Name : Jawad Ahmed

Roll No : 20P-0165

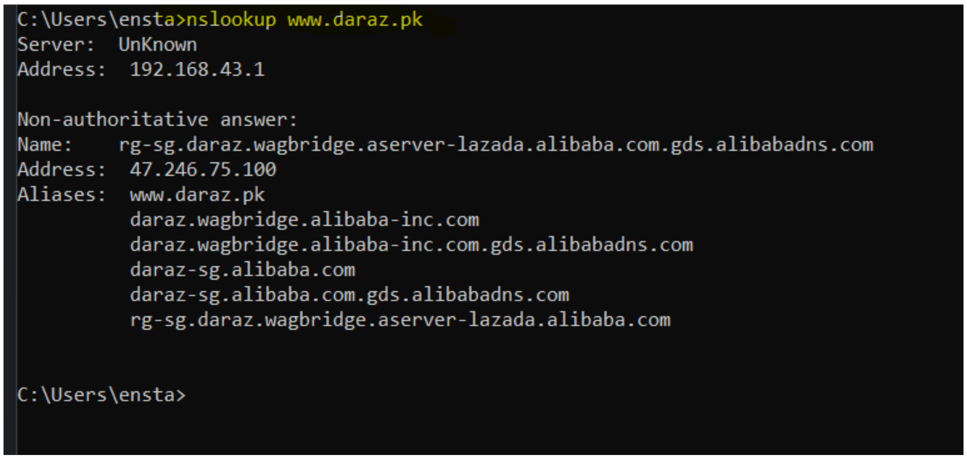
Section : BCS-5A

Lab 9 Homework

Task: Do the following (and write down the results):

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

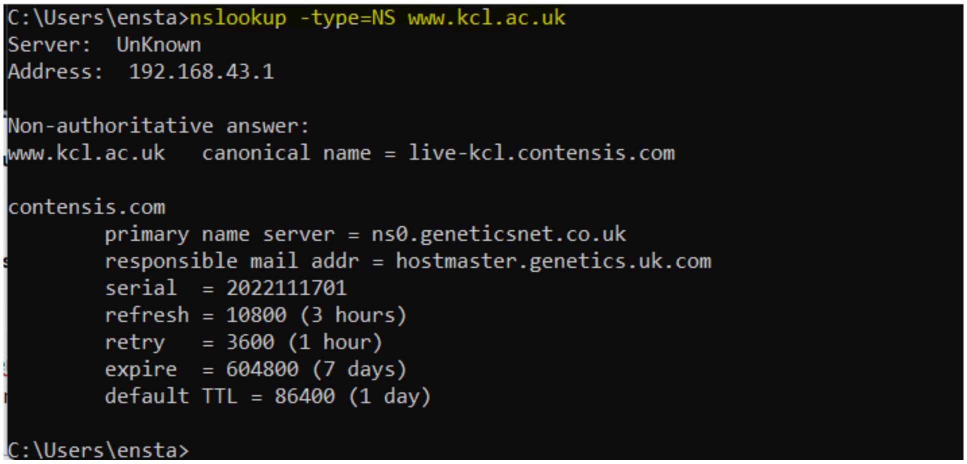
Ans: Result: The web server www.daraz.pk has an IP Address **47.246.75.100**.



```
C:\Users\ensta>nslookup www.daraz.pk
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    rg-sg.daraz.wagbridge.aserver-lazada.alibaba.com.gds.alibabadns.com
Address:  47.246.75.100
Aliases:  www.daraz.pk
          daraz.wagbridge.alibaba-inc.com
          daraz.wagbridge.alibaba-inc.com.gds.alibabadns.com
          daraz-sg.alibaba.com
          daraz-sg.alibaba.com.gds.alibabadns.com
          rg-sg.daraz.wagbridge.aserver-lazada.alibaba.com


C:\Users\ensta>
```

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

Ans: I have determined the authoritative DNS servers of **King's College London. In this command, we have provided the option "-type=NS" and the domain "mit.edu". This causes nslookup to send a query for a type-NS record to the default local DNS server. In words, the query is saying, "please send me the host names of the authoritative DNS for www.kcl.ac.uk".**



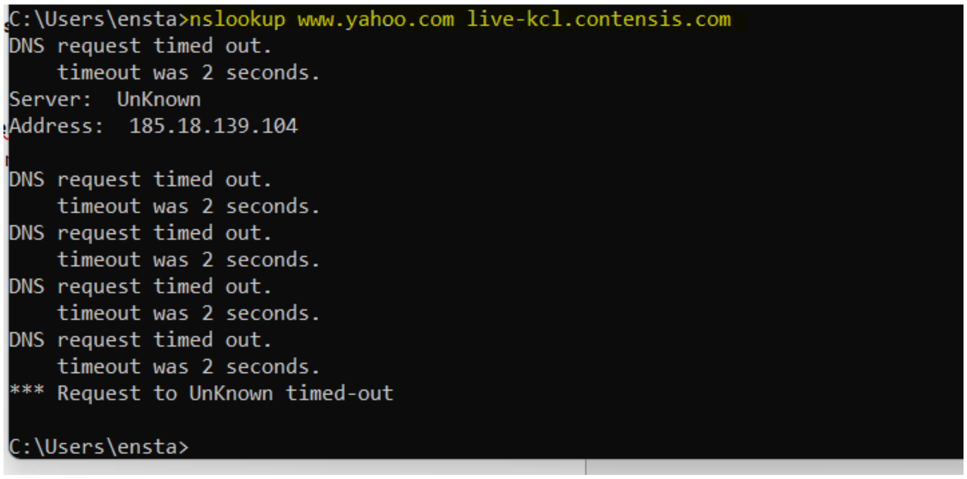
```
C:\Users\ensta>nslookup -type=NS www.kcl.ac.uk
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
www.kcl.ac.uk   canonical name = live-kcl.contensis.com

contensis.com
        primary name server = ns0.geneticsnet.co.uk
        responsible mail addr = hostmaster.genetics.uk.com
        serial  = 2022111701
        refresh = 10800 (3 hours)
        retry   = 3600 (1 hour)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)

C:\Users\ensta>
```

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 DNS server obtained in question 2 is **live-kcl.contensis.com.** The command will be as follows:

=> nslookup www.yahoo.com live-kcl.contensis.com

This command mean that “send the query to the **live-kcl.contensis.com** rather than to the defult DNS server (www.yahoo.com). Thus, the query and reply transaction takes place directly between our querying host (**www.yahoo.com**) and **live-kcl.contensis.com**.

