01 2c 00 0b   ce·>·S·· ·····,··
00a0  03 6f 6f 63 04 74 6d 2d  32 c0 61 c0 76 00 01 00   ·ooc·tm- 2·a·v···
00b0  01 00 00 00 0a 00 04 34  62 20 02 c0 76 00 01 00   ·····4 b ··v···
00c0  01 00 00 00 0a 00 04 34  62 5f d2 c0 76 00 01 00   ·····4 b_··v···
00d0  01 00 00 00 0a 00 04 34  62 3d 32 c0 76 00 01 00   ·····4 b=2·v···
00e0  01 00 00 00 0a 00 04 34  62 3d 22                  ·····4 b="
```

Source	Destination	Protocol	Length	Info

Wireshark · Packet 4 · Wi-Fi (port 53)

```
> Frame 4: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interf
> Ethernet II, Src: AzureWav_61:d0:0d (80:91:33:61:d0:0d), Dst: HuaweiTe_9a:ae
> Internet Protocol Version 4, Src: 192.168.18.21, Dst: 192.168.18.1
v User Datagram Protocol, Src Port: 59374, Dst Port: 53
    Source Port: 59374
    Destination Port: 53
    Length: 54
    Checksum: 0x418c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (46 bytes)
v Domain Name System (query)
```

```
0000  44 a1 91 9a ae b5 80 91  33 61 d0 0d 08 00 45 00   D······ 3a····E·
0010  00 4a b1 6f 00 00 80 11  e3 cc c0 a8 12 15 c0 a8   ·J·o···· ........
0020  12 01 e7 ee 00 35 00 36  41 8c 68 db 01 00 00 01   ·····5·6 A·h·····
0030  00 00 00 00 00 00 0e 66  70 2d 61 66 64 2d 6e 6f   ·......·f p-afd-no
0040  63 61 63 68 65 09 61 7a  75 72 65 65 64 67 65 03   cache·az ureedge·
0050  6e 65 74 00 00 01 00 01                            net·····
```

Souce of packet 3 is equal to destination of packet 4

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

default local DNS server?

Yes

```
> Frame 3: 235 bytes on wire (1880 bits), 235 bytes captured (1880 bits)
> Ethernet II, Src: HuaweiTe_9a:ae:b5 (44:a1:91:9a:ae:b5), Dst: AzureWav
> Internet Protocol Version 4, Src: 192.168.18.1, Dst: 192.168.18.21
v User Datagram Protocol, Src Port: 53, Dst Port: 49883
    Source Port: 53
```

13. Examine the DNS query message. What "Type" of DNS query is it? Does the

query message contain any "answers"?

```
> User Datagram Protocol, Src Port: 53, Dst Port: 49883
v Domain Name System (response)
    Transaction ID: 0x0248
  v Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the se
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > b6e6298ad476d20492ca25df932ebed2.nrb.footprintdns.com: type A, class IN
  > Answers
    [Request In: 1]
    [Time: 0.393893000 seconds]