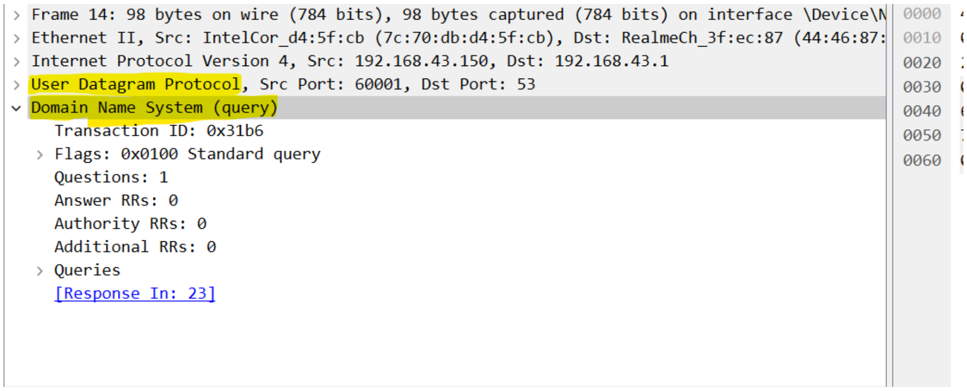


```
C:\Users\ensta>nslookup www.yahoo.com live-kcl.contensis.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  185.18.139.104

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

C:\Users\ensta>
```

Task: Answer The following

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

Ans: Messages are sent over UDP (**User Detagram Protocol**). DNS query shown below:

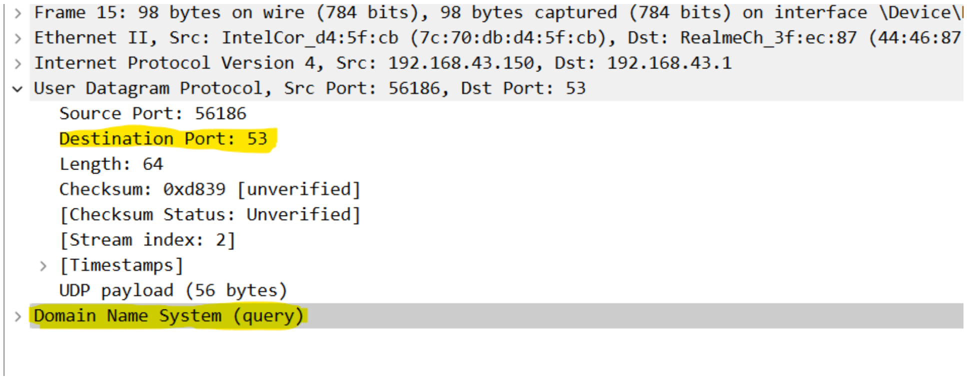


```
> Frame 14: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\N
> Ethernet II, Src: IntelCor_d4:5f:cb (7c:70:db:d4:5f:cb), Dst: RealmeCh_3f:ec:87 (44:46:87:
> Internet Protocol Version 4, Src: 192.168.43.150, Dst: 192.168.43.1
> User Datagram Protocol, Src Port: 60001, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x31b6
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 23]
```

```
0000
0010
0020
0030
0040
0050
0060
```

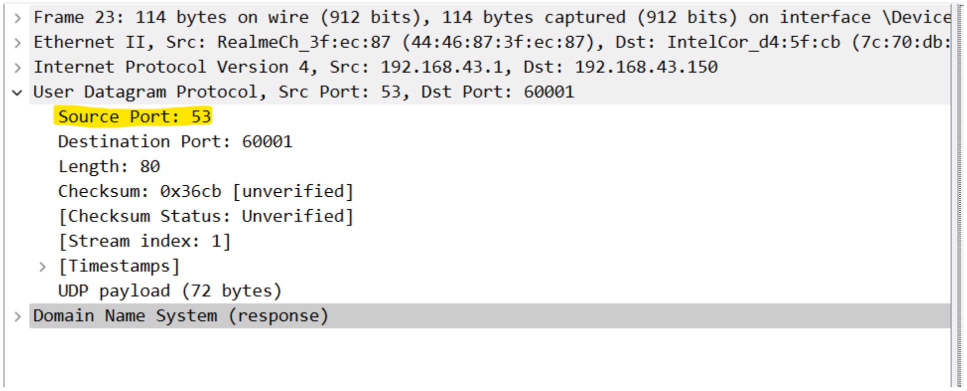
2. What is the destination port for the DNS query message? What is the source port of DNS response message?

Ans: 1. The destination port of the DNS query message is **53**.



```
> Frame 15: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\
> Ethernet II, Src: IntelCor_d4:5f:cb (7c:70:db:d4:5f:cb), Dst: RealmeCh_3f:ec:87 (44:46:87
> Internet Protocol Version 4, Src: 192.168.43.150, Dst: 192.168.43.1
v User Datagram Protocol, Src Port: 56186, Dst Port: 53
    Source Port: 56186
    Destination Port: 53
    Length: 64
    Checksum: 0xd839 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
    UDP payload (56 bytes)
> Domain Name System (query)
```

2. Source Port of the DNS response message is **53**.



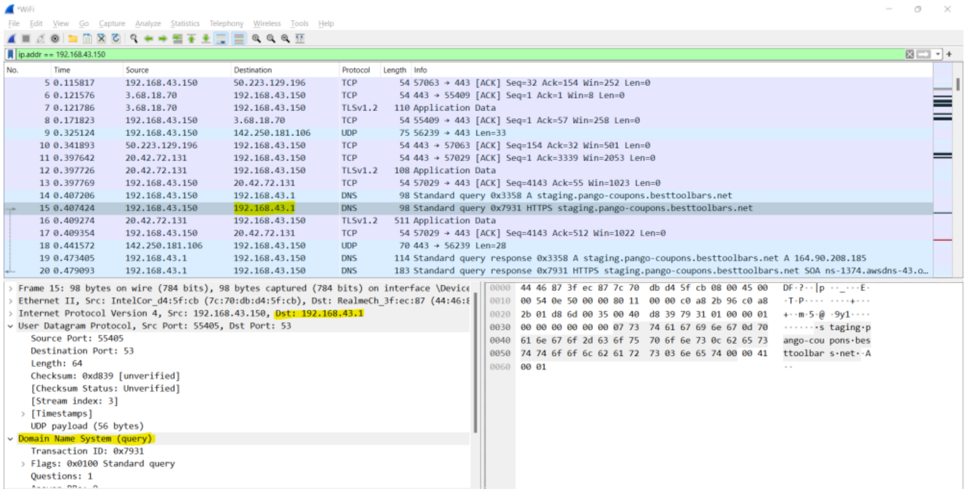
```
> Frame 23: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface \Device
> Ethernet II, Src: RealmeCh_3f:ec:87 (44:46:87:3f:ec:87), Dst: IntelCor_d4:5f:cb (7c:70:db:
> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.150
v User Datagram Protocol, Src Port: 53, Dst Port: 60001
    Source Port: 53
    Destination Port: 60001
    Length: 80
    Checksum: 0x36cb [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (72 bytes)
> Domain Name System (response)
```

3. 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: Yes, these two IP addresses are same.

Reason:

The IP address of the DNS query message sent is **192.168.43.1**.

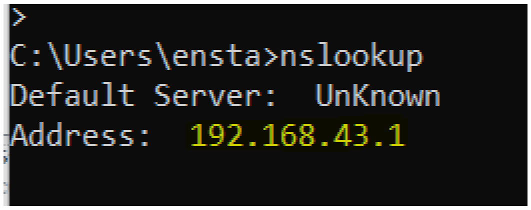

*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 192.168.43.150

No.  Time      Source          Destination     Protocol Length Info
   5 0.115817  192.168.43.150  50.223.129.196  TCP        54 57063 → 443 [ACK] Seq=32 Ack=154 Win=252 Len=0
   6 0.121576  3.68.18.70      192.168.43.150  TCP        54 443 → 55409 [ACK] Seq=1 Ack=1 Win=8 Len=0
   7 0.121786  3.68.18.70      192.168.43.150  TLSv1.2   110 Application Data
   8 0.171823  192.168.43.150  3.68.18.70      TCP        54 55409 → 443 [ACK] Seq=1 Ack=57 Win=258 Len=0
   9 0.325124  192.168.43.150  142.250.181.106 UDP        75 56239 → 443 Len=33
  10 0.341893  50.223.129.196  192.168.43.150  TCP        54 443 → 57063 [ACK] Seq=154 Ack=32 Win=501 Len=0
  11 0.397642  20.42.72.131    192.168.43.150  TCP        54 443 → 57029 [ACK] Seq=1 Ack=3339 Win=2053 Len=0
  12 0.397726  20.42.72.131    192.168.43.150  TLSv1.2   108 Application Data
  13 0.397769  192.168.43.150  20.42.72.131    TCP        54 57029 → 443 [ACK] Seq=4143 Ack=55 Win=1023 Len=0
  14 0.407206  192.168.43.150  192.168.43.1    DNS        98 Standard query 0x3358 A staging.pango-coupons.besttoolbars.net
  15 0.407424  192.168.43.150  192.168.43.1    DNS        98 Standard query 0x7931 HTTPS staging.pango-coupons.besttoolbars.net
  16 0.409274  20.42.72.131    192.168.43.150  TLSv1.2   511 Application Data
  17 0.409354  192.168.43.150  20.42.72.131    TCP        54 57029 → 443 [ACK] Seq=4143 Ack=512 Win=1022 Len=0
  18 0.441572  142.250.181.106 192.168.43.150  UDP        70 443 → 56239 Len=28
  19 0.473405  192.168.43.1    192.168.43.150  DNS       114 Standard query response 0x3358 A staging.pango-coupons.besttoolbars.net A 164.90.208.185
  20 0.479093  192.168.43.1    192.168.43.150  DNS       183 Standard query response 0x7931 HTTPS staging.pango-coupons.besttoolbars.net SOA ns-1374.awsdns-43.o…
```

```
> Frame 15: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device
> Ethernet II, Src: IntelCor_d4:5f:cb (7c:70:db:d4:5f:cb), Dst: RealmeCh_3f:ec:87 (44:46:8
> Internet Protocol Version 4, Src: 192.168.43.150, Dst: 192.168.43.1
v User Datagram Protocol, Src Port: 55405, Dst Port: 53
    Source Port: 55405
    Destination Port: 53
    Length: 64
    Checksum: 0xd839 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  > [Timestamps]
    UDP payload (56 bytes)
v Domain Name System (query)
    Transaction ID: 0x7931
  > Flags: 0x0100 Standard query
    Questions: 1
```

```
0000  44 46 87 3f ec 87 7c 70  db d4 5f cb 08 00 45 00   DF·?··|p ··_···E·
0010  00 54 0e 50 00 00 80 11  00 00 c0 a8 2b 96 c0 a8   ·T·P···· ····+···
0020  2b 01 d8 6d 00 35 00 40  d8 39 79 31 01 00 00 01   +··m·5·@ ·9y1····
0030  00 00 00 00 00 00 07 73  74 61 67 69 6e 67 0d 70   ·······s taging·p
0040  61 6e 67 6f 2d 63 6f 75  70 6f 6e 73 0c 62 65 73   ango-cou pons·bes
0050  74 74 6f 6f 6c 62 61 72  73 03 6e 65 74 00 00 41   ttoolbar s·net··A
0060  00 01                                              ··
```

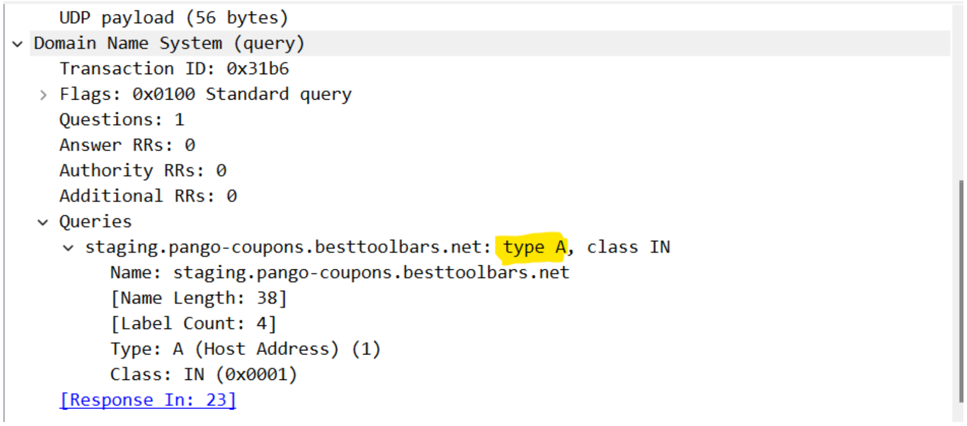
The Ip address of my local DNS server is **192.168.43.1**.