0000  80 91 33 61 d0 0d 44 a1  91 9a ae b5 08 00 45 00   ··3a··D· ····· ··E·
0010  00 dd d7 d5 40 00 40 11  bc d3 c0 a8 12 01 c0 a8   ····@·@· ····· ····
0020  12 15 00 35 c2 db 00 c9  f5 37 02 48 81 80 00 01   ···5···· ·7·H····
0030  00 06 00 00 00 00 20 62  36 65 36 32 39 38 61 64   ····· b 6e6298ad
0040  34 37 36 64 32 30 34 39  32 63 61 32 35 64 66 39   476d2049 2ca25df9
0050  33 32 65 62 65 64 32 03  6e 72 62 0c 66 6f 6f 74   32ebed2· nrb·foot
```

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

ip.addr==192.168.18.21

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.18.21	192.168.18.1	DNS	113	Standard query 0x0248 A b6e6298ad476d20492ca25df932ebed2.nrb.footprintdns.com
2	0.193355	192.168.18.21	192.168.18.1	DNS	113	Standard query 0x0248 A b6e6298ad476d20492ca25df932ebed2.nrb.footprintdns.com
3	0.393893	192.168.18.1	192.168.18.21	DNS	235	Standard query response 0x0248 A b6e6298ad476d20492ca25df932ebed2.nrb.footprintdns.com CNAME atm-
4	0.936302	192.168.18.21	192.168.18.1	DNS	88	Standard query 0x68db A fp-afd-nocache.azureedge.net
5	1.115825	192.168.18.1	192.168.18.21	DNS	280	Standard query response 0x68db A fp-afd-nocache.azureedge.net CNAME fp-afd-nocache.afd.azureedge.
6	20.895458	192.168.18.21	192.168.18.1	DNS	89	Standard query 0x099d A addons-pa.clients6.google.com
7	20.962573	192.168.18.1	192.168.18.21	DNS	105	Standard query response 0x099d A addons-pa.clients6.google.com A 216.58.207.106
8	21.805377	192.168.18.21	192.168.18.1	DNS	94	Standard query 0x4525 A r2---sn-jtcxg-2xfl.googlevideo.com
9	21.822755	192.168.18.1	192.168.18.21	DNS	156	Standard query response 0x4525 A r2---sn-jtcxg-2xfl.googlevideo.com CNAME r2.sn-jtcxg-2xfl.google
10	63.422324	192.168.18.21	192.168.18.1	DNS	76	Standard query 0xe897 A mtalk.google.com

No of responses equal to no of answers here both are 5

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

default local DNS server?

ip.addr==192.168.18.21

No.	Time	Source	Destination	Protocol	Length	Info
6	20.895458	192.168.18.21	192.168.18.1	DNS	89	Standard query 0x099d A addons-pa.clients6.google.com
7	20.962573	192.168.18.1	192.168.18.21	DNS	105	Standard query response 0x099d A addons-pa.clients6.googl
8	21.805377	192.168.18.21	192.168.18.1	DNS	94	Standard query 0x4525 A r2---sn-jtcxg-2xfl.googlevideo.co
9	21.822755	192.168.18.1	192.168.18.21	DNS	156	Standard query response 0x4525 A r2---sn-jtcxg-2xfl.googl
10	63.422324	192.168.18.21	192.168.18.1	DNS	76	Standard query 0xe897 A mtalk.google.com
11	63.471387	192.168.18.1	192.168.18.21	DNS	121	Standard query response 0xe897 A mtalk.google.com CNAME m
12	63.881846	192.168.18.21	192.168.18.1	DNS	89	Standard query 0x3930 A d27xxe7juh1us6.cloudfront.net
13	64.057435	192.168.18.1	192.168.18.21	DNS	153	Standard query response 0x3930 A d27xxe7juh1us6.cloudfron
14	79.640319	192.168.18.21	192.168.18.1	DNS	71	Standard query 0xbe8f A b1.nel.goog
15	79.703852	192.168.18.1	192.168.18.21	DNS	87	Standard query response 0xbe8f A b1.nel.goog A 172.217.19

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

Wireshark · Packet 3 · Wi-Fi (port 53)

```
        .... .... 1... .... = Recursion available: Server can do recursive queries
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenti
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
    ⌄ b6e6298ad476d20492ca25df932ebed2.nrb.footprintdns.com: type A, class IN
        Name: b6e6298ad476d20492ca25df932ebed2.nrb.footprintdns.com
        [Name Length: 53]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ⌄ Answers
    > b6e6298ad476d20492ca25df932ebed2.nrb.footprintdns.com: type CNAME, class IN, cname at
    > atm-fp-direct.office.com: type CNAME, class IN, cname ooc.tm-2.office.com
    > ooc.tm-2.office.com: type A, class IN, addr 52.98.32.2
    > ooc.tm-2.office.com: type A, class IN, addr 52.98.95.210
    > ooc.tm-2.office.com: type A, class IN, addr 52.98.61.50
    > ooc.tm-2.office.com: type A, class IN, addr 52.98.61.34
```