```
>
C:\Users\ensta>nslookup
Default Server:  UnKnown
Address:  192.168.43.1
```

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

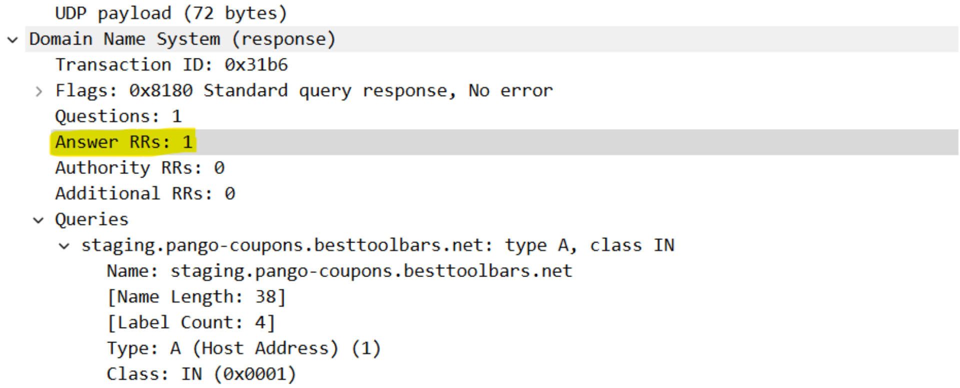
Ans: The DNS query message does not contain any answers. The type of the DNS query is 'Type A'**.**



```
    UDP payload (56 bytes)
v Domain Name System (query)
    Transaction ID: 0x31b6
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v staging.pango-coupons.besttoolbars.net: type A, class IN
        Name: staging.pango-coupons.besttoolbars.net
        [Name Length: 38]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 23]
```

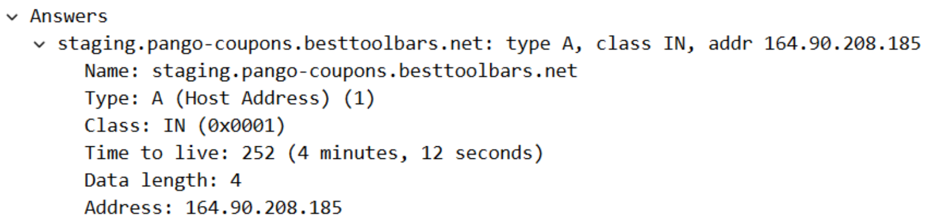
5. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

Ans: Yes, the DNS response message contain one answer.



```
    UDP payload (72 bytes)
v Domain Name System (response)
    Transaction ID: 0x31b6
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v staging.pango-coupons.besttoolbars.net: type A, class IN
        Name: staging.pango-coupons.besttoolbars.net
        [Name Length: 38]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

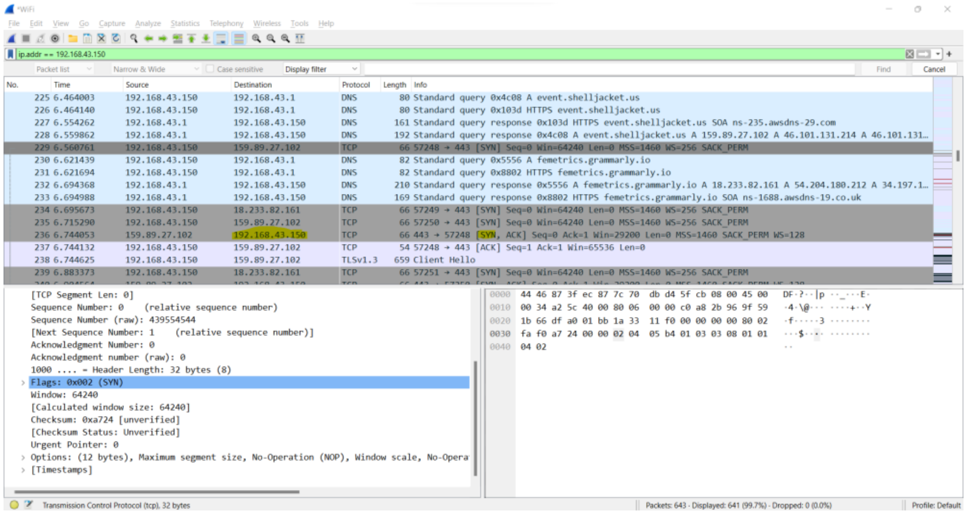
The answer contains the following information



```
v Answers
  v staging.pango-coupons.besttoolbars.net: type A, class IN, addr 164.90.208.185
      Name: staging.pango-coupons.besttoolbars.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 252 (4 minutes, 12 seconds)
      Data length: 4
      Address: 164.90.208.185
```

6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet corresponds to any of the IP addresses provided in the DNS response message?

Ans: The TCP destination IP is **192.168.43.150. Sent by host 159.89.27.102.**


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel

```
ip.addr == 192.168.43.150
```

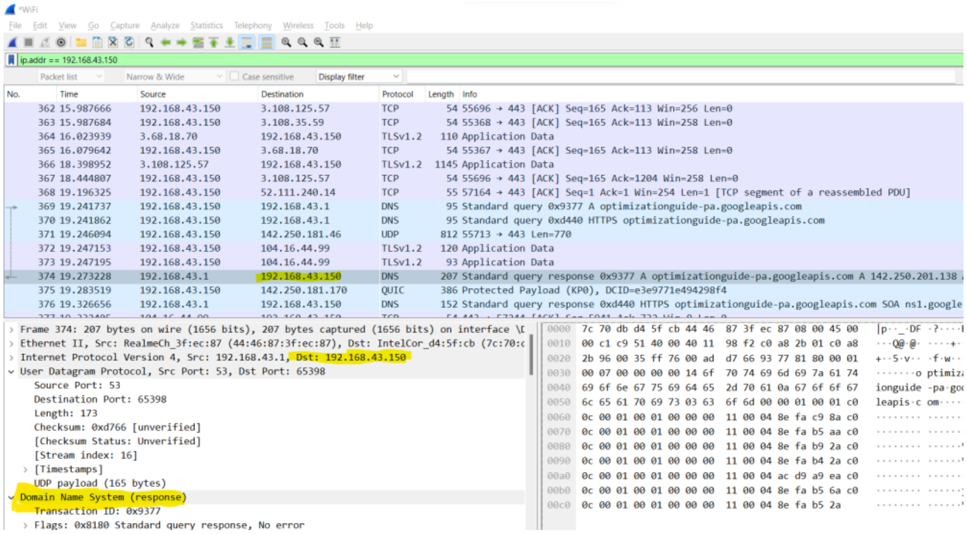
```
No.  Time        Source          Destination     Protocol Length Info
 225 6.464003    192.168.43.150  192.168.43.1    DNS        80 Standard query 0x4c08 A event.shelljacket.us
 226 6.464140    192.168.43.150  192.168.43.1    DNS        80 Standard query 0x103d HTTPS event.shelljacket.us
 227 6.554262    192.168.43.1    192.168.43.150  DNS       161 Standard query response 0x103d HTTPS event.shelljacket.us SOA ns-235.awsdns-29.com
 228 6.559862    192.168.43.1    192.168.43.150  DNS       192 Standard query response 0x4c08 A event.shelljacket.us A 159.89.27.102 A 46.101.131.214 A 46.101.131…
 229 6.560761    192.168.43.150  159.89.27.102   TCP        66 57248 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 230 6.621439    192.168.43.150  192.168.43.1    DNS        82 Standard query 0x5556 A femetrics.grammarly.io
 231 6.621694    192.168.43.150  192.168.43.1    DNS        82 Standard query 0x8802 HTTPS femetrics.grammarly.io
 232 6.694368    192.168.43.1    192.168.43.150  DNS       210 Standard query response 0x5556 A femetrics.grammarly.io A 18.233.82.161 A 54.204.180.212 A 34.197.1…
 233 6.694988    192.168.43.1    192.168.43.150  DNS       169 Standard query response 0x8802 HTTPS femetrics.grammarly.io SOA ns-1688.awsdns-19.co.uk
 234 6.695673    192.168.43.150  18.233.82.161   TCP        66 57249 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 235 6.715290    192.168.43.150  159.89.27.102   TCP        66 57250 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 236 6.744053    159.89.27.102   192.168.43.150  TCP        66 443 → 57248 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
 237 6.744132    192.168.43.150  159.89.27.102   TCP        54 57248 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 238 6.744625    192.168.43.150  159.89.27.102   TLSv1.3   659 Client Hello
 239 6.883373    192.168.43.150  18.233.82.161   TCP        66 57251 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
```

```
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 439554544
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0xa724 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Opera
  > [Timestamps]
```

```
0000  44 46 87 3f ec 87 7c 70  db d4 5f cb 08 00 45 00   DF·?··|p ··_···E·
0010  00 34 a2 5c 40 00 80 06  00 00 c0 a8 2b 96 9f 59   ·4·\@··· ····+··Y
0020  1b 66 df a0 01 bb 1a 33  11 f0 00 00 00 00 80 02   ·f·····3 ········
0030  fa f0 a7 24 00 00 02 04  05 b4 01 03 03 08 01 01   ···$···· ········
0040  04 02                                              ··
```

```
Transmission Control Protocol (tcp), 32 bytes    Packets: 643 · Displayed: 641 (99.7%) · Dropped: 0 (0.0%)    Profile: Default
```

Yes, the destination IP address **192.168.43.150** of the TCP SYN packet corresponds to the IP address of the destination of the response message **192.168.43.150.**


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packet list
Narrow & Wide
Case sensitive
Display filter

```
ip.addr == 192.168.43.150
```

```
No.  Time        Source          Destination     Protocol Length Info
 362 15.987666   192.168.43.150  3.108.125.57    TCP        54 55696 → 443 [ACK] Seq=165 Ack=113 Win=256 Len=0
 363 15.987684   192.168.43.150  3.108.35.59     TCP        54 55368 → 443 [ACK] Seq=165 Ack=113 Win=258 Len=0
 364 16.023939   3.68.18.70      192.168.43.150  TLSv1.2   110 Application Data
 365 16.079642   192.168.43.150  3.68.18.70      TCP        54 55367 → 443 [ACK] Seq=165 Ack=113 Win=258 Len=0
 366 18.398952   3.108.125.57    192.168.43.150  TLSv1.2  1145 Application Data
 367 18.444807   192.168.43.150  3.108.125.57    TCP        54 55696 → 443 [ACK] Seq=165 Ack=1204 Win=258 Len=0
 368 19.196325   192.168.43.150  52.111.240.14   TCP        55 57164 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1 [TCP segment of a reassembled PDU]
 369 19.241737   192.168.43.150  192.168.43.1    DNS        95 Standard query 0x9377 A optimizationguide-pa.googleapis.com
 370 19.241862   192.168.43.150  192.168.43.1    DNS        95 Standard query 0xd440 HTTPS optimizationguide-pa.googleapis.com
 371 19.246094   192.168.43.150  142.250.181.46  UDP       812 55713 → 443 Len=770
 372 19.247153   192.168.43.150  104.16.44.99    TLSv1.2   120 Application Data
 373 19.247195   192.168.43.150  104.16.44.99    TLSv1.2    93 Application Data
 374 19.273228   192.168.43.1    192.168.43.150  DNS       207 Standard query response 0x9377 A optimizationguide-pa.googleapis.com A 142.250.201.138 
 375 19.283519   192.168.43.150  142.250.181.170 QUIC      386 Protected Payload (KP0), DCID=e3e9771e494298f4
 376 19.326656   192.168.43.1    192.168.43.150  DNS       152 Standard query response 0xd440 HTTPS optimizationguide-pa.googleapis.com SOA ns1.google
```

```
> Frame 374: 207 bytes on wire (1656 bits), 207 bytes captured (1656 bits) on interface \D
> Ethernet II, Src: RealmeCh_3f:ec:87 (44:46:87:3f:ec:87), Dst: IntelCor_d4:5f:cb (7c:70:c
> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.150
v User Datagram Protocol, Src Port: 53, Dst Port: 65398
    Source Port: 53
    Destination Port: 65398
    Length: 173
    Checksum: 0xd766 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 16]
  > [Timestamps]
    UDP payload (165 bytes)
v Domain Name System (response)
    Transaction ID: 0x9377
  > Flags: 0x8180 Standard query response, No error
```

```
0000  7c 70 db d4 5f cb 44 46  87 3f ec 87 08 00 45 00   |p··_·DF ·?····E
0010  00 c1 c9 51 40 00 40 11  98 f2 c0 a8 2b 01 c0 a8   ···Q@·@· ····+··
0020  2b 96 00 35 ff 76 00 ad  d7 66 93 77 81 80 00 01   +··5·v·· ·f·w····
0030  00 07 00 00 00 00 14 6f  70 74 69 6d 69 7a 61 74   ·······o ptimizat
0040  69 6f 6e 67 75 69 64 65  2d 70 61 0a 67 6f 6f 67   ionguide -pa·goog
0050  6c 65 61 70 69 73 03 63  6f 6d 00 00 01 00 01 c0   leapis·c om······
0060  0c 00 01 00 01 00 00 00  11 00 04 8e fa c9 8a c0   ········ ········
0070  0c 00 01 00 01 00 00 00  11 00 04 8e fa b5 aa c0   ········ ········
0080  0c 00 01 00 01 00 00 00  11 00 04 8e fa b9 2a c0   ········ ······*·
0090  0c 00 01 00 01 00 00 00  11 00 04 8e fa b4 2a c0   ········ ······*·
00a0  0c 00 01 00 01 00 00 00  11 00 04 ac d9 a9 ea c0   ········ ········
00b0  0c 00 01 00 01 00 00 00  11 00 04 8e fa b5 6a c0   ········ ······j·
00c0  0c 00 01 00 01 00 00 00  11 00 04 8e fa b5 2a      ········ ······*
```