```
0000  80 91 33 61 d0 0d 44 a1  91 9a ae b5 08 00 45 00   ··3a··D· ····· ··E·
0010  00 dd d7 d5 40 00 40 11  bc d3 c0 a8 12 01 c0 a8   ····@·@· ····· ····
0020  12 15 00 35 c2 db 00 c9  f5 37 02 48 81 80 00 01   ···5···· ·7·H····
0030  00 06 00 00 00 00 20 62  36 65 36 32 39 38 61 64   ····· b 6e6298ad
0040  34 37 36 64 32 30 34 39  32 63 61 32 35 64 66 39   476d2049 2ca25df9
0050  33 32 65 62 65 64 32 03  6e 72 62 0c 66 6f 6f 74   32ebed2· nrb·foot
```

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 namesers?

```
        Class: IN (0x0001)
    Answers
      > b6e6298ad476d20492ca25df932ebed2.nrb.footprintdns.com: type CNAME, class IN, cname atm-fp-direc
      > atm-fp-direct.office.com: type CNAME, class IN, cname ooc.tm-2.office.com
      > ooc.tm-2.office.com: type A, class IN, addr 52.98.32.2
      > ooc.tm-2.office.com: type A, class IN, addr 52.98.95.210
      > ooc.tm-2.office.com: type A, class IN, addr 52.98.61.50
      > ooc.tm-2.office.com: type A, class IN, addr 52.98.61.34
    [Request In: 1]
    [Time: 0.393893000 seconds]
```

20. To what IP address is the DNS query message sent? Is this the IP address of your

ip.addr==192.168.18.21

No.	Time	Source	Destination	Protocol	Length	Info
6	20.895458	192.168.18.21	192.168.18.1	DNS	89	Standard query 0x099d A addons-pa.clients6.google.com
7	20.962573	192.168.18.1	192.168.18.21	DNS	105	Standard query response 0x099d A addons-pa.clients6.google.com A 216.58.207.106
8	21.805377	192.168.18.21	192.168.18.1	DNS	94	Standard query 0x4525 A r2---sn-jtcxg-2xfl.googlevideo.com
9	21.822755	192.168.18.1	192.168.18.21	DNS	156	Standard query response 0x4525 A r2---sn-jtcxg-2xfl.googlevideo.com CNAME r2.sr
10	63.422324	192.168.18.21	192.168.18.1	DNS	76	Standard query 0xe897 A mtalk.google.com
11	63.471387	192.168.18.1	192.168.18.21	DNS	121	Standard query response 0xe897 A mtalk.google.com CNAME mobile-gtalk.l.google.c
12	63.881846	192.168.18.21	192.168.18.1	DNS	89	Standard query 0x3930 A d27xxe7juh1us6.cloudfront.net
13	64.057435	192.168.18.1	192.168.18.21	DNS	153	Standard query response 0x3930 A d27xxe7juh1us6.cloudfront.net A 143.204.119.18
14	79.640319	192.168.18.21	192.168.18.1	DNS	71	Standard query 0xbe8f A b1.nel.goog
15	79.703852	192.168.18.1	192.168.18.21	DNS	87	Standard query response 0xbe8f A b1.nel.goog A 172.217.19.3

default local DNS server? If not, what does the IP address correspond to?

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

query message contain any “answers”?

```
Domain Name System (response)
    Transaction ID: 0x0248
  Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the serve
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  > Answers
    [Request In: 1]
    [Time: 0.393893000 seconds]
```

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

```
Queries
  b6e6298ad476d20492ca25df932ebed2.nrb.footprintdns.com: type A, class IN
      Name: b6e6298ad476d20492ca25df932ebed2.nrb.footprintdns.com
      [Name Length: 53]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
> Answers
  [Request In: 1]
```