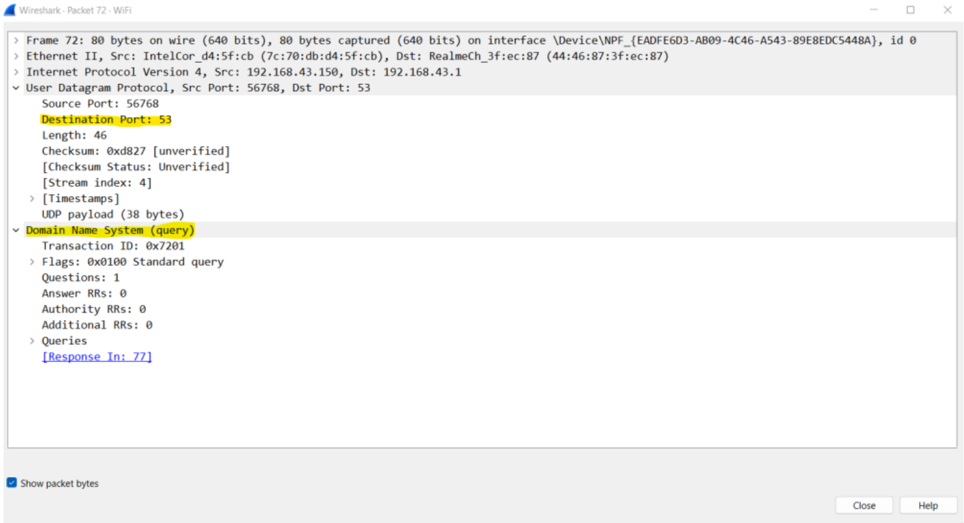
7. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Ans: Before retrieving each image, my host does not issue new DNS queries. The images are all loaded from www.ietf.org, so no additional DNS queries are necessary.

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

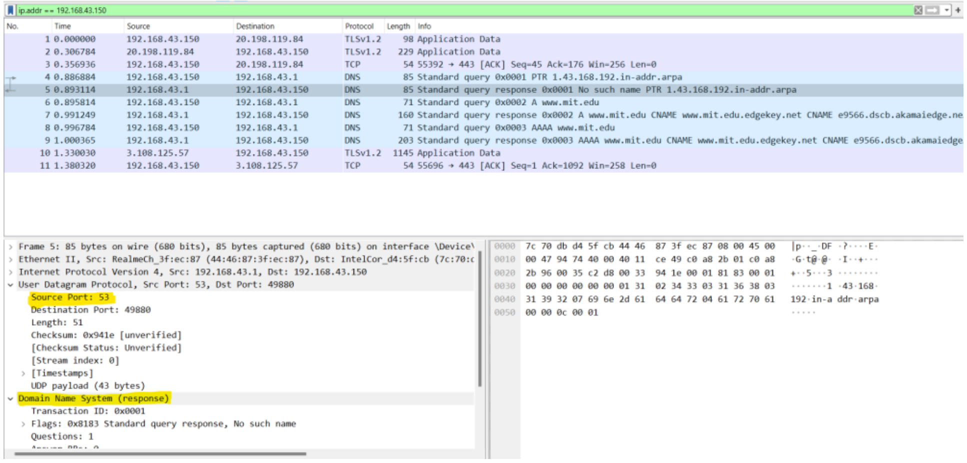
response message?

Ans: The destination port of the DNS query message is **53**.



```
> Frame 72: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{EADFE6D3-AB09-4C46-A543-89E8EDC5448A}, id 0
> Ethernet II, Src: IntelCor_d4:5f:cb (7c:70:db:d4:5f:cb), Dst: RealmeCh_3f:ec:87 (44:46:87:3f:ec:87)
> Internet Protocol Version 4, Src: 192.168.43.150, Dst: 192.168.43.1
v User Datagram Protocol, Src Port: 56768, Dst Port: 53
    Source Port: 56768
    Destination Port: 53
    Length: 46
    Checksum: 0xd827 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
    UDP payload (38 bytes)
v Domain Name System (query)
    Transaction ID: 0x7201
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 77]
```

The source port of the response message is also **53**.



```
ip.addr == 192.168.43.150

No.  Time       Source          Destination     Protocol Length Info
   1 0.000000   192.168.43.150  20.198.119.84   TLSv1.2    98 Application Data
   2 0.306784   20.198.119.84   192.168.43.150  TLSv1.2   229 Application Data
   3 0.356936   192.168.43.150  20.198.119.84   TCP        54 55392 → 443 [ACK] Seq=45 Ack=176 Win=256 Len=0
   4 0.886884   192.168.43.150  192.168.43.1    DNS        85 Standard query 0x0001 PTR 1.43.168.192.in-addr.arpa
   5 0.893114   192.168.43.1    192.168.43.150  DNS        85 Standard query response 0x0001 No such name PTR 1.43.168.192.in-addr.arpa
   6 0.895814   192.168.43.150  192.168.43.1    DNS        71 Standard query 0x0002 A www.mit.edu
   7 0.991249   192.168.43.1    192.168.43.150  DNS       160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.ne
   8 0.996784   192.168.43.150  192.168.43.1    DNS        71 Standard query 0x0003 AAAA www.mit.edu
   9 1.000365   192.168.43.1    192.168.43.150  DNS       203 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge
  10 1.330030   3.108.125.57    192.168.43.150  TLSv1.2  1145 Application Data
  11 1.380320   192.168.43.150  3.108.125.57    TCP        54 55696 → 443 [ACK] Seq=1 Ack=1092 Win=258 Len=0
```

```
> Frame 5: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\
> Ethernet II, Src: RealmeCh_3f:ec:87 (44:46:87:3f:ec:87), Dst: IntelCor_d4:5f:cb (7c:70:c
> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.150
v User Datagram Protocol, Src Port: 53, Dst Port: 49880
    Source Port: 53
    Destination Port: 49880
    Length: 51
    Checksum: 0x941e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (43 bytes)
v Domain Name System (response)
    Transaction ID: 0x0001
  > Flags: 0x8183 Standard query response, No such name
    Questions: 1
```

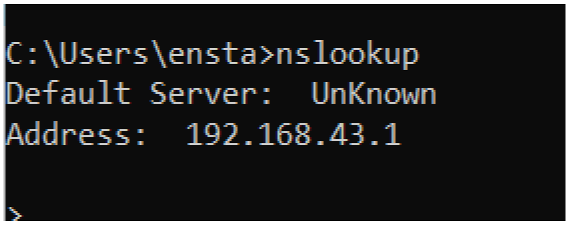
```
0000  7c 70 db d4 5f cb 44 46  87 3f ec 87 08 00 45 00   |p··_·DF ·?····E·
0010  00 47 94 74 40 00 40 11  ce 49 c0 a8 2b 01 c0 a8   ·G·t@·@· ·I··+···
0020  2b 96 00 35 c2 d8 00 33  94 1e 00 01 81 83 00 01   +··5···3 ········
0030  00 00 00 00 00 00 01 31  02 34 33 03 31 36 38 03   ·······1 ·43·168·
0040  31 39 32 07 69 6e 2d 61  64 64 72 04 61 72 70 61   192·in-a ddr·arpa
0050  00 00 0c 00 01                                     ·····
```

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

Ans: Yes, this is the IP address of my default local DNS server.

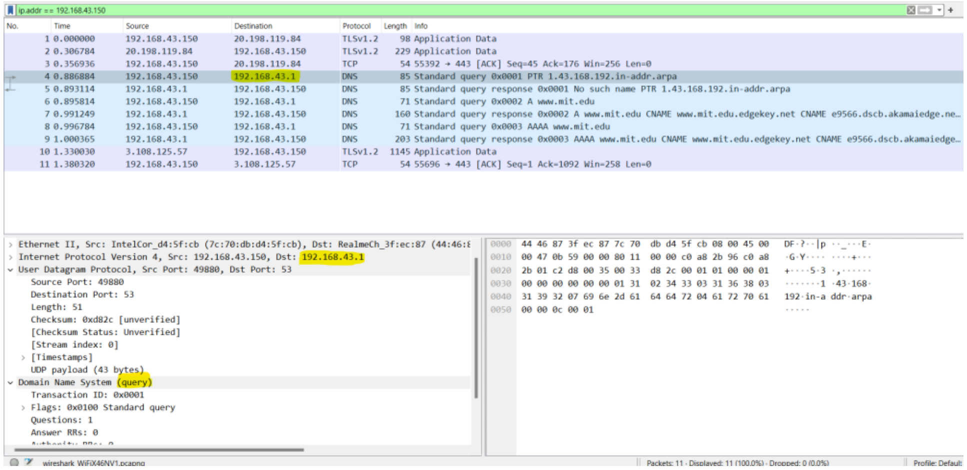
Reason:

The IP address of may default local DNS server is **192.168.43.1**.



```
C:\Users\ensta>nslookup
Default Server:  UnKnown
Address:  192.168.43.1

>
```

DNS query message was sent to **192.168.43.1**.



```
ip.addr == 192.168.43.150
No.   Time        Source           Destination      Protocol Length Info
    1 0.000000    192.168.43.150   20.198.119.84    TLSv1.2    98 Application Data
    2 0.306784    20.198.119.84    192.168.43.150   TLSv1.2   229 Application Data
    3 0.356936    192.168.43.150   20.198.119.84    TCP        54 55392 → 443 [ACK] Seq=45 Ack=176 Win=256 Len=0
    4 0.886884    192.168.43.150   192.168.43.1     DNS        85 Standard query 0x0001 PTR 1.43.168.192.in-addr.arpa
    5 0.893114    192.168.43.1     192.168.43.150   DNS        85 Standard query response 0x0001 No such name PTR 1.43.168.192.in-addr.arpa
    6 0.895814    192.168.43.150   192.168.43.1     DNS        71 Standard query 0x0002 A www.mit.edu
    7 0.991249    192.168.43.1     192.168.43.150   DNS       160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.ne…
    8 0.996784    192.168.43.150   192.168.43.1     DNS        71 Standard query 0x0003 AAAA www.mit.edu
    9 1.000365    192.168.43.1     192.168.43.150   DNS       203 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge…
   10 1.330030    3.108.125.57     192.168.43.150   TLSv1.2  1145 Application Data
   11 1.380320    192.168.43.150   3.108.125.57     TCP        54 55696 → 443 [ACK] Seq=1 Ack=1092 Win=258 Len=0
```

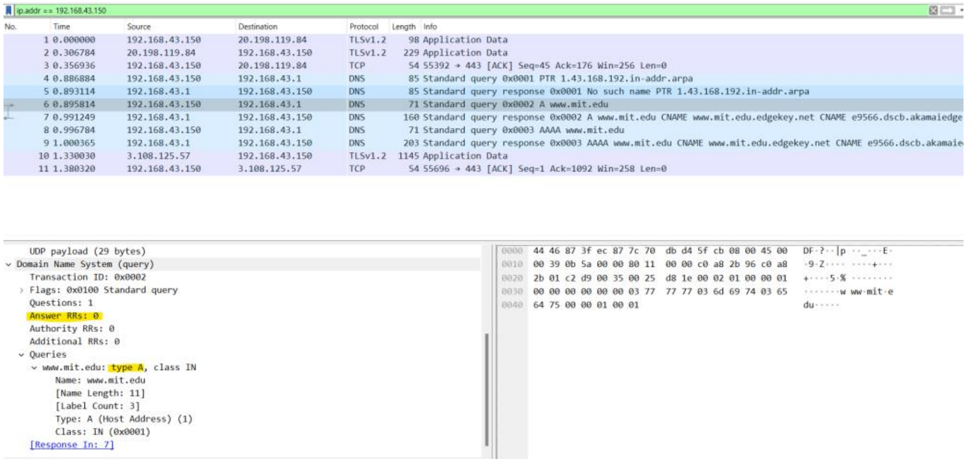
```
> Ethernet II, Src: IntelCor_d4:5f:cb (7c:70:db:d4:5f:cb), Dst: RealmeCh_3f:ec:87 (44:46:8
> Internet Protocol Version 4, Src: 192.168.43.150, Dst: 192.168.43.1
v User Datagram Protocol, Src Port: 49880, Dst Port: 53
    Source Port: 49880
    Destination Port: 53
    Length: 51
    Checksum: 0xd82c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (43 bytes)
v Domain Name System (query)
    Transaction ID: 0x0001
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
```

```
0000  44 46 87 3f ec 87 7c 70  db d4 5f cb 08 00 45 00   DF·?··|p ··_···E·
0010  00 47 0b 59 00 00 80 11  00 00 c0 a8 2b 96 c0 a8   ·G·Y···· ····+···
0020  2b 01 c2 d8 00 35 00 33  d8 2c 00 01 01 00 00 01   +····5·3 ·,······
0030  00 00 00 00 00 00 01 31  02 34 33 03 31 36 38 03   ·······1 ·43·168·
0040  31 39 32 07 69 6e 2d 61  64 64 72 04 61 72 70 61   192·in-a ddr·arpa
0050  00 00 0c 00 01                                     ·····
```

wireshark WiFiX46NV1.pcapng | Packets: 11 · Displayed: 11 (100.0%) · Dropped: 0 (0.0%) | Profile: Defaul

10. 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 of Type ‘A’. The query message does not contain any answers.



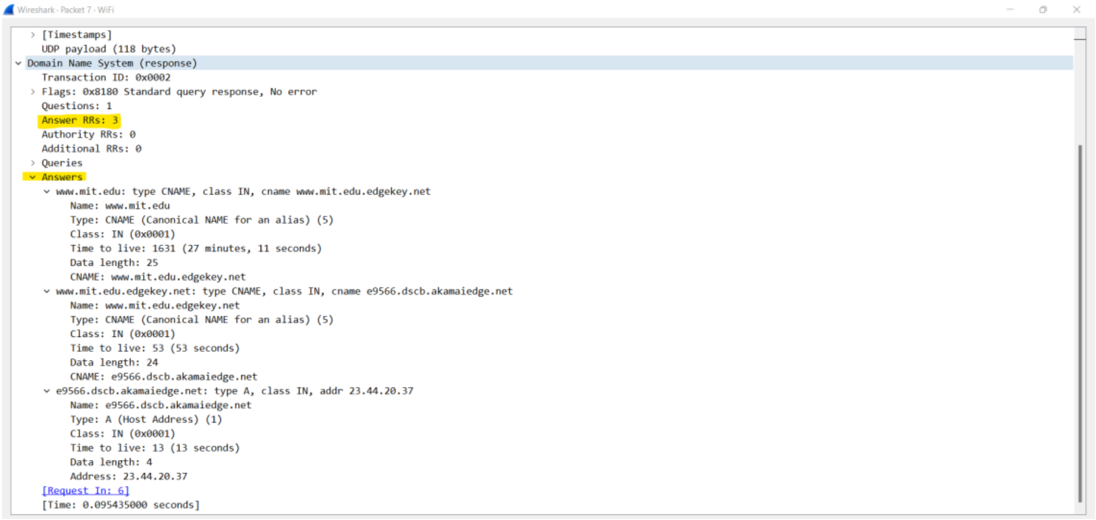
```
ip.addr == 192.168.43.150
No.   Time        Source           Destination      Protocol Length Info
    1 0.000000    192.168.43.150   20.198.119.84    TLSv1.2    98 Application Data
    2 0.306784    20.198.119.84    192.168.43.150   TLSv1.2   229 Application Data
    3 0.356936    192.168.43.150   20.198.119.84    TCP        54 55392 → 443 [ACK] Seq=45 Ack=176 Win=256 Len=0
    4 0.886884    192.168.43.150   192.168.43.1     DNS        85 Standard query 0x0001 PTR 1.43.168.192.in-addr.arpa
    5 0.893114    192.168.43.1     192.168.43.150   DNS        85 Standard query response 0x0001 No such name PTR 1.43.168.192.in-addr.arpa
    6 0.895814    192.168.43.150   192.168.43.1     DNS        71 Standard query 0x0002 A www.mit.edu
    7 0.991249    192.168.43.1     192.168.43.150   DNS       160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge
    8 0.996784    192.168.43.150   192.168.43.1     DNS        71 Standard query 0x0003 AAAA www.mit.edu
    9 1.000365    192.168.43.1     192.168.43.150   DNS       203 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaie
   10 1.330030    3.108.125.57     192.168.43.150   TLSv1.2  1145 Application Data
   11 1.380320    192.168.43.150   3.108.125.57     TCP        54 55696 → 443 [ACK] Seq=1 Ack=1092 Win=258 Len=0
```

```
    UDP payload (29 bytes)
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.mit.edu: type A, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 7]
```

```
0000  44 46 87 3f ec 87 7c 70  db d4 5f cb 08 00 45 00   DF·?··|p ··_···E·
0010  00 39 0b 5a 00 00 80 11  00 00 c0 a8 2b 96 c0 a8   ·9·Z···· ····+···
0020  2b 01 c2 d9 00 35 00 25  d8 1e 00 02 01 00 00 01   +····5·% ········
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 00 00 01 00 01                               du·····
```

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

Ans: The DNS response message contain one answer. Count of entries in the answer section are three (Answer RRs: 3).



```
  > [Timestamps]
    UDP payload (118 bytes)
v Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        Name: www.mit.edu
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 1631 (27 minutes, 11 seconds)
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
    v www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
        Name: www.mit.edu.edgekey.net
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 53 (53 seconds)
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
    v e9566.dscb.akamaiedge.net: type A, class IN, addr 23.44.20.37
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 13 (13 seconds)
        Data length: 4
        Address: 23.44.20.37
    [Request In: 6]
    [Time: 0.095435000 seconds]
```

It contains information on 3 authoritative nameservers and 3 additional records